Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären

Prof.Dr.Gerald Spindler

Universität Göttingen

unter Mitwirkung von:

Ass.iur. Andreas Lönner, Universität Göttingen

Ref.iur. Judith Nink, Universität Göttingen

Inhaltsverzeichnis

A. Einleitung

1 Informationstechnologie durchdringt heute alle Lebensbereiche. Von der privaten Nutzung des Internets und E-Mails über die Nutzung durch gewerbliche Anwender jeglicher Art bis hin zum Einsatz von IT in kritischen Infrastrukturen wie Energie- oder Gesundheitsversorgung[1] – das private, wirtschaftliche und öffentliche Leben ist heute ohne Computertechnologie kaum vorstellbar. IT-Produkte finden in jeder Form von Geräten heutzutage, sei als embedded systems in Konsumgeräten oder als spezielle Steuerungsgeräte in Industrieanlagen.

2 Vor diesem Hintergrund besitzen Sicherheitsaspekte einen überragenden Stellenwert. Der drohende volkswirtschaftliche Schaden schadhafter IT-Produkte, die Betriebsabläufe und Steuerungen zum Erliegen bringen, liegt auf der Hand. Auch aus betriebswirtschaftlicher Sicht ist die Beherrschung der bestehenden IT-Risiken von fundamentaler Bedeutung. Zu den Krisenszenarien aus unternehmerischer Sicht zählen nicht nur die vertraglichen Risiken; vielmehr ist IT-Sicherheit zu einem entscheidenden Faktor in der Wertschöpfungskette generell geworden, der die Risikoexposition eines Unternehmens, seine Kreditwürdigkeit ebenso wie seine Haftpflichtversicherungsprämien entscheidend beeinflussen kann. Auch wenn im vertraglichen Verhältnis zahlreiche Vorkehrungen gegen Krisenszenarien getroffen werden können, verbleiben sowohl gegenüber Dritten als auch für das Unternehmen intern zahlreiche Pflichten, die sich in erheblicher Weise auswirken können.

3 Dies wurde schon im Rahmen des damals befürchteten Jahr 2000-Problems deutlich[2] und hat sich seitdem eher noch verschärft.[3] Fast wöchentliche Meldungen über neu entdeckte Sicherheitslücken in Softwareprogrammen und neue Varianten von Würmern oder Viren werfen die Frage nach der **Pflichtenlage, Verantwortlichkeit und Haftung im geltenden Recht** der an der Herstellung, dem Einsatz und der Nutzung von IT-

---

[1] Dazu BSI-Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, 2005, abrufbar unter: http://www.bsi.de/fachthem/kritis/Regelungsumfang_ITSich_KRITIS.pdf; *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, 2005.

[2] Dazu mit weiteren Zahlenmaterial und Nachweisen *Heckeroth*, DB 1999, 702 (703); *Wohlgemuth*, MMR 1999, 59 (59); *Hohmann*, NJW 1999, 521 (521); *Heussen/Damm*, BB 1999, 481 (482); *Bartsch*, Software und das Jahr 2000 - Haftung und Versicherungsschutz für ein technisches Großproblem, S. 1 ff.; *Stretz*, in: v.Westphalen/Langheid/Streitz, Der Jahr-2000 Fehler, Rz. 1, 82 ff.; aus der schweizerischen Literatur: *Rigamonti*, SJZ 1998, 430 (431 ff.); *R. Weber*, Informatik und das Jahr 2000, 1998, S. 19 ff.

[3] „Störfälle im Internet nehmen zu", Beitrag von *Th. Stollberger* des Online-Nachrichtenservices Verivox v. 18.11.2004, abrufbar unter: http://www.verivox.de/news/ArticleDetails.asp?PM=1&aid=2542 (zuletzt abgerufen am 26.09.2006).

Produkten Beteiligten auf, angefangen beim Hersteller, über die IT-Intermediäre, die sowohl IT-Produkte einsetzen als auch selbst wiederum Dienstleistungen erbringen, wie etwa die Provider (Host-, Access-Provider), bis hin zu den IT-Anwendern, die ihrerseits bestimmten Pflichten unterliegen.

4 Aber auch **aus rechtspolitischer Sicht** stellt sich die Frage, ob das Recht mit seinen bisherigen Steuerungsinstrumenten in der Lage ist (und war), den neuen Risiken ausreichend Rechnung zu tragen. Das nunmehr seit etlichen Jahren diskutierte Problem der IT-Sicherheit scheint nach wie vor nicht bewältigt zu sein, so dass Defizite des geltenden Rechts nahe liegen.

5 Die tatsächliche Relevanz dieser Problematik steht in einem gewissen Gegensatz zur rechtlichen Durchdringung der bestehenden Sicherheitspflichten im Bereich der Informationstechnologie. Schwierigkeiten bereitet einerseits die lediglich partiell bestehende spezialgesetzliche Normierung dieser Pflichten, anderseits die starke Zersplitterung der Materie auf eine Vielzahl von Einzelgesetzen. Zudem sind bislang nur ansatzweise die traditionellen Verantwortlichkeitsnormen auf ihre Tragfähigkeit zur Bewältigung und Zuweisung von Risiken hin untersucht worden. [4]

B. Allgemeiner Teil

I. Rechtliche Grundlagen von Sicherheitspflichten

6 Ziel des Teils 1 ist es, einen Überblick über die derzeit bestehenden Sicherheitsanforderungen zu geben, die die Rechtsordnung – teilweise in Gestalt von Spezialgesetzen, in erster Linie jedoch durch die Auslegung bestehender allgemeiner Rechtsvorschriften – an alle Verwender von IT-Produkten stellt. Dazu ist es nötig, die für diesen Bereich in Frage kommenden Rechtsmaterien und den in Ihnen niedergelegten Bestand an Rechtspflichten zu sichten. Als Pflichten kommen nicht nur öffentlichrechtlich normierte Verhaltensstandards in Betracht, sondern auch und in erster Linie zivilrechtlich begründete Sicherheitspflichten, deren (schuldhafte) Verletzung zur Haftung des Verantwortlichen führt.

7 Im **öffentlichen Recht** können grundsätzlich zwei Normenkreise voneinander unterschieden werden, die spezifische IT-Sicherheitspflichten statuieren können: Zum einen die produktbezogenen Vorschriften, zum anderen die tätigkeits- oder branchenbezoge-

[4] So etwa *Günther*, Produkthaftung für Informationsgüter, S. 157 ff.; *Sodtalbers*, Softwarehaftung im Internet, S. 101 ff.

nen Vorschriften, die die Sicherheit bestimmter Anlagen oder Tätigkeiten regeln. Zu dem ersten Kreis der produktbezogenen Vorschriften gehören insbesondere als allgemeine Rahmennorm das Geräte- und Produktsicherheitsgesetz (GPSG) sowie als Beispiel für ein spezifisches produktbezogenes Gesetz das MedizinprodukteG oder das Chemikaliengesetz (ChemG). Zu dem zweiten Kreis der tätigkeits- oder anlagenbezogenen Normen zählen etwa die spezifischen Aufsichtsgesetze wie das Kreditwesengesetz oder das Versicherungsaufsichtsgesetz, die mittelbar[5] besondere Vorgaben für den Umgang mit unternehmensinternen IT-Risiken enthalten.

8 **Aus zivilrechtlicher Sicht** sind hier zunächst Pflichten innerhalb **vertraglicher Sonderverbindungen** zu nennen, deren Übernahme jedoch zur Disposition der Parteien steht. Auszuloten sind in diesem Bereich somit in erster Linie die Grenzen der Vertragsgestaltung mittels Allgemeiner Geschäftbedingungen. Besonderes Gewicht erlangen dabei die Schutz- und Nebenpflichten innerhalb von vertraglichen Beziehungen. Demgegenüber können vertragliche Hauptleistungspflichten hier nur am Rande Berücksichtigung finden, da sie nur in besonderen Fällen die IT-Sicherheit zum Gegenstand gegenseitig geschuldeter Pflichten machen. Dies schließt nicht aus, dass die Gewährleistung einer grundlegenden IT-Sicherheit zu den sog. Kardinal- oder auch vertragswesentlichen Pflichten zählt, von denen sich ein Anwender nicht freizeichnen kann.[6]

9 Diese Schutz- und Nebenpflichten entsprechen oftmals[7] den vor allem im **Deliktsrecht** dem IT-Verwender auferlegten Sicherheitspflichten, die gegenüber jedermann, also nicht nur gegenüber Vertragspartnern bestehen. In erster Linie sind hier die von der Rechtsprechung entwickelten Verkehrssicherungspflichten Gegenstand der Untersuchung. Trotz der Schuldrechtsreform mit ihrer Verlängerung der Gewährleistungsfristen im Kauf- und Werkvertragsrecht[8] und der Einführung einer allgemeinen vertragsrechtlichen Schadensersatzhaftung spielt das Deliktsrecht nach wie vor eine wichtige Rolle: Zum einen entstehen Sicherheitsprobleme oft auch noch nach Ablauf der vertraglichen Gewährleistungsrechte; zum anderen dürften die meisten vertragsrechtlichen Schadensersatzansprüche am mangelnden Verschulden der Softwarehändler als Vertragspartner

---

[5] Über entsprechende Konkretisierungen in der Verwaltungspraxis und Auslegung von Tatbestandselementen.

[6] Zu den Kardinalpflichten s. BGH NJW 1993, 335; BGH NJW-RR 1993, 560 (561); BGH NJW 2002, 673 (674); zuletzt BGH NJW-RR 2005, 1496 (1505 ff.) = WM 2005, 2002 (2013) = CR 2006, 228 (229) ; NJW-RR 2006, 267 (269).

[7] Natürlich kann durch besondere Vertrauensbeziehungen und gerade im Vertragsverhältnis geweckten Sicherheitserwartungen eine Verschärfung der Sicherheitspflichten gegenüber den deliktischen Pflichten eintreten.

[8] Die Frage, wie Software einzuordnen ist, insbesondere im Hinblick auf § 651 BGB, ist anderweitig vertieft worden, s. dazu *Spindler/Klöhn*, CR 2003, 81 ff., sowie *dies*. VersR 2003, 273 ff.; dazu auch *Redeker*, CR 2004, 88 ff., *Marly*, Softwareüberlassungsverträge, Rn. 35 ff.

scheitern.[9] Abgesehen davon können IT-Hersteller, Intermediäre und Anwender mit Ansprüchen Dritter konfrontiert werden, die aus dem Einsatz fehlerhafter Software resultieren und die nicht auf vertraglichen Ansprüchen fußen.[10]

II. Kriterien für die Pflichtenbestimmung

10 Die verschiedenen Normen für Sicherheitspflichten verfolgen unterschiedliche Zwecke und unterliegen selbstverständlich unterschiedlichen rechtsdogmatischen Grundlagen. Während die vertragliche Haftung in erster Linie auf dem Gedanken einer besonderen, durch Vertrag begründeten Vertrauensbeziehung zwischen den Parteien beruht,[11] statuiert das Deliktsrecht Verhaltensanforderungen an jedermann.[12] Spezialgesetzliche Vorschriften sind in erster Linie an besondere Branchen gerichtet und haben insoweit einen abgegrenzten Adressatenkreis.

11 Konsequenz dieser Unterschiede hinsichtlich der Schutzzwecke und der dogmatischen Grundlagen ist daher an sich, dass die Konkretisierung der Schutzpflichten in den jeweiligen Bereichen unterschiedlichen Grundsätzen zu folgen hat. Trotz dieser Unterschiede im Einzelnen können **bestimmte Pflichtenkriterien** destilliert werden, die quasi **abstrakt für alle Pflichtenbestimmungen** gelten, da sie das Fundament für alle weiteren Pflichtenverschärfungen oder –präzisierungen bilden. Diese Grundsätze sollen hier zunächst vorgestellt werden, um in einem weiteren Schritt – als Ergebnis der Anwendung dieser Grundsätze – die konkreten Rechtspflichten der IT-Verwender aufzuzeigen. Da im Deliktsrecht die für jedermann geltenden Pflichten bestimmt werden, liegt es nahe, an die Kriterien, die für Verkehrspflichten entwickelt wurden, anzuknüpfen. Denn der Maßstab der im Verkehr üblichen Sorgfalt nach § 276 BGB, der für das gesamte Schuldrecht und damit auch für vertragliche Pflichten gilt, ebenso für das Mitverschulden nach § 254 BGB (und damit die Pflichten zum Eigenschutz) entspricht strukturell weitgehend den deliktisch abgeleiteten Verkehrspflichten.[13]

---

[9] Zu den vergleichbaren vertragsrechtlichen Fragen im Rahmen des Jahr-2000-Fehlers s. *Spindler,* DB 1999, 1991; *Wohlgemuth*, MMR 1999, 59; *v.Westphalen,* in: v.Westphalen/Langheid/Streitz, Der Jahr-2000-Fehler, Rz. 383 – 637; *Hohmann*, NJW 1999, 521 ff.; mwN. bei *Junker,* NJW 2000, 1304 (1311); s. auch LG Leipzig NJW 1999, 2975 m. Anm. *Hörl*, CR 1999, 605; allgemein zur Leistungsstörung bei Software s. *Marly*, Softwareüberlassungsverträge, Rn. 588 ff., 750 ff. et passim; *Schneider,* Handbuch des EDV-Rechts, Kap. D Rz. 728 ff. et passim.

[10] Einen Anspruch aus positiver Forderungsverletzung bzw. §§ 280 I, 241 II BGB können Dritte demgegenüber nur dann geltend machen, wenn sie in den Schutzbereich des Vertrages zwischen Softwareveräußerer und –abnehmer einbezogen sind, was selten der Fall sein dürfte, aA. im Rahmen des Jahr-2000-Fehlers noch *Hohmann*, NJW 1999, 521 (524).

[11] S. dazu auch *Larenz*, Schuldrecht I, § 2 I.

[12] Hierzu *Larenz/Canaris*, Schuldrecht II/2, § 75.

[13] Vgl. zu den Kriterien der Bestimmung der im Verkehr erforderlichen Sorgfalt Bamberger/Roth-*Unberath*, § 276 BGB Rn. 20 ff.; Palandt-*Heinrichs*, § 276 BGB Rn. 15 ff.; MünchKommBGB-*Grundmann*, § 276 BGB Rn. 53 ff. sowie den Krite-

1. Allgemeine Grundsätze der deliktischen Haftung, insbesondere Verkehrssicherungspflichten

12 Zentral für die deliktische Haftung ist das Konzept der Verkehrssicherungspflichten; sie sind ausschlaggebend, um Schäden, die durch mittelbare Verletzungen enstanden sind, wie etwa in der Produzentenhaftung, zuzurechnen. Sie beanspruchen aber auch allgemeine Geltung für die Ableitung von Pflichten, die aus der Beherrschung von Gefahrenquellen erwachsen. Für die Konkretisierung dieser, durch richterliche Rechtsfortbildung entwickelten Pflichten, sind insbesondere die **berechtigten Sicherheitserwartungen des Verkehrs und der zumutbare Aufwand** maßgeblich.[14]

13 Im Bereich der Produkthaftung ist dies für Hersteller (von IT-Produkten) dahingehend präzisiert worden, dass diese sich nicht nach individuellen besonderen Sicherheitserwartungen[15] oder Schadensanfälligkeiten[16] richten müssen. Ebenso wenig müssen Produkte, deren Gefahren jedermann bekannt sind, gegen Missbrauch gesichert werden; auch vor deren Fehlgebrauch muss nicht gewarnt werden.[17] Die Pflichten des Produzenten, insbesondere zur Instruktion und Warnung, werden weiter eingeschränkt, wenn die Abnehmer selbst fachkundigen Kreisen angehören und daher weitestgehend selbst die Gefahren des Produktes beurteilen können.[18] Andererseits haftet der Produzent auch für Schäden infolge eines nicht bestimmungsgemäßen Gebrauchs, sofern dieser sich noch im Rahmen der allgemeinen Zweckbestimmung des Produktes hält[19] und vom Hersteller objektiv vorhergesehen werden kann oder nahe liegt.[20]

14 Einfluss auf die berechtigten Sicherheitserwartungen haben ferner vor allem der Preis und die Bestimmung des Produktes, einschließlich dessen allgemeiner Anpreisung in der Werbung.[21] Im Rahmen einer gewissen Bandbreite kann ein niedrigerer Preis auch

---

rien zur Bestimmung der deliktischen Verkehrspflichten Palandt-*Sprau*, § 823 BGB Rn. 45; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 233 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 248 ff.; dezidiert für eine Gleichsetzung von deliktischer Verkehrspflichtverletzung und Außerachtlassung der im Verkehr erforderlichen Sorgfalt MünchKommBGB-*Wagner*, § 823 BGB Rn. 63 ff.

[14] BGHZ 104, 323 (329) = NJW 1988, 2611; *Libertus*, MMR 2005, 507 (509); wN. bei Bamberger/Roth-*Spindler*, § 823 BGB Rn. 532.

[15] *v. Bar*, in: Produktverantwortung und Risikoakzeptanz, S. 29 (31 f.).

[16] OLG Hamm NJW-RR 2001, 1248 (1249) - Osteoporosegeschädigter Benutzer eines Sprungbootes.

[17] BGH NJW 1990, 906.

[18] BGH NJW 1992, 2016 (2018); s. aber auch BGH NJW 1996, 2224 (2226).

[19] BGHZ 105, 346 (351) = NJW 1989, 707; BGHZ,116, 60 (65 ff.) = NJW 1992, 560; OLG Oldenburg NJW-RR 1997, 1520 (1521); MünchKommBGB-*Wagner*, § 823 BGB Rn. 588; Staudinger-*J. Hager*, Kap. F Rn. 36; dagegen *Littbarski,* NJW 1995, 217 (219).

[20] BGHZ 105, 346 (351) = NJW 1989, 707; BGHZ 106, 273 (283) = NJW 1989, 1542; BGHZ 116, 60 (65 ff.) = NJW 1992, 560; BGHZ 139, 79 (84) = NJW 1998, 2905; OLG Karlsruhe VersR 1998, 63; MünchKommBGB-*Wagner*, § 823 BGB Rn. 588 (591).

[21] Ausführlich dazu *Foerste,* in: v. Westphalen, ProdHaftHdb, § 24 Rn. 10, 48.

ein niedrigeres Sicherheitsniveau rechtfertigen, da der Verkehr allgemein nicht von der Einhaltung höherer Standards ausgeht, sofern dies offenbar wird.[22]

15 Stets ist jedoch eine **Basissicherheit** zu gewährleisten, von deren Einhaltung der Verkehr auf jeden Fall ausgeht.[23] Eng damit verknüpft ist der Einfluss von möglichen Selbstschutzmaßnahmen:[24] Je mehr dem Produktbenutzer an **Eigenschutz** zugemutet werden kann, desto eher wird der Verkehrspflichtige nur zu Warnhinweisen verpflichtet sein. Für den Hersteller hat dies zur Folge, dass er sich auf einen objektiv zu bestimmenden Mindestsicherheitsstandard einrichten muss, der nach denjenigen Sicherheitserwartungen festzulegen ist, die allgemein bezüglich der gesamten *Produktkategorie* vorherrschen, also z.B. auch von anderen Herstellern erbracht werden.

16 Erheblich ist ferner, ab welcher Schwelle der Bedrohung von Rechtsgütern Dritter der Produzent Maßnahmen zur Sicherung ergreifen muss. Die Pflicht zum Eingreifen wird umso eher ausgelöst, **je höherrangiger die bedrohten Rechtsgüter** sind.[25] Daraus folgt, dass bei Bedrohung von Gesundheit und Leben der Hersteller bereits bei ernstlichen Verdachtsmomenten tätig werden muss; er kann nicht bis zum ersten Schadensfall abwarten[26]. Der Hersteller muss die einschlägigen Veröffentlichungen hierzu auswerten und den **Stand von Wissenschaft und Technik** berücksichtigen. Andererseits muss er sich nicht mit vereinzelt gebliebenen Auffassungen zu Gefahrenmomenten auseinandersetzen, sondern kann sich idR auf die vorherrschende Überzeugung in Fachkreisen verlassen.[27] Sind Gefahren bekannt, aber nicht die Möglichkeiten zu ihrer Vermeidung, kann das Produkt nur in Verkehr gebracht werden, wenn der Verkehr eine entsprechend reduzierte Sicherheit erwartet,[28] wobei dem Hersteller ein Anpassungsermessen bei Wandel des Gefahrenbewusstseins,[29] und bei neuen technischen Entwicklungen[30] zuge-

---

[22] BGH NJW 1990, 906 (907); BGH NJW 1990, 908 (909); MünchKommBGB-*Wagner*, § 823 BGB Rn. 576; *Kötz*, Deliktsrecht Rn. 449; Staudinger-*J. Hager*, Kap F Rn. 8.

[23] BGH NJW 1990, 908 (909); *Foerste,* in: v. Westphalen, ProdHaftHbd, § 24 Rn. 10; MünchKommBGB-*Wagner*, § 823 BGB Rn. 576; *Kötz,* Deliktsrecht Rn. 449.

[24] BGHZ 104, 323 (328) = NJW 1988, 2611; BGH NJW 1990, 906; BGH NJW 1987, 372 f.; Kullmann/Pfister-*Kullmann*, Produzentenhaftung, Kz. 1520 S. 3 f.

[25] BGHZ 80, 186 (192) = NJW 1981, 1603; vgl. BGHZ 104, 323 (329) = NJW 1988, 2611; MünchKommBGB-*Wagner*, § 823 BGB Rn. 591.

[26] BGHZ 106, 273 (283) = NJW 1989, 1542; BGHZ 80, 186 (192) = NJW 1981 (1603).

[27] S. auch OLG Frankfurt NJW-RR1995, 406.

[28] *Foerste*, in: v. Westphalen, ProfHaftHdb, § 24 Rn. 84 ff.; *Schmidt-Salzer*, Produkthaftung, Bd. III/1, Rn. 4.1113 f.; Kullmann/Pfister-*Kullmann*, Produzentenhaftung, Kz. 1520 S. 4 f.; diff. *Brüggemeier*, WM 1982, 1294 (1302).

[29] Insbes. bei uneinheitlichen Verbrauchererwartungen wie z.B. bei Kopfstützen, ABS-Bremssysteme oder Airbags in KfZ, vgl. *Foerste,* in: v. Westphalen, ProfHaftHdb, § 24 Rn. 89 ff.; *Schmidt-Salzer*, Produkthaftung, Bd. III/1, Rn. 4.675 ff.; ähnl. *Hollmann*, DB 1985, 2389 (2392); *Schlechtriem*, VersR 1986, 1033 (1036); abl. gegenüber dem Kriterium der Verbrauchererwartung *Möllers*, Rechtsgüterschutz im Umwelt- und Haftungsrecht, 254 ff.

[30] Kullmann/Pfister-*Kullmann*, Produzentenhaftung, Kz. 1520, S. 15 f.

standen wird. Der Hersteller muss den Weg der größeren Vorsicht wählen, wenn Unsicherheiten über die Sicherheitsvorkehrungen bestehen.[31]

17 Besonders bedeutsam für die Konkretisierung der geschuldeten Verkehrspflichten ist in diesem Zusammenhang **der Stand von Technik und Wissenschaft** hinsichtlich der Sicherheit des Produktes. Maßgeblich sind die Erkenntnisse, die zum Zeitpunkt der erforderlichen Gefahrenabwehr verfügbar waren.[32] In diesem Rahmen stellen öffentlich-rechtliche Vorschriften und **Regelwerke privater Gremien, wie DIN-Normen**, zwar wichtige, aber keineswegs abschließende Konkretisierungen des Standes der Technik im zivilrechtlichen Sinne dar,[33] da im Einzelfall eine höhere Sicherheit erforderlich sein mag oder die technische Entwicklung die Normen überholt hat.[34] Der Hersteller muss selbstverantwortlich prüfen, welche Gefahren entstehen können.[35] So binden die Sicherheitsanforderungen nach dem Gesetz über technische Arbeitsmittel und Verbraucherprodukte (Geräte- und Produktsicherheitsgesetz - GPSG)[36] oder den jeweiligen Produktsicherheitsrichtlinien als Mindeststandards den Produzenten nicht und stehen höheren zivilrechtlich relevanten Sicherheitserwartungen nicht entgegen.[37] Ist für den Hersteller trotz Einhaltung der technischen Regeln und Wahrung etwaiger behördlicher Zulassungsvoraussetzungen eine von seinem Erzeugnis ausgehende Gefahr erkennbar, so hat er die darüber in Unkenntnis befindlichen Benutzer zumindest zu warnen.[38]

18 Auch **Zertifizierungen** und Prüfungen berühren hinsichtlich der materiell-rechtlichen Pflichten grundsätzlich nicht die zivilrechtliche Haftung des Herstellers. Sie können nur die Risiken und damit die Wahrscheinlichkeit eines Schadens mindern, nicht aber wei-

---

[31] Kullmann/Pfister-*Kullmann*, Produzentenhaftung, Kz. 1520, S. 15 unter Verweis auf BGH NJW 1990, 906 (907) - und Berufung auf arzthaftungsrechtliche Grundsätze, wie z.B. BGHZ 8, 138 (140); weniger restriktiv BGH NJW 1987, 2927.

[32] BGHZ 80, 186 (192) = NJW 1981, 1603.

[33] Zum öffentlich-rechtlichen Verständnis ausführlich *Spindler*, Unternehmensorganisationpflichten, 505 ff.

[34] BGH NJW 1998, 2814 (2815); BGH NJW 1994, 3349 (3350); LG Berlin MDR 1997, 246 (247); MünchKommBGB-*Wagner*, § 823 BGB Rn. 273; Staudinger-*J. Hager*, Kap. F Rn. 10; *Kullmann*, NJW 1996, 18 (22).

[35] BGHZ 99, 167 (176 f.) = NJW 1987, 1009 (für Zubehörteile).

[36] Mit dem Gesetz über technische Arbeitsmittel und Verbraucherprodukte (Geräte- und Produktsicherheitsgesetz – GPSG) wurden das Gerätesicherheitsgesetz (GSG) und das Produktsicherheitsgesetz (ProdSG) zu einem Gesetz zusammengeführt, sowie die Richtlinie über die allgemeine Produktsicherheit (Richtlinie 2001/95/EG v. 3.12.2001; ABlEG 2002 Nr. L 11 S. 4) in nationales Recht umgesetzt. Das GPSG wurde am 6. Jan. 2004 veröffentlicht (BGBl. I 2004, S. 2) und trat am 1. Mai 2004 in Kraft, GSG und ProdSG traten am 1. Mai 2004 außer Kraft; erster Überblick bei *Klindt*, NJW 2004, 465 ff.; *Potinecke*, DB 2004, S. 55 ff.; *Littbarski*, VersR 2005, 448; *Lenz*, MDR 2004, 918.

[37] BGH VersR 1972, 149; Kullmann/Pfister-*Kullmann*, Produzentenhaftung, Kz. 1520 S. 26; *Schmatz/Nöthlichs*, Sicherheitstechnik, Bd. I Teil 1, § 3 GSG Anm. 5.3.7; *Taschner/Frietsch*, § 1 ProdHaftG Rn. 89, Richtl. Art. 7 Rn. 31; *Wagner*, BB 1997, 2541 (2541 f.); *Niebling*, DB 1996, 80 (81); *Taupitz*, in: Produktverantwortung und Risikoakzeptanz, 119 (135), zum Einfluß des § 22 KrW-/AbfG auf den Mindestsicherheitsstand und die Sicherheitserwartungen bei Abfall s. *Gesmann-Nuissl/Wenzel*, NJW 2004, 117 ff.

[38] BGHZ 99, 167 (176) = NJW 1987, 1009; BGHZ 139, 79 (83) = NJW 1998, 2905; BGH NJW 1999, 2815 (2816); krit. dazu *Littbarski*, NJW 2000, 1161 (1162).

tergehende Sicherheitserwartungen des Verkehrs beschränken.[39] Sie können jedoch auf der Ebene der Entlastung für bestimmte Pflichten eine Rolle spielen: Andere in den Fertigungsprozess eingeschaltete Unternehmer, wie z.B. ein Auftragsfertiger, die hinsichtlich Konstruktionsgefahren geringeren Sorgfaltspflichten als der eigentliche Hersteller unterliegen, können sich jedoch im Einzelfall damit entlasten, dass das Produkt durch den TÜV oder einen anderen Sachverständigen überprüft wurde.[40] Auf diese Auswirkungen von Zertifizierungen ist später noch zurückzukommen.[41]

19 Die Anforderungen an die Verkehrspflicht stehen in einem engen Verhältnis zu den dem Dritten abzuverlangenden Bemühungen an **vernünftigem Eigenschutz**. Nicht gegen jedes Risiko kann Schutz verlangt werden, wenn der Dritte einfacher und mit geringerem Aufwand eine Schädigung als der Pflichtige vermeiden kann.[42] Allerdings darf nicht jede Möglichkeit des Eigenschutzes dazu führen, dass die Grenze zum Mitverschulden gem. § 254 BGB verschwimmt.[43] Vielmehr muss die Prüfung eindeutig ergeben, dass der Dritte ohne großen Aufwand die Verletzung vollständig vermeiden kann, während dem Pflichtigen selbst mit hohen Kosten die vollständige Gefahrenbeherrschung nicht möglich ist. So hat die Rechtsprechung anerkannt, dass der Verkehrspflichtige darauf vertrauen kann, dass bei einer Gefahr, die mit Händen zu greifen ist und der ohne weiteres ausgewichen werden kann, der Betroffene diese erkennt und sich selbst schützt.[44] Bei jedermann erkennbaren und bekannten Gefahren, muss auf diese nicht besonders hingewiesen oder vor ihnen geschützt werden.[45] Erst recht sind Siche-

---

[39] Darauf deuten auch die Ausführungen der EG -Kommission hin, vgl. ein Globales Konzept für Zertifizierung und Prüfwesen - Instrument zur Gewährleistung der Qualität bei Industrieerzeugnissen -, KOM(89) 209 endg. - SYN 208, Mitteilung Nr. 89/C 267/03 der Kommission an den Rat, vorgelegt am 15.6.1989, Abl. EG Nr. C 267/3 vom 19.10.1989, S. 12 (Kapitel II Ziff.4); Präambel der Richtlinie 92/59/EWG des Rates vom 29. Juni 1992 über die allgemeine Produktsicherheit, Abl. EG Nr. L 228, S. 24; ebenso *Niebling*, DB 1996, 80 (81), allerdings nicht für sog. C-Normen des höchsten Sicherheitsstandards; auch nach § 1 II Nr. 4 ProdHaftG liegt wegen der Beschränkung auf Mindeststandards kein Zwangstatbestand vor, vgl. *Marburger*, in: FS Lukes, 97 (100).

[40] BGH NJW-RR 1990, 406 f.; dazu *Kullmann*, NJW 1991, 675 (678 f.).

[41] S. Rn. 145 ff.

[42] Dies ist die Kernaussage der unten (Fn. 160) erwähnten Lehre vom *cheapest cost avoider*.

[43] Insoweit zutr. *Möllers,* VersR 1996, 153 (158); *Hasselblatt*, Die Grenzziehung zwischen verantwortlicher Fremd- und eigenverantwortlicher Selbstgefährdung im Deliktsrecht, S. 131 ff.; für stärkere Überlappung von Fremd- und Eigenverantwortlichkeit dagegen *Zeuner*, in: FS Medicus, S. 693 (699 ff.).

[44] BGHZ 104, 323 (328) = NJW 1988, 2611; BGH NJW-RR 1989, 219 (220); OLG Köln VersR 1993, 1494 f.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 251; Staudinger-*J. Hager*, Kap. E Rn. 32.

[45] BGHZ 104, 323 (328 f.) = NJW 1988, 2611 – Getränkeflasche; BGH NJW 1999, 2815 (2816); BGH NJW 1986, 52 (53) – Feuerwerk Silvesternacht; BGH NJW 1985, 1076 (1077) – Nicht fertig gestellte Loggia.

rungspflichten nicht gegenüber denjenigen angebracht, die gerade selbst zur Gefahrenkontrolle oder -beseitigung bestellt oder beauftragt wurden.[46]

20 Die vorstehend genannten Kriterien sind zwar auf den ersten Blick allein auf die Produkthaftung zugeschnitten; bei näherer Analyse wird jedoch deutlich, dass sie **verallgemeinerungsfähige Aussagen** enthalten, die auf das Ausmaß und die Kontrolle einer Gefahrenquelle, die bedrohten Rechtsgüter, die Zumutbarkeit von Gefahrenabwehrmaßnahmen, den Sicherheitserwartungen des Verkehrs (und gegebenenfalls des Vertragspartners) und dem möglichen Ausmaß des Eigenschutzes abstellen. Diese Maßstäbe können zwar im Einzelfall durch vertragliche Vereinbarungen modifiziert werden; doch sind sie immer wieder bei der Konkretisierung der im Verkehr erforderlichen und üblichen Sorgfalt nach § 276 BGB anzutreffen.[47]

2. Methodischer Hintergrund: Die rechtsökonomische Perspektive

21 Gerade in neuen Regelungsbereichen wie dem IT-Recht können sich die Denkmodelle der ökonomischen Rechtsanalyse als besonders nützlich erweisen.[48] Ausgangspunkt ökonomischer Denkmodelle ist die **Ressourcenknappheit.** Ziel ist eine effiziente Verteilung dieser Ressourcen.[49] Wann eine effiziente Verteilung, also **Alokationseffizienz** erreicht ist, lässt sich nach verschiedenen Kriterien messen: Nach dem **Pareto**-Kriterium besteht Allokationseffizienz, wenn eine ökonomische Situation erreicht ist, in der niemand besser gestellt werden kann, ohne jemand anderen schlechter zu stellen.[50] Weiter gefasst ist das **Kaldor-Hicks**-Kriterium. Danach ist Allokationseffizienz erreicht, wenn keine Veränderung mehr möglich ist, bei der die Gewinner ihre Gewinne höher bewerten als die Verlierer ihre Verluste.[51]

22 Die ökonomische Analyse lässt sich dabei sowohl auf der Ebene der Rechtsetzung als auch auf der Ebene der Rechtsanwendung fruchtbar machen. Auf der Ebene der Rechts-

---

[46] OLG Köln VersR 1992, 470 (471) – Feuerwehr; OLG Zweibrücken BauR 1994, 781 (782), Rev. nicht angenommen, BGH Beschl. v. 5.7.1994 VI ZR 346/93 – Sicherungsposten einer Baustelle; OLG Jena VersR 1998, 903 (904), Rev. nicht angenommen, BGH Beschl. v. 24.3.1998 VI ZR 274/97 – Sachverständige zur Gefahrenbegutachtung.

[47] Vgl. bspw. zum Einfluss technischer Regelwerke auf die im Verkehr erforderliche Sorgfalt Bamberger/Roth-*Unberath*, § 276 BGB Rn. 24; Palandt-*Heinrichs*, § 276 BGB Rn. 18; MünchKommBGB-*Grundmann*, § 276 BGB Rn. 64, zu Möglichkeiten des Selbstschutzes des Verletzten MünchKomm BGB-*Grundmann*, § 276 BGB Rn. 63.

[48] *Freiwald*, Harvard Journal of Law and Technology, Vol. 14, 2001 S. 574, 580.

[49] *Kübler*, in: FS Steindorff, S. 687, 689; *Salje*, Rechtstheorie 15 (1984), 277, 285.

[50] *R. Zebre Jr.*, Economic Efficiency in Law and Economics, S. 3; *Behrens*, Die ökonomischen Grundlagen des Rechts, S. 83 ff.

[51] *Mathis*, Effizienz statt Gerechtigkeit?, S. 70; *Baumol, W.*, Economic Theory and Operations Analysis, S. 402; *R. Zebre Jr.*, Economic Efficiency in Law and Economics, S. 4.

anwendung können einzelne Tatbestandsmerkmale insbesondere im Haftungsrecht auch nach ökonomischen Kriterien ausgelegt werden.[52] Auf der Ebene der Rechtssetzung (Teil 2) ist die Grundfrage hingegen, wie Rechtsnormen gestaltet sein müssen, um eine präventiv schadensmindernde Regelungsstruktur zu erhalten.

a) Steuerungsfunktion für das Niveau der Schutzmaßnahmen

23 Bekanntermaßen entstehen durch IT-Sicherheitsprobleme Schäden mit beträchtlichem wirtschaftlichem Ausmaß. Solche Schäden können durch entsprechende Maßnahmen (z.B. Rechtebeschränkung in IT-Systemen) eingedämmt werden. Diese Maßnahmen verursachen aber wiederum selbst Kosten (z.B. Lizenzgebühren für die Schutzsoftware, Personalaufwand). Es entsteht somit ein **Optimierungsproblem**: Ab einem gewissen Aufwand für Schutzmaßnahmen ist die unter Kostengesichtspunkten optimale Struktur erreicht, denn zusätzlicher Aufwand würde höhere Kosten verursachen als Schäden verhindert würden.

24 Exemplarische Darstellung des Optimierungsproblems

Aufwand für Schutzmaßnahmen	Erwarteter Schaden (Schadenshöhe * Wahrscheinlichkeit)	Gesellschaftliche Gesamtkosten
0	+ 40	= 40
10	+ 25	**= 35**
20	+ 20	= 40

25 Im obigen Beispiel (Tabelle): Betreibt der Akteur einen Sicherungsaufwand von 10 Einheiten ist der zu erwartende Schaden 25 Einheiten, Sicherungsaufwand und Schaden ergeben gesellschaftliche Gesamtkosten von 35 Einheiten. Damit ist das Optimum erreicht. Würde der Aufwand auf 0 Einheiten gesenkt oder 20 Einheiten gesteigert, würden die gesamtgesellschaftlichen Kosten steigen. Der zu erwartende Schaden berechnet sich dabei aus der Schadenshöhe bei einem einzelnen Schadensereignis multipliziert mit der Wahrscheinlichkeit des Eintritts eines solchen Ereignisses.

[52] *Taupitz*, AcP 196 (1996), 114 (125 ff.); Beispiele bei *Kötz/ Schäfer*, Judex oeconomicus, 2003.

26 Mit dem Haftungsrecht ist dem Gesetzgeber ein Werkzeug an die Hand gegeben, um Anreize für einen effizienten Aufwand für Sicherungsmaßnahmen zu schaffen.[53] Denkt man Haftungsregeln zunächst hypothetisch hinweg, so sind die erwarteten Schäden im obigen Beispiel **externe Effekte**; also negative Folgen für Dritte, die der Akteur *nicht* in seine Entscheidung einbezieht.[54]

27 Eine **Verschuldenshaftung** ist aus ökonomischer Perspektive nun die Festlegung eines bestimmten Sorgfaltstandards, dessen Nichteinhaltung zur Haftung führt.[55] Dieser Sorgfaltsmaßstab wird objektiv bestimmt und ist - juristisch beim Terminus des Verschuldens verortet[56] – nicht von den individuellen Fähigkeiten des Schädigers abhängig.[57] Im obigen Beispiel kann durch Festlegung der erforderlichen Sorgfalt bei 10 Einheiten eine Optimierung erreicht werden, da für den Akteur ein Anreiz besteht, diesen Sorgfaltsmaßstab einzuhalten, da er ansonsten haftet, also die externen Effekte zu tragen hat.

28 Diese Feststellungen lassen sich zur sogenannten marginalisierten **Learned-Hand** Formel verallgemeinern.[58] Danach ist dann kein Verschulden anzunehmen, wenn das Sorgfaltsniveau so gewählt ist, dass weitere Sorgfaltsanstrengungen (V) höhere Kosten verursachen würde als sie Schadenshöhe (S) mal Schadenswahrscheinlichkeit (q) reduzieren. Ein Verschulden ist also zu verneinen wenn: [59]

V' < S * q'

29 Ist der Sorgfaltsmaßstab durch Rechtsprechung oder gesetzliche Regelung zu hoch angesetzt, so ist es für den Schädiger nicht unbegrenzt wirtschaftlich sinnvoll, diesen einzuhalten.[60] An einem bestimmten Punkt, im obigen Beispiel ab einem Vorsorgeaufwand von 40 Einheiten, fährt der Schädiger am Besten, wenn er keine Sorgfaltsmaßnahmen trifft und die Schadenskosten i.H.v. 40 Einheiten auf sich nimmt.

30 Wird der Sorgfaltsmaßstab nicht kodifiziert sondern mit dem unbestimmten Rechtsbegriff der Fahrlässigkeit negativ umschrieben, so liegt es in der Hand des Richters im

---

[53] MünchKommBGB-*Wagner*,Vor § 823 BGB Rn. 40.

[54] *Behrens*, Die ökonomischen Grundlagen des Rechts, S. 83 ff.

[55] Vgl. statt vieler *Brown*, J., Towards a Theory of Liability, 323ff.

[56] Vgl. § 276 II BGB: „Fahrlässig handelt, wer die im Verkehr erorderliche Sorgfalt außer acht lässt."

[57] Wohl h.M., vgl. etwa *Brüggemeier*, Deliktsrecht, Rn. 113.

[58] Zuerst angewendet in United States v. Caroll Towing Co., 159 F. 2d 169 (2d Cir. 1947); vgl. *Cooter*, Journal of Economic Perspectives, Vol. 5, 1991, 11 ff., 14.

[59] Vgl. dazu etwa *Cooter/Ulen,* Law & Economics, S. 334.

[60] Ebenso *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, S. 172.

Einzelfall,[61] ob er die Fahlässigkeitsgrenze aufgrund obiger Erwägungen nach der Learned Hand Formel bei 10 Einheiten ansetzt.[62]

31 Auch mit einer **Gefährdungshaftung** werden die externen Effekte **internalisiert,** dh. es erfolgt eine Angleichung der privaten an die gesellschaftlichen Kosten.[63] Durch Einführung einer Gefährdungshaftung muss der Akteur sowohl alle Kosten für Schutzmaßnahmen als auch den erwarteten Schaden tragen: damit minimiert er schon in eigenem Interesse die gesellschaftlichen Gesamtkosten. Bezüglich der Wahl eines effizienten Sorgfaltniveaus ergibt sich also zwischen der Gefährdungshaftung und der Verschuldenshaftung (so die Gerichte hier einen effizienten Fahrlässigkeitsmaßstab festgelegt haben) i.E. kein Unterschied.[64] Allerdings führt die Gefährdungshaftung auch zu einer tendenziellen Reduktion des Aktivitätsniveaus überhaupt, da gleichgültig wieviel der Schädiger an Schutzmaßnahmen durchführt, er auf jeden Fall für eintretende Schäden haftet, so daß Anreize auch zu einer Verringerung des Gefährdungsniveaus bestehen (unten Rn. 32ff.).

b) Aussagen über die Auswahl des Haftenden

32 Die ökonomische Analyse kann aber nicht nur bei der Frage nutzbar gemacht werden, wann ein potentieller Schädiger zu haften hat, sondern auch *wer* unter einer Vielzahl von Verursachern die Kosten tragen sollte. Anreize zur Implementierung von Schutzvorkehrungen bestehen für denjenigen, der weiß, dass er im Schadensfall haftet. Wird nun demjenigen die Haftung auferlegt, der die Schutzvorrichtungen mit niedrigstem Kostenaufwand umsetzen kann, entstehen die gesamtgesellschaftlich geringsten Kosten, der sog. „**cheapest cost avoider“**.[65]

33 Vor einer rechtlichen Umsetzung dieses Modells stellt sich aber immer zunächst die Frage, ob nicht durch Marktmechanismen von vornherein die Schutzaufwendungen dem cheapest cost avoider auferlegt werden. Letztendlich bietet es sich ja für den Schädiger an, die Schutzvorkehrungen nicht selbst zu treffen, sondern vertragliche Beziehungen bezüglich der Schutzvorkehrungen mit dem (eventuell vom Haftenden unterschiedlichen) cheapest cost avoider (gegebenenfalls sogar den Geschädigten) einzugehen. Eine

---

[61] Fallbeispiele für die Anwendung ökonomischer Kriterien etwa OLG Hamm NJW RR 2002, 1459; BGH NJW 2005, 422.

[62] Zuerst angewendet in United States v. Caroll Towing Co., 159 F. 2d 169 (2d Cir. 1947); vgl. *Cooter*, Journal of Economic Perspectives, Vol. 5, 1991, 11 ff., 14.

[63] Diese Definition für Internalisierung findet sich auch bei *Schumann*, Grundzüge der Mikroökonomischen Theorie, S. 38 und S. 492 ff.; *K. Mathis*, Effizienz statt Gerechtigkeit?, S. 70.

[64] Ebenso *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, S. 208.

[65] *G. Calabresi*, The Costs of Acidents, S. 136 ff.; *Coase*, The Problem of Social Cost, S. 146 f.

solche vertragliche Optimierung ist ein Beispiel für das **Coase-Theorem**. Nach diesem erfolgt, allgemein formuliert, die Allokation (hier: der Einsatz) von Ressourcen unabhängig von der genauen Ausgestaltung der Rechtsordnung – aber nur sofern keine Transaktionskosten bestehen.[66]

34 **Transaktionskosten** sind die Kosten, die aufgewendet werden müssen um einen Vertrag abzuschließen und durchzusetzen.[67] Da entsprechende Kosten immer entstehen kann das Coase-Theorem auch anders gewendet werden: in der realen durch Transaktionskosten bestimmten Welt ist die Allokation der Ressourcen *immer* auch von der Rechtsordnung mitbestimmt.[68] Folglich behält der Grundgedanke, die rechtlich ausgestaltete Haftung am cheapest cost avoider auszurichten, praktisch immer seine Berechtigung, wird aber durch das Gedankenexperiment der idealen Welt (Coaseanischen Welt) gegenkontrolliert.[69]

c) Steuerung des Aktivitätsniveaus

35 Über eine ökonomische Analyse lassen sich also Hinweise gewinnen, wie das Haftungssystem ausgestaltet sein muss, um ein effizientes Niveau von Schutzmaßnahmen zu erreichen und Anreize setzen, dass derjenige die Schutzmaßnahmen durchführt, dem dies am kostengünstigsten möglich ist. Darüber hinaus lassen sich aber auch Aussagen darüber gewinnen, wie durch das Haftungssystem das **Aktivitätsniveau** beeinflusst werden kann: Ein rational handelnder Akteur wird bei der Abwägung von Nutzen und Kosten einer Handlung auf der Kostenseite das mögliche Haftungsrisiko mit einstellen.[70] Steigt nun das Haftungsrisiko durch schärfere Haftungsregelungen, so steigen auch die Kosten. Mit den Kosten steigt in einer funktionsfähigen Marktwirtschaft auch der Preis eines Produktes oder einer Dienstleistung. Bei ansonsten gleichen Umständen wird das teurere Produkt weniger nachgefragt. Damit wird das Aktivitätsniveau durch schärfere Haftungsregelungen gesenkt.[71]

---

[66] *Thomas J. Miceli*, Economics of the Law, S. 9; *Coase*, The Problem of Social Cost, Journal of Law and Economics 3; *ders.*, in: Assmann/Kirchner/Schanze, Ökonomische Analyse des Rechts, S. 129, 148 ff.

[67] *R. Coase*, The Problem of Social Cost, Journal of Law and Economics 3, S. 15.

[68] *R. Coase*, Law and Economics, S. 251.

[69] Vgl. auch *Siemer*, Das Coase-Theorem, S. 82 f.

[70] Zur Grundannahme des rational handelnden Akteurs vgl. *Coleman*, Foundations of Social Theory, S. 5; *Kirchgässner*, Homo Oeconomicus, S. 66 ff.; *Tietzel*, Jahrbuch der Sozialwissenschaften (1981), S. 115 ff.; *Eder*, Zeitschrift für Rechtssoziologie 8 (1987), 193 (207 ff.).

[71] *Sailer*, Prävention im Haftungsrecht, S. 186.

36 Durch eine **Gefährdungshaftung** erfolgt dabei sogar eine Senkung der Aktivität auf das gesamtgesellschaftliche Optimum.[72] Denn die Gefährdungshaftung bürdet dem Schädiger alleinig das Haftungsrisiko auf. Damit fließen alle Nutzen und Kosten der Aktivität in der Person des Schädigers zusammen. Folglich ist absolute Parallelität zwischen dem Interesse des Schädigers und dem Interesse der Gesellschaft erreicht. Im Ergebnis wird der Schädiger, indem er aus eigenem Interesse handelt, gleichzeitig den Nutzen für die Gesellschaft maximieren.

37 Damit kann mittels der Gefährdungshaftung theoretisch eine stärkere Steuerungswirkung erreicht werden[73] - dass in Deutschland trotzdem die Verschuldenshaftung die Regel ist, ist historisch[74] bzw. dadurch bedingt, dass der Hauptaugenmerk auf die Kompensationsfunktion[75] und nicht die Steuerungsfunktion des Haftungsrechts liegt. Im Übrigen ist der Unterschied in der normpraktischen Ausgestaltung geringer als soeben theoretisch skiziert, da die Steuerungswirkung durch Haftungsobergrenzen, Informationsdefizite und Versicherungsmöglichkeiten begrenzt ist:

38 **Haftungsobergrenzen** schränken die Steuerungsfunktion des Haftungsrechts ein und führen so zu einem höheren Aktivitätsniveau. So wie der Akteur Schäden bei denen er mangels Verschulden nicht haftet nicht in seine Kalkulation mit einbezieht, bezieht der Akteur bei Haftungsobergrenzen Schäden oberhalb dieser Grenzen nur mit der maximalen Haftungssumme in seine Kalkulation ein.

39 Bei einer **Verschuldenshaftung** wird dieser Effekt nicht vollständig erzielt.[76] Wie gesehen kann zwar durch richtige Wahl des Verschuldensmaßstabes ein optimales Maß an Sorgfalt erreicht werden. Allerdings wird das Aktivitätsniveau nicht auf das gesamtgesellschaftliche Optimum gesenkt. Denn für Schäden, die trotz Einhaltung der Sorgfaltspflichten entstehen, haftet der Akteur nicht. Diese werden von Dritten getragen. Ergo verursachen seine Handlungen bei ihm weniger Kosten als bei der Gesellschaft insgesamt. Und Schäden, für die er nicht haftet, wird der Akteur nicht in seine Kalkulation

---

[72] Für den mathematischen Nachweis, *S. Shavell*, Economic Analysis of Accident Law, S. 23 ff., 32 ff.; vgl. auch *Sailer*, Prävention im Haftungsrecht, S. 186; Miceli, Economics of the Law, S. 28.

[73] *Sailer*, Prävention im Haftungsrecht, S. 185 mwN.

[74] Vgl. *Benöhr*, Die Entscheidung des BGB für das Verschuldensprinzip, Tijdschrift voor Rechtsgeschiedenis, 1978, S. 1 ff.; „Nicht der Schaden verpflichtet zum Schadensersatz, sondern die Schuld“, *Jhering*, das Schuldmoment im römischen Privatrecht, S.40.

[75] *Larenz*, Lehrbuch des Schuldrechts, S. 423; vgl. auch *Sailer*, Prävention im Haftungsrecht, S. 1 mwN.

[76] Vgl. *Miceli,* Economics of the Law, S. 28.

einbeziehen. Er wird die Handlung damit häufiger ausführen, als dies für die Gesamtgesellschaft optimal wäre.

40 Die Internalisierung der externen Effekte erfüllt auch dann keine Steuerfunktion, wenn der **Schaden nicht vorhersehbar** ist[77] - für IT-Schäden eines der zentralen Probleme. Denn mit einem solchen Schaden kalkuliert der Akteur nicht. Ein ähnlich gelagertes Problem besteht dann, wenn der Akteur spontane Entscheidungen treffen muss – die Steuerfunktion ist größer, wenn der Akteur die Möglichkeit hat, die Situation „planend zu überdenken".[78] Durch **Versicherungen** wird das Interesse des Akteurs von dem der Allgemeinheit entkoppelt, denn durch Einschaltung der Versicherung trägt der Akteur nicht direkt den Schaden – die Steuerungswirkung ist entsprechend weiter eingeschränkt.[79]

d) Mehrpersonenkonstellationen

41 In der Realität, insbesondere im IT-Bereich, wird eine effektive Schadensvermeidung häufig erst durch die Anstrengung sowohl des Akteurs als auch des Geschädigten zu erreichen sein. Bei einer Verschuldenshaftung ist der Geschädigte schon aus Eigeninteresse unabhängig von **Mitverschuldensregelungen** zu Schutzmaßnahmen angehalten.[80] Schließlich muss der Geschädigte damit rechnen, dass der Schädiger alle Sorgfaltsstandards einhält und er, der Geschädigte, somit etwaige Schäden alleine tragen muss. Bei einer Gefährdungshaftung allerdings ist eine Mitverschuldensregelung erforderlich, um Anreize für Schutzmaßnahmen durch den Geschädigten zu setzen.[81]

42 Ebenso wie die Sorgfaltsanstrengungen des Schädigers als auch des Geschädigten die Schadenswahrscheinlichkeit beeinflussen, beeinflusst in der Regel nicht nur das Aktivitätsniveau des Akteurs, sondern auch das des Geschädigten die Schadenswahrscheinlichkeit. Nach dem Theorem von *Shavell* lassen sich aber weder durch eine Verschuldenshaftung noch durch eine Gefährdungshaftung beide Aktivitätsniveaus auf das gesellschaftliche Optimum reduzieren.[82] Eine solche Steuerung tritt nämlich wie dargelegt[83] nur dann ein, wenn die jeweilige Person das volle Risiko des Schadenseintritts

---

[77] *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, S. 214.

[78] *Weyers*, Unfallschäden, S. 466 ff.

[79] Details bei *Pauly*/*Kenneth,* The Economics of Moral Hazard, S. 531.

[80] *M. Adams*, Ökonomische Analyse der Gefährdungs- und Verschuldenshaftung, S. 73 ff; *Endres*, Ökonomische Grundlagen des Haftungsrechts, S. 9 ff.

[81] Ebenso *Miceli*, Economics of the Law, S. 29.

[82] *Shavell,* The Journal of Legal Studies, Vol. 9, No. 1 1980, S. 1 ff.; *ders.*, Economic Analysis of Accident Law, S. 29.

[83] S. Rn. 27 f.

trifft – dieses Risiko kann aber nicht gleichzeitig sowohl dem Schädiger als auch dem Geschädigten auferlegt werden.

43 Können mehrere Personen durch ein Ereignis sowohl einen Schaden verursachen als auch geschädigt werden, so kann die Situation eintreten, dass schon ohne Haftungsregelungen gesamtgesellschaftlich effiziente Sorgfaltsmaßstäbe angewendet werden. Zur Vereinfachung soll dies an einem Beispiel aus der Schifffahrt illustriert werden[84] – wobei eine gewisse Vergleichbarkeit mit der Situation in größeren Netzwerken besteht: Angenommen, durch die Einführung von Funkgeräten lässt sich das Kollisionsrisiko zwischen zweier so ausgerüsteter Schiffe eliminieren. Ein Funkgerät kostet 5 Einheiten, der erwartete Schaden (Wahrscheinlichkeit mal Schadenshöhe) durch Kollisionen beträgt 10 Einheiten. Sind nun in der Ausgangssituation mehr als 50% der Schiffe mit einem Funkgerät ausgestattet, ist es unter Kostengesichtspunkten effektiv, neue Schiffe mit einem Funkgerät auszurüsten. Im Laufe der Zeit haben so alle Schiffe ein Funkgerät. Keiner der Akteure hat Veranlassung, sein Verhalten zu ändern, weshalb ein stabiler Zustand (**Nash-Gleichgewicht**) erreicht ist.[85] Damit hat sich die gesamtgesellschaftlich effiziente Sorgfalt herausgebildet.

44 Sind allerdings in der Ausgangssituation weniger als 50% der Schiffe mit einem Funkgerät ausgestattet, ist es ineffektiv, neue Schiffe mit einem solchen auszurüsten. Es besteht wiederum ein Nash-Gleichgewicht, allerdings auf gesamtgesellschaftlich ineffizientem, niedrigem Sorgfaltsniveau. Dieses Gleichgewicht kann nun aber mit Hilfe einer Veschuldenshaftung durchbrochen werden: Wird das Fahren ohne Funkgerät als fahrlässig definiert, besteht dadurch auch bei einer Funkgerätepenetration von weniger als 50% ein Anreiz dafür, Schiffe mit einem Funkgerät auszurüsten. Das ineffiziente Nash-Gleichgewicht wird durchbrochen.

3. Anwendung auf IT-Bereiche

45 Diese allgemeinen Kriterien lassen sich ohne weiteres auch auf IT-Produkte und Dienstleistungen übertragen – allerdings mit der Maßgabe, dass der Komplexität der Produkte und der diffizilen Fehlerentdeckung Rechnung getragen werden muss.

a) Technische Standards

[84] Bsp. stark modifiziert nach *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, S. 231 ff.

[85] Es handelt sich um ein evolutorisch stabiles Nash-Gleichgewicht.

46 Allgemeingültige technische Standards, etwa in Gestalt von ISO-Normen, liegen – soweit ersichtlich – für IT-Produkte und erst recht für IT-Dienstleistungen bislang nicht breitflächig vor. Von Relevanz werden im Rahmen der weiteren Analyse vor allem auf Seiten der Produzenten die sog. **Common Criteria-Standards**, die sich als internationaler Standard für IT-Produkte und deren Sicherheitsbewertung (ISO-Norm) [86] herausgebildet haben.[87] Im Zusammenhang mit sog. Protection Profiles, die halbstandardisiert für Sicherheitsbedürfnisse von IT-Anwendungen erstellt werden, können diese Produktstandards rechtliche Wirkung entfalten, indem sie die nötige Mindestsicherheit für bestimmte Bereiche konkretisieren.

47 Aber auch auf der Seite der IT-Nutzer bzw. Verwender können Standards eine Rolle spielen, wie die jüngst verabschiedete ISO 27000 ff. Normenreihe, die Grundsätze für das IT-Riskmanagement aufstellt.

b) Anpassung an bestimmte Marktanforderungen

48 Ebenso spielen aber auch besondere Anforderungen in bestimmten Märkten eine Rolle, die die berechtigten Verkehrserwartungen prägen können, etwa im Gesundheits-, Sicherheits- oder Finanzsektor. Umgekehrt können an eine Massensoftware mit niedrigem Gefährdungspotential (und geringem Preis) vergleichsweise reduzierte Sicherheitsanforderungen gestellt werden. Indes ist nicht zu verkennen, dass der Trend zur Erstellung der Protection Profiles bereits diese Spezifika berücksichtigt.

c) Verhältnis zum Eigenschutz

49 Schließlich spielen im IT-Bereich die Fragen des Eigenschutzes bei der Bestimmung der Pflichten eine gewichtige Rolle: Hier gilt zunächst wiederum in Anwendung der allgemeinen Grundsätze, dass gegenüber professionellen IT-Anwendern prinzipiell reduzierte Pflichten gelten, sofern diese selbst in der Lage sind, den nötigen Eigenschutz zu gewährleisten. Allerdings versagt dies gerade dort, wo der **Code nicht zugänglich** ist oder der IT-Anwender nicht über entsprechende Kenntnisse verfügt. Ferner kommt es darauf an, ob und inwieweit allgemein bekannte Tools oder Softwareschutzmechanismen dem Nutzer zur Verfügung stehen.[88]

---

[86] Gemeinsame Kriterien für die Prüfung und Bewertung von Sicherheit von Informationstechnik nach der im Jahre 2000 beschlossenen ISO-Norm 15408 bezeichnet; zur Entwicklung s. *Münch*, RDV 2003, 223.

[87] Näheres dazu auch abrufbar unter: http://www.bsi.bund.de.

[88] Ausführlich dazu unten Rn. 277 ff.

4. Sicherheitspflichten innerhalb von Vertragsverhältnissen

50 Im Unterschied zum Deliktsrecht zeichnet sich das Vertragsrecht dadurch aus, dass es den Parteien aufgrund der Privatautonomie hier selbst obliegt, die Pflichtensphären für die IT-Sicherheit festzulegen. Im Rahmen von Individualverträgen haben die Parteien hier weiteste Gestaltungsspielräume, die lediglich durch zwingende gesetzliche Regelungen und gesetzliche Verbote bzw. Sittenwidrigkeit (§§ 134, 138) begrenzt werden. Größerer Kontrolle unterliegt jedoch die Vertragsgestaltung durch Allgemeine Geschäftsbedingungen. Für Verträge zwischen Unternehmen und Verbrauchern statuieren die §§ 308 f. BGB zahlreiche Klauselverbote. Diese sind auch für Verträge über IT-Produkte anwendbar, für spezifische IT-Risiken treffen sie jedoch keine gesonderten Regelungen. Umso größere Bedeutung erlangt somit die Generalklausel des § 307 BGB. Danach sind Bestimmungen in Allgemeinen Geschäftsbedingungen dann unwirksam, wenn sie den Vertragspartner des Verwenders unangemessen benachteiligen. Genauere Konkretisierung erfährt diese Generalklausel durch Abs. 2 der Vorschrift, nach dem eine unangemessene Benachteiligung im Zweifel dann anzunehmen ist, wenn die vertragliche Klausel mit dem Grundgedanken der gesetzlichen Regelung nicht zu vereinbaren ist oder wesentliche Rechte und Pflichten, die sich aus der Natur des Vertrages ergeben, so einschränkt, dass die Erreichung des Vertragszweckes gefährdet ist. Insbesondere der letztgenannte Unwirksamkeitsgrund für AGB-Klauseln ist eine für IT-Verträge bedeutsame Grenze der Privatautonomie.

51 Die Regelungen der §§ 308, 309 BGB gelten nur für Verträge zwischen Verbrauchern und Unternehmern. Auf andere Verträge finden sie keine Anwendung. Indes findet gerade die allgemeine Inhaltskontrolle nach § 307 BGB – freilich mit größerem Gestaltungsspielraum – auch bei Verträgen zwischen Unternehmern Anwendung.

III. Gefahrenpotential und Gegenmaßnahmen

52 Um zu verdeutlichen, welche Risiken und daraus folgend Haftungen eintreten können, ist es notwendig, die sich bei der Nutzung von Informationstechnik, insbesondere IT-Netzen, ergebenden Gefahren näher zu beleuchten. Aus Sicht der Nutzer ist des weiteren zu erläutern, welche Gegenmaßnahmen grundsätzlich ergriffen werden können, da sich daraus deren Pflichtenprogramm ableiten kann.

53 Werden Pflichten an eine wie auch immer geartete Zumutbarkeitsabwägung geknüpft, wird auch eine Einschätzung über die **voraussichtlichen Kosten** benötigt. Diese ist

natürgemäß im vorgegebenen Rahmen dieser Untersuchung ungenau und soll nur eine Richtlinie darstellen. Notwendig ist im Rahmen einer solchen Abwägung jeweils eine Einzelfallbetrachtung und nähere technisch-betriebswirtschaftliche Analyse. So können Kosten bei größeren Systemen überdurchschnittlich skalieren, wobei auch die Gefahrensituation mit der Größe von Rechensystemen und –netzen wachsen können.

54 Anhaltspunkte für Bedrohungspotentiale und Gefahrenlagen lassen sich aus den Aufgaben des IT-Managements im Allgemeinen und für die IT-Sicherheit im Speziellen entnehmen, die darin bestehen, die **Integrität, Verfügbarkeit und Vertraulichkeit von Daten und Diensten, sowie die Authentizität eines Senders/Empfängers sicherzustellen**:[89]

- Integrität bedeutet, dass nur autorisierte und im Sinne der Systemfunktionalität gewollte Modifizierungen von Hardware, Software und Daten durchgeführt werden können.[90]
- Unter Authenzität versteht man die eindeutige Identifizierung eines Senders/Empfängers von Daten[91], wie sie z.B. in einer sog. „Public Key Infrastructure“[92] gewährleistet ist.
- Der Begriff der Verfügbarkeit meint, dass ein IT-System zum gewünschten Zeitpunkt mit den erforderlichen Funktionen und Daten zur Verfügung steht. Es handelt sich somit um eine zentrale Anforderung.
- Unter Vertraulichkeit ist der Schutz im Hinblick auf Lesen, Schreiben, Modifizieren oder Löschen von Daten vor den unbefugten Zugriff und/oder die Weitergabe von Daten durch unbefugte Personen oder Prozesse zu verstehen.[93]

55 Für die **Netz- und Informationssicherheit** kann schließlich die Definition der EU im Rahmen der Errichtung einer europäischen Agentur zur Netz- und Informationssicherheit herangezogen werden, wonach darunter die Fähigkeit eines Netz- oder Informationssystems zu verstehen ist, Störungen oder rechtswidrige oder böswillige Angriffe abzuwehren, die die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität der ge-

[89] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 7.2, S. 9 Rn. 2, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (zuletzt abgerufen am 20.02.2006).

[90] Datensicherheit in Industrie und Wirtschaft, *S&S International GmbH, uti-maco GmbH*, (1994).

[91] *Nirvikar Singh*, in: *Bidgoli*, Handbook of Information Security, Volume 1, S. 28.

[92] Zur Funktionsweise: *Radia Perlman,* in *Bogdali,* Handbook of Information Security, Volume 1, S. 852 ff. und *Bradley S. Rubin* in; *Bogdali,* Handbook of Information Security, Volume 2, S. 548 ff.

[93] *Nirvikar Singh*, in: *Bidgoli*, Handbook of Information Security, Volume 1, S. 28.

speicherten oder übermittelten Daten und damit verbunden über das betreffende Netz angebotene Dienste beeinträchtigen können.[94]

56 Zur möglichst vollständigen Erreichung dieser Schutzziele müssen alle Beteiligten (d.h. Hersteller, Intermediäre und Nutzer von IT-Systemen) eng zusammenarbeiten und entsprechende Schutzvorkehrungen treffen. Besondere Sorgfalt ist geboten, wenn besondere Gefahrenpotentiale vorliegen, die in diesem Abschnitt beschrieben werden. Dies beinhaltet eine Abschätzung des Risikos eines Gefahrenpotentials und möglichen Gegenmaßnahmen, jedoch keine rechtliche Bewertung.

57 Der Schwerpunkt wird nachfolgend auf Szenarien gelegt, bei denen Angreifer das Ziel verfolgen, fremde Systeme unter ihre Kontrolle zu bringen, um mit diesen kompromittierten Systemen wiederum Angriffe gegen Dritte durchzuführen. Vergleichbare Szenarien bzw. Schadensfälle lassen sich für zahlreiche andere Länder nachweisen, etwa für Österreich.[95]

1. Angriffe gegen Einzelsysteme

a) Systeme unter Kontrolle des Angreifers bringen

(1) Viren

58 Bis heute hat sich in der Forschung keine einheitliche Definition für den Begriff des Computervirus` durchgesetzt.[96] Grundsätzlich werden unter **Computerviren** werden sich selbst vermehrende Computerprogramme verstanden.[97] Viren treten niemals alleine auf, sondern benötigen einen Wirt,[98] um ausgeführt zu werden, sich zu verbreiten und evtl. vorhandene Schadfunktionen auszuführen.[99] Bei einem Wirt handelt es sich meist um ausführbare Dateien, die von einem Virus infiziert wurden oder infiziert werden können. Als Wirt können aber auch Programme dienen, die Makros enthalten.[100] Durch Infektion wird der Wirt so verändert, dass mit seiner eigenen Ausführung auch die Funktionen des Virus ausgeführt werden, wobei Viren stets versuchen, die eigene Existenz zu verdecken und gleichzeitig möglichst viele Wirte zu infizieren. Zur Reprodukti-

[94] Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit, Abl. L 77, 13.3.2004; *Holznagel*, Recht der IT-Sicherheit, S. 11; *Eckert*, IT-Sicherheit, S. 5.

[95] *Fallenböck* Annex II – Österreich - Rn. 1226 ff.

[96] *Bigdoli*, Handbook of Information Security, Volume 3, S. 95.

[97] *Anonymous*, der neue hacker's guide, S. 401; *Eckert*, IT-Sicherheit, S. 45 f.

[98] *Lang*, JurPC 205/2001, Rn. 50.

[99] *Slade* in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S.256, 258 f., 358 f.

[100] *Tita*, VW 2001, 1696; *Lang*, JurPC 205/2001, Rn. 61, *Anonymous*, der neue hacker's guide, 413.

on und Verbreitung sind in jedem Fall Ressourcen des Rechners erforderlich. Nicht selten ist dies sogar die einzige Schadfunktion.[101]

59 Im Gegensatz zu Computerwürmern,[102] die sich autark verbreiten können, muss ein Anwender eine mit einem Virus infizierte Datei ausführen, damit der Virus sich weiterverbreiten kann.[103] Die Verbreitung infizierter Dateien erfolgte - vor der Verfügbarkeit von weltweiten Netzwerken wie dem Internet - hauptsächlich über Wechseldatenträger wie Disketten und CD-ROMs.[104] Diese Verbreitungswege wurden jedoch nahezu komplett durch netzbasierte Verbreitungen wie E-Mail und Downloads von FTP- oder Web-Servern verdrängt.

60 Mögliche Gegenmaßnahmen: Virenscanner[105] sind, wie der Name bereits nahe legt, eine effektive und gängige Maßnahme, um die Infektion mit Viren zu verhindern und stellen die Grundvoraussetzung für den Schutz vor Viren dar. Neben dem Einsatz auf lokalen PCs als Wächterprogramm, welches jeden Dateizugriff auf einen möglichen Virenbefall überprüft und dem regelmäßigen Prüfen aller lokal vorhandener Dateien, ist in vernetzten Umgebungen der Einsatz zentraler Virenscanner auf den E-Mail- und Dateiservern zu empfehlen. Oberstes Gebot ist es jedoch, die Virendefinitionsinformationen für die jeweilige Antivirensoftware stets aktuell zu halten. Alle wichtigen Anbieter haben dafür standardmäßig eine automatische, webbasierte Updatefunktion in ihre Produkte implementiert, so dass der Anwender sich nach der erstmaligen Einrichtung kaum noch persönlich darum kümmern muss.

61 Einschätzung des Gefährdungspotentials: Aufgrund der Eigenschaft von Computerviren, sich nur unter Mithilfe des Anwenders weiterverbreiten zu können und durch den routinemäßigen Einsatz von Virenscannern, stellen klassische Computerviren heute keine besonders große Gefahr mehr für die IT-Sicherheit dar. Viren wurden von sich selbstständig verbreitenden Computerwürmern abgelöst,[106] die sich die weltweite Vernetzung von Computern und Schwachstellen von Software zu Nutze machen, um sich schneller und effektiver zu verbreiten als Viren.

---

[101] *Bigdoli*, Handbook of Information Security - Volume 3, S. 95.

[102] S. u. B.III.1.a)(2).

[103] *Lang*, JurPC 205/2001, Rn. 50.

[104] *Unbekannt*, VW 1996, 580; weiter dazu AG Köln DuD 2001, 298; LG Köln NJW 1999, 3206; *Leible/Sosnitza*, K&R 2002, 51.

[105] *Slade* in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S.263.

[106] 80% der bei der Bundesverwaltung erkannten Schadprogramme waren Würmer und Trojaner, BSI-Lagebericht 2005, abrufbar unter: http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf, S. 17 (zuletzt abgerufen am 09.10.2006).

(2) Würmer

62 Während Viren darauf ausgelegt sind möglichst viele Wirte (Dateien) zu infizieren und auf eine Verbreitung dieser infizierten Dateien durch den Anwender angewiesen sind, nutzen **Computerwürmer**[107] die Netzwerkinfrastruktur, um sich selbst zu verbreiten, indem sie Netzwerkdienste missbrauchen (bspw. massenhafter Versand von E-Mails, die u.a. den Wurm enthalten[108] oder „Erweiterungen" gebräuchlicher Protokolle wie IRC-, P2P oder Instantmessaging-Protokolle) oder Sicherheitslücken in Netzwerkdiensten, ebenso wie in sonstiger (populärer) Software, ausnutzen.[109] Von Würmern sind auch Plattformen betroffen, die von Viren bisher verschont geblieben sind. So sind gegenwärtig auch Mobiltelefone mit fehlerhafter Implementierung des Bluetooth-Standards bedroht.[110] Im Gegensatz zu Viren, die versuchen möglichst viele Dateien zu infizieren, nisten sich Würmer im Wirtssystem so ein, dass sie möglichst unerkannt bleiben und bei jedem Systemstart ausgeführt werden. Das Ziel von Würmer muss nicht die Ausführung von Schadfunktionen sein, sondern kann auch in der reinen Weiterverbreitung liegen, die an sich bereits großen wirtschaftlichen Schaden anrichten kann, da zur Weiterverbreitung häufig enorme Ressourcen auf Seiten der infizierten, der zu infizierenden und vermittelnden Systeme gebunden werden.

63 Mögliche Gegenmaßnahmen: Neben dem standardmäßigen Einsatz von Virenscannern, die neben Viren auch Würmer und andere schadhafte Software (sog. Malware) erkennen und deren Ausführung verhindern können, ist der Einsatz von **Firewalls**[111] zu empfehlen, die an Schnittstellen zwischen Netzen oder Computersystemen den Datenverkehr kontrollieren und regulieren können.[112] Zu unterscheiden ist zwischen sog. Personal Firewalls, die lokal auf PCs eingesetzt werden können und zentralen Firewalls, die den Zugriff zwischen Netzen beschränken können. Firewalls ermöglichen es ebenso einzelnen Anwendungen Zugriff auf Netzwerkfunktionen zu ermöglichen bzw. zu verweigern wie auch den Zugang zu Netzwerkdiensten zu regulieren. Eine häufig angewandte Strategie zur Konfiguration von Firewalls sieht vor, allen Dienste/Anwendungen den Netzwerkzugriff zu verweigern und nur die benötigten Dienste/Anwendungen freizuschal-

---

[107] *Slade* in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S.259, 358 f.
[108] *Tita*, VW 2001, 1696.
[109] *Lang*, JurPC 205/2001, Rn. 41; *Eckert*, IT-Sicherheit, S. 57.
[110] *Eckert*, IT-Sicherheit, S. 870 ff.; *Tanenbaum*, Computer Networks, S. 784.
[111] *Chari* in: Bidgoli, Encyclopedia of Informationsystems Volume 2, 2002, S. 313.
[112] *Fuhrberg/Häger/Wolf*, Internet-Sicherheit, S. 137; *Lang*, JurPC 205/2001, Rn. 99.; zur Funktionsweise: *Tanenbaum*, Computer Networks, S. 776 ff.

ten, um die Angriffsfläche möglichst klein zu halten und somit auch der Infektion und Verbreitung von Würmern vorzubeugen.

64 Weiter lässt sich gegen die Verbreitung von Würmern empfehlen, dem **Nutzer vom Betriebssystem nur die Rechte einzuräumen, die er wirklich benötigt**. was sich bei allen modernen Plattformen (Windows, Linux, Mac OS etc.) einfach dadurch realisieren lässt, im Alltag ohne Administratorrechte zu arbeiten.

65 Zusätzlich zu dem Einsatz von Firewalls und dem Entzug überflüssiger Rechte, empfiehlt sich die Installation von Systemen, die Angriffe aufgrund typischer Angriffsmuster erkennen und entsprechende Gegenmaßnahmen auslösen können. Solche Systeme werden als **Intrusion-Detection-Systeme**[113] (IDS) bzw. als **Intrusion-Prevention-Systeme** (IPS) bezeichnet, wobei der Unterschied darin liegt, dass ein IDS Angriffe zwar erkennen, aber nicht verhindern kann, während IPS zusätzlich in der Lage sind Gegenmaßnahmen einzuleiten. Bei IDS und IPS wird zwischen system- oder hostbasierten und netzwerkbasierten Ansätzen unterschieden.[114] IDS werden auf dem zu überwachenden System installiert und sammeln Informationen über das System und dessen aktuellen Zustand, um anhand von in einer Datenbank hinterlegten Mustern bzw. Heuristiken,[115] Angriffe zu erkennen und dann zuvor definierte Gegenmaßnahmen (bspw. Administratoren informieren, verdächtige Prozesse beenden, Firewall-Regeln anpassen, etc.) auszulösen.[116] Netzwerkbasierte IDS werden an zentralen Netzwerkknoten eingerichtet, so dass sie in der Lage sind möglichst alle Datenpakete in einem Netzwerk zu analysieren, verdächtige Aktivitäten zu melden und ggf. Gegenmaßnahmen einzuleiten.[117] Als Maßnahme gegen einen Wurmangriff, kann ein netzwerkbasiertes IPS in der Lage sein, die erhöhte Netzwerkaktivität zu erkennen und die Firewall-Regeln so anzupassen, dass der Angriff gestoppt werden kann.

66 **Einschätzung des Gefährdungspotentials:** Die Gefahr, die von Würmern ausgeht, ist signifikant höher als die von Viren. Durch die selbstständige Weiterverbreitung nach

---

[113] Dazu ausführlich BSI-Studie Einführung von Intrusion-Detection-Systemen, abrufbar unter: http://www.bsi.bund.de/literat/studien/ids02/dokumente/Grundlagenv10.pdf, S. 5 ff.; *Anonymous*, der neue hacker's guide, S. 290 ff.; *Chari* in: Bidgoli, Encyclopedia of Informationsystems Volume 2, 2002, S. 327.

[114] *Peikari/Chuvakin*, Kenne Deinen Feind, S. 462 f.

[115] Funktionsweise, Probleme und Beispiele bei *Zhang/Lee/Huang*, Intrusion Detection Techniques for Mobile Wireless Networks, abrufbar unter: http://citeseer.ist.psu.edu/zhang03intrusion.html, (zuletzt abgerufen am 09.10.2006).

[116] *Eckert*, IT-Sicherheit, S. 676.

[117] *Peikari/Chuvakin*, Kenne Deinen Feind, S. 463.

einer Infektion und die Nutzung der Netzwerkinfrastruktur, sind Würmer in der Lage in kürzester Zeit einen enormen wirtschaftlichen Schaden anzurichten.

(3) Trojaner

67 Als **Trojanische Pferde** (kurz auch **Trojaner** genannt) werden Programme bezeichnet, die als nützliche Anwendung getarnt sind, aber zusätzliche Funktionen beinhalten, die ohne Wissen und Zutun des Anwenders ausgeführt werden.[118] Das Ziel besteht darin, heimlich Aktionen auf dem System auszuführen, so dass diese vom Anwender nicht bemerkt werden. Trojaner verbreiten sich ähnlich wie Viren meist mit Hilfe des Anwenders, der im Glauben eine sinnvolle Anwendung zu installieren gleichzeitig den Trojaner installiert.[119]

68 Die Unterscheidung zwischen Viren, Würmern, Trojanern und anderer Malware wie bspw. Spyware (siehe dazu mehr Rn. 72) oder Backdoors (ermöglicht Dritten unbefugten Zugang zum System) fällt häufig schwer, da sich die verwendeten Konzepte häufig überschneiden. So kann ein Wurm die Schadfunktion eines Virus besitzen und sich zusätzlich als Trojaner tarnen, um sich zu verbreiten. In der Literatur wird häufig vertreten, dass Viren Spezialfälle von Trojanern seien.[120]

69 Oftmals funktionieren Trojaner auch nach dem Client-Server-Prinzip. Der eigentliche Trojaner ist dabei nur der Server. Er nistet sich als nützliche Anwendung getarnt auf dem Zielrechner ein und sorgt für seinen eigenen automatischen Start mit dem Betriebssystem. Der potentielle Angreifer kann nun mittels des passenden Clients aktiv bei seinem Opfer Schaden anrichten und Informationen ausspionieren.

70 **Mögliche Gegenmaßnahmen:** Zusätzlich zu den bereits oben genannten Schutzmöglichkeiten durch Virenscanner und Firewalls, ist der generelle Hinweis zum Verzicht auf Programme aus unbekannten oder unsicheren Quellen für einen Schutz gegen Trojanern sinnvoll. Benutzer von PCs eines Unternehmensnetzwerks sollte es durch entsprechende Beschränkung der Rechte in einem System grundsätzlich nicht möglich

[118] BSI-Lagebericht 2005, abrufbar unter: http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf, S. 19 (zuletzt abgerufen am 09.10.2006); RFC 1244 Site Security Hand Book, abrufbar unter: http://www.faqs.org/rfcs/rfc1244.html, 3.9.8.1.2 (zuletzt abgerufen am 09.10.2006); *Bölscher/Kaiser/Schulenburg*, VW 2002, 565; *Lang*, JurPC 205/2001, Rn. 44.

[119] *Slade*, in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S. 260, 360.

[120] *Bidgoli* (2006), Handbook of Information Security – Volume 3, S. 97.

sein, selbst Software zu installieren oder Software auszuführen, die nicht explizit freigegeben ist.[121]

71 **Einschätzung des Gefährdungspotentials:** Insgesamt geht von Trojanern eine erhebliche Gefahr für die IT-Sicherheit, da der durch sie entstehende Schaden nicht unbedingt zeitnah ersichtlich sein muss.

(4) Spyware

72 Unter Spyware versteht man Programme, die keinen direkten Schaden am System des Nutzers verursachen, es dafür aber ausspionieren.[122] Wie bei der Attacke mit einem trojanischen Pferd soll auch dieser Angriff für den betroffenen Benutzer unsichtbar ablaufen, um vor der Entdeckung möglichst viele Daten über die Tätigkeiten des Benutzers zu sammeln. Spyware wird häufig zusammen mit kostenfreien Programmen installiert,[123] doch auch bereits das Besuchen einer Website, die den (u.U. automatischen) Download von bestimmter Software benötigt, um richtig angezeigt zu werden, kann zur Infizierung genügen.[124] Die gesammelten Daten werden dann an einen Dritten (meist den Anbieter des Programms) weitergeleitet – dieser kann die gesammelten Daten dann verkaufen oder mit anderen Datenbanken verschmelzen.

73 **Mögliche Gegenmaßnahmen**: Neben den bereits erwähnten Firewalls und Intrusion-Detection-Systemen (IDS), empfiehlt sich der Einsatz eines Anti-Spyware Scanners, sowie der Einsatz von Pop-Up-Blockern.[125] Zudem sollte der Nutzer das sog. „Safe and Sane Browsing“[126] verfolgen, in dem er bei der Installation von kostenfreien Programmen vorsichtig agiert.

74 **Einschätzung des Gefährdungspotenzials:** Während der Schaden, der durch eine akute Virusinfektion oder eine massive Wurmattacke ausgelöst wurde, offensichtlich ist, kann eine durch einen Trojaner eingeschleuste oder auf anderem Wege installierte

[121] *Eckert*, IT-Sicherheit, S. 62.
[122] *Tom S. Chan*, in: *Bigdoli*, Handbook of Information Security – Volume 3, S. 136.
[123] *Tom S. Chan*, in: *Bigdoli*, Handbook of Information Security – Volume 3, S. 137.
[124] *Tom S. Chan*, in: *Bigdoli*, Handbook of Information Security – Volume 3, S. 137.
[125] *Tom S. Chan*, in: *Bigdoli*, Handbook of Information Security – Volume 3, S. 141 f.
[126] *Tom S. Chan*, in: *Bigdoli*, Handbook of Information Security – Volume 3, S. 142 f.

Spyware Geschäftsgeheimnisse an Dritte weiterleiten, wodurch ebenfalls ein schwerwiegender Schaden entstehen kann.[127]

(5) Unsichere Konfiguration

75 Viele der oben erklärten Angriffsmöglichkeiten werden erst durch **unsichere Konfiguration** von Computersystemen ermöglicht. Dies betrifft hauptsächlich private IT-Anwender, die weder das Wissen noch die finanziellen Möglichkeiten haben, um ihre Systeme sicher einzurichten und durch Wartung auch langfristig sicher zu betreiben. Unternehmen besitzen eigene IT-Abteilungen oder nehmen Dienstleister in Anspruch, um eine sichere Konfiguration ihrer Netze und Systeme zu erreichen.

76 Der erste Schritt zu einem sicheren System ist der Einsatz aktueller Software, um bekanntgewordene und durch den Hersteller beseitigte **Sicherheitslücken** zeitnah zu schließen. Dies betrifft neben dem Betriebssystem insbesondere Schutzsoftware wie Virenscanner und Firewalls und alle durch Dritte nutzbaren Serverdienste. Ebenfalls muss die Aktualität der Anwendungssoftware (Textverarbeitung, Mediaplayer, etc.) sichergestellt sein, um indirekte Angriffe zu verhindern. Besonders Würmer nutzten in den vergangenen Jahren Sicherheitslücken, die nicht ausreichend schnell geschlossen wurden, um sich rasant zu verbreiten. Daher ist es absolut notwendig die besonders kritischen Softwarekomponenten (Betriebssystem, Schutzsoftware und Serverdienstsoftware) stets aktuell zu halten, was durchaus bedeuten kann, mehrmals täglich Aktualisierungen einzuspielen. Neben der Aktualisierung der eigentlichen Software, müssen auch die Datenbanken von Virenscannern und anderer Schutzsoftware aktuell gehalten werden, damit diese neue Malware und Angriffsmuster erkennen und die Anwender davor schützen können.

77 Der zweite Schritt zu einem sicheren System besteht in dem Anpassen der **Sicherheitseinstellungen des Computers**. Grundsätzlich kann der Rat gegeben werden, den Benutzern eines Systems immer nur die Rechte einzuräumen, die sie benötigen, um ihre Aufgaben zu erfüllen. Keinesfalls sollten Anwender mit unbeschränkten Rechten (Administrator-Rechte unter Windows) arbeiten, um zu verhindern, dass ggf. vorhandene Malware ebenfalls unbeschränkte Rechte erhält.

(6) Webbasierte Dienste

[127] Nach Schätzungen sind rund 15% aller Notebooks und 20% aller Desktop-Systeme mit Spyware infiziert, PC PitStop Statistics, 2004.

78 Durch die Verbreitung des Internets werden häufig Anwendungen als **webbasierte Dienste** angeboten; d.h. die Anzeige/Repräsentation von Anwendungen erfolgt mit Hilfe eines lokal installierten Webbrowsers, während die Logik und Datenhaltung auf zentralen Webservern geschieht.[128] Für die Repräsentation wird in der Regel die Auszeichnungssprache HTML verwendet, die vom Browser interpretiert und als Internetseite dargestellt wird. Da es sich bei HTML um keine Programmiersprache handelt, sind die Möglichkeiten der Interaktion deutlich eingeschränkt und jede Veränderung der lokalen Repräsentation (bspw. Eingabe eines Suchbegriffs) ist mit einem Anfrage-Antwort-Zyklus an den zentralen Server verbunden. Um diese Einschränkung zu umgehen, wurden die so genannten **Aktiven Inhalte** (JavaScript,[129] Microsoft Active X, Plug-Ins wie Flash oder Java[130]) entwickelt, die Erweiterungen des Browsers darstellen und es erlauben dynamisch auf Benutzeraktionen zu reagieren. Aktive Inhalte, vor allem Active X und Java Applets werden als sog. „mobile code"[131] bezeichnet, da sie auf dem Computer des Nutzers ausgeführt werden, also vor dem Ausführen vom Server zum Client übertragen werden.[132] Durch teilweise fehlerhafte Implementierungen dieser Erweiterungen in nahezu allen am Markt relevanten Browsern und der Ausnutzung dieser Schwachstellen durch Malware, sind Aktive Inhalte in den letzten Jahren zu einem ernsthaften Sicherheitsproblem geworden.[133]

79 **Mögliche Gegenmaßnahmen**: Neben der Grundvoraussetzung der Aktualität des benutzten Browsers, ist das grundsätzliche Deaktivieren der Unterstützung für Aktive Inhalt anzuraten.[134] Da viele webbasierte Anwendungen die Unterstützung von Aktiven Inhalten voraussetzen, sollten Browser eingesetzt werden, die es ermöglichen einzelnen, vertrauenswürdigen Seiten die Benutzung von Aktiven Inhalten ausdrücklich zu erlauben. Zur Verhinderung eines Angriffes durch webbasierte Anwendungen ist zusätzlich der Einsatz einer sog. „Personal Firewall" zu empfehlen, die zusätzlich zu der das gesamte Netzwerk schützenden Firewall in der Peripherie des Netzes auf dem jeweiligen

[128] *Eckert*, IT-Sicherheit, S. 69 ff.; *Tanenbaum*, Computer Networks, S. 816.

[129] *Seila/Miller*, in: Bidgoli, Encyclopedia of Informationsystems Volume 2, 2002, S. 693.

[130] Garfol,o in: Bidgoli, Encyclopedia of Informationsystems Volume 2, 2002, S. 715.

[131] *Opyrchal*, in : van Tilborg, Encyclopedia of Crypthography and Security, S. 657.

[132] *Song Fu und Cheng-Zhong Hu*, in: *Bidgoli*, Handbook of Information Security, Volume 3,S. 146; *Charles Border* in: *Bidgoli*, Handbook of Information Security, Volume 3,S. 345.

[133] Dazu BSI abrufbar unter: http://www.bsi-fuer-buerger.de/browser/02_03.htm.

[134] Beispiel Netscape-Browser: *Charles Border*, in: *Bidgoli*, Handbook of Information Security, Volume 3,S. 346.

Computer des Nutzers arbeitet.[135] Wie üblich ist außerdem der Einsatz eines Virenscanners von Vorteil.

80 **Einschätzung des Gefährdungspotentials**: Durch Fehler in der Implementierung von Aktiven Inhalten sind besonders Anwender gefährdet, die häufig verschiedenste Internetseiten besuchen oder webbasierte Anwendungen nutzen, deren Vertrauenswürdigkeit sie nicht kennen. Anwender, die firmeneigene Intranet-Applikationen und vertrauenswürdige Seiten mit Hilfe eines Webbrowsers besuchen, sind entsprechend weniger gefährdet. Allerdings sollte die Gefahr, die von solchen webbasierten Angriffen aufgrund des Einsatzes von unsicheren Browsern ausgeht, keinesfalls unterschätzt werden.

b) Koordination der angegriffenen Systeme (Bot-Netze)

81 Angegriffene Systeme können auch für koordinierte Angriffe verwendet werden. Hierfür hat sich der Begriff der Bot-Netze etabliert. Unter **Bot-Netzen** (Abkürzung von Roboter-Netzwerk) werden fernsteuerbare Netzwerke von PCs verstanden, welche aus untereinander kommunizierenden Bots bestehen.[136] Bei Bots handelt es sich um Software, die im Hintergrund auf den betroffenen PCs und meist ohne Kenntnis des Anwenders ausgeführt wird.[137] Bots werden häufig in Folge eines Wurm- oder Trojanerangriffs eingerichtet und sind darauf vorbereitet ist, Befehle von einer zentralen Instanz zu empfangen. So werden Bot-Netze für den Versand von Spam-Mails oder koordinierte Angriffe gegen Dritte benutzt. Technisch sind Bot-Netze meist so organisiert, dass sich jeder Bot bei einem zentralen Server melden, von dem aus der Angriff koordiniert wird, indem der Angreifer allen Bots den gleichen Befehl sendet. Dies potenziert die Wirksamkeit eines Angriffs (bspw. DoS-Angriff, siehe unten), da Bot-Netze mit mehreren tausend Bots eine enorme Bandbreitensumme besitzen können, die in der Regel die Bandbreite des Angegriffenen übersteigt. Die Struktur von Bot-Netzen ermöglicht durch gezieltes Ausschalten des zentralen Servers, die Koordination des Netzwerk und damit auch die Nutzbarkeit zu verhindern. Daher benutzen aktuelle Bot-Netze aus dem

---

[135] *Charles Border*, in: *Bidgoli*, Handbook of Information Security, Volume 3,S. 347; *Tanenbaum*, Computer Networks, S. 816; *Opyrchal*, in: van Tilborg, Encyclopedia of Crypthography and Security, S. 657.

[136] Dazu BSI-Lagebericht 2005 abrufbar unter: http ://www.bsi.de/literat/lagebericht/lagebericht2005.pdf, S. 21 (zuletzt abgerufen am 09.10.2006); *Tanenbaum*, Computer Networks, S. 818, 819, *Opyrchal*, in: van Tilborg, Encyclopedia of Crypthography and Security, S. 661.

[137] *Cronin*, in: van Tilborg, Encyclopedia of Crypthography and Security, S. 144, Tanenbaum; Computer Networks, S. 778.

Bereich der P2P-Anwendungen bekannte verschlüsselte, dezentrale Kommunikationsstrukturen.[138]

82 Mögliche Gegenmaßnahmen: Für den Anwender eines von einem Bot befallenen PCs gleicht dies den Maßnahmen, die bereits für Computerviren und -würmer erläutert wurden.[139]

83 Einschätzung des Gefährdungspotentials: Die Gefährdung für einen von einem Bot befallenen PC bzw. dessen Anwender bestehen hauptsächlich durch die von dem Bot verbrauchten Ressourcen. Bots enthalten meist keine Schad- oder Weiterverbreitungsfunktionen, damit sie dem Anwender nicht auffallen. Eine große Gefährdung stellen Bot-Netze hingegen für die Opfer eines koordinierten Bot-Netz-Angriffs dar.

2. Koordinierte Angriffe

84 Im ersten Schritt wurden Gefahrenpotentiale beschrieben, die geeignet sind, Einzelsysteme anzugreifen und unter die Kontrolle des Angreifers zu bringen. Im zweiten Schritt werden Gefahren beschrieben, die im Rahmen von koordinierten Angriffen von kompromittierten Systemen ausgehen, um Systeme Dritter zu schädigen.

a) Ausnutzung von Software-Schwachstellen (exploits)

(1) Sicherheitslücken

85 Durch nicht geschlossene **Sicherheitslücken in Software**, die Internetdienste erbringt und daher über das Internet erreichbar ist, sind Angreifer in der Lage, das System zu kompromittieren. Ein solcher Fehler kann bspw. bewirken, dass der Dienst ausfällt oder der Schadcode auf dem System ausgeführt werden kann. Derartige Lücken werden häufig von Würmern ausgenutzt, um sich im System einzunisten. Erwähnt sei an dieser Stelle der Wurm „Sasser“, welcher im Mai 2004 einen Systemdienst in Microsoftbetriebssystemen ab Windows NT dazu missbrauchte, den Rechner zufällig auszuschalten. Die wirtschaftlichen Schäden waren enorm.[140] Diese Art von Angriffen, ließen sich auch direkt – d.h. ohne Bot-Netze – ausführen, jedoch verhindert dieser „Umweg“ die Rückverfolgungen des Angreifers. Die Ausnutzung der Lücke ist folglich der erste Schritt zum Ausführen koordinierter Angriffe.

---

[138] Dazu auch abrufbar unter: http ://www.heise.de/newsticker/meldung/print/72557 (zuletzt abgerufen am 09.10.2006).

[139] Zu den Gegenmaßnahmen s.u. Rn. 88.

[140] Siehe dazu heise-Newsmeldung vom 6.7.2005, abrufbar unter: http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/61451&words=Sasser.

(2) Input-Validierung

86 Ähnliche Folgen wie nicht geschlossene Sicherheitslücken kann **mangelhafte Eingabeüberprüfung** (Input-Validierung) der durch den Anwender eingegebenen Daten bei webbasierten Diensten haben.[141] Dadurch kann z.B. eigener Code eingeschleust werden, der anschließend direkt eine Schadfunktion ermöglicht, oder ein entsprechendes Programm nachlädt und installiert. Auf diese Art und Weise kann der Angreifer weit reichende Kontrolle über das System erlangen.[142] Die fehlende Input-Validierung ist somit ein Spezialfall der Sicherheitslücken.[143]

b) Gezielte Überlastung von Diensten (Denial-of-Service-Angriffe)

87 Ein typisches Einsatzgebiet für Bot-Netze sind so genannte **Denial-of-Service**-Angriffe (DoS-Angriffe)[144], deren Ziel darin besteht eine gezielte Überlastung von Diensten zu erreichen, so dass diese Dienste nicht mehr nutzbar sind.[145] Bei DoS-Angriffen wird das angegriffene System massenhaft mit Anfragen belastet, bis die Ressourcen des Systems ausgeschöpft sind und es nicht mehr auf reguläre Anfragen antworten kann.[146] Wird ein solcher DoS-Angriff von mehreren Bots eines Bot-Netzes ausgeführt, so spricht man von einem Distributed-Denial-of-Service-Angriff (DDoS), da es sich um eine Vielzahl von Angreifern handelt, die allerdings koordiniert handeln.[147] Eine weitere Variante, die ebenfalls mit Hilfe von Bot-Netzen durchgeführt werden kann, sind so genannte Distributed-Reflected-Denial-of-Service-Angriffe (DRDoS). Hierbei sendet der Angreifer seine Datenpakete nicht direkt an das Opfer, sondern an reguläre Internetdienste Unbeteiligter, trägt jedoch als Absenderadresse die des Opfers ein.[148] Die Antworten auf diese Anfragen stellen für das Opfer den eigentlichen DoS-Angriff dar. Für das Opfer erscheint es, als würde des Angriff von diesen Internetdiensten ausgehen - der Ursprung

---

[141] Zum Pufferüberlauf, der sowohl bei lokal ausgeführter Software, aber gerade auch für ans Netz angebundene Server gefährlich ist *Peikari/Chuvakin*, Kenne Deinen Feind, S. 171 ff.

[142] *Sviatoslav Braynow*, in: *Bigdoli*, Handbook of Information Security, Volume 3, S. 58.

[143] Siehe dazu auch: *Rhodenizeri*, in: Bidgoli, Encyclopedia of Informationsystems Volume 4, 2002, S. 49 ff.

[144] *Kabay*, in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S. 356.

[145] BSI-Lagebericht 2005, abrufbar unter: http ://www.bsi.de/literat/lagebericht/lagebericht2005.pdf, S. 19 (zuletzt abgerufen am 09.10.2006); *Anonymous*, der neue hacker's guide, 375 ff.; *Cronin*, in: van Tilborg, Encyclopedia of Crypthography and Security, S. 143.

[146] *Bölscher/Kaiser/Schulenburg*, VW 2002, 565; *Kurose/Ross*, Computer Networking, S. 648.

[147] *Anonymous*, der neue hacker's guide, 393 f.; *Kurose/Ross*, Computer Networking, S. 649; *Todd*, Distributed Denial of Service Attacks, abrufbar unter: http://www.linuxsecurity.com/resource_files/intrusion_detection/ddos-faq.html (zuletzt abgerufen am 09.10.2006).

[148] *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service, abrufbar unter: http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html (zuletzt abgerufen am 09.10.2006).

des Angriffs ist durch diese Vorgehensweise praktisch nicht mehr ermittelbar.[149] DoS-Situationen können auch auf anderen Wegen, als durch eine gezielte Attacke auf das betroffene System, entstehen: So können Fehler in der Software zu einer Überlastung des Systems führen.[150] Weiterhin können Sicherheitslücken von Viren ausgenutzt werden, um eine solche Situation herbeizuführen (so geschehen mit dem MSBlaster-Wurm)[151].

88 **Mögliche Gegenmaßnahmen**: Da die Absender der böswilligen Anfragen aufgrund der Struktur von Bot-Netzen über das gesamte Internet verteilt sind, können die böswilligen Anfragen nicht anhand ihrer Absenderadressen von regulären Anfragen durch eine Firewall unterschieden und gesperrt werden. Eine Möglichkeit besteht darin, die Anzahl der Anfragen pro Zeiteinheit und pro Absender zu begrenzen, was zwar den DoS-Angriff lindern würde, doch ggf. auch reguläre Anfragen behindern könnte.[152] Im Fall eines DRDoS-Angriffs gilt im Wesentlichen das Gleiche. Zusätzlich sollten Provider an den Übergangspunkten zum Internet (Router) nur solche Datenpakete passieren lassen, deren Absenderadresse aus ihrem eigenen Adressraum stammt, damit keine Pakete mit offensichtlich gefälschten Absenderadressen in das öffentlich Internet gelangen können.[153] Weiterhin empfiehlt sich auch gegen DoS-Angriffe eine Firewall.[154] Im Falle eines DDoS- oder DRDoS-Angriffs sind die Möglichkeiten einer Firewall jedoch begrenzt.[155] Für den Fall, dass ein DoS-Angriff bereits erfolgreich stattgefunden hat, bestehen ebenfalls Möglichkeiten, diesen zu beseitigen: So kann der Betreiber des betroffenen Systems z.B. in bestimmten Fällen durch sog. „Failover Systems and Devices“ den Betrieb unmittelbar wieder sicherstellen.[156]

---

[149] Dazu abrufbar unter: http://de.wikipedia.org/wiki/Denial_of_Service (zuletzt abgerufen am 09.10.2006); zwar werden in der theoretischen Informatik Methoden zur Rückverfolgen (Traceback) auch bei gefälschten Adressen behandelt, ihnen ist jedoch gemein, dass sie entweder eine Erweiterung des Internet Protocol (IP) oder der Routerprogrammierung benötigen oder einen erheblichen Aufwand erfordern, den die angegriffene Maschine in der Regel nicht wird leisten können. Gegen DDoS-Angriffe wächst der Aufwand natürlich mit der Anzahl der angreifenden Systeme, bei DRDoS-Angriffen kann nur der vermeintliche Angreifer emittelt werden; s. bspw. *Stone*, CenterTrack: An IP Overlay Network for Tracking DoS Floods, abrufbar unter: http://www.arbornetworks.com/downloads/research51/stone00centertrack_new.pdf (zuletzt abgerufen am 09.10.2006).

[150] *E. Eugene Schulz*, in: *Bigdoli*, Handbook of Information Security, Volume 3, S. 206.

[151] *E. Eugene Schulz*, in: *Bigdoli*, Handbook of Information Security, Volume 3: Threats, Vulnerabilities, Prevention, Detection, and Management, S. 207 (2006).

[152] Weitere mögliche Reaktionen auf einen Angriff in: Results of the Distributed-Systems Intruder Tools Workshop, abrufbar unter: http://www.cert.org/reports/dsit_workshop-final.html, S. 14 f. (zuletzt abgerufen am 09.10.2006).

[153] *E. Eugene Schulz*, in: *Bigdoli*, Handbook of Information Security, Volume 3, S. 215.

[154] *E. Eugene Schulz*, in: *Bigdoli*, Handbook of Information Security, Volume 3,S. 215; *Tanenbaum*, Computer Networks, S. 778.

[155] *Tanenbaum*, Computer Networks, S. 778, 779.

[156] *E. Eugene Schulz*, in: *Bigdoli*, Handbook of Information Security, Volume 3,S. 215, weitere präventive und reaktive Maßnahmen finden sich auf den S. 214 ff.

89 **Einschätzung des Gefährdungspotentials**: Die Gefahr, Opfer eines massiven DoS-Angriffs zu werden, ist trotz aller möglichen Gegenmaßnahmen relativ hoch. Besonders Unternehmen, die Dienstleistungen über das Internet anbieten, können durch einen erfolgreichen DoS-Angriff und dem damit verbundenen Ausfall der betroffenen Dienste nicht nur einen enormen wirtschaftlichen Schaden, sondern auch einen Image-Schaden erleiden. An dieser Stelle seien vor allem eBay, Yahoo und CNN als Opfer von DoS-Angriffen erwähnt.[157] Der Internet Service Provider (ISP) CloudNine.com musste in Folge eines DoS-Angriffes sogar den Betrieb einstellen.[158]

3. Ergebnis

90 Wie sich zeigt, gibt es eine Vielzahl von möglichen Angriffsszenarien. Nicht gegen alle kann sich der Nutzer effektiv wehren. Die gefährlichsten sind jedoch durchaus mit den entsprechenden Maßnahmen abwendbar.

IV. Abgrenzung der Verantwortlichkeitssphären: Hersteller – Nutzer – Intermediäre (Dienstleister)

91 Mit dem erforderlichen Maß des Eigenschutzes im Bereich der Verkehrssicherungspflichten ist bereits eine Hauptaufgabe der Rechtsordnung im Bereich der Gewährleistung von Sicherheit – ob im IT-Sektor oder in anderen Bereichen – angesprochen: Die Verteilung der sicherheitsnotwendigen Anforderungen auf bestimmte Risikosphären. Potentielle Normadressaten sind dabei drei Gruppen von Personen, die mit Informationstechnik in Berührung kommen: Die Hersteller von IT-Produkten, die Nutzer dieser Produkte sowie die Gruppe der IT-Intermediäre[159], die eine Zwischenstellung einnehmen, da sie sowohl selbst Nutzer von IT-Produkten sind als auch Dritten die Nutzung von Informationstechnik als Host-, Content- bzw. Access-Provider ermöglichen.

92 Die Auswahl einer dieser Gruppen als Adressat von Sicherheitspflichten hat prinzipiell nach deren Verantwortungsbereichen zu erfolgen, die sich wiederum in Anwendung des aus der Ökonomischen Analyse des Rechts entstammenden Kriteriums des„**cheapest**

[157] *Kurose/Ross*, Computer Networking, S. 649.

[158] *E. Eugene Schulz*, in: *Bigdoli*, Handbook of Information Security, Volume 3, S. 207.

[159] Eingehend zum Begriff des Intermediärs für elektronische Märkte: *Sarkar/Butler/Steinfield,* Intermediaries and Cybermediaries: A continuing role for mediating players in Electronic Markets, in: Journal of Computer Mediated Communication (JCMC), Vol. 1, Nr. 3, 1995, abrufbar unter: http://jcmc.indiana.edu/vol1/issue3/sarkar.html (zuletzt abgerufen am 09.10.2006).

cost avoider“[160] danach bestimmen läßt, wer über die besten Gefahrabwendungsmöglichkeiten sowie Kenntnisse über mögliche Gefahren verfügt[161].

93 Demgemäß kann vergröbert von einer **Skala** gesprochen werden, an deren einem Ende die IT-Hersteller als diejenigen stehen, die am intensivsten Schutzpflichten unterliegen, am anderen Ende die IT-Anwender, die je nach Professionalität am wenigsten in der Lage sind, IT-Risiken zu beherrschen. Allerdings ist auch hier danach zu differenzieren, ob es sich um professionelle IT-Anwender handelt, insbesondere Unternehmen, die über entsprechende Ressourcen zum Selbstschutz verfügen könnten. In der Mitte der Skala sind diejenigen Unternehmen platziert, die selbst IT-Produkte professionell einsetzen, ihrerseits aber wiederum IT-Dienstleistungen erbringen (IT-Intermediäre), insbesondere die Gruppe der Access- und Host-Provider. Sie sind zwar primär Dienstleister, doch ändert dies nichts daran, dass sie im Grundsatz ähnlichen Pflichten wie die IT-Hersteller für ihre Produkte unterliegen.

C. Verantwortlichkeit der IT-Hersteller (Produktbezogene Pflichten)

I. Überblick

94 Die Hersteller von IT-Produkten – sei es Hard- oder sei es Software – stehen am Anfang der IT-Wertschöpfungskette. Folgerichtig gelten für Hersteller von IT-Produkten im Grundsatz dieselben Anforderungen wie für andere Hersteller auch, in erster Linie die Grundsätze der **deliktischen Produzentenhaftung** (Rn. 104 ff.) und des verschuldensunabhängigen **ProdHaftG** (Rn. 189 ff.) Neben diese Ansprüche können im Einzelfall **vertragliche Ansprüche** gegen den Hersteller treten (Rn. 98).

95 Überlagert werden die zivilrechtlichen Anforderungen durch **öffentlich-rechtliche Regulierungen im Bereich der Produktsicherheit**, insbesondere des Geräte- und Produktsicherheitsgesetzes (GPSG) als grundlegendes Gesetz. Hauptinstrument der Gewährleistung von Sicherheit sind hier in materiell-rechtlicher Hinsicht bestimmte Grundpflichten der Hersteller, in verfahrensrechtlicher Hinsicht Zertifikate für sichere

[160] Diese von der Lehre der ökonomischen Analyse des Rechts entwickelte Argumentationsfigur weist die Sicherheitspflichten demjenigen zu, der den eingetretenen Schaden mit dem geringsten Aufwand zu vermeiden vermag (s. dazu ausführlicher: *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, S. 227 f.; *Calabresi*, The Cost of Accidents, S. 136 ff.; von “least-cost-avoiding” sprechend *Shavell*, Foundations of Economic Analalysis of Law, Kap. 8. Rn. 2.11). Im in Deutschland vorherrschenden System der Wertungsjurisprudenz können ökonomische Rationalitätsgesichtspunkte jedoch nur neben andere – in erster Linie rechtsethische – Gesichtspunkte treten. Als alleiniger Begründungsansatz für rechtliche Lösungen können sie indes nicht ausreichen. Einen kurzen Überblick über die Problematik bietet Palandt-*Heinrichs*, Einleitung Rn. 34 ff., 39.

[161] Zur Verteilung von Sorgfaltsmaßnahmen allgemein s. auch MünchKommBGB-*Wagner*, Vor § 823 BGB Rn. 44.

Produkte, gegebenenfalls auch die Genehmigungsbedürftigkeit von Produkten. Typisch für das deutsche und europäische Produktsicherheitsrecht ist dabei der Rückgriff auf bestimmte, in einem den Vorschriften des Gesetzes entsprechenden Verfahren erlassene technische Normen, an die sich unter Umständen sogar Vermutungswirkungen knüpfen können.

96 Öffentlich-rechtliches Produktsicherheitsrecht und zivilrechtliche Produkthaftung sind dabei in doppelter Hinsicht **miteinander verzahnt**: Zum einen können die öffentlich-rechtlichen Produktsicherheitsvorschriften als Schutzgesetze gem. § 823 Abs. 2 BGB qualifiziert werden, so dass sie deliktsrechtlich flankiert werden;[162] zum anderen können aber auch öffentlich-rechtliche Normen und erteilte Zertifizierungen unter Umständen eine Einschränkung der deliktischen Haftung herbeiführen, sei es materiell-rechtlich, sei es verfahrensrechtlich über bestimmte prozessuale Wirkungen. Umgekehrt können deliktische Produkthaftungspflichten die Bestimmung öffentlich-rechtlicher Pflichten beeinflussen.

97 Beide Bereiche sind daher von **zentraler Bedeutung** für die Pflichten und die Risiken von IT-Herstellern; beide Bereiche können in **rechtspolitischer Hinsicht** gestaltend die Verteilung der Risiken aus IT-Produkten beeinflussen.

II. Vertragliche Mängelhaftung

98 Je nach gewähltem Vertriebsweg kommen bei fehlerhaften IT-Produkten auch vertragliche Ansprüche gegen den Hersteller in Betracht. **Hardwareprodukte** werden auch im Internet regelmäßig nicht vom Hersteller selbst, sondern von selbständigen Vertriebsgesellschaften angeboten, so dass idR kein Vertrag mit dem Hersteller zustande kommt.

99 Insbesondere im **Unternehmensbereich** (B2B-Geschäft) bei Software steht die vertragliche Haftung des IT-Herstellers klar im Vordergrund,[163] da hier häufig direkte Verträge mit den Softwareherstellern geschlossen werden. Oftmals handelt es sich auch um dauerhafte oder zumindest langfristige Vertragsverhältnisse, die eine Mischung aus Softwareherstellung und Softwarepflege umfassen,[164] wobei die Pflege häufig als Zusatzleistung angeboten wird - so etwa bei den sog. Volumenlizenzverträgen der Fa. Microsoft – sei es als entgeltlicher Pflegevertrag oder unentgeltliche Zusatzleistung in Form

[162] Ähnlich auch das englische Recht, s. *Reed* – Annex II – Rn. 1249 ff.

[163] *Spindler*, in: FS Nagel, S. 22.

[164] S. dazu *Spindler*, in: FS Nagel, S. 22; *Marly*, Rn. 508; *Peter*, in: Schneider/von Westphalen, Software-Erstellungsverträge, G Rn. 7 ff.; *Baum*, CR 2002, 705 ff.; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 505.

von frei verfügbaren Patches im Internet.[165] Je nach Art des Softwarevertriebs werden z.B. bei Online-Beschaffung von Software AGB genutzt,[166] die wiederum – je nach Markt- bzw. Verhandlungsmacht – Haftungs- und Gewährleistungsausschlussklauseln enthalten. Grundsätzlich gilt selbstverständlich die Privatautonomie. Soweit es sich dabei um individuelle Vereinbarungen und keine AGB handelt, muss sich die Wirksamkeit dieser Vereinbarungen daher lediglich an den Grenzen der Sittenwidrigkeit nach § 138 BGB und des gesetzlichen Verbots (§ 134 BGB) messen lassen.[167] Handelt es sich aber um Haftungs- und Gewährleistungsausschlüsse in allgemeinen Geschäftsbedingungen, bildet die Inhaltskontrolle nach den § 307 BGB die Grenze der Privatautonomie,[168] selbst bei B2B-Geschäften (im Gegensatz zu anderen Rechtsordnungen)[169] und sorgt dadurch dafür, daß auch in vertraglichen Beziehungen ein Mindestmaß an Sicherheit nicht abbedungen werden kann.[170]

100 In diesem Zusammenhang stellt sich die Frage, ob durch die Schuldrechtsreform auch die Haftungsfreizeichnung für **mangelbezogene Folgeschäden** – die nunmehr direkt über § 280 I BGB erfaßt werden – klauselfest ist, mithin der Vertragspartner (Hersteller) für sämtliche Vermögensfolgeschäden, die seine schadhafte Software angerichtet hat, einstehen muss oder ob er eine solche Einstandspflicht abbedingen kann. Grundsätzlich ist eine Freizeichnung für die Schadensersatzhaftung auch im Verbrauchsgüterkauf möglich, sofern kein Vorsatz vorlag oder eine Beschaffenheitsgarantie übernommen wurde.[171] Die Haftung für Mangelfolgeschäden hängt davon ab, ob der Vertragspartner den Schaden iSd § 276 BGB zu vertreten hat, d.h. ob er vorsätzlich oder fahrlässig gehandelt hat. Die Zulässigkeit der Freizeichnung unterliegt der Inhaltskontrolle der §§ 307 ff. BGB. Nach dem Wortlaut des § 309 Nr. 7b BGB ist eine Haftungsfreizeichnung für sonstige Schäden bei leicht fahrlässiger Pflichtverletzung zulässig. Ob dies aber auch für eine Freizeichnung bezüglich mangelbezogenen Folgeschäden gilt, ist höchst umstritten,[172] kann hier aber nicht weiter vertieft werden. Pauschale Aussagen

---

[165] *Peter*, in: Schneider/von Westphalen, Software-Erstellungsverträge, G Rn. 7 ff.

[166] *Schneider*, Handbuch des EDV-Rechts, J Rn. 6; *Spindler*, in: FS Nagel, S. 23.

[167] *v. Westphalen*, in: Schneider/v. Westphalen, Software-Erstellungsverträge, H Rn. 6.

[168] Erman-*Roloff*, § 307 BGB Rn. 1.

[169] Deutlich hier etwa das britische Recht, das generell große Zurückhaltung bei der Inhaltskontrolle jedenfalls von B2B-Verträgen übt, s. dazu *Reed* – Annex II – Rn. 1305.

[170] Zur Wirksamkeit derartiger Klauseln generell *v. Westphalen*, in: Schneider/v. Westphalen, Software-Erstellungsverträge, H Rn. 6; bezogen auf Gewährleistungsbeschränkungen und die wegen § 307 BGB nicht erlaubte Verkürzung der Verjährungsfrist bei Software auf ein Jahr *Bartsch*, CR 2005, 9; *Schneider*, Handbuch des EDV-Rechts, J Rn. 244.

[171] Palandt-*Weidenkaff*, § 475 BGB Rn. 14; Erman-*Grunewald*, § 475 BGB Rn. 10; *Schulze/Ebers*, JuS 2004, 466.

[172] S. zum Meinungsstand *Schulze/Ebers*, JuS 2004, 466 mwN.

verbieten sich hier, letzlich wird auf die Frage der Vorhersehbarkeit[173] eines konkreten Schadens abgestellt werden müssen.[174] Klauseln, die die Haftung für Mangelfolgeschäden bei leichter Fahrlässigkeit auf vorhersehbare Schäden beschränken, dürften daher eher nicht zu beanstanden sein,[175] ebensowenig auch Klauseln, die für Folgeschäden versuchen, eine Haftungsobergrenze einzuführen.[176]

101 Unmittelbare vertragliche Beziehungen mit dem IT-Hersteller werden auch beim Bezug von **kommerziell hergestellter Software** über das Internet in der Regel bestehen. Ein praktisch wichtiges Beispiel sind **automatische Updates** für Betriebssysteme und Anti-Virus-Programme, welche oftmals schon im Lieferumfang handelsüblicher Computer enthalten sind und deren Abonnement später auf der Hersteller-Homepage verlängert werden kann. Auch in sonstigen Fällen, in denen der Hersteller Software direkt auf seiner Homepage zum Download bereitstellt, bestehen unmittelbare vertragliche Ansprüche. Inhalt und Umfang der Pflichten des IT-Herstellers richten sich wiederum primär nach den vertraglichen Regelungen einschließlich etwaiger AGB-Klauseln, wiederum unter dem Vorbehalt der Zulässigkeit nach § 307 BGB, in deren Rahmen die deliktischen Wertungen durchaus einfließen können (ausführlich unten Rn. 536 ff.). Darüberhinaus ist gerade bei Internet-Downloads zu beachten, daß jedenfalls im B2B-Geschäft eine Rechtswahl nach Art. 27 EGBGB zulässig ist, auch durch entsprechende AGB-Klauseln[177]. Die Wirksamkeit einer solchen Wahl richtet sich nach Art. 31 I EGBGB iVm Art. 29 IV EGBGB nach demjenigen Recht, das nach der Klausel angewendet werden soll.[178] Damit wird auch die gesamte Inhaltskontrolle und ihr Ergebnis (Wirksamkeit oder Unwirksamkeit der Klausel) dem deutschen Recht entzogen und ist allein Angelegenheit des nach Art. 31 Abs. 1 EGBGB anwendbaren Rechts.[179] Der Gesetzge-

---

[173] Ausführlich zur Vorhersehbarkeit *Spindler*, in: FS Nagel, S. 27.

[174] Ähnlich das britische Recht s. *Reed* – Annex II – Rn. 1251 ff.

[175] So auch *Litzenburger*, NJW 2002, 1245; aA Bamberger/Roth-*Becker*, § 309 Nr. 7 Rn 20 ff. und Nr. 8 Rn. 30, 35, der die Haftung für Mangelfolgeschäden als unabdingbare Kardinalpflicht sieht, ohne die die Verwendergegenseite ihr Interesse an ordnungsgemäßer Vertragserfüllung nicht durchsetzen könne; *Intveen*, ITRB 2003, 13 f.

[176] So auch tendierend *Intveen*, ITRB 2003, 14.

[177] *Schmidt/Prieß*, in: Spindler/Börner, S. 175; Palandt-*Heldrich*, EGBGB Art. 27 Rn. 6.

[178] BGH NJW-RR 2005, 1071, 1072; BGHZ 123, 380, 383; Staudinger-*Hausmann*, BGB, 2002, Art. 31 EGBGB Rn. 72; Palandt-*Heldrich*, Art. 31 EGBG Rn. 1, 3, Art. 27 EGBGB Rn. 8; Bamberger/Roth-*Spickhoff*, Art. 31 EGBGB Rn. 6 ff.; Erman-*Hohloch*, Art. 27 EGBGB Rn. 12, 16, Art. 31 EGBGB Rn. 6, 8; *Tiedemann*, IPRax 1991, 424 (425); *Mankowski*, RIW 2003, 2 (4); ausführlich *Heiss*, RabelsZ 65 (2001), 634 (635 ff.); *Rühl*, Rechtswahlfreiheit und Rechtswahlklausel in Allgemeinen Geschäftsbedingungen, 1999.

[179] MünchKommBGB-*Martiny*, Art. 27 EGBGB Rn. 13 mwN; Palandt-*Heldrich*, Art. 31 EGBGB Rn. 3; *Looschelders*, Internationales Privatrecht, Art. 31 Rn. 9; schon vor der Reform: *Meyer-Sparenberg*, RIW 1989, 347 (350); *Grundmann*, IPrax 1992, 1 (2); abw. nur *Heiss* RabelsZ 65 (2001), 634 (636 ff.), der sich für allgemeine Missbrauchskontrollen ausspricht.

ber der IPR-Reform hat die nach dem früheren § 10 Nr. 8 AGBG aF vorgesehene Inhaltskontrolle von Rechtswahlklauseln bewusst ausgeschlossen, da sie in Widerspruch zu der von Art. 27 geschützten Rechtswahlfreiheit stehe.[180]

102 Sofern Software nicht unmittelbar vom Hersteller bezogen wird, sondern über einen Händler, sind die Anreize für den Hersteller, sichere Software zu produzieren, von vornherein mediatisiert. Nur soweit der Händler ihn in Regress nehmen kann, werden Schäden auf den Hersteller zurückverlagert. Handelt es sich um mangelhafte Standardsoftware, greift zwar zugunsten des Händlers die zwingende Regelung des § 478 BGB ein, so daß er stets Regress nehmen kann. Doch zeigt schon § 478 IV S. 2 BGB, daß der Hersteller den Schadensersatzanspruch bzw. den diesbezüglichen Regress abbedingen kann – so daß gerade die für IT-Schäden relevanten Mangelfolgeschäden nicht mehr vom Regress erfaßt wären. Zudem kann der Händler nur dann vom Käufer auf Schadensersatz belangt werden, wenn er den Fehler und den Mangelfolgeschaden damit zu vertreten hat – dies wird indes in den seltensten Fällen gelingen, da der Händler (nicht der Hersteller!) den Code hätte kennen und zudem der konkrete Schaden hätte vorhersehbar sein müssen; meist wird es daher am Vertretenmüssen des Händlers fehlen. Abgesehen davon ist auch schon strittig, ob Software überhaupt zu den von der Verbrauchsgüterkaufrichtlinie erfaßten Produkten zählt[181] – denn hier schlägt sich wiederum die alte Diskussion um die Sacheigenschaft von Software nieder (s. dazu Rn. 103). Bislang ist diese Frage von der Rechtsprechung nicht entschieden worden; sinnvollerweise sollte indes der Produktbegriff – vergleichbar der Diskussion im ProdHaftG (Rn.209 ff.) – auch im Verbrauchsgüterkauf entsprechend erweitert verstanden werden.[182] Schließlich kann der Regress für den gerade international wichtigen IT-Softwareverkauf durch Rechtswahl nach Art. 27 EGBGB abbedungen werden, da § 478 BGB nicht zu den international zwingenden Normen nach Art. 34 EGBGB zählt.[183]

103 Wie Software rechtlich zu qualifizieren ist, war lange Zeit, und ist es seit der Schulrechtsreform wieder, umstritten. Während vor der Schuldrechtsmodernisierung durch die stetige Rechtsprechung weitestgehend Einigkeit herrschte, dass Software zumindest wenn sie in irgendeiner Weise verkörpert ist, als Sache zu qualifizieren sei und so die

---

[180] Begr. Reg E BT-Drucks. 10/504 S. 95.

[181] Aus der umfangreichen Diskussion dazu: *Mankowski,* MDR 2003, 854 ff.; *Spindler*/*Klöhn,* CR 2003, 81 ff; *Marly*, Softwareüberlassungsverträge, Rn. 55 ff., 63.

[182] *Spindler/Klöhn*, CR 2003, 85; *Mankowski*, MDR 2003, 857.

[183] MünchKommBGB-*Lorenz*, § 478 Rn. 10; *Staudinger*, ZGS 2002, 64.

Vorschriften über den Kauf (der lediglich für Sachen und Rechte gilt) anwendbar seien.[184] Durch die Schuldrechtsreform wurde § 453 BGB eingefügt, wonach die kaufrechtlichen Vorschriften nun auch auf sonstige Gegenstände anwendbar sind. In der Gesetzesbegründung wurde weiter Software als sonstiger Gegenstand genannt,[185] was ein Teil der Literatur zum Anlass nahm, die Diskussion um die Einordung von Software erneut zu aufzunehmen, da eine Qualifikation als Sache insbesondere im Rahmen des neu fomulierten § 651 BGB nach dem Wortlaut die Konsequenz hätte, dass bei Lieferung oder Erzeugung von Software nicht Werkvertragsrecht sondern Kaufrecht anzuwenden wäre. Insgesamt lassen sich zu dieser Problematik aktuell drei Strömungen herauskristallisieren: Ein Teil der Literatur verneint die Sachqualität von Software, so dass § 651 BGB schon vom Wortlaut nicht greife und Werkvertragsrecht unproblematisch bei individuell hergestellter Software Anwendung finde.[186] Andere bejahen weiterhin die Sachqualität von Software. Diese Auffassung untergliedert sich weiter in den Teil, der konsequent § 651 BGB auf individuell hergestellte bzw. angepasste Software anwendet und so zum Kaufrecht gelangt[187] und den Teil, der § 651 BGB mit unterschiedlichen Begründungen (z.B. teleologische Reduktion,[188] keine „sklavische“ Anwendung des Sachbegriffs im Rahmen des § 651 BGB,[189] Schwerpunkt der Leistung[190]) auf Software nicht anwenden will und so zum Werkvertragsrecht gelangt.[191] Aufgrund der jahrelangen stetigen Rechtsprechung wird man aber wohl weiter Software als Sache qualifizieren müssen. Der XII. Zivilsenat hat jüngst ebenfalls Software aufgrund der nötigen Verkörperung eindeutig als Sache bezeichnet.[192] Um dennoch im zu einer interessengerechten Lösung zu gelangen, sollte man darauf verzichten, den Sachbegriff im Rahmen

[184] So die ständige Rechtsprechung: BGH GRUR 1985, 1055 (1056); 1988, 406 (408); NJW 1990, 320 (321); NJW 1993, 2436 (2437); NJW 2000, 1415 ff.; CR 2007, 75 (76); zustimmend in der Literatur: *Marly*, Softwareüberlassungsverträge, Rn. 96 ff. insb. Rn. 110; Palandt-*Heinrichs*, § 90 BGB Rn. 2; MünchKommBGB-*Holch*, § 90 Rn. 27; *Schneider*, Handbuch des EDV-Rechts, D Rn. 96; Erman-*Michalski*, § 90 BGB Rn. 3.

[185] BT-Drucks. 14/6040, S. 242.

[186] *Stichtenoth*, K&R 2003, 106 f.; *Junker*, NJW 2005, 2831; *Heussen*, CR 2004, 7; *Redeker*, CR 2004, 88 f.; *Diedrich*, CR 2002, 475; *Schneider*, in: Schneider/v. Westphalen, Software-Erstellungsverträge, B Rb. 39 ff.

[187] *Schweinoch/Roas*, CR 2004, 330; *Mankowski*, MDR 2003, 857; *Lapp*, in: Gounalakis, § 43 Rn. 6.

[188] *Rücker*, CR 2006, 366 ff.

[189] *Spindler/Klöhn*, CR 2003, 84.

[190] *Schmidl*, MMR 2004, 592 f.

[191] *Marly*, Softwareüberlassungsverträge, Rn. 53 ff. und 119; *Rücker*, CR 2006, 366 ff.; *Spindler/Klöhn*, CR 2003, 84; *Schmidl*, MMR 2004, 592 f.; *Müller-Hengstenberg/Krcmar*, CR 2002, 549 ff.; MünchKommBGB-*Busche*, § 651 BGB Rn. 12.

[192] BGH, K&R 2007, 91 = CR 2007, 75 m.Anm. *Lejeune* = WM 2007, 467 sowie Anm. *Marly/Jobke*, LMK 2007, 209583

des § 651 BGB derart strikt anzuwenden, um bei der Erzeugung von Individualsoftware dennoch zur Anwendbarkeit des Werkvertragsrecht zu gelangen.[193]

III. Außervertragliche Produkthaftung

1. Verschuldensabhängige Produzentenhaftung

104 Weitestgehend unstreitig ist inzwischen, dass die verschuldensabhängige Haftung nach §§ 823 ff. BGB auch auf Software als Produkt Anwendung findet, da anders als im ProdHaftG der Streit um die Sacheigenschaft der Software für die Anwendung der §§ 823 ff. BGB unerheblich ist, da es nur auf das Vorhandensein einer Gefahrenquelle ankommt, gleich welcher Natur das Produkt ist, von dem die Gefahr ausgeht.[194] Vor allem im gewerblichen Bereich spielt die verschuldensabhängige Produkthaftung nach §§ 823 ff. BGB daher eine entscheidende Rolle.

105 Die verschuldensabhängige Produkthaftung kann dabei grob in zwei Bereiche unterteilt werden, zum einen der Rechtsgutsverletzung nach § 823 Abs. 1 BGB, zum anderen der Schutzgesetzverletzung nach § 823 Abs. 2 BGB:

a) Rechtsgüterbezogene Produkthaftung (§ 823 Abs. 1 BGB)

(1) Softwareversagen und Rechtsgüterschutz

106 Maßgeblich für die Anwendung der deliktischen Produzentenhaftung ist zunächst die Verletzung eines der durch § 823 Abs. 1 BGB geschützten Rechtsgüter und Rechte. Bereits auf dieser Ebene ergeben sich bereits eine Reihe von Fragen in Bezug auf IT-Produkte:

(a) Verletzung personenbezogener Rechtsgüter

107 Eine Verletzung der Rechtsgüter **Leben**, **Körper** und **Gesundheit** ist beispielsweise bei einem Brand infolge eines Kurzschlusses in der Hardware denkbar. Durch Softwarefehler werden die Rechtsgüter des § 823 Abs. 1 BGB dagegen nicht unmittelbar beeinträchtigt, allerdings können infolge von Fehlfunktionen oder Ausfällen auch Schäden an

---

193 So auch *Spindler/Klöhn*, CR 2003, 83 f.

194 Grundlegend *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 239 ff.; *Günther*, Produkthaftung für Informationsgüter, S. 253 ff.; *Schneider*, Handbuch des EDV-Rechts, Kap. J Rz. 294 ff.; *Marly*, Softwareüberlassungsverträge, Rn. 1309 ff.; grundsätzlich zur Unabhängigkeit von der Sacheigenschaft: MünchKommBGB-*Wagner*, § 823 BGB Rn. 554; Erman-*Schiemann,* § 823 BGB Rn. 114.

Leben, Körper, Gesundheit oder Freiheit auftreten.[195] Die Relevanz von durch **Softwarefehler** verursachten Personenschäden wird in Zukunft wohl zunehmen, wenn Steuerungsaufgaben mehr und mehr auf den Computer übertragen werden. Dies gilt besonders für den Bereich der softwaregesteuerten Arbeitsmittel und industriellen Fertigung (z. B. Software zur Steuerung chemischer Anlagen, Industrieroboter) Personenschäden können auch dort auftreten, wo die Verkehrssteuerung auf dem Einsatz von Software basiert (z. B. Flugsicherung, Verkehrsleitsysteme) oder Software im medizinischen Bereich eingesetzt wird.[196] Im privaten Bereich steigt die Bedeutung softwaregesteuerter Systeme und damit auch die Gefahr von durch Softwarefehler verursachten Personenschäden beispielsweise durch den Softwareeinsatz im privaten Pkw (z.B. Anti-Blockier-System (ABS), elektronisches Stabilitätsprogramm (ESP), automatische Fahrabstandsregelung, elektronischer Bremskraftverstärker). Als seltenes Beispiel einer Verletzung der persönlichen **Freiheit** wird der Ausfall softwaregesteuerter Fahrstühle oder Türen genannt.[197]

(b) Verletzungen des Eigentums

108 Häufiger als Personenschäden ziehen Softwarefehler Beeinträchtigungen in Form eines Eingriffs in die Sachsubstanz (Hardware), der Verfügbarkeit und Integrität von Daten, sowie von System- und Betriebsausfällen nach sich. Bei fehlender Verletzung der Sachsubstanz entscheidend ist hierbei die Abgrenzung zwischen deliktsrechtlich sanktionierten **Eigentumsverletzungen** und insoweit unbeachtlichen, weil nicht ersatzfähigen primären Vermögensschäden. Gegenüber der Verletzung des Eigentums[198] kommt dem **Recht am eingerichteten und ausgeübten Gewerbebetrieb** nur subsidiäre Bedeutung zu.[199] Regelmäßig wird es zudem am erforderlichen betriebsbezogenen, finalen Eingriff[200] fehlen.[201] Hinsichtlich des Eigentums kann wie folgt differenziert werden:

(i) Substanzverletzungen

---

[195] *Koch*, NJW 2004, 801 (802); *Taeger*, Außervertraglice Haftung für fehlerhafte Computerprogramme, S. 259 f.; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 185, 355, 632; *Hoeren/Pichler,* in: Loewenheim/Koch, Praxis des Online-Rechts, S. 381 (406).

[196] Vgl. *Schneider/Günther*, CR 1997, 389 (392).

[197] *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 260.

[198] BGHZ 138, 311 (315); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 114 mwN.

[199] Dazu ausführlich *Koch*, Versicherbarkeit von IT-Risiken, Rn. 360; *Sodtalbers*, Softwarehaftung im Internet, Rn. 523; *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 262; Staudinger-*Hager*, § 823 BGB Rn. D 67.

[200] BGHZ 29, 65 (74); BGHZ 90, 113 (123); näher dazu: Bamberger/Roth-*Spindler*, § 823 BGB Rn. 108; MünchKommBGB-*Wagner*, § 823 BGB Rn. 185.

[201] *Bartsch,* Software und das Jahr 2000, S. 159; s. dagegen für Virenbefall *Koch,* NJW 2004, 801 (803).

109 Eine Eigentumsverletzung im Sinne einer Substanzverletzung kommt in den Fällen in Betracht, in denen Geräte, Maschinen oder Anlagen mit Hilfe von Software gesteuert werden und die Software somit indirekt **in mechanischer Weise auf die Umwelt einwirkt**.[202] In diesem Zusammenhang stellt sich das Problem des sog. **Weiterfresserschadens**, wenn der Fehler einer in eine Maschine usw. eingebauten Software zu einer Beschädigung oder Zerstörung der Gesamtsache führt.[203] Nach gefestigter Rechtsprechung des BGH sind Schäden an einem ansonsten fehlerfreien Produkt, welche durch ein integriertes fehlerhaftes Teilprodukt verursacht wurden, nach § 823 Abs. 1 BGB wegen Verletzung des Eigentums am fehlerfreien Rest zu ersetzen (zum ProdHaftG s. unten Rn 193 ff.).[204] Nachdem der BGH eine Eigentumsverletzung zunächst bei funktionaler Abgrenzbarkeit des fehlerhaften Teils bejahte, stellt er nunmehr auf die Unterscheidung zwischen dem vertraglich geschützten Äquivalenzinteresse und dem deliktisch geschützten Integritätsinteresse ab. Eine Eigentumsverletzung liegt demnach vor, wenn der Minderwert, welcher der Sache von Anfang an anhaftete, nicht mit dem eingetretenen Schaden „stoffgleich" ist.[205] Dies wird man regelmäßig dann bejahen können, wenn ein Softwarefehler zur Beschädigung oder Zerstörung der Sache (z.B. Maschine, Fahrzeug usw.) führt, in die sie eingebaut ist.[206]

(ii) Verletzung der Datenintegrität und -verfügbarkeit

110 Im Grundsatz erfasst das nach § 823 Abs. 1 BGB geschützte **Eigentum** auch die Integrität von Daten,[207] da schon die **Funktionalität und innere Ordnung** des Eigentums, z.B. einer Sammlung, auch ohne Substanzschädigung geschützt wird.[208] Da jede Festplatte eine innere Ordnung der gespeicherten Daten voraussetzt, führt die Zerstörung dieser Ordnung durch Veränderung oder Löschung von Daten grundsätzlich zu einer Eigentumsverletzung.[209] Ein erheblicher Teil von Daten und Datenbanken fällt somit in

---

[202] *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 260 f..

[203] Ausführlich *Koch*, Versicherbarkeit von IT-Risiken, Rn. 633 ff..

[204] BGHZ 67, 359 (364 f.); BGHZ 86, 256 (258); BGH NJW 1998, 1942 (1943); ausführlich Bamberger/Roth-*Spindler*, § 823 BGB Rn. 60 ff .

[205] BGHZ 86, 256 (258 f.).

[206] *Sodtalbers*, Softwarehaftung im Internet, Rn. 513 ff., 518; *Taeger*, Außervertragliche Softwarehaftung für fehlerhafte Computerprogramme, S. 260 f.; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 69.

[207] OLG Karlsruhe NJW 1996, 200 (201); zust. *Meier/Wehlau*, NJW 1998, 1585 (1587 ff.); Staudinger-*Hager*, § 823 BGB Rn. B 60; *Imhof/Wahl*, WpK-Mitt. 1998, 136 (137); *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 261; aA LG Konstanz NJW 1996, 2662; AG Dachau NJW 2001, 3488.

[208] BGHZ 76, 216 (220f.) = NJW 1980, 1518.

[209] OLG Karlsruhe NJW 1996, 200 (201); *Bartsch,* CR 2000, 721 (723); *Spindler,* NJW 1999, 3737 (3738); *Spindler,* NJW 2004, 3145 (3146); *Meier/Wehlau,* NJW 1998, 1585 (1588); *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn.

den Schutzbereich von § 823 Abs. 1 BGB in den Bereich des Rechts am Eigentum.[210] Zudem werden urheberrechtlich oder andere immaterialgüterrechtlich geschützte Werke, die auch in Gestalt von Daten verkörpert sein können, ebenso wie Software gleichermaßen nach den jeweiligen Spezialregelungen, z.B. § 97 UrhG, geschützt. Darüberhinaus wird auch ein **Recht am (verkörperten) Datenbestand** als sonstiges Recht nach § 823 Abs. 1 BGB angenommen.[211] Dadurch soll der Schutz der Verfügbarkeit der Daten, auch bei ausgelagerten Daten, gewährleistet werden.[212]

111 Ermöglicht demnach eine Softwarelücke einen **Virenbefall** des Computers und werden gespeicherte Daten durch diesen Virus vernichtet, liegt eine Eigentumsverletzung gemäß § 823 Abs. 1 BGB vor. Voraussetzung für eine Eigentumsverletzung ist jedoch stets, dass die Daten auf einem Datenträger im Eigentum des Geschädigten gespeichert waren. Die Veränderung oder Vernichtung von Daten, die auf dem Rechner eines Providers gespeichert waren, genügt dagegen nicht.[213] Keine deliktische Ansprüche kommen wegen des fehlerhaften Programms selbst in Betracht, wenn dieses infolge des Fehlers gelöscht wird, da insoweit nur das vertraglich geschützte Äquivalenzinteresse betroffen ist.[214] Keine Verletzung der Datenintegrität im oben beschriebenen Sinne liegt auch vor, wenn ein **Trojaner** eine Schwachstelle in der Software nutzt und dadurch Daten ausgespäht werden. Denn es erfolgt keine Störung der inneren Ordnung des Datenträgers.

(iii) Beeinträchtigung der bestimmungsgemäßen Verwendung

112 Eine Eigentumsverletzung kommt auch dann in Betracht, wenn eine Beeinträchtigung der bestimmungsgemäßen Verwendung erfolgt.[215] Bei der Annahme einer Eigentumsverletzung ist indessen Vorsicht geboten, da die Grenze zum nach § 823 Abs. 1 BGB **nicht ersatzfähigen primären Vermögensschaden** nicht überschritten werden darf.[216] Die Rechtsprechung hat jedoch die **erhebliche** Beeinträchtigung der bestimmungsge-

---

440 f.; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 357 f.; *Sodtalbers*, Softwarehaftung im Internet, Rn. 511; MünchKommBGB-*Wagner*, § 823 BGB Rn. 96; Bamberger/Roth-*Spindler,* § 823 BGB Rn. 55; a.A. *Bauer*, PHi 1989, 98 (105 f.), nach dem die Zerstörung der Information physikalisch allenfalls eine elektronische Zustandsveränderung darstellt.

[210] Dem grds. zustimmend dann aber den Weg über ein eigenes Recht am Datenbestand als gangbarer sehend *Faustmann*, VuR 2006, 260 ff.

[211] *Faustmann*, VuR 2006, 262 f.; *Meier/Wehlau*, NJW 1998, 1588.

[212] *Faustmann*, VuR 2006, 262.

[213] *Spindler*, in: Hoeren/Sieber, Rn. 364.

[214] *Sodtalbers*, Softwarehaftung im Internet, Rn. 518.

[215] Grundlegend BGHZ 55, 153 (159) - Fleetfall; ausführlich Bamberger/Roth-*Spindler*, § 823 BGB Rn. 50 ff.

[216] BGHZ 86, 152 (155); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 51.

mäßen Verwendung einer Sache als Eigentumsverletzung angesehen.[217] Maßgebliche Kriterien sind letztlich die **Intensität** und der **Zeitraum** der Nutzungsbeeinträchtigung.[218]

113 Insbesondere im unternehmerischen Bereich drohen durch Softwarefehler hohe Schadenssummen, wenn der **Ausfall des EDV-Systems** zu Betriebsstörungen und Produktionsausfällen führt. Ebenso kann bei privater Nutzung ein Softwaremangel die Verwendung des Computers einschränken, wobei jedoch ungleich geringere Haftungsrisiken bestehen (denkbar sind etwa Kosten zur Wiederherstellung der Betriebsbereitschaft) bzw. oftmals überhaupt kein ersatzfähiger Schaden vorliegen wird. Eine Eigentumsverletzung wird man beim Systemausfall nur in engen Grenzen annehmen können, da sich die Funktionsuntauglichkeit der Sache, die mit der Software gesteuert wird, in der Regel in einem temporären Vorgang erschöpft, der die Sache (Hardware) nicht auf Dauer ihrer Gebrauchstauglichkeit enthebt, sondern die mit einer neuen Software wieder einsatzbereit gemacht werden kann. Anders kann im Einzelfall zu entscheiden sein, wenn das auf System über einen längeren Zeitraum nicht zugegriffen werden kann.[219]

114 Keine Eigentumsverletzung wird man regelmäßig auch bei der **Installation eines Trojaners** auf dem Rechner bejahen können. Zwar mag mit der Präsenz dieses Schadprogramms eine gewisse psychologische Hemmschwelle hinsichtlich einer Nutzung im Internet verbunden sein. Die Gebrauchstauglichkeit des Computers wird im Übrigen (z. B. Textverarbeitung usw.) aber nicht berührt und der Trojaner kann meist innerhalb relativ kurzer Zeit entfernt werden, wodurch die volle Gebrauchsfähigkeit wiederhergestellt wird.

(c) Verletzung sonstiger Rechte

(i) Allgemeines Persönlichkeitsrecht

115 Das Allgemeine Persönlichkeitsrecht schützt auch die unzulässige Erhebung Nutzung und Verarbeitung persönlicher und personenbezogener Daten, wodurch Ansprüche auf Unterlassung, Beseitigung, Auskunft und Ersatz des materiellen und immateriellen

[217] BGHZ 55, 153 (159 ff.); BGHZ 105, 346 (350); BGH NJW 1994, 517 (518); BGH NJW-RR 1995, 342 (342 f.); BGH NJW 1996, 2507 (2508); *Larenz/Canaris*, § 76 II 3 b, S. 387; Erman-*Schiemann*, § 823 BGB Rn. 31; Staudinger-*Hager*, § 823 BGB Rn. D 98.

[218] BGH NJW 1994, 517 (518); *Sodtalbers*, Softwarehaftung im Internet, Rn. 512.

[219] *Sodtalbers*, Softwarehaftung im Internet, Rn. 512; vgl. auch *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 261.

Schadens nach den §§ 823, 1004 BGB und §§ 7, 8 BDSG ausgelöst werden können.[220] Davon umfasst wird iSd Rechts auf informationelle Selbstbestimmung, die Befugnis des einzelnen, grundsätzlich selbst darüber zu entscheiden, ob und wer über seine persönlichen und sachlichen Verhältnisse unterrichtet ist oder wird.[221] Zu denken ist hier an den Schutz bei besonders gefahrenträchtiger Informationsverwaltung, wie zB der Speicherung von Fingerabdrücken, politischen Einstellungen, Gesundheitsbilder, Informationen zum eigenen Vermögensstand oder der Kreditfähigkeit uä.[222] Derartig sensible Daten müssen entsprechend geschützt aufbewahrt werden. Lassen sich die Daten dagegen unproblematisch durch Dritte mithilfe von Trojanern etc. ausspähen, kann dies uU zur Verletzung des Allgemeinen Persönlichkeitsrechts führen.

(ii) Recht am eigenen Datum

116 ZT werden im Rahmen des § 823 Abs. 1 BGB eigene Rechte in Bezug auf Daten als sonstige Rechte diskutiert. So wurde in der Vergangen gefordert, in „**Recht am eigenen Datum**“, das sich aus dem Recht auf informationelle Selbstbestimmung ableiten soll, als absolut geschütztes sonstiges Recht im Sinne von § 823 Abs. 1 BGB anzuerkennen.[223] Das Recht am eigenen Datum soll ein umfassendes Selbstbestimmungsrecht des einzelnen über ihn betreffende Informationen umfassen.[224] Die Vertreter des Rechts am eigenen Datum begründen die Notwendigkeit damit, dass das Interesse der Selbstbestimmung über personenbezogene Informationen, wie das Eigentum, gegenüber jedermann schutzwürdig sein müsse.[225] Zu Recht ist ein solches Recht aber überwiegend nicht anerkannt.[226] Das BVerfG hat im Volkszählungsurteil, in dem das Recht auf informationelle Selbstbestimmung begründet wurde, ausdrücklich betont, dass der Einzelne kein Recht auf absolute und unbeschränkbare Herrschaft über seine Daten hat und auch personenbezogene Information nicht ausschließlich dem Betroffenen allein zuge-

---

[220] Bamberger/Roth-*Bamberger*, § 12 Rn. 160; Simitis-*Simitis*, § 7 Rn. 29 ff.

[221] MünchKommBGB-*Rixecker*, Anh § 12 Rn. 102.

[222] Siehe dazu MünchKommBGB-*Rixecker*, Anh § 12 Rn. 106.

[223] Entwickelt von *Meister*, Datenschutz im Zivilrecht, S. 121 ff. noch vor der Anerkennung des Rechts auf informationelle Selbstbestimmung im Volkszählungsurteil; grds. demgegenüber positiv äußernd *Bruns*, Informationsansprüche gegen Medien, 65 f.; ergebnisoffen BGHZ 91, 231 (237 ff.).

[224] *Meister*, Datenschutz im Zivilrecht, S. 114 f.

[225] *Meister*, Datenschutz im Zivilrecht, S. 124.

[226] *Meier/Wehlau*, NJW 1998, 1585 (1588 f.); *Spindler/Klöhn*, VersR 2003, 410 (412); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 93; Staudinger-*Hager*, § 823 Rn. C 173; *Wente*, 97; Simitis-*Simitis*, Einleitung Rn. 26; *Ehmann*, AcP 188 (1988), 266 f.; ausführlich *Sodtalbers*, Softwarehaftung im Internet, Rn. 524 f.

ordnet werden können.[227] Diese Aussage steht daher in Widerspruch zur Annahme eines absolut geschützten Rechts am eigenen Datum.

(iii) Recht am Unternehmen

117 Bei fahrlässigen Datenlöschungen könnte eine Verletzung des als sonstiges Recht iSd § 823 Abs. 1 BGB anerkannten Rechts am eingerichteten und ausgerichteten Gewerbebetrieb in Betracht kommen. Voraussetzung für eine Verletzung dieses Rechts ist aber das korrektiv der Betriebsbezogenheit. Das bedeutet, dass sich der Eingriff gegen den Betrieb als solchen richten muss und nicht lediglich vom Gewerbebetrieb ablösbare Rechtspositionen beeinträchtigen darf.[228] Bei fahrlässigen Datenlöschungen, die zB aufgrund von Stromunterbrechung erfolgen, fehlt es daher meist an der Betreibsbezogenheit, so dass dem Recht am eingerichteten und ausgeübten Gewerbebetrieb in Bezug auf Daten wenig Bedeutung zukommt.[229]

(2) Verantwortlichkeit für von Dritten verursachte Verletzungen?

118 Steht die Verletzung eines Rechtsguts fest, bedarf es ferner der Zurechnung der Verletzung zum Hersteller. Während normalerweise das Produkt und sein Fehler selbst die entsprechende Rechtsgutsverletzung herbeiführen, etwa schadhafte Bremsen bei einem KfZ, die zu einem Unfall mit Verletzungsfolgen führen, sind bei IT-Produkten oftmals Einflüsse Dritter im Spiel, die Zurechnungsfragen aufwerfen:

(a) Haftung für Verhalten Dritter (Hacker)

119 Grundsätzlich treffen den Beherrscher der Gefahrenquelle Sicherungspflichten auch dann, wenn erfahrungsgemäß mit einem Fehlverhalten Dritter zu rechnen ist.[230] Beispiele hierfür sind Sicherungsvorkehrungen des Grundstückseigentümers gegen missbräuchliches Verhalten Dritter,[231] eines Veranstalters gegen Übergriffe der Zuschauer auf Nachbargrundstücke,[232] die Beseitigung von durch mutwillige Aktionen auf eine Fahrbahn geratenen Hindernisse[233] oder die Sicherung von Kraftfahrzeugen gegen Benut-

---

[227] BVerfGE 65, 1 (43 f.) – Volkszählungsurteil.

[228] St. Rspr. BGH NJW 1951, 643 (644); NJW 1952, 660 (661) – Constanze I; NJW 1959, 479 (481) – Stromkabel; NJW 1983, 810; NJW 1998, 2141; NJW-RR 2005, 673 (675); Bamberger/Roth-*Spindler*, § 823 Rn. 108; MünchKommBGB-*Wagner*, § 823 Rn. 185.

[229] *Meier/Wehlau*, NJW 1998, 1589; *Faustmann*, VuR 2006, 262; LG Konstanz NJW 1996, 2662.

[230] BGHZ 165 (170) = NJW 1962, 1565; BGH NJW 1990, 1236 (1237); OLG Köln VersR 1992 (1241).

[231] So sind Lichtroste gegen ein Abheben zu sichern BGH NJW 1990, 1236 (1237); anders OLG Frankfurt Rev. nicht angenommen BGH 4.11.1997 VI ZR 165/97 VersR 1998, 250 (Ls.) für einen Schacht im Schotterstreifen.

[232] BGH NJW 1980, 223.

[233] BGHZ 37, 165 (170) = NJW 1962, 1565; OLG Koblenz NVwZ 2002, 745 – Fahrbahnverschmutzung durch Sand.

zung durch Unbefugte.[234] Demgemäß ist sowohl im allgemeinen Deliktsrecht[235] als auch in der Produkthaftung anerkannt, dass der Beherrscher der Gefahrenquelle – der Software – auch für Schäden einstehen muss, die erst durch das vorsätzliche Ausnutzen der durch das Produkt entstandenen latenten Gefahr durch Dritte entstehen.[236] **Überträgt** man diese **Grundsätze auf** die **IT-Produkthaftung**, wird die Verantwortlichkeit von Softwareproduzenten bei IT-Sicherheitslücken ihrer Programme nicht dadurch ausgeschlossen, dass letztlich Dritte, wie Programmierer von Viren oder Würmern oder Hacker, die Schäden verursachen. Eine solche latente Gefahr besteht insbesondere bei Sicherheitslücken, die von Hackern ausgenutzt werden können.[237]

(b) Haftung für Fremdprodukte und -dienste (Zubehör; Kompatibilitäten)

120 Eng damit verwandt, aber nicht gleichbedeutend ist die Haftung für **fremde Software**, die in Verbindung mit der eigenen Software eingesetzt wird – in Übertragung der von der Rechtsprechung entwickelten Haftung des Herstellers für fremd produziertes **Zubehör**, die hier zumindest eine Produktbeobachtungspflicht annimmt;[238] dementsprechend sind diese Komplexe im Rahmen der Produktbeobachtung zu thematisieren.

121 Allerdings muss von vornherein der Anwendungsbereich der Produkthaftung eingegrenzt werden: Denn für **mangelnde Kompatibilität** mit einzelnen Fremdprodukte kann keine deliktische Haftung eingreifen, da damit der Bereich des deliktisch geschützten Integritätsinteresses verlassen würde.[239] Denn die Inkompatibilität der eigenen Hard- und Software mit einzelnen Fremdkomponenten liegt bereits beim Erwerb vor, so dass von vornherein mangelhaftes Eigentum erworben wurde. Allein das Äquivalenzinteresse ist damit betroffen, für dessen Ausgleich ausschließlich das Gewährleistungsrecht sorgt.[240]

---

[234] BGH NJW 1971, 459 (460).

[235] Bamberger/Roth-*Spindler*, § 823 BGB Rn. 245 mwN; MünchKommBGB-*Wagner*, § 823 BGB Rn. 255 f.

[236] BGH NJW 1990, 1236 (1237).

[237] *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 442; *Bartsch*, CR 2000, 721 (721 ff.).

[238] Grundlegend dazu BGH v. 9.12.1986 – VI ZR 65/86 – Honda, BGHZ 99, 167 = MDR 1987, 396 = CR 1987, 230; dazu *Ulmer*, ZHR 152, 564 (570 ff.); *Foerste,* in: v. Westphalen, ProdHaftHdb, § 25 Rz. 176 ff.; Kullmann/Pfister-*Kullmann*, Rz. 1520, S. 52; *Pfister*, EWiR 1987, 235.

[239] BGHZ 86, 256 (258 ff.) = NJW 1983, 810 (811) = JZ 1983, 499 m. Anm. *Stoll*; MünchKommBGB-*Wagner*, § 823 BGB Rn. 122; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 60 mwN.

[240] BGHZ 39, 366 (367) = NJW 1963, 1827; BGHZ 67, 359 (364) = NJW 1977, 379; BGHZ 86, 256 (259) = NJW 1983, 810; BGHZ 96, 221 (228) = NJW 1986, 922; BGH NJW 1992, 1678; 1994, 2231 (2232); 2001, 1346 (1347) – Grundstück mit Schlacke führt zur Beschädigung von darauf stehenden Bauwerken; OLG Düsseldorf NJW-RR 1997, 1344 (1346); OLG Koblenz NJW-RR 1998, 374; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 60; Staudinger-*J. Hager,* Kap. B Rn. 108; Soergel-*Spickhoff,* Vor § 823 BGB Rn. 49; *Hinsch,* VersR 1992, 1053.

(3) Pflichten vor Inverkehrgabe: IT-Sicherheitslücken als Konstruktionsfehler

122 In der Produkthaftung unterscheidet man typischerweise Konstruktions- und Fabrikationsfehler, für die gehaftet werden muss,[241] während für Entwicklungsfehler keine Haftung eingreift.[242] Bei Hardwareprodukten können beide Fehlerkategorien auftreten. Dagegen spielt für Software eindeutig der Konstruktionsfehler die maßgebliche Rolle, wird doch Software digital eins-zu-eins kopiert, so dass nur in seltenen Fällen eine fehlerhafte Fabrikation ursächlich für eine Rechtsgutsverletzung sein dürfte, z.B. wenn Software-CDs/DVDs fehlerhaft kopiert wurden.

123 Maßgeblich sind daher **Konstruktionsfehler**, wenn bei der Inverkehrgabe des Produktes nicht der Stand von Wissenschaft und Technik[243] berücksichtigt wurde, da der gesamten Serie der Software derselbe Fehler anhaftet.[244] Ähnlich der Produktbeobachtungspflicht ist der Hersteller gehalten, alle allgemein oder ihm speziell zugänglichen Erkenntnisquellen auszuschöpfen.[245] **Entscheidend** ist demnach, ob dem Softwarehersteller bereits **bei der Inverkehrgabe die Sicherheitslücken bekannt** sein mussten. Die Kenntnis wird auch bereits durch eine einzelne Mitteilung über eine Sicherheitslücke an den Softwarehersteller begründet, selbst wenn sie geheimgehalten wird, da nicht auszuschließen ist, dass andere ebenfalls diese Lücke entdecken und ausnützen. Umgekehrt führen **Sicherheitslücken, die erst später bekannt werden**, nicht dazu, dass dem Hersteller ein Konstruktionsfehler anzulasten wäre; hier handelt es sich vielmehr um einen **Entwicklungsfehler**, so dass allein nachträgliche Pflichten im Rahmen der Produktbeobachtung eingreifen können.

124 Ferner ist der Hersteller selbstverständlich gehalten, seine Konstruktion, Fertigung oder Instruktion[246] zu ändern, um den Fehler in Zukunft zu verhindern.[247] Sind Gefahren be-

---

[241] Bamberger/Roth-*Spindler*, § 823 BGB Rn. 494 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 581 ff., 584 ff.

[242] Bamberger/Roth-*Spindler*, § 823 BGB Rn. 493; MünchKommBGB-*Wagner*, § 823 BGB Rn. 264, 579f.; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 18, 82 ff.

[243] Zur Relevanz des Standes von Wissenschaft und Technik für die Produkthaftung bei fehlerhaften Computerprogrammen *Littbarski*, in: Kilian/Heussen, Kap. 180 Rn. 53.

[244] Eingehend zum Konstruktionsfehler als Programmierfehler *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 244 ff.; *Günther*, Produkthaftung für Informationsgüter, S. 300 f.; *Meier/Wehlau*, CR 1990, 95 (96); *Reese,* DStR 1994, 1121 (1123).

[245] BGHZ 116, 60 (70 f.); BGH NJW 1990, 906 (907 f.); BGH NJW 1952, 1091; *Kullmann,* NJW 2002, 30 (32); Kullmann/Pfister-*Kullmann*, Kz. 1520 S. 14; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 494 mwN.

[246] Bei der Instruktion käme es z.B. darauf an, dass der Nutzer eindringlich auf die Notwendigkeit von periodischen Sicherheitsupdates hingewiesen wird.

[247] BGH NJW 1990, 906 (908); BGH NJW 1994, 3349 (3350); MünchKommBGB-*Wagner,* § 823 BGB Rn. 602; *Michalski,* BB 1998, 961 (964).

kannt, aber nicht die Möglichkeiten zu ihrer Vermeidung, kann das Produkt im Prinzip nicht in den Verkehr gebracht werden.[248] Allerdings ist dem Hersteller ein Anpassungsermessen bei Wandel des Gefahrenbewusstseins[249] und bei neuen technischen Entwicklungen[250] zuzugestehen. Der Hersteller muss den Weg der größeren Vorsicht wählen, wenn Unsicherheiten über die Sicherheitsvorkehrungen bestehen.[251] Auch wenn Software ein äußerst komplexes Produkt darstellt, dessen Fehlerbehebung erheblichen Aufwands bedarf, führt dies nicht daran vorbei, dass bekannte Sicherheitsprobleme unverzüglich beseitigt werden müssen, bevor das Produkt auf den Markt gebracht wird.[252]

125 Der Hersteller darf nicht sehenden Auges Software auch bereits vorhandener Versionen weiterhin in Umlauf bringen, von denen er weiß, dass sie fehlerbehaftet sind. Ebenso wenig kann der Hersteller darauf vertrauen, dass bei der Installation fehlerhafter Software gleichzeitig die nötigen **Sicherheitspatches** aus dem Internet eingespielt und übertragen werden; denn es ist nicht auszuschließen, dass schon während dieser Zeit der Nutzer Angriffen ausgesetzt ist oder dass die entsprechenden Server der IT-Hersteller nicht erreichbar bzw. überlastet sind. Problematisch ist allerdings oft, dass die Software bereits in der ersten Vertriebsstufe (Großhändler) etwa auf Hardware aufgespielt wird (OEM-Versionen) und der Softwarehersteller häufig außerhalb von Vertriebsbindungen und –systemen keine Kontrolle mehr darüber hat, bei wem sich welche Versionen der Software befinden. Hier ist die Software bereits in Verkehr gebracht und nicht mehr im unmittelbaren Einflußbereich des Produzenten, so dass nur die nachträglichen Pflichten des Herstellers eingreifen (s. Rn. 127 ff.).

126 Fraglich kann daher nur sein, **wie viel Zeit** dem Hersteller eingeräumt werden kann, **um die Sicherheitslücke zu beseitigen**; hier ist mit Sicherheit zu bedenken, dass Software ein komplexes Produkt darstellt und die Korrektur solcher Lücken nicht mit der Aktualisierung von Virenscannern verglichen werden kann, da es um das Einpassen neuen

---

[248] Vgl. *Foerste,* in: v. Westphalen, ProdHaftHdb, § 24 Rn. 84 ff., 86; Kullmann/Pfister-*Kullmann*, Kz. 1520 S. 4 f.; diff. *Brüggemeier*, WM 1982, 1294 (1302).

[249] Insbes. bei uneinheitlichen Verbrauchererwartungen wie z.B. bei Kopfstützen, ABS-Bremssysteme oder Airbags in KfZ, vgl. *Foerste,* in: v. Westphalen, ProdHaftHdb, § 24 Rn. 89, 90 ff.; ähnlich *Hollmann*, DB 1985, 2389 (2392); *Schlechtriem*, VersR 1986, 1033 (1036); abl. gegenüber dem Kriterium der Verbrauchererwartung *Möllers*, Rechtsgüterschutz im Umwelt- und Haftungsrecht, S. 254 ff.

[250] Kullmann/Pfister-*Kullmann*, Kz. 1520 S. 15 f.

[251] Kullmann/Pfister-*Kullmann*, Kz. 1520 S. 15 unter Verweis auf BGH NJW 1990, 906 (907) - und Berufung auf arzthaftungsrechtliche Grundsätze, wie z.B. BGHZ 8, 138 (140); weniger restriktiv BGH NJW 1987, 2927; ähnlich LG Itzehoe JurPC 87/2003, 17 f.

[252] *Meier/Wehlau,* CR 1990, 95 (97); *Bauer*, PHi 1989, 38 (47); s. auch *Schneider*/*Günther*, CR 1997, 389 ff.; *Bartsch,* CR 2000, 721 (722 ff.).

Codes in vorhandene Software geht. Andererseits kann der Softwarehersteller sich nicht darauf berufen, dass ihm die nötigen Ressourcen zur Anpassung fehlen, da er zumindest in den letzten Jahren angesichts sich häufender Sicherheitslücken allgemein damit rechnen muss, dass neue Probleme auftauchen. Welcher Zeitraum hier angemessen ist, kann nur im Einzelfall beurteilt werden; dabei werden als Ausgangspunkt die in der Branche üblichen Anpassungszeiten, aber auch eine „best practice" herangezogen werden müssen, da ein niedriger Sicherheitsstandard nicht maßgeblich sein kann. Zudem sind Schadensumfang und –ausmaß sowie die Bedeutung der Software einschließlich der Vorteilsziehung für den Softwarhersteller im Sinne einer Kosten-Nutzen-Abwägung in die Beurteilung einzubeziehen.

(4) Pflichten nach Inverkehrgabe

127 Nach Inverkehrgabe wird der Hersteller nicht vollständig von seiner Verantwortung für das Produkt frei. Vielmehr muss er bei Kenntnis von Schäden durch das Produkt die zu diesem Zeitpunkt erforderlichen und ihm zumutbaren Gefahrenabwehrmaßnahmen ergreifen. Zu Schäden muss es noch nicht gekommen sein.[253] Anknüpfungspunkt für die Haftung des Produzenten ist die Verletzung der **Produktbeobachtungspflicht**.[254] Haftungsgrund ist die Schaffung einer andauernden Gefahrenquelle, deren Ursachen aus der Sphäre des Herstellers stammen, unabhängig davon, welcher Fehlerkategorie sie angehören.[255]

(a) Produktbeobachtungs- und Warnpflichten

(i) Grundsätze

128 Für bereits vor Bekanntwerden der Sicherheitslücken vertriebene Software ist der Hersteller zur Produktbeobachtung, insbesondere zur Sammlung und Auswertung zugänglicher[256] Literatur und Erkenntnisse über mögliche Defekte seiner Software,[257] und zur Warnung, gegebenenfalls auch zum Rückruf verpflichtet. Gerade aus dem Wissen um die objektive Unvermeidbarkeit von Programmierungsfehlern („Bugs") erwächst eine

[253] OLG Karlsruhe VersR 1998, 63; hierzu *Kullmann,* NJW 1997, 1746 (1750).

[254] Vgl. *v. Bar*, in: Produktverantwortung und Risikoakzeptanz, S. 29 (33).

[255] *Foerste,* in: v. Westphalen, ProdHaftHdb, § 24 Rn. 292; *Michalski,* BB 1998, 961 (962 f.); Staudinger-*J. Hager*, § 823 BGB F Rn. 20 f.

[256] International tätige Unternehmen sind etwa zur weltweiten Informationsbeschaffung und –auswertung verpflichtet, s. BGHZ 80, 199 (203) = NJW 1981, 1606; *Foerste,* in: v. Westphalen, ProdHaftHdb, § 24 Rn. 296.

[257] Zu den Anforderungen an die Produktbeobachtungspflicht grundlegend BGHZ 80, 199 (202 f.); BGH NJW 1990, 906 (907 f.); *Foerste,* in: v. Westphalen, ProdHaftHdb, § 24 Rn. 245, 290 ff.; Kullmann/Pfister-*Kullmann*, Kza 1520 S. 54 f.

Pflicht des Herstellers zur besonders sorgfältigen Produktbeobachtung.[258] Bei drohenden Gefahren für Leib und Leben ist sogar bereits ein ernst zu nehmender Verdacht hinreichend, um Warnpflichten auszulösen[259]; bei Sachschäden und nicht akuter Bedrohung kann sich der Produzent im Falle eines Verdachts zunächst auf eigene Ermittlungen und aktive Beobachtung des Produktes beschränken, ohne vor dem Produkt oder dessen spezifische Verwendung warnen zu müssen.[260]

129 Allerdings darf der Hersteller nicht zuwarten, bis die Gefahr zur Gewissheit feststeht; bei sich häufenden Beschwerden muss der Hersteller vor den Gefahren warnen.[261] Häufig werden **IT-Sicherheitslücken durch Dritte** festgestellt und öffentlich bekannt gemacht; ab diesem Zeitpunkt kann sich der Hersteller nicht mehr nur auf eine passive Beobachtung beschränken, sondern muss selbst tätig werden.

(ii) Kontraproduktive öffentliche Sicherheitswarnungen?

130 Allerdings ist bei der Pflichtenbestimmung auch zu berücksichtigen, dass öffentliche Warnungen in kontraproduktiver Weise geradezu Dritte herausfordern können, eine IT-Sicherheitslücke zu nutzen, wie dies offenbar bei dem Wurm Sasser der Fall war. Sind die Lücken nur dem Hersteller bekannt geworden, etwa aufgrund eigener Tests oder aufgrund einer vertraulichen Mitteilung eines Dritten, muss ihm ein Ermessen zugestanden werden, ob er eine öffentliche Warnung ausspricht oder versucht, über Sicherheitspatches, die die Lücke nicht offenlegen, das Sicherheitsproblem zu beseitigen. Insbesondere wenn der Hersteller aufgrund seiner Vertriebsstrukturen die Möglichkeit hat, die Verwender seiner Software individuell anzusprechen, ist eine öffentliche Warnung nicht geboten, sogar unter Umständen pflichtwidrig. Mehren sich jedoch die Hinweise Dritter, so dass anzunehmen ist, dass die Kenntnis von der Lücke sich verbreiten könnte, oder kann der Hersteller den Weg seines Produktes nicht nachverfolgen, ist der Hersteller gehalten, eine öffentliche Warnung auszusprechen, da nicht mehr auszuschließen ist, dass die Sicherheitslücke in erheblichem Umfang ausgenutzt wird und dadurch Schäden bei Nutzern entstehen. Denn der Hersteller kann nicht mehr davon ausgehen,

---

[258] AA LG Köln NJW 1999, 3206: Keine Pflicht zur Warnung bei nachträglichen Erkenntnissen über Virenbefall einer Diskette.

[259] BGHZ 80, 186 (192) = NJW 1981, 1603; OLG Frankfurt NJW-RR 1995, 406 (408); OLG Frankfurt NJW-RR 2000, 1268 (1270); OLG Karlsruhe VersR 1998, 63 (64 f.).

[260] BGHZ 80, 186 (192)= NJW 1981, 1603; *Kullmann,* NJW 1996, 18 (23).

[261] BGH NJW-RR 1995, 342 (343).

dass seine Sicherheitspatches Beachtung finden oder der Nutzer genügend lang im Netz sich befindet, damit etwa eine automatische Updateerkennung eingreift.

131 Die **Warnhinweise** müssen **geeignet** sein, die in Betracht kommenden Verkehrskreise anzusprechen und auf die vom Produkt ausgehende Gefahr aufmerksam zu machen, wobei angesichts der heutigen Massenverbreitung einiger EDV-Programme nicht davon ausgegangen werden kann, dass alle Nutzer computerbezogene Zeitschriften beziehen oder entsprechende Online-Foren besuchen;[262] ebenso wenig genügt eine passive, produktspezifische Warnung in der Internet-Homepage des Herstellers. Vielmehr muss der Hersteller von weitverbreiteten Produkten zahlreiche Kanäle gleichzeitig zur Warnung nutzen.[263] Sofern es sich indes um gewerbliche Abnehmer mit Kenntnissen im EDV-Bereich handelt, treffen den Hersteller die Warnpflichten von vornherein nicht in derselben Intensität wie bei anderen Abnehmern, da diesen die Problematik grundsätzlich vertraut ist.[264]

(iii) Herausgabe des Quellcodes

132 Eine deliktsrechtlich[265] begründete Herausgabepflicht des Quellcodes ist in aller Regel nicht anzunehmen. Denn die Pflicht des Herstellers ist darauf gerichtet, eine Schädigung anderer Rechtsgüter des Softwarenutzers abzuwenden, was allein schon durch den Nichtgebrauch der Software erreicht wird; Maßnahmen zur Fehlerbehebung an der Software selbst sind dagegen auf das Äquivalenzinteresse gerichtet.[266]

(iv) Ende des Supports bei älteren Produkten?

---

[262] Vgl. *Marly*, Softwareüberlassungsverträge, Rn. 1311; allgemein: Kullmann/Pfister-*Kullmann*, Kza 1520 S. 61 ff.; *Foerste,* in: v. Westphalen, ProdHaftHdb, § 24 Rn. 251ff. mwN.

[263] Ausführlich dazu *Marly*, Softwareüberlassungsverträge, Rn. 1311.

[264] Vgl. etwa zu abgeschwächten Instruktionspflichten gegenüber gewerblichen Abnehmern BGH NJW 1996, 2224 (2225 f.); Kullmann/Pfister-*Kullmann*, Kza 1520 S. 47 f.

[265] Zu Ausnahmen im Werkvertragsrecht vgl. BGH NJW-RR 2004, 782: Die Herausgabepflicht beurteilt sich nach Umständen des Einzelfalls. Neben der Höhe des vereinbarten Werklohns kann dabei insbesondere dem Umstand Bedeutung zukommen, ob das Programm zur Vermarktung durch den Besteller erstellt wird und dieser zur ihm obliegenden Wartung und Fortentwicklung des Programms des Zugriffs auf den Quellcode bedarf; BGH NJW 1987, 1259 (1259 f.); LG München I CR 1989, 990 (991); LG Köln CR 2003, 484: grundsätzlich Übergabe des Quellcodes weder bei Individual- noch bei Standardsoftware Leistungspflicht des Herstellers; LG Köln CR 2000, 505 = NJW-RR 2001, 1711: Herausgabe bei Individualsoftware, wenn kein Wartungsvertrag besteht; OLG Karlsruhe CR 1999, 11: Herausgabepflicht, wenn Dokumentation zur Bedienung und Wartung geschuldet ist; abl. für Standardsoftware OLG München CR 1992, 208 (209): ohne Vereinbarung grundsätzlich keine Herausgabe des Quellcodes; *Schneider*, CR 2003, 317 (318 f.); *Ernst*, MMR 2001, 208 (211); *Schneider*, Handbuch des EDV-Rechts, A Rn. 90 ff., 99, H Rn. 24 f., 76 ff, J Rn. 328; *Brandi-Dohrn*, Gewährleistung bei Hard- und Softwaremängeln, S. 32 f.; auf den Einzelfall abstellend *Köhler/Fritzsche*, in: Lehmann, Rechtsschutz und Verwertung von Computersoftware, Kap. XIII Rz. 146 f.; *Seffer/Horter*, ITRB 2005, 169; *Conrad*, ITRB 2005, 12; *Hoeren*, CR 2004, 721; ebenso wohl *Marly*, Softwareüberlassungsverträge, Rn. 64 ff.; *Malzer*, CR 1989, 991 (992).

[266] Dies wird von *v. Westphalen/Langheid/Streitz*, Rz. 829 f. zu wenig berücksichtigt.

133 Im schnellebigen IT-Markt ist schließlich von besonderem Interesse, wann die Produktbeobachtungspflicht endet; so stellen auch bekannte Softwarefirmen wie Microsoft nach ca. 5-7 Jahren den Support für ihre Produkte ein. Hier ist zu differenzieren:

134 Allgemein gilt, dass die **Produktbeobachungspflicht** selbst nach längerer Bewährung eines Produktes nur dort enden kann, wo keine Langzeitschäden zu befürchten sind. Insoweit kann allerhöchstens von einer graduellen Abschwächung der Beobachtungspflichten und Orientierung an anderen Arten von Schäden, wie Spätschäden, ausgegangen werden.[267]

135 Indes ist mit der Produktbeobachtungspflicht **nicht der „Support" (Patches) zu verwechseln**: Denn selbst eine länger wirkende Produktbeobachtungspflicht besagt bei älteren Softwareprodukten nichts darüber, zu welchen Maßnahmen der Hersteller gehalten ist – hier könnte etwa eine allgemeine Warnung vor Sicherheitslücken genügen.

(v) Produktbeobachtung für Fremdsoftware

136 Die Produktbeobachtungspflicht erstreckt sich nach der Rechtsprechung auch auf Gefahren, die durch die Kombination des eigenen mit fremden Produkten, insbesondere mit auf dem Markt angebotenen Zubehörteilen entstehen können.[268] Die Produktbeobachtungspflicht hängt hier entscheidend von der Art und Größe der geschaffenen Gefahr ab: Sind Leib und Leben bedroht, hat der Hersteller über die Pflicht zur Sammlung und Verwertung einschlägiger Informationen hinaus bei konkretem Anlaß auch die durch die Kombination entstandenen Gefahren sowie die durch Verwendung von fehlerhaftem Zubehör mit dem Produkt entstehenden Risiken[269] selber zu überprüfen.[270] Diese Pflichten reduzieren sich erheblich, sofern nicht hochrangige Rechtsgüter bedroht sind oder der Markt zu unübersichtlich ist, um allen Gefahren nachgehen zu können.[271]

---

[267] Zutr. *Foerste,* in: v. Westphalen, ProdHaftHdb, § 24, Rn. 298; *Hölzlwimmer*, Produkthaftungsrechtliche Risiken des Technologietransfers durch Lizenzverträge, S. 40; *v. Bar*, in: Produktverantwortung und Risikoakzeptanz, S. 29, 40; Staudinger-*Hager*, § 823 BGB F Rn. 21; aA LG Frankfurt NJW 1977, 1108; *Löwe*, DAR 1978, 288 (290); *Dietrich*, Produktbeobachtungspflicht und Schadenverhütungspflicht der Produzenten, S. 121 f.: Produktbeobachtungspflicht endet spätestens nach 10 Jahren; diff. *Pauli*, PHi 1985, 134 (139), der von einem späteren Wiederaufleben der Produktbeobachtungspflicht bei Schäden ausgeht.

[268] BGHZ 99, 167 (172 ff.) = NJW 1987, 1009; BGH NJW 1995, 1286 (1287 f.); ausführlich dazu *Ulmer,* ZHR 152, 564 (575 ff.), der sich allerdings dogmatisch auf die Herausforderungfälle im Schadensrecht stützt; dem BGH zust. *Kunz,* BB 1994, 450 (451); *Dietrich*, Produktbeobachtungspflicht und Schadenverhütungspflicht der Produzenten, S. 76 ff.; ausführlich *Klinger*, Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, S. 56 ff.

[269] Vgl. *Kunz,* BB 1994, 450 (451 f.); anders *Ulmer,* ZHR 152, 564 (575 ff.): nur Kombinationsrisiken, nicht Fehlerfreiheit des Zubehörs.

[270] Zumindest hinsichtlich der von Marktführern angebotenen Zubehörteile, BGHZ 99, 167 (174 f.) = NJW 1987, 1009; *Michalski,* BB 1998, 961 (963); *Birkmann*, DAR 1990, 124 (128).

[271] BGHZ 99, 167 (175 f.) = NJW 1987, 1009; *v. Bar*, in: Produktverantwortung und Risikoakzeptanz, S. 29, 35.

Auch kann sich ein Hersteller grundsätzlich auf den eigenverantwortlichen Umgang weiterer Produzenten mit einem Vorprodukt verlassen.[272]

137 Die Rechtsprechung schießt indes über ihr Ziel hinaus: Eine generelle **Ausdehnung der Beobachtungspflichten auf Zubehörteile oder Kombinationsgefahren** kann nicht allein damit begründet werden, dass der Hersteller ohnehin zur Beobachtung der Produkte verpflichtet ist; grundsätzlich ist der Hersteller nur für die Gefahren verantwortlich, die er selbst geschaffen hat, nicht aber für Gefahrenerhöhungen, die durch Dritte verursacht werden,[273] erst recht, wenn die Zubehörprodukte wesentlich später nach Entwicklung, Konstruktion und Fabrikation auf den Markt gebracht werden. Jedenfalls muss es als ausreichend angesehen werden, wenn der Hersteller den Produktbenutzer dahingehend instruiert, dass nur von ihm selbst freigegebene bzw. als unbedenklich eingestufte Zubehörteile gefahrlos benützt werden können und dass die Benützung nicht autorisierten Zubehörs auf Gefahr des Benutzers erfolgt.[274] Anders ist dies zu beurteilen, wenn der Hersteller etwa selbst Schnittstellen für andere Programme vorsieht oder es sich um allgemein gebräuchliche Programme handelt, mit dem der Hersteller von vornherein rechnen muss.

138 Demgemäß ist die **Haftung für fremde Software weitgehend ausgeschlossen**; sie kann allenfalls in Betracht kommen, wenn die fremde Software, wie Plug-Ins, Add-Ons etc. spezifisch auf das Produkt des Herstellers zugeschnitten ist. Nur dann wird man überhaupt von einer solchen Produktbeobachtungspflicht ausgehen können.

(b) Rückrufpflichten

139 Auch wenn in den Grundzügen größtenteils anerkannt, fehlt bislang eine klare dogmatische Grundlage für die Pflicht, das Produkt zurückzunehmen und gegen ein funktionstüchtiges auszutauschen,[275] da sie das vertragsrechtlich geregelte Äquivalenzinteresse berührt.[276] Nur dann, wenn erhebliche Folgen für Gesundheit und Eigentum zu befürchten sind und Warnhinweise entsprechende Schäden nicht ohne weiteres verhindern kön-

[272] OLG Stuttgart VersR 2001, 465 (467): Zimmermann, der einen Holzbalken hergestellt hat, auf das korrekte Anstreichen durch einen Maler, Rev. n. angen. BGH Beschl. v. 24.10.2000 – VI ZR 89/00.

[273] Ähnlich *Ulmer,* ZHR 152, 564 (579); zust. *v. Bar*, in: Produktverantwortung und Risikoakzeptanz, S. 29, 36.

[274] In der Tendenz auch BGHZ 99, 167 (174) = NJW 1987, 1009.

[275] Zusammenfassend MünchKommBGB-*Wagner,* § 823 BGB Rn 603 ff.; Staudinger-*J. Hager*, § 823 Rz. F 20 f.; Bamberger/Roth-*Spindler*, § 823 BGB Rn 516 ff.; *Pieper*, BB 1991, 985; *v. Bar*, 25 Jahre Karlsruher Forum, S. 80 ff.; *Hager*, VersR 1984, 799 ff.; *Herrmann*, BB 1985, 1801 ff.; *Schwenzer*, JZ 1987, 1059 ff.; *Sack*, BB 1985, 1801 ff.

[276] Zu Recht abl. *Foerste,* in: v. Westphalen, ProdHaftHdb, § 24 Rn. 260 ff., 266, 274, 280 mwN.

nen, kann eine entsprechende Fehlerbehebung[277] anstelle eines Warnhinweises in Betracht kommen.[278] Im Vordergrund der Herstellerpflichten steht aber die Vermeidung von Schäden an anderen Rechtsgütern durch den weiteren Gebrauch des Produktes, so dass in fast allen Fällen eine ausdrückliche Warnung genügt, die den Softwarenutzer von der weiteren Verwendung des Produktes abhält; alles andere wäre auf das Äquivalenzinteresse gerichtet. Modifiziert werden kann diese Lage allenfalls durch das öffentlich-rechtliche Produktsicherheitsrecht.[279]

140 Unklar ist auch, ob mit der Rückrufpflicht auch eine **Pflicht zur kostenlosen Beseitigung der Gefahr** einhergeht[280] und welche Kosten ersetzt verlangt werden können: Die Rspr. tendiert dazu, den Schaden auf die Kosten des Ausbaus der fehlerhaften Teile zu beschränken, nicht jedoch die Kosten für den Einbau neuer, fehlerloser Teile zu erstatten.[281] Während der Hersteller bei zuvor unterlassenem Rückruf für einen eingetretenen Schaden ersatzpflichtig ist,[282] fehlt es grundsätzlich an einer Rechtsgutsverletzung und einem Schaden, wenn lediglich die Gefahr einer Schädigung besteht.[283] Jedoch ist der Hersteller verpflichtet, Gefahren für von § 823 Abs. 1 BGB geschützte Rechtsgüter zu vermeiden, so dass zumindest ein Anspruch aus § 1004 BGB anzunehmen ist. Daher hat der Hersteller die Kosten in vollem Umfang[284] jedenfalls für die Rücknahme des Produktes zu tragen, wenn von dem Produkt Gefahren für andere Rechtsgüter drohen.[285] Bei einem drohenden Schaden allein am Produkt selbst genügt eine Warnung des Pro-

[277] *Bartsch*, Der Jahr-2000-Fehler, S. 157 f.; *Imhof/Wahl*, WpK-Mitt. 1998, 136 (139) weisen zutreffend darauf hin, dass eine Deinstallation der Software im Sinne eines physischen Rückrufs wenig Sinn machen würde.

[278] Vgl. OLG Frankfurt NJW-RR 2000, 1268 (1272); OLG München NJW-RR 1999, 1657, Rev. n. angen. BGH 27.5.1999 – III ZR 103/98; BGH NJW 1990, 2560; *Foerste*, DB 1999, 2199 (2199 f.); *Schwenzer*, JZ 1987, 1059 (1061 f.); Kullmann/Pfister-*Kullmann*, Kza 1520 S. 62 f.; MünchKommBGB-*Wagner,* § 823 BGB Rn. 605; *v. Bar*, in: Produktverantwortung und Risikoakzeptanz, S. 29 (40 f.).

[279] Vgl. § 5 I Nr. 1 c) GPSG = § 4 II ProdSG aF: öffentlich-rechtliche Produktbeobachtungspflicht des Herstellers sowie § 8 Abs. 4 Nr. 7 GPSG = § 9 ProdSG aF: behördliche Anordnung des Rückrufs; zur Rückrufpflicht aufgrund von § 823 BGB Abs. 2 iVm. § 8 Abs. 4 Nr. 7 GPSG bzw. § 9 ProdSG aF; vgl. Bamberger/Roth-*Spindler,* § 823 BGB Rn. 522.

[280] Etwa durch Reparatur oder Austausch des Produktes, so OLG Düsseldorf NJW-RR 1997, 1344 (1345); OLG Karlsruhe NJW-RR 1995, 594 (597); *J. Hager*, VersR 1984, 799 (800); *Mayer,* DB 1985, 319 (320); G. *Hager,* AcP 184 (1984), 413 (423 ff.) mit dem Hinweis, dass auch in der Praxis so verfahren wird; ausführlich *Koch,* AcP 203 (2003), 603 ff.

[281] OLG Stuttgart NJW 1967, 572; zust. OLG Düsseldorf NJW-RR 1997, 1344 (1346).

[282] BGH VersR 1971, 80 (81); BGHZ 80, 199 (203) = NJW 1981, 1606; BGH NJW 1994, 517 (518 f.); BGH NJW-RR 1995, 342.

[283] Abl. deswegen wohl (obiter dictum) OLG München NJW-RR 1999, 1657, Rev. n. angen. BGH 27.5.1999 – III ZR 103/98.

[284] *Dietrich*, Produktbeobachtungspflicht und Schadenverhütungspflicht der Produzenten, S. 223 f.; abw. *Foerste,* in: v. Westphalen, ProdHaftHdb § 24 Rn. 285: ausnahmsweise Kostenteilung.

[285] OLG Düsseldorf NJW-RR 1997, 1344 (1345); OLG Karlsruhe NJW-RR 1995, 594 (597); MünchKommBGB-*Wagner*, § 823 BGB Rn. 605; Staudinger- *Hager*, § 823 BGB F Rn. 26; *G. Hager,* AcP 184 (1984), 413 (423) ff.; *J. Hager,* VersR 1984, 799 (802); *Mayer,* DB 1985, 319 (320); *Dietrich*, Produktbeobachtungspflicht und Schadenverhütungspflicht der Produzenten, S. 236; nur für Gefahren für Leib und Leben: *Schwenzer,* JZ 1987, 1059 (1063); *Michalski,* BB 1998, 961 (965).

duktbenutzers, da ansonsten das Äquivalenzinteresse und die Erwartung, das Produkt nutzen zu können, geschützt würde.[286]

141 Dementsprechend kann aus dem Produkthaftungsrecht prinzipiell keine Pflicht abgeleitet werden, dass Patches oder ein Support zur Verfügung gestellt wird, da es genügen würde, dass der Kunde das Produkt nicht mehr benützt, um seine Integritätsinteressen zu wahren. Eine Pflicht zur fortdauernden Softwarepflege kann daher deliktisch nicht abgeleitet werden.

(5) Herstellerpflichten und technische Standards

142 Art und Umfang der Pflichten von IT-Herstellern werden nicht nur durch die Erwartungen des Verkehrs, sondern auch maßgeblich vom Erkenntnisstand von Wissenschaft und Technik mitbestimmt. Die Rechtsprechung rekurriert hierbei vielfach an die dem öffentlichen Sicherheitsrecht als Eingriffsvoraussetzung für Behörden entstammenden Kategorien der „anerkannten Regeln der Technik", den „Stand der Technik" sowie den „Stand von Wissenschaft und Technik",[287] ohne die Verwendung dieser Begriffe näher zu erläutern. Im Ergebnis ausschlaggebend für die Pflichtenbestimmung ist das konkrete Gefährdungspotential eines Produkts.[288]

143 Untergrenze der Sorgfaltsanforderungen bilden jedenfalls die **anerkannten Regeln der Technik**, d.h. die in den Kreisen der betreffenden Techniker bekannten und als richtig anerkannten Regeln, welche in der Praxis erprobt, dort verbreitet und bewährt sind.[289] Nach oben werden die Sorgfaltsanforderungen begrenzt durch den **Stand von Wissenschaft und Technik** im Zeitpunkt des Inverkehrbringens des Produkts,[290] welcher das realisierbare Ergebnis neuester naturwissenschaftlicher Forschung und ingenieurwissenschaftlicher Erfahrungssätze, deren Akzeptanz durch die Mehrheit der Praktiker noch

[286] Zutr. *Foerste*, DB 1999, 2199 (2200); *Taschner/Frietsch*, Einführung Rn. 89; ähnlich *Pieper,* BB 1991, 985 (988) mit dem Hinweis, dass andernfalls eine „deliktische Gewährleistung" entstünde; anders *v. Westphalen,* DB 1999, 1369 (1370); *Koch,* AcP 203 (2003), 603 (624 ff., 631f.), will Ersatz der Aus- und Einbaukosten unter Ausschluss von Materialkosten gewähren.

[287] BGH NJW 1971, 1313 (anerkannte Regeln der Technik); BGH DB 1972, 1335 (Stand der Technik); BGH NJW 1981, 1603 (Stand von Wissenschaft und Technik); ausführlich zur Abgrenzung der Begriffe BVerfG NJW 1979, 359, (362); *Marburger*, Die Regeln der Technik im Recht, §§ 14-16.

[288] Dazu ausführlich *Finke*, Die Auswirkungen der europäischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht, S. 9 ff.

[289] *Marburger*, Die Regeln der Technik im Recht, S. 157, 162 f., 439; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 16; *Wilrich*, § 2 GPSG Rn. 107; *Vieweg*, in: Schulte, Handbuch des Technikrechts, S. 353.

[290] *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 18 f.; *Spindler*, Unternehmensorganisationspflichten, S. 796.

aussteht widerspiegelt.[291] Für danach nicht voraussehbare Gefahren (Entwicklungsfehler) haftet der Hersteller nicht.[292]

144 Für die Ausfüllung dieser unbestimmten Rechtsbegriffe und damit die Pflichtenbestimmung im Bereich der Produkthaftung von herausragender Bedeutung sind Standards, welche in **überbetrieblichen technischen Normen** niedergelegt sind:

(a) Haftungsrechtliche Bedeutung technischer Normen

145 Technischen Normen werden von privaten Normungsorganisationen wie beispielsweise dem deutschen DIN e.V. erlassen und sind folglich keine Rechtsnormen.[293] Nach Auffassung der Rechtsprechung handelt es sich vielmehr um **auf freiwillige Anwendung angelegte Empfehlungen** der privaten Normungsorganisationen.[294] Da die technischen Regeln keine (rechtliche) Bindungswirkung entfalten, ist der Hersteller ferner nicht gehindert, das erforderliche Sicherheitsniveau auf abweichende, aber gleich geeigneten oder besseren, als dem in der technischen Norm vorgezeichnetem Wege **(alternative Sicherheitslösungen)** zu erreichen.[295]

146 Die Bedeutung überbetrieblicher technischer Normen im Haftungsrecht liegt nach ständiger Rechtsprechung des BGH darin, dass sie anerkannte Regeln der Technik wiedergeben und daher **zur Bestimmung des nach der Verkehrsauffassung zur Sicherheit Gebotenen in besonderer Weise geeignet** sind.[296] Technische Normen können herangezogen werden, um den Inhalt von Verkehrspflichten zu konkretisieren. Die technischen Regeln können indes nur als der zu fordernde **Mindeststandard** herangezogen werden, der nicht ausschließt, dass die Zivilgerichte im Einzelfall über die dort niedergelegten Verhaltensanforderungen hinausgehen.[297] Sie bestimmen mithin die Sorgfalts-

---

[291] BVerfG NJW 1979, 359, (362); OLG Köln NJW-RR 1991, 1077 (1079); *Marburger*, Die Regeln der Technik im Recht, S. 164 f.; *Foerste,* in: v. Westphalen, ProdHaftHdB, § 24 Rn. 16.

[292] Bamberger/Roth-*Spindler*, § 823 BGB Rn. 493; MünchKommBGB-*Wagner*, § 823 BGB Rn. 264, 579f.; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 18, 82 ff.

[293] *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 159; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 255; MünchKommBGB-*Wagner*, § 823 BGB Rn. 578.

[294] BGH NJW 2004, 1449 (1450); BGHZ 139, 16 (19); BGHZ 103, 338 (341); *Röthel*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 31 (45); *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 159.

[295] Bamberger/Roth-*Spindler*, § 823 BGB Rn. 257; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 20; MünchKommBGB-*Wagner*, § 823 BGB Rn. 273, 578.

[296] BGH NJW 2004, 1449 (1450); BGH NJW-RR 2002, 525 (526); BGH NJW 2001, 2019 (2020); BGH VersR 1988, 632 (633); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 255; MünchKommBGB-*Wagner*, § 823 BGB Rn. 272; *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 159, 161 ff.

[297] BGH NJW 2004, 1449 (1450); BGH VersR 1987, 102 (103); *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 161; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 20, 255; Soergel-*Krause*, Anh II § 823 BGB Rn. 49;

anforderungen nicht abschließend und binden die Zivigericht mangels Rechtsnormqualität nicht.[298]

147 Die technischen Normen geben jedoch **nicht in jedem Fall die anerkannten Regeln der Technik** wider;[299] sie können im Einzelfall auch hinter ihnen zurückbleiben.[300] Der Hersteller muss daher nach Ansicht des BGH grundsätzlich selbständig prüfen, ob und welche Sicherungsmaßnahmen erforderlich sind.[301] Die Einhaltung der einschlägigen technischen Norm entlastet nur dann, wenn sie die jeweiligen Gefahren ausreichend berücksichtigt, also z.B. auch besonders gefährdete Verkehrskreise mit einbezieht.[302] Über die normierten Standards hinausgehende Sicherheitsmaßnahmen wird man dann fordern müssen, wenn die technischen Normen veraltet sind, besonderen Gefahrenlagen zu begegnen ist oder sich das Produkt an einen besonders gefährdeten Nutzerkreis wendet.[303] Insbesondere für DIN-Normen besteht bei Einhaltung der in technischen Normen geregelten Standards jedoch eine **tatsächliche Vermutung für die Wiedergabe der anerkannten Regeln der Technik**, die nicht unterschritten werden dürfen.[304]

148 Keine anderen Grundsätze gelten auch für **europäisch harmonisierte Normen** im Rahmen des sog. **„New Approach"** (dazu ausführlich Teil 2 Rn. 841 ff.). Auch technische Normen, welche von den europäischen Normungsorganisationen CEN, CENELEC und ETSI erarbeitet werden bleiben rechtliche unverbindliche Empfehlungen privater Organisationen[305], welche auf freiwillige Einhaltung angelegt sind (so ausdrücklich § 2 Abs. 16 GPSG).[306] Bei harmonisierten Normen wird wegen der an sie anknüpfenden

---

MünchKommBGB-*Wagner*, § 823 BGB Rn. 272; Staudinger-*Hager*, § 823 BGB Rn. G 34; *Vieweg*, in: Schulte, Handbuch des Technikrechts, S. 355.

[298] Bamberger/Roth-*Spindler*, § 823 BGB Rn. 255; *Vieweg*, in: Schulte, Handbuch des Technikrechts, S. 360.

[299] BGH NJW 1987, 372 (373); *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 37.

[300] BGHZ139, 16 (20); OLG Nürnberg NJW-RR 2002, 1538; *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 161 f.

[301] BGH NJW 2001, 2019 (2020); BGH NJW 1982, 1049; *Köhler*, BB 1985 Beil. 4, S. 10 (10 f.); *Marburger*, VersR 1983, 587 (603).

[302] BGH NJW 1987, 372; OLG Zweibrücken NJW 1977, 111 f.; *Marburger*, VersR 1983, 597 (600); *Spindler*, Unternehmensorganisationspflichten, S. 805.

[303] Bamberger/Roth-*Spindler*, § 823 BGB Rn. 255, 489; Soergel-*Krause*, Anh II § 823 BGB Rn. 46; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 41.

[304] BGH NJW 1988, 2667 (2668); BGH VersR 1984, 270; BGH VersR 1972, 767 (768); OLG Celle NJW 2003, 2544; *Köhler*, BB 1985 Beil. 4, S. 10 (11); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 255; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 38, 41; *Spindler*, Unternehmensorganisationspflichten, S. 803, 805.

[305] CEN und CENELEC sind Vereine nach belgischem Recht, ETSI ist ein Verein nach französischem Recht, s. dazu *Röthel*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 31 (41).

[306] Siehe auch *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfassten Richtlinen, 2000, S. 7, 9, abrufbar unter http://ec.europa.eu/enterprise/newapproach/legislation/guide/document/guidepublicde.pdf; *Röthel*, in: Marburger, Technische

Vermutungswirkung (s. z.B. § 4 Abs. 1 Satz 2 GPSG) zwar verbreitet von einer Bindungswirkung oder gar einer „Rechtswirkung“ gesprochen.[307] Diese Bindungswirkung ist indes auf die Prüfung der Konformität mit den Richtlinienanforderungen beschränkt (Adressaten sind insoweit Marktüberwachungsbehörden und Verwaltungsgerichte), welche zivilrechtlich – wie ausgeführt – nur den zu fordernden Mindeststandard markieren[308], die zivilrechtliche Sorgfalt aber nicht abschließend definieren. Auch die Einhaltung der in harmonisierten Normen niedergelegten Sicherheitsanforderungen vermag den Produkthersteller daher in Bezug auf die zivilrechtliche Haftung nicht in jedem Fall zu entlasten.[309] Dies wird auf europarechtlicher Ebene schließlich durch das Nebeneinander von Produktsicherheits- und Produkthaftungsrichtlinie verdeutlicht.[310]

149 Nicht zu unterschätzen ist indes die **faktische Autorität** harmonisierter wie rein nationaler Normen für die Bestimmung der Verkehrspflichten, so dass die Einhaltung der Normvorgaben den Hersteller im praktischen Ergebnis oftmals gleichbedeutend mit der Wahrung der im Verkehr erforderlichen Sorgfalt sein wird.[311] In der Tat gehen die Gerichte nur in seltenen Fällen über die Anforderungen der einschlägigen technischen Norm hinaus.[312] Dagegen werden Pflichtverstöße oftmals schon allein deshalb bejaht, weil technische Normen missachtet wurden.[313]

(b) Technische Standards für den IT-Bereich: Common Criteria und Protection Profiles

150 Bislang existieren im IT-Bereich keine allgemeingültigen Sicherheitsstandards, so dass hinsichtlich der Sicherheitserwartungen des Verkehrs praktisch keine Konkretisierung durch technische Normen erfolgt.[314] Vor allem der rasante Fortschritt in der Software-

---

Regeln im Umwelt- und Technikrecht, S. 31 (45 f.); *Taupitz*, in: Produktverantwortung und Risikoakzeptanz, S. 119 (124); *Wilrich*, Einleitung Rn. 39.

[307] *Roßnagel*, DVBl. 1996, 1181 (1184); *Spindler*, Unternehmensorganisationspflichten, S. 161 f. mwN.

[308] Siehe *Taschner/Frietsch*, Art. 7 ProdHaft-RL Rn. 31: „Es handelt sich bei diesen Sicherheitsanforderungen gemeinschaftsrechtlichen Charakters [...] um Mindestanforderungen auf EG-Ebene. Ihr Ziel ist in erster Linie die Herstellung des freien Warenverkehrs auf dem Gemeinsamen Markt durch Beseitigung technischer Handelshemmnisse. Die Beseitigung von Gefährdungen für den Verwender technischer Geräte ist lediglich von zweitrangigem Interesse.“

[309] *Taupitz*, in: Produktverantwortung und Risikoakzeptanz, S. 119 (132 ff., insbes. 135, 136); *Wandt*, Internationale Produkthaftung, Rn. 646; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 489.

[310] *Taupitz*, in: Produktverantwortung und Risikoakzeptanz, S. 119 (135); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 489.

[311] MünchKommBGB-*Mertens*, 3. Aufl. 1997, § 823 BGB Rn. 30.

[312] *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 155 (166). Ein Beispiel ist BGH NJW 1985, 164, wo das Gericht über die einschlägigen DIN-Normen und die Bestimmungen der Bayerischen VersammlungsstättenVO hinausging. Siehe auch BGH VersR 1987, 783 zur Abweisung einer Unterlassungsklage gegen die Stiftung Warentest, die ein Produkt trotz Einhaltung der maßgeblichen DIN-Norm mit „mangelhaft“ bewertet hatte.

[313] Siehe z.B. BGH NJW-RR 2002, 525.

[314] *Sodtalbers*, Softwarehaftung im Internet, Rn. 273; *Hoeren*, in: von Westphalen, Vertragsrecht und AGB-Klauselwerke, IT-Verträge, Rn. 94.

entwicklung behindert dabei die Versuche zur Festlegung eines allgemeingültigen Sicherheitsstandards, der nicht sofort wieder überholt ist.[315]

151 Zunehmend werden IT-Produkte nach den sog. **Common Criteria-Standards** zertifiziert und geprüft, die sich als internationaler Standard für IT-Produkte herausgebildet haben.[316] Im Zusammenhang mit sog. Protection Profiles, die halbstandardisiert für Sicherheitsbedürfnisse von IT-Anwendungen erstellt werden, können diese Produktstandards (mittelbar) rechtliche Wirkung entfalten, indem sie die nötige Mindestsicherheit für bestimmte Bereiche konkretisieren. Als Common Criteria werden die „Gemeinsamen Kriterien für die Prüfung und Bewertung von Sicherheit von Informationstechnik" nach der im Jahre 2000 beschlossenen ISO-Norm 15408 bezeichnet,[317] die den amerikanischen Standard TCSEC sowie den europäischen Standard ITSEC ablösen sollen. Sie stellen ein weltweit anerkanntes Rahmenwerk für die Bewertung von Softwareprodukten dar.[318] Ziel ist eine vergleichbare Überprüfung und entsprechend auch Zertifizierung von IT-Produkten mit unterschiedlich modellierbarer Prüfungsintensität.[319] Common Criteria definieren somit an sich keine Überprüfung für IT-Produkte, sondern legen für die Bewertung eine gemeinsame Basis fest. Dafür definieren die Common Criteria 11 Funktionalitätsklassen sowie deren Abhängigkeiten, die für ein Produkt sicherheitsrelevante Vorgänge beschreiben. Die Funktionalitätsklassen sind allgemeine Grundfunktionen der Sicherheitsarchitektur eines zu zertifizierenden Produkts bzw. einer Produktklasse wie z.B. der Schutz der Benutzerdaten, die Privatsphäre, Kommunikation oder Sicherheitsprotokollierung.[320] Diese Grundfunktionen sind getrennt zu bewerten.

152 Allein für sich genommen würden jedoch die Common Criteria keine Sicherheitsbewertung erlauben. Hierzu sind **Protection Profiles** erforderlich, die Dokumente darstellen, in denen Anwender auf der Basis der 11 Funktionsklassen ihre Sicherheitsbedürfnisse benutzerorientiert formal beschreiben und anschließend registrieren können.[321] Protection Profiles stellen produktunabhängige Profile zur Bewertung bestimmter IT-Produkte dar. Aus ihnen kann für konkrete Produkte ein sogenanntes Security Target, sprich spe-

[315] Bereits in der Begründung zum ProdHaftG wird auf das Problem veralteter Normen hingewiesen: BT-Drucks. 11/2447, 19; ferner *Bartl*, § 3 ProdHaftG, Rn. 43.
[316] Näher dazu unter http://www.bsi.bund.de.
[317] Zur Entwicklung s. *Münch*, RDV 2003, 223.
[318] *Mackenbrock*, http://www.bsi.de/cc/cc_20d.htm; *Ernestus*, DuD 2003, 68; *Probst*, DSB 2003, Heft 5, 10.
[319] *Probst*, DSB 2003, Heft 5, 10.
[320] Common Criteria v3.0 Rev. 2 Teil 1, http://www.bsi.bund.de/cc/CCMB2005V3T2.pdf, Rn. 119 ff.
[321] *Ernestus*, DuD 2003, 68; *Probst*, DSB 2003, Heft 5, 10; *Roßnagel*, Freundesgabe für Büllesbach, S. 131 (141); eine Liste der aktuell registrierten Schutzprofile findet sich unter http://www.bsi.de/cc/pplist/pplist.htm.

zielle Sicherheitsvorgaben, erstellt werden, gegen das dann die Evaluation durchgeführt werden kann.[322] Ein Protection Profile besteht u.a. aus der Beschreibung des Sicherheitsproblems, der Spezifizierung von Sicherheitszielen sowie der notwendigen Anforderungen an das Produkt, um den Sicherheitszielen genügen zu können.[323]

153 Zusammen können Common Criteria und Protection Profiles den nötigen Mindest-IT-Sicherheitsstandard bezogen auf ein bestimmtes Anwendungsgebiet ergeben. Für eine bestimmte Produktklasse stellt ein Protection Profile, sofern es vorliegt, eine entsprechende Normierung für diese Produktklasse dar. Damit können sie als Orientierung für die Pflichtenbestimmung dienen und wirken als Mindeststandard bzw. als Festlegung der allgemein **anerkannten Regeln der Technik** im Sinne der Überzeugung aller Fachleute in einem Technikgebiet (zum Begriff der anerkannten Regeln der Technik s. Rn. 146). Anders formuliert, können durch die Festlegung von Protection Profiles die Mindestanforderungen an alle Produkte, die die im Protection Profile enthaltenen Ziele erfüllen sollen, im Wege eines Mindeststandards bzw. der Schwelle der zu erfüllenden Anforderungen bei Produktion und Vertrieb eines entsprechenden Produkts im Sinne eines Pflichtenprogramms wie bei anderen Normierungen verbindlich festgelegt werden. Damit kommt den Protection Profiles im Zusammenspiel mit den Common Criteria aber auch eine erhebliche Bedeutung hinsichtlich der Konkretisierung der im Verkehr erwarteten Sicherheit zu – was sich im Bereich der mit der Einhaltung (oder Verletzung) der allgemein anerkannten Regeln der Technik verknüpften Vermutungswirkungen auswirkt.[324]

(c) Zwischenergebnis

154 Nach dem derzeitigen Stand können Standards grundsätzlich nur sektorspezifisch Wirkung entfalten. Dies wird vor allem bei Softwarestandards wie z.B. den Common Criteria und den Protection Profiles deutlich. Es wird zwar versucht, die Profile möglichst allgemein zu halten, dennoch betreffen sie nur einen speziellen Anwendungsfall.

155 Allerdings entspricht gerade eine sektorspezifische Regelung den allgemeinen Regeln der Produkthaftung, etwa wenn die Haftung des Herstellers durch besonderes Expertenwissen auf Seiten des Nutzers oder besondere Einsatzgebiete (die aber dem Herstel-

---

[322] *Mackenbrock*, http://www.bsi.de/cc/cc_20d.htm.

[323] Common Criteria v3.0 Rev. 2 Teil 1, http://www.bsi.bund.de/cc/CCMB2005V3T1.pdf, Rn. 272; dazu auch *Probst*, DSB 2003, Heft 5, 10 ff.

[324] S. unten Rn 174 ff.

ler bekannt sein müssen) beeinflusst werden kann. Die Standardisierungen können demnach rechtlich beachtlich als Konkretisierung der Verkehrspflichten und der geschuldeten Sorgfalt herangezogen werden, wenn sie auf das aktuell hergestellte Produkt passen. Sollte nur ein Teil des Profiles nicht aussagekräftig genug oder nicht allein anwendbar sein, so treffen den Hersteller die Pflichten des Standards nicht. Sofern jedoch ein entsprechend anwendbarer Standard besteht, kann er auch sektorspezifisch angewendet werden.

(6) Haftungsrechtliche Bedeutung von Zertifikaten

156 Im Gegensatz zum öffentlichen Produktsicherheitsrecht, das dem Zertifikat Vermutungswirkungen beimisst,[325] sind dessen zivil- bzw. haftungsrechtliche Auswirkungen gesetzlich nicht ausdrücklich geregelt und bislang **nicht abschließend geklärt**. Hierbei sind zwei grundlegende Fragen zu unterscheiden: erstens, ob Zertifikaten – seien es Zertifikate des BSI oder privater Zertifizierungsunternehmen – eine haftungsbefreiende Wirkung zukommt (dazu Rn. (a)) und – zweitens –, ob Zertifizierungen geeignet sind, die Sicherheitserwartungen der Nutzer von IT-Produkten für die Bestimmung des Inhalts der Herstellerpflichten maßgebend zu beeinflussen (dazu Rn. (b)).

(a) Keine pauschale Haftungsfreizeichnung durch Zertifizierung

157 Zertifikate bewirken keine pauschale Entlastung des Herstellers im Sinne einer abschließenden Definition der vom Hersteller einzuhaltenden Sicherheitsanforderungen. Selbst einer **behördlichen Genehmigung oder Zulassung** wird eine pauschale Rechtfertigungswirkung gegenüber der zivilrechtlichen Haftung von der ganz hM versagt, da diese jeweils nur den **Mindeststandard** konkretisieren, den Hersteller im Übrigen aber nicht von eigenverantwortlichen Gefahrenerforschung und Gefahrenabwehr befreien.[326] Auch insoweit gilt, dass der zivilrechtliche Sorgfaltsmaßstab „deliktsautonom“ zu bestimmen ist und die haftungsrechtliche Verantwortung nicht vom Hersteller auf den Zertifizierer übergeht.[327]

---

[325] S. § 8 Abs. 2 Satz 3, 4 GPSG für das CE-Kennzeichen und das GS-Zeichen und unten Rn. 253 ff.

[326] *Spindler*, Unternehmensorganisationspflichten, S. 833; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 253, 490; Soergel-*Krause*, Anh II § 823 BGB Rn. 48, Anh III § 823 BGB Rn. 16; MünchKommBGB-*Wagner*, § 823 BGB Rn. 275 f.; Staudinger-*Hager* § 823 BGB, E Rn. 34; *Laranz/Canaris*, § 76 III 4 f, S. 416; *Foerste*, in v.Westphalen, ProdHaftHdb, § 24 Rn. 94.

[327] Bamberger/Roth-*Spindler*, § 823 BGB Rn. 490; Soergel-*Krause*, Anh II § 823 BGB Rn. 48.

158 So hat beispielsweise der BGH der behördlichen Betriebserlaubnis für ein Kfz eine entlastende Wirkung zugunsten des Herstellers versagt.[328] Durch die behördliche Genehmigung geht die Verantwortung grundsätzlich nicht vom Hersteller auf die Behörde über.[329] Er darf sich folglich nicht darauf verlassen, eine Genehmigungs- oder Zulassungsbehörde werde etwaige Mängel aufdecken und dann die Genehmigung bzw. Zulassung versagen.[330] Rechte Dritter werden durch öffentlich-rechtliche Genehmigungen nur insoweit ausgeschlossen, als verwaltungsrechtliche Fachgesetze eine Präklusion privater Rechte Dritter ausdrücklich anordnen (z.B. § 14 BImSchG; § 11 WHG).[331]

159 Diese Grundsätze gelten erst Recht für Prüfungen und Zertifizierungen durch den **TÜV** oder sonstige private Zertifizierungsunternehmen. Insbesondere die Verleihung des **GS-Zeichens** („Geprüfte Sicherheit", s. § 7 GPSG und unten Rn. 250) kann den Hersteller damit nicht *pauschal* entlasten.[332] Außerhalb des Bereichs der Produkthaftung hat das OLG Hamm TÜV-Gerätesicherheitsprüfungen im Rahmen der Konkretisierung der berechtigen Sicherheitserwartungen als Indiz herangezogen und einer TÜV-Genehmigung für den Betrieb einer Anlage eine indizielle Bedeutung dafür zugesprochen, dass die Anlage den Sicherheitserwartungen der Benutzer entspricht.[333]

160 Auch **Zertifizierungen und Prüfungen nach der Neuen Konzeption der EU** über Produktsicherheit berühren nicht die zivilrechtliche Haftung des Herstellers.[334] Auch insoweit ist zu bedenken, dass sich die Konformitätsbewertung jeweils nur auf die in den Richtlinien festgelegten Sicherheitsanforderungen bezieht, welche nur den Mindeststandard wiedergeben und nicht zwangsläufig identisch mit dem zivilrechtlichen Verkehrspflichten sind.[335] Das **CE-Kennzeichen** (unten Rn. 248) mag zwar als „formales

[328] BGH NJW 1987, 1009 (1011); BGH NJW 1987, 372 (373).

[329] BGH NJW 1987, 372 (373); Kullmann/Pfister-*Kullmann*, Kz. 1520, S. 5; *Foerste*, v.Westphalen, ProdHaftHdB, § 24 Rn. 94; *Schmidt-Salzer*, Produkthaftung², III/1, Rn. 4.761.

[330] BGH NJW 1987, 372 (373); BGH NJW 1987, 1009 (1011).

[331] Bamberger/Roth-*Spindler*, § 823 BGB Rn. 19; MünchKommBGB-*Wagner*, § 823 BGB Rn. 275, 307 f.; *Wagner*, Öffentlich-rechtliche Genehmigung und zivilrechtliche Rechtswidrigkeit, S. 123 ff.; *Foerste*, in v.Westphalen, ProdHaftHdb, § 24 Rn. 95.

[332] Siehe BGH NJW-RR 1990, 406 f.; s. auch OLG Celle NJW 2003, 2544 (2545); MünchKommBGB-*Wagner*, § 823 BGB Rn. 578.

[333] OLG Hamm NJW-RR 2001, 1248 (1249): Die Einhaltung der normativen Voraussetzungen (TÜV-Genehmigung) für den Betrieb einer Anlage (hier: Nautic-Jet-Sprungboot) spricht indiziell dafür, dass die Anlage den Sicherheitserwartungen der Benutzer entspricht.

[334] *Niebling,* DB 1996, 80 (81); *Niebling*, Die CE-Kenzeichnung, S. 23 f.; *Foerste*, in: v.Westphalen, ProdHaftHdb, § 24 Rn. 94; Bamberger/Roth-*Spindler* § 823 BGB Rn. 490; *Wilrich*, § 6 GPSG Rn. 31.

[335] S. dazu *Taupitz*, in: Produktverantwortung und Risikoakzeptanz, S. 119 (134 ff.).

Schutzschild“[336] gegen behördliche Maßnahmen wirken, enthält aber keine Qualitätsaussage[337] und kann den Hersteller keinesfalls von der Produkthaftung entlasten. Dies gilt unabhängig davon, ob der Hersteller selbst oder eine (neutrale) benannte Stelle die Konformitätsbewertung durchgeführt hat.[338] § 6 Abs. 4 MPG (als Umsetzung der Medizin-Produktrichtlinie, die dem New Approach folgt) stellt ausdrücklich klar, dass die Durchführung eines Konformitätsbewertungsverfahrens die zivil- und strafrechtliche Verantwortlichkeit unberührt lässt.

161 Die dargestellten Grundsätze gelten auch für Zertifikate des BSI oder privater Zertifizierungsunternehmen in Bezug auf **IT-Produkte**. Zertifizierungen können auch hier in aller Regel nicht per se haftungsbefreiend wirken. Der Aussagegehalt einer Zertifizierung anhand technischer Normen, welche – wie oben (Rn. 146) ausgeführt – stets nur den Mindeststandard widerspiegeln, beschränkt sich naturgemäß auf die Dokumentation der Einhaltung der (Mindest-)Anforderungen der technischen Norm. Von der Frage der pauschalen Haftungsentlastung ist die Bedeutung von Zertifikaten im Rahmen des Nachweises der Einhaltung der erforderlichen Sicherheitsanforderungen zu unterscheiden (dazu unten Rn. 181 ff.).

(b) Verschärfung der Haftung durch Zertifizierung?

(i) Grundsätze

162 Schwieriger ist die Frage, inwiefern sich Zertifikate auf die Sicherheitserwartungen der maßgeblichen Verkehrskreise auswirken können. In beschränktem Umfang dürften Zertifikate bei der Bestimmung des Inhalts von Verkehrspflichten relevant werden, sofern Produktzertifikate Einfluss auf die Erwartungen der Nutzer nehmen. Mit Zertifikaten können – insbesondere bei Werbung mit dem Zertifikat – beim Kunden oder Verbraucher **erhöhte Erwartungen hinsichtlich Sicherheit und Qualität** begründet werden, an denen sich das jeweilige zertifizierte Unternehmen festhalten lassen muss, wenn seine Produkte oder seine Produktionstätigkeit von diesen Erwartungen abweichen.[339] Zer-

[336] So *Wilrich*, § 4 GPSG Rn. 26, § 8 GPSG Rn. 18.

[337] *Klindt*, EuZW 2002, 133 (135 Fn. 27); *Niebling*, DB 1996, 80; *Niebling*, Das CE-Kennzeichen, S. 15; *Wilrich*, § 6 GPSG Rn. 6.

[338] Siehe dazu auch *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfaßten Richtlinien, S. 45: „Die Gesamtverantwortung für die Konformität eines Produktes mit allen Anforderungen der anzuwendenden Richtlinie verbleibt jedoch immer beim Hersteller, selbst wenn einige Etappen der Konformitätsbewertung unter der Verantwortung einer benannten Stelle durchgeführt werden“.

[339] *Spindler*, Unternehmensorganisationspflichten, S. 815; Vgl. *Wagner/Janzen*, BFuP 1994, 573 (596 f); insofern auch *Kassebohm/Malorny*, ZfB 1994, 693 (701 f).

tifikate können die Einhaltung eines generell höheren Sicherheitsniveaus suggerieren, da durch eine entsprechende Sicherheitsorganisation die Wahrscheinlichkeit von Fehlern beim Pflichtigen verringert werden soll. Dabei kommt es nicht auf die objektive Geeignetheit solcher Zertifikate zur Feststellung einer ordnungsgemäßen Produktbeschaffenheit an, sondern nur, wie im Rahmen von Werbeaussagen, auf deren generelle Eignung, gesteigerte Sicherheitserwartungen bei den Adressaten hervorzurufen.

163 Auch Zertifikate hinsichtlich des **Qualitätsmanagements wie DIN EN ISO 9000 ff.** können durchaus für sich eine deutliche Aussage auch für den Bereich der Werbung enthalten. Die Werbung mit dem Zertifikat ist relativ leicht mit der Werbung in Einklang zu bringen, dass ein hoher Qualitätsstandard bei der Softwareerstellung verfolgt wird. Unter Zugrundelegung ähnlicher Erfahrungen bzw. Kenntnis z.B. über den Automobilbereich können leicht Parallelen gezogen werden, die eine zumindest laienhafte Bewertung eines Qualitätsmanagement im Softwarebereich ermöglichen. Damit können Zertifikate **im Bereich Qualitätsmanagement** durchaus **Einfluss auf die Sicherheitserwartunge**n nehmen.[340]

(ii) Anwendung auf IT-Hersteller

164 Derzeit wird man davon auszugehen müssen, dass die Sicherheitserwartung der Nutzer aufgrund von **Zertifikaten für IT-Produkte** erst dann signifikant steigen, wenn sich einzelne Prüfmethoden in einem Produktbereich durchgesetzt haben und in Nutzerkreisen einen entsprechenden Bekanntheitsgrad erreicht haben. Beispielsweise die Zertifikat-Angabe, dass ein Produkt einem gewissen Protection Profile mit einer bestimmten Vertrauenswürdigkeitsstufe genügt, kann erst dann die Sicherheitserwartungen der Nutzer maßgeblich beeinflussen, **wenn Existenz *und* Inhalt der Zertifizierung weitgehend bekannt** sind.

165 Bei den Common Criteria erfolgt eine **Zertifizierung anhand eines Protection Profile** und den entsprechenden Zertifikatsbedingungen wie z.B. besonderer Konfigurationen. Zudem kann der Hersteller auch die Vertrauenswürdigkeitsstufe des Zertifikats wählen. Der tatsächliche Inhalt eines Zertifikats ergibt sich somit aus dem Dreigespann von Profil, Bedingungen und Vertrauenswürdigkeitsstufe. Zwar können das Profil und die Stufe als objektivierter Maßstab angesehen werden, dennoch verkompliziert sich die Aussage erheblich. Nimmt man die vom Hersteller vorgegebenen Bedingungen hinzu, so lassen

[340] Ausführlich *Spindler*, Unternehmensorganisationspflichten, S. 815 f.

sich bereits bei demselben Produkt keine eindeutigen Aussagen mehr treffen. Die Aussage, ein Produkt an sich entspreche einem Profil in einer bestimmten Vertrauenswürdigkeitsstufe, könnte also nur als allgemeingültig angesehen werden, wenn das Zertifikat sich auf die Auslieferungskonfiguration beziehen würde, und Änderungen an der Konfiguration nicht auch Änderungen des Sicherheitsstandards nach sich ziehen würden. Eine sinngemäße Übertragung einer vom Nutzerkreis vorgestellten Sicherheitsstufe von einem Produkt auf ein anderes der gleichen Produktklasse wird damit erheblich erschwert. Selbst unter Annahme der Bekanntheit der Common Criteria und des Profils wäre somit eine Einordnung schwierig. Hinzu kommt die **Unbekanntheit** der Common Criteria sowie die Vielzahl der möglichen Protection Profiles.

166 Zur angemessenen Bewertung des Evaluierungsergebnisses muß auch der **Evaluierungsreport** berücksichtigt werden.[341] Insbesondere Prüftiefe, Prüfmethoden und –bedingungen geben erst gemeinsam eingehend Auskunft über die Qualität des Zertifikats. Der Hersteller des Produkts kann sich bzw. sein Produkt nämlich unterschiedlich strengen Evaluationen unterziehen. Das erhaltene Zertifikat sagt demnach nur unter Berücksichtigung auch des Prüfungsumfangs etwas über den eingehaltenen Standard aus. Bei Betrachtung dieser Bewertungskriterien als Grundlage für eine gesteigerte Sicherheitserwartung durch den Einsatz eines Zertifikats wird deutlich, dass der durchschnittliche Nutzer aus der bloßen Konfrontation mit einem solchen Standard **ohne weitergehende Informationen bzgl. Inhalt und Verlässlichkeit der Sicherheitsprüfung** häufig **keinerlei Rückschlüsse** ziehen kann. Der Einsatz eines Produktzertifikats im Bereich der IT-Produkte kann also in der Regel die Sicherheitserwartungen der entsprechenden Kreise nicht steigern.

167 Die Normenreihe **DIN EN ISO 9000 ff.** stellt auch im IT-Bereich ein branchenübergreifendes Qualitätssicherungsmodell dar, dessen Anwendung auf die Softwareentwicklung in DIN EN ISO 9000-3 vermittelt wird. Sowohl auf Seiten des Softwareherstellers, als auch auf Seiten des -einkäufers ist die Regelung zur unabhängigen Überprüfung der Qualitätssicherungsmaßnahmen auf große Resonanz gestoßen.[342] Dennoch sind diese Normen für die Sicherheitserwartung der Käufer und somit für die Haftung nach § 823 Abs. 1 BGB insofern nur von begrenzter Bedeutung, als dass sie praktisch nur bei Softwarekäufen zwischen Unternehmen und im Wesentlichen auch nur bei Individualsoft-

[341] Ebenso *Fuhrberg/Häger/Wolf*, Internet-Sicherheit, Kap. 2.4.2 (S. 46).

[342] *Sodtalbers*, Softwarehaftung im Internet, Rn. 274; *Thaller*, ISO 9001, S. 25; *Wilhelm*, DuD 1995, 330 (331, 335).

ware herangezogen werden.[343] Nur in diesem abgesteckten Rahmen kann die Einhaltung der Sicherheitsnormen auch die Verkehrserwartung beeinflussen.

168 Zusätzlich stellen die Normen **nur Anforderungen an das Software-Produktionsverfahren**: Da Softwareprodukte aufgrund ihrer Komplexität praktisch nicht fehlerfrei zu konstruieren sind,[344] zielt das effektive Qualitätsmanagement darauf ab, die Bedingungen bzw. ein Umfeld dafür zu schaffen, möglichst hochwertige und fehlerarme Produkte zu schaffen. Inhaltlich wird jedoch im Unterschied zu Produktsicherheitszertifikaten nicht die Eigenschaft und Qualität der Software selbst unter sicherheitstechnischen Aspekten überprüft, weshalb die Einhaltung der Normen nicht automatisch einen bestimmten Sicherheitsstandard der Software sichern kann.[345] Die Zertifizierung dient demnach nur der Einhaltung von Qualitätsstandards.

(7) Beweislast

(a) Produkthaftungsrechtliche Beweislastverteilung

169 Auch für IT-Produkte greifen die von der Rechtsprechung entwickelten Regeln zur Beweislastumkehr zugunsten des Geschädigten ein. Danach obliegt dem Geschädigten der Beweis der Rechtsgutsverletzung, des Produktfehlers sowie der Nachweis, dass der Produktfehler im Organisationsbereich des Herstellers entstanden ist und bereits im Zeitpunkt des Inverkehrbringens vorlag.[346] Hinsichtlich der **objektiven Verkehrspflichtverletzung** als auch des **Verschuldens** greift zugunsten des Geschädigten eine Beweislastumkehr ein,[347] wonach sich der Hersteller in Bezug auf alle seine Hilfskräfte zu entlasten hat.[348]

170 Keine Beweiserleichterung nicht aber dafür greift dagegen hinsichtlich des Umstandes, dass bei ordnungsgemäßer **Instruktion** der Schaden nicht eingetreten wäre.[349] Auch bei Verletzungen der **Produktbeobachungspflicht** greift keine Beweislastumkehr zugunsten des Geschädigten hinsichtlich des objektiven Pflichtverstoßes ein, da hier nur all-

---

[343] *Burgartz/Blum*, QM-Optimizing der Softwareentwicklung, S. 178; *Sodtalbers*, Softwareentwicklung im Internet, Rn. 275.

[344] OLG Hamburg CR 1986, 83 (84); LG Heidelberg CR 1989, 197 (198); *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 37, 40 f.; MünchKommBGB-*Wagner*, § 3 ProdHaftG Rn. 15.

[345] *Wilhelm*, DuD 1995, 330 (335); *Sodtalbers*, Softwarehaftung im Internet, Rn. 275; *Koch*, Computer-Vertragsrecht, Rn. 287.

[346] Bamberger/Roth-*Spindler*, § 823 BGB Rn. 553; MünchKommBGB-*Wagner*, § 823 BGB Rn. 612.

[347] Vgl. BGHZ 80, 186 (196 f.); bestätigt wiederum in BGH NJW 1996, 2507 (2508); BGH NJW 1999, 1028; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 30 Rn. 46 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 608; Staudinger-*Hager*, § 823 BGB Rn. F 43.

[348] BGH NJW 1968, 247 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 609.

[349] Vgl. BGH DB 1999, 891 (891); OLG Frankfurt NJW-RR 1999, 27 (30).

gemein zugängliche Informationen in Rede stehen, zu denen der Geschädigte notfalls durch Sachverständigengutachten ebenso Zugang wie der Hersteller hat.[350]

171 Die von der Rechtsprechung entwickelte **Befundsicherungspflicht** des Herstellers, sich vor Inverkehrgabe seiner Produkte über den Status bzw. Befund seiner Produkte und deren etwaige Fehlerhaftigkeit zu vergewissern, und der damit verbundenen Beweislastumkehr hinsichtlich des Vorliegens eines Fehlers bei Inverkehrgabe des Produktes[351] kann nicht übertragen werden. Denn diese Pflicht beschränkt sich auf diejenigen Produkte, deren erhebliche Risiken für den Verbraucher „in der Herstellung geradezu angelegt sind und deren Beherrschung deshalb einen Schwerpunkt des Produktionsvorganges darstellt, so dass über die übliche Warenendkontrolle hinaus besondere Befunderhebungen des Herstellers erforderlich sind“[352]. Gerade daran fehlt es aber bei den stets identischen Produkten im Bereich des Softwarevertriebs.[353]

172 Die Beweislast für die **Kausalität** des Produktfehlers bzw. der Verkehrspflichtverletzung des Herstellers für die eingetretene Rechtsgutsverletzung trägt der Geschädigte.[354] Eine Beweislastumkehr greift ferner grundsätzlich **nicht** ein. Der Geschädigte muss daher beispielsweise den Einwand des Herstellers, der Schaden sei auf einen Fehlgebrauch des Produktnutzers daher widerlegen.[355] Doch kann im Einzelfall ein **Beweis des ersten Anscheins** in Betracht kommen, wenn es beispielsweise im Zusammenhang mit der Verwendung des betreffenden Produkts zu parallelen Schadensfällen gekommen ist (zur Nichteinhaltung technischen Normen unten Rn. 179).[356]

173 Gerade bei **IT-Produkten** ist der Nachweis der haftungsbegründenden Kausalität in der Praxis für den Geschädigten schwer zu führen, da er häufig mit dem Einwand konfrontiert wird, dass sein Schaden auf anderen Ursachen – insbesondere andere schadhafter

---

[350] Vgl. die in BGHZ 80, 186 (195 ff.); s. auch BGHZ 116, 69 (72 f.) aufgestellten Grundsätze, wonach ab Inverkehrgabe der Geschädigte die Verletzung der Pflicht zu beweisen hat; *Prütting*, in: Produktverantwortung und Risikoakzeptanz, S. 49 (52); krit. demgegenüber *Foerste,* in: v. Westphalen, ProdHaftHdb, § 30 Rn. 89; MünchKommBGB-*Wagner*, § 823 BGB Rn. 611; *Tiedtke*, in: FS Gernhuber, S. 471 (480 f.).

[351] BGHZ 104, 323 (332 ff.); BGH NJW 1993, 528 (529); bestätigt in BGHZ 129, 353 (361 f., 365 f.); ausführlicher dazu Bamberger/Roth-*Spindler*, § 823 BGB Rn. 500 f. mwN.

[352] So BGH NJW 1993, 528 (529); OLG Dresden NJW-RR 1999, 34, Rev. vom BGH nicht angenommen, Beschl. v. 26. Mai 1998 VI ZR 294/97, referiert bei *Kullmann*, NJW 1999, 96 (101); *Kullmann,* NJW 1994, 1698 (1705); Kullmann/Pfister-*Kullmann*, Kz. 1520 S. 35 f.; krit. *Rolland*, Produkthaftungsrecht Teil II Rn. 42a: kaum kalkulierbar.

[353] Ausführlicher dazu *Spindler*, NJW 1999, 3737 (3741 f.).

[354] BGH NJW 1989, 1542 (1545); BGH NJW 1992, 560 (562f.); MünchKommBGB-*Wagner*, § 823 BGB Rn. 614.

[355] *Foerste*, in: v.Westphalen, ProdHaftHdB, § 30 Rn.95.

[356] *Foerste*, in: v.Westphalen, ProdHaftHdB, § 30 Rn. 99 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 614; Staudinger-*Hager*, § 823 BGB Rn. F 39.

Software oder mangelhafter Installation – beruht. Gerade in diesem Zusammenhang kommt daher Beweiserleichterungen besondere Bedeutung zu.

(b) Beweisrechtliche Bedeutung technischer Normen

174 Die Rechtsprechung geht zunächst davon aus, dass für technische Normen eine tatsächliche Vermutung für die Wiedergabe der anerkannten Regeln der Technik eingreift (oben Rn. 147). Zumindest im Ausgangspunkt lässt sich die **Einhaltung einer technischen Norm** daher mit der Einhaltung der im Verkehr erforderlichen Sorgfalt gleichsetzen, wobei überwiegend wohl von einem starken **Indiz** für die Wahrung der Sorgfalt[357], zum Teil aber auch eine tatsächliche Vermutung (Anscheinsbeweis) angenommen wird[358]. Einschränkend gilt hier jedoch, dass die Einhaltung einer technischen Norm die Gewährleistung des erforderlichen Sicherheitsstandards nur dann indiziert, wenn die technische Norm die jeweiligen Gefahren ausreichend berücksichtigt hat, also z. B. auch besonders gefährdete Verkehrskreise einbezog.[359] Hierzu ist der Zweck der betreffenden technischen Norm durch Auslegung zu ermitteln.[360] Ebenso bewahrt die Befolgung der Norm nicht vor dem Rechtswidrigkeitsvorwurf, wenn eine technische Norm nicht dem Stand der Technik entspricht, insbesondere wenn die technische Regel falsch oder unzureichend ist[361]. Ähnlich behandelt auch das brititsche Recht technische Standards.[362] Begründete Zweifel an der Richtigkeit von technischen Regeln, z. B. wegen neuerer technischer Erkenntnisse, zwingen zur Aufklärung des technischen Sachverhalts durch den Pflichtigen.[363] In ähnlicher Weise verfährt die österreichische Rechtspre-

[357] Ausdrücklich OLG Celle NJW 2003, 2544; Soergel-*Krause*, Anh III § 823 BGB Rn. 16; *Foerste*, in: v. Westphalen, ProdHaftHdB, § 24 Rn 41; *Vieweg*, in: Schulte, Handbuch des Technikrechts, S. 362; *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 167.

[358] So *Marburger*, Die Regeln der Technik im Recht, S. 464; *Marburger*, VersR 1983, 597 (602 f.).

[359] Vgl. BGH NJW 1987, 372 – Zinkspray – für Technische Regeln für Druckgase TRG 300 vom Mai 1978; OLG Zweibrücken NJW 1977, 111 f; *Marburger*, VersR 1983, 597 (600); *Brüggemeier*, DeliktsR, Tz. 579; *Foerste*, in: v.Westphalen, ProdHaftHdb, § 24 Rn. 41; *Schmidt-Salzer*, Produkthaftung², Bd. III/1, Rn. 4.756. S. dagegen als Negativbeispiel OLG Saarbrücken VersR 1997, 377 (378 f), das DIN-Normen praktisch als eine Art gesetzliche Konkretisierung von Verkehrspflichten behandelt.

[360] BGH VersR 2002, 247; BGH NJW 2001, 2019 (2020); *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 167 ff.

[361] BGH NJW 1987, 372 (373); BGH NJW 1984, 801; MünchKommBGB-*Mertens*, 3. Aufl. 1997, § 823 BGB Rn. 28, der allerdings in diesem Fall zum Wegfall des Verschuldensvorwurfs tendiert.

[362] S. dazu *Reed* – Annex II – Rn. 1307 ff.

[363] BGH NJW 1982, 1049; *Köhler*, BB 1985, Beil. Nr. 4, 10 (10 f); *Marburger*, Die Regeln der Technik im Recht, S. 462 ff, 466; *Marburger*, VersR 1983, 597 (603).

chung,[364] indem die normgerechte oder sonstigen technischen Standards entsprechende übliche Herstellungsart die Fehlerfreiheit des Produkts indizieren soll.[365]

175 Zum Teil wird auch angenommen, dass die Einhaltung von technischen Standards geeignet ist, den Pflichtigen **von einem Verschulden zu entlasten**,[366] auch wenn mitunter grundsätzliche Zweifel an der Objektivität und Neutralität privater Normierungsgremien bestehen[367]. Jedenfalls hat die Rechtsprechung stets betont, dass die Haftung des Verkehrspflichtigen trotz Einhaltung einer DIN-Norm eingreifen kann, wenn die (technische) Entwicklung über sie hinweggegangen ist oder sich bei der Benutzung Gefahren zeigen, die in den DIN-Normen noch nicht berücksichtigt sind.[368] Der Pflichtige muss daher stets prüfen, ob die technische Norm in der gegebenen Situation anwendbar ist und ob sie für den konkreten Fall ausreicht, insbesondere über die technischen Regelwerke hinaus neuere Erkenntnisse berücksichtigen, vor allem wenn die betreffende Norm älteren Ursprungs ist, oder Divergenzen zwischen verschiedenen Normen bestehen.[369] Gerade wenn die technische Norm keine abschließende Erfassung sämtlicher relevanten Fragen enthält, muss der Anwender sorgfältig untersuchen, ob er weitere Maßnahmen für den konkreten Einzelfall zu treffen hat.[370]

176 Bei **Nichteinhaltung der technischen Regeln** wird zum Teil ein Anscheinsbeweis für eine Verkehrspflichtverletzung bejaht,[371] was in dieser Pauschalität indes nicht zutrifft, da technische Normen keine zwingenden Verhaltensnormen und abweichende, tech-

---

[364] OGH 6 Ob 73/04k; 3 Ob 547/95; 6 Ob 157/98a.

[365] S. dazu den Bericht von *Fallenböck* Annex II – Österreich - Rn. 1114 ff.

[366] So für die ISO 9000 ff *Heussen/Schmidt*, CR 1995, 321 (328); *Schlutz*, PHI 1996, 122 (123, 135); *Adams/Löhr*, QZ 36 (1991), 24 (26); allgemeiner wohl auch *Marburger*, AcP 192 (1992), 1 (11); *Möllers*, Rechtsgüterschutz im Umwelt- und Haftungsrecht, S. 244; *Möllers*, DB 1996, 1455 (1460 f); *Cosack*, Umwelthaftung im faktischen GmbH-Konzern, S. 61; vorsichtiger *Ensthaler/Füßler/Nuissl*, Juristische Aspekte des Qualitätsmanagements, S. 195: ISO 9004 grundsätzlich geeignet, aber ergänzungsbedürftig; generell für die Einhaltung von technischen Regelwerken als Wahrung der erforderlichen Sorgfalt *Marburger*, VersR 1983, 597 (602 f); *v. Westphalen*, DB 1987, Beil. Nr. 11 S. 10. Gegen ein Entfallen des Verschuldensvorwurfs *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 168.

[367] Abl. daher generell zur Haftungsentlastung durch Einhaltung von DIN-Normen bzw. allgemein anerkannten Regeln der Technik *Huth*, Die Bedeutung technischer Normen, S. 210 ff.

[368] BGH NJW 1994, 3349 (3350); OLG Hamm VersR 1996, 1517 (1518).

[369] BGH NJW 1984, 801 (802); BGH NJW 1987, 372 (373); im Werkvertragsbereich BGH NJW 1998, 2814 (2815); *Foerste*, in: v. Westphalen, ProdHaftHdB, § 24 Rn. 42; *Schmidt-Salzer*, Produkthaftung[2], Bd. III/1, Rn. 4.754 f; *Hollmann*, DB 1985, 2389 (2395); RGRK[12]-*Steffen*, § 823 BGB Rn. 277; Kullmann/Pfister-*Kullmann*, Kz 1520 S. 13 f; *Schmatz/Nöthlichs*, Sicherheitstechnik, Bd. I Teil 1, § 3 GSG Anm. 5.3.3 zur Produkthaftung; *Falke*, Rechtliche Aspekte der Normung in den EG-Mitgliedsstaaten und der EFTA, S. 451 f.; restriktiver *Marburger*, Die Regeln der Technik im Recht, S. 467 f; *Marburger*, VersR 1983, 597 (602 f.) mwN., der eine generelle Prüfungspflicht nur für die besondere Risikolage annimmt, nicht aber hinsichtlich der Richtigkeit der Regel; dagegen *Huth*, Die Bedeutung technischer Normen, S. 208 f.

[370] Vgl. *Schmidt-Salzer*, Produkthaftung[2], Bd. III/1, Rn. 4.757; *Marburger*, VersR 1983, 597 (603); *Huth*, Die Bedeutung technischer Normen, S. 219 ff.; insoweit auch *Bayer*, Auswirkungen eines zertifizierten Qualitätsmanagementsystems, S. 102, 105; übertragen auf die Arzthaftung im Hinblick auf Qualitätsmanagementsysteme *Steffen*, in: FS Deutsch, S. 799 (807 f.).

[371] *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 171 mwN.

nisch ebenso sichere Lösungen folglich zulässig sind.[372] Der BGH bejaht im Falle der Nichteinhaltung einer technischen Norm zwar keinen Anscheinsbeweis für die Pflichtwidrigkeit, geht aber zumindest von einer starken **Indizwirkung** des Verstoßes gegen technische Normen für das Vorliegen einer Verkehrspflichtverletzung aus.[373]

177 In der Literatur wird überwiegend wird eine differenzierende Betrachtungsweise zugrunde gelegt. Die Nichteinhaltung einer technischen Norm ist danach regelmäßig mit der Verletzung einer Verkehrspflicht gleichzusetzen, wenn jegliche Sicherheitsmaßnahmen unterlassen werden oder das Sicherheitsniveau der technischen Norm durch die vom Verkehrspflichtigen gewählte Lösung unterschritten wird.[374] Dem Verkehrspflichtigen steht es aber jederzeit frei, das erforderliche Sicherheitsniveau durch gegenüber der technichen Norm **alternative Lösungen** zu erreichen (Rn. 145). Er trägt in diesem Fall aber die Beweislast dafür, dass die gewählte Sicherheitsleistung den Vorgaben der technischen Norm äquivalent ist.[375] Die Beweislastverschiebung zu Lasten des Herstellers für die Erreichung eines gleichwertigen Sicherheitsniveaus kann im praktischen Ergebnis einer Vermutung für eine Verkehrspflichtverletzung bei der Abweichung von technischen Regelwerken recht nahe.[376]

178 Für den Bereich der **Produkthaftung** ist bei Nichteinhaltung technischer Normen in Bezug auf den Nachweis der *Sorgfaltswidrigkeit* des Herstellerhandelns zu bedenken, dass die Darlegungs- und Beweislast für die Verletzung der äußeren und inneren Sorgfalt ohnehin beim Hersteller liegt (Rn. 169), dieser sich also vom Vorwurf der objektiven Verkehrspflichtverletzung und des Verschuldens entlasten muss. Hier wird der Hersteller in (seltenen) Einzelfällen versuchen nachzuweisen, dass die von ihm gewählte Alternativlösung gleiche oder höhere Sicherheit gegenüber der Norm bietet.[377]

---

[372] *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 171; *Spindler*, Unternehmensorganisationspflichten, S. 805.

[373] BGH VersR 1984, 270 (271); in einer Reihe von Entscheidungen bejaht der BGH die Pflichtwidrigkeit ganz maßgeblich aufgrund des Verstoßes gegen technische Normen: BGH NJW 2004, 1449 (1450); BGH NJW 2001, 2019 (2020); BGH NJW 1991, 2019 (2021); ebenso im Ergebnis die Literatur, wonach das Unterschreiten der technischen Normen regelmäßig eine Verkehrspflichtverletzung darstellt, Soergel-*Krause*, Anh III § 823 BGB Rn. 16; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 39; MünchKommBGB-*Wagner,* § 823 BGB Rn. 578; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 257.

[374] *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 171; *Spindler*, Unternehmensorganisationspflichten, S. 805; *Foerste*, in: v.Westphalen, ProdHaft HdB, § 24 Rn. 20; *Marburger*, Die Regeln der Technik im Recht, S. 470.

[375] MünchKommBGB-*Wagner,* § 823 BGB Rn. 578; *Köhler*, BB 1985 Beilage 4, S. 10 (11); *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 172; *Spindler*, Unternehmensorganisationspflichten, S. 806; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 20; *Marburger*, Die Regeln der Technik im Recht, S. 472.

[376] *Spindler*, Unternehmensorganisationspflichten, S. 806.

[377] *Vieweg*, in: Schulte, Handbuch des Technikrechts, S. 361.

179 Die Beweislast hinsichtlich der **Kausalität** des Produktfehlers bzw. der Verletzung der Herstellerpflichten obliegt im Grundsatz dem Geschädigten (Rn. 172). Steht fest, dass der Hersteller eine technische Norm verletzt hat, spricht nach BGH ein **Anscheinsbeweis** dafür, dass die Schädigung, die in örtlichem und zeitlichem Zusammenhang mit dem Verstoß eingetreten ist, durch die Pflichtverletzung verursacht wurde.[378] Der Schädiger muss den Anscheinsbeweis erschüttern, indem er darlegt und beweist, dass der Schaden auch dann eingetreten wäre, wenn er die Norm eingehalten hätte. Der BGH geht wohl zum Teil von einer Beweislastumkehr aus, wenn er davon spricht, die „Bekl. hätten daher *darzulegen und zu beweisen*, dass die Schäden nicht auf der Verletzung anerkannter Regeln der Technik beruhen".[379]

180 Zusammengefasst haben technische Standards damit eine **dreifache Wirkung**:

- Sie begründen eine Vermutung dafür, dass sie die anerkannten Regeln der Technik wiedergegeben.
- Ihre Befolgung begründet starkes Indiz (nach aA einen Anscheinsbeweis) dafür, dass der Pflichtige die im Verkehr erforderliche Sorgfalt eingehalten hat, sofern keine besonderen Gefahrenlagen vorlagen.
- Ihre Verletzung begründet ein starkes Indiz (nach aA einen Anscheinsbeweis) dafür, dass der Pflichtige die im Verkehr erforderliche Sorgfalt verletzt hat. Steht die Nichteinhaltung einer technischen Norm fest, spricht ein Anscheinsbeweis dafür, dass die Schädigung, die in örtlichem und zeitlichem Zusammenhang mit dem Verstoß eingetreten ist, durch die Pflichtverletzung verursacht wurde

(c) Beweisrechtliche Bedeutung von Zertifikaten

(i) Grundsätze

181 In diesem Rahmen ist auch die beweisrechtliche Bedeutung von erteilten Zertifikaten einzuordnen. Wie oben (Rn. 157) dargestellt, können Zertifikate den Hersteller zwar nicht pauschal von der Haftung entlasten, doch kann ihnen im Einzelfall eine beweisrechtliche Bedeutung zukommen. Auch hier ist indessen Zurückhaltung angebracht. Zudem ist – wie im österreichischen Recht – genau darauf abzustellen, wofür das Zertifikat erteilt wurde, ob für ein Herstellungsverfahren, ein Produkttyp oder für das Pro-

[378] BGH NJW 2001, 2019 (2020); BGH NJW 1991, 2021 (2022); *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 162, 172ff.; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 30 Rn. 103; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 280; Staudinger-*Hager*, § 823 BGB Rn. E 72; Soergel-*Krause*, Anh II § 823 BGB Rn. 74; MünchKommBGB-*Wagner*, § 823 BGB Rn. 272, 316; Palandt-*Sprau*, § 823 BGB Rn. 80; *Marburger*, Die Regeln der Technik im Recht, S. 448 ff., insb. 453 f.

[379] BGH NJW 2001, 2019 (2020); dazu *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 173 f.

dukt selbst; das Zertifikat kann allenfalls für den jeweiligen Bereich eine entlastende Wirkung entfalten.[380]

182 So begründet nach der Rechtsprechung des BGH die **Betriebserlaubnis** für ein Kfz **keine Vermutung für die ordnungsgemäße Beschaffenheit des Produkts**, sondern besagt nur, dass der Kontrollbeamte nichts Vorschriftswidriges gefunden hat. Der Hersteller von Fahrzeugen oder Fahrzeugteilen, für die eine allgemeine Betriebserlaubnis erteilt ist, darf soch folglich nicht darauf verlassen, dass die Zulassungsstelle etwaige Mängel entdeckt.[381] Ein Hersteller wird sich allenfalls dann auf eine behördliche Prüfung verlassen dürfen, wenn durch die gesetzlichen Genehmigungsvoraussetzungen und die personelle und technische Ausstattung der Behörde sowie deren Prüfverfahren gewährleiset ist, dass das Produkt nach den neuesten Erkenntnissen von Wissenschaft und Technik gefahrlos verwendet werden kann.[382]

183 Für eine Prüfung durch den **TÜV** und die Vergabe des **GS-Zeichens** hat der BGH entschieden, dass ein *Hersteller*, der seine Produkte selbst konstruiert, aufgrund der Prüfung nicht ohne weiteres von seiner Haftung für konstruktive Mängel freigestellt wird.[383] In einer neueren Entscheidung geht das OLG Oldenburg davon aus, dass der Endhersteller seine Pflicht zur stichprobenartigen Materialprüfung von Zulieferprodukten im Hinblick auf die große Anzahl der zu verarbeitenden Zulieferteile durch ein eigenes Materialprüfungszertifikat, durch ein entsprechendes TÜV-Zertifikat oder durch ein aussagekräftiges Prüfzertifikat des Herstellers der Zulieferprodukte erbringen könne.[384] Umgekehrt kann die **fehlende TÜV-Zulassung** eine Beweiserleichterung für den Geschädigten (welcher den Produktfehler zu beweisen hat, s. Rn. 169) bieten, indem der Hersteller die sicherheitstechnische Ordnungsmäßigkeit des Produktes zu beweisen hat.[385]

184 Für *andere* in den Herstellungsprozess und den Vertrieb von Produkten eingeschaltete Unternehmer, die in Bezug auf Konstruktionsgefahren geringere Sorgfaltspflichten als

---

[380] S. dazu die Entscheidung des OGH 10 Ob 98/02p, sowie unten Fallenböck – Annex II – Rn. 1139.

[381] BGH NJW 1987, 1009 (1011); BGH NJW 1987, 372 (373); BGH NJW-RR 1990, 406 f.; Kullmann/Pfister-*Kullmann*, Kz. 1520, S. 5.

[382] Kullmann/Pfister-*Kullmann*, Kz. 1520, S. 5; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 96.

[383] BGH NJW-RR 1990, 406 f. unter Hinweis auf BGH NJW 1987, 1009 (1011); BGH NJW 1987, 372 (373); s. auch OLG Celle NJW 2003, 2544; MünchKommBGB-*Wagner*, § 823 BGB Rn. 578.

[384] OLG Oldenburg NJW-RR 2005, 1338 (1339).

[385] OLG Stuttgart bei *Schmidt-Salzer*, Entscheidungssammlung Produkthaftung, II.117 (1 f) – Schleifscheibe –; *Schmidt-Salzer*, Produkthaftung, Bd. III/1, Rn. 4.887.

der eigentliche Hersteller und Konstrukteur des Produktes zu erfüllen haben, können Zertifikate wie das GS-Zeichen weitergehende entlastende Wirkung entfalten.[386] So kann sich ein **Importeur** in Bezug auf seine Pflicht zu stichprobenartiger Untersuchung unter Umständen damit entlasten, dass er ein eingeführtes Gerät durch einen Sachverständigen überprüfen lässt oder es gem. § 3 Abs. 4 GSG aF (jetzt § 7 GPSG) von einer zugelassenen Prüfstelle auf ihre Sicherheit untersuchen lässt.[387] Entsprechendes gilt für den **Auftragsfertiger** im Rahmen der horizontalen Arbeitsteilung, welcher von dem Hersteller des Endprodukts beauftragt worden ist, bestimmte Produktteile unter Verwendung der ihm von dem Endprodukthersteller zur Verfügung gestellten Formen herzustellen.[388]

185 Die in der industriellen Praxis häufig anzutreffenden Zertifikate nach **DIN ISO 9001 ff.** können dem Hersteller nicht seinen Entlastungsbeweis abnehmen,[389] da kein Auditorenteam in den für die Qualitätszertifizierungen üblichen, kurzen Zeitspannen in der Lage sein dürfte, alle möglichen Fehlerquellen einer Betriebsorganisation zu überprüfen.[390] Der Nachweis einer lückenlosen Qualitätsregelung reicht im Bereich der Produkthaftung angesichts der erforderlichen Entlastung hinsichtlich sämtlicher Hilfspersonen,[391] durch deren individuelle Fehlleistung der Produktfehler entstanden oder unentdeckt sein kann, nicht aus.[392] Ebenso wenig darf sich derjenige, der Verkehrspflichten im Wege vertraglicher Arbeitsteilung delegiert, allein auf die Zertifizierung des Übernehmers verlassen.[393]

(ii) Anwendung auf IT-Hersteller

186 Ausgehend von den oben dargestellten Grundsätzen wird man auch Zertifikaten für **IT-Produkte** im zivilen Haftungsrecht nur eine **eingeschränkte beweisrechtliche Bedeutung** beimessen können (zur Bedeutung im öffentlichen Produktsicherheitsrecht siehe unten Rn. 253 ff.). Insbesondere kann ein Zertifikat den konstruktionsveranwortlichen Hersteller regelmäßig nicht entlasten. Bei der Herstellung von Hardwarekomponeten in

---

[386] Bamberger/Roth-*Spindler*, § 823 BGB Rn. 490.

[387] BGH NJW-RR 1990, 406 f.; *Foerste*, in: V.Westphalen, ProdHaftHdB, § 26 Rn. 61; Soergel-*Krause*, Anh III § 823 BGB Rn. 16.

[388] BGH NJW-RR 1990, 406 f.; *Kullmann* NJW 1991, 675 (678 f.).

[389] Anders wohl *Kassebohm/Malorny*, BB 1994, 1361 (1365).

[390] Zutr. *Wagner/Janzen*, BFuP 1994, 573 (596); *Kassebohm/Malorny* ZfB 1994, 693, (701,704).

[391] BGH NJW 1968, 247 ff.

[392] *Bayer*, Auswirkungen eines zertifizierten Qualitätsmanagementsystems, S. 97 ff.; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 560; skeptisch zur Wirkung der Zertifizierung auch *Heussen/Schmidt*, CR 1995, 321 (329).

[393] *Merz*, in: v.Westphalen, ProdHaftHdb, § 44 Rn. 57; ähnlich aus strafrechtlicher Sicht *Goll/Winkelbauer*, in: v.Westphalen, ProdHaftHdb, § 48 Rn. 51.

horizontaler Arbeitsteilung können die oben genannten Grundsätze (Rn. 184) zum Tragen kommen.[394] Gleiches gilt für Software, die allerdings kaum typische Fabrikationsfehler aufweisen wird, da sie 1:1 vom Original kopiert wird, daher allenfalls Kopierfehler etc. eine Rolle spielen können.

187 Der Zertifizierung anhand anerkannter technischer Normen, welche die anerkannten Regeln der Technik wiedergeben, wird im Einzelfall **indizielle Bedeutung** für den Nachweis der Normkonformität des Produkts zukommen. Denn wenn IT-Standards als technische Normen und Mindeststandard eine Aussage über die allgemein anerkannten Regeln der Technik treffen, so ist unter Anwendung der allgemeinen Grundsätze zumindest von einer Inditzwirkung zugunsten des Herstellers auszugehen, wenn er die Einhaltung eben dieses Standards mit einem Zertifikat belegen kann.[395] Auch hier gilt aber, dass sich die allgemein anerkannten Regeln der Technik bereits über die Festlegungen des Standards hinaus entwickelt haben können, so dass trotz Zertifikat eine Prüfung im Einzelfall erfolgen muss.

b) Produkthaftung infolge Schutzgesetzverletzung (§ 823 Abs. 2 BGB): öffentlich-rechtliche Produktsicherheitsnormen

188 Die verschuldensabhängige Produkthaftung nach § 823 Abs. 1 BGB wird durch zahlreiche Schutzgesetze flankiert, deren Verletzung nach § 823 Abs. 2 BGB eine Haftung nach sich ziehen kann. Von Bedeutung sind indes für die Produkthaftung im wesentlichen nur die öffentlich-rechtlichen Normen zur Produktsicherheit, allen voran das als Rahmengesetz für die Produktsicherheit gedachte **Geräte- und Produktsicherheitsgesetz** (GPSG),[396] daneben aber auch Spezialgesetze wie das Medizinproduktegesetz,[397] die individuellen Schutz entfalten können. Da das GPSG als Schutzgesetz nach § 823 Abs. 2 BGB zu qualifizieren[398] und Software nicht vom GSPG ausgenommen ist (näher unten Rn. 209 ff.),[399] sind entsprechende zivilrechtliche Schadensersatzansprüche

[394] Die Herstellung von Software erfolgt regelmäßig nicht im Wege der Arbeitsteilung, sondern alleine durch einen Hersteller.

[395] Bamberger/Roth-*Spindler*, § 823 BGB Rn. 491.

[396] Näher unten Rn. 206 ff.; allgemein zum GPSG *Klindt,* NJW 2004, 465 ff.; *Potinecke*, DB 2004, 55 ff.

[397] *Deutsch/Spickhoff*, Medizinrecht, Rn. 1248; *Foerste,* in: v. Westphalen, ProdHaftHdb, § 32 Rn. 13; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 190.

[398] Zum Schutzgesetzcharakter des GPSG s. *Potinecke*, DB 2004, 55 (60); *Spindler*, NJW 2004, 3145 (3148); *Molitoris*, in: RAnwHdb, C.14 Rn. 221; *Klindt*, GPSG, § 4 GPSG Rn. 75; *Reinicke/Tiedtke*, Rn. 1024; noch zum alten ProdSG: *G. Wagner,* BB 1997, 2541 (2542); *Nickel/Kaufmann,* VersR 1998, 948 (951 f.); *v. Westphalen,* DB 1999, 1369 (1371) *Marburger,* FS Deutsch, 271 (288).

[399] Zur alten Rechtslage nach dem ProdSG Kullmann/Pfister-*Kullmann*, Kz. 2705, S. 8f.

grundsätzlich denkbar[400] - in ähnlicher Weise wie in Österreich.[401] Ein Anspruch des Produktbenutzers besteht aufgrund des eingeschränkten Schutzbereichs des GPSG jedoch nur bei Personenschäden,[402] so dass der Anwendungsbereich des GPSG bei fehlerhaften IT-Produkten gering sein dürfte (unten Rn. 209 ff.). Bei fehlerhaften Medizinprodukten mit Softwaresteuerung (s. § 3 Nr. 1 MPG) können ggf. die Vorschriften des MPG als Schutzgesetz zu Anwendung gelangen.

2. Verschuldensunabhängige Produkthaftung (ProdHaftG)

189 Neben die Haftung nach Deliktsrecht (s. § 15 Abs. 2 ProdHaftG) tritt die verschuldensunabhängige Haftung nach dem ProdHaftG[403], welches der Umsetzung der EG-Produkthaftungsrichtlinie[404] dient. In seiner praktischen Bedeutung bleibt das ProdHaftG wegen seiner engeren Voraussetzungen hinter der deliktischen Haftung zurück. Das ProdHaftG und kann nach § 14 ProdHaftG vertraglich nicht abbedungen werden (§ 14 ProdHaftG).

a) Produktbegriff des ProdHaftG (§ 2 ProdHaftG)

190 § 2 ProdHaftG definiert als Produkt „jede bewegliche Sache, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bildet sowie Elektrizität“. Als bewegliche Sache fällt **Hardware** unproblematisch unter den Produktbegriff des § 2 ProdHaftG. Gleiches gilt für alle Arten körperlicher **Datenträger** als solcher.[405] Ebenso wie in anderen europäischen Ländern, etwa Österreich,[406] ist nach wie vor die Frage umstritten, ob **Software** unter den Produktbegriff des ProdHaftG fällt. Rechtsprechung zu dieser Frage existiert soweit ersichtlich nicht. Teilweise wird die Produkteigenschaft von Software verneint, da es sich hierbei um keine bewegliche Sache (vgl. § 2 ProdHaftG), sondern um ein immaterielles Gut handele.[407] Das Computerprogramm als solches sei von dem körperlichen Datenträger zu unterscheiden. Das ProdHaftG finde

---

[400] Noch zur alten Rechtslage: Kullmann/Pfister-*Kullmann*, Kza 2705 S. 3, 14; *Wagner*, BB 1997, 2541 (2541 f.).

[401] S. dazu den Bericht von *Fallenböck* – Annex II – Rn. 1123.

[402] *Klindt*, GPSG, § 4 GPSG Rn. 8; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 159.

[403] Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz – ProdHaftG) vom 15.12.1989, BGBl. I 1989, S. 2191.

[404] Richtlinie 85/374/EWG des Rates vom 25.7.1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedsstaaten über die Haftung für fehlerhafte Produkte, ABl. EG Nr. L, S. 210.

[405] *Taschner/Frietsch*, § 2 ProdHaftG Rn. 22; Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 68.

[406] S. dazu den Bericht von *Fallenböck* – Annex II – Rn. 1128.

[407] So *Redeker*, NJW 1992, 1739 f.; *Müller-Hengstenberg*, NJW 1994, 3128 (3131); *Honsell*, JuS 1995, 211 (212); *Taschner/Frietsch*, § 2 ProdHaftG Rn. 22.

zwar Anwendung, wenn die Gefahr von der Körperlichkeit der Sache ausgehe, nicht aber wenn sie von der Software herrühre, welche in der Sache verkörpert ist.[408]

191 Die wohl überwiegende Meinung bejaht dagegen zu Recht die Produkteigenschaft von auf einem Datenträger wie Disketten, CD-Rom, Festplatten u. ä. gespeicherter und damit **verkörperter Software**.[409] Denn die Software ist mit dem Datenträger fest verbunden und bildet mit dieser eine bewegliche Sache. Es genügt mithin, wenn die Software auf irgendeinem Datenträger beim Benutzer gespeichert ist.[410] Diese Ansicht stimmt mit der vertragsrechtlichen Rechtsprechung des BGH zur Sacheigenschaft von Software überein[411] und trägt auch der Verkehrsauffassung Rechnung, welche den Datenträger unter Einschluss der Software als bewegliche Sache ansieht.[412] Eine Unterscheidung zwischen **Indivdual- und Standardsoftware** wird dabei nicht getroffen.[413] In einer Stellungnahme zu der dem ProdHaftG zugrundeliegenden EG-Produkthaftungsrichtlinie 85/374/EWG geht auch die Kommission der Europäischen Gemeinschaften davon aus, dass Software als Produkt im Sinne der Richtlinie anzusehen ist.[414]

192 Streitig ist die Produktqualität von **online übertragener Software**.[415] Denkbar wäre es, die Übertragung von Daten mittels elektromagnetischer Ströme als Unterfall des Produktes „**Elektrizität**“ einzuordnen, welche in § 2 S. 1 ProdHaftG ausdrücklich als Produkt im Sinne des ProdHaftG genannt wird.[416] Allerdings bietet die Elektrizität als einzige Ausnahme keinen Raum für die Annahme einer Regelungslücke und damit für

---

[408] *Beckmann/Müller*, MMR 1999, 14 (15); *Redeker*, NJW 1992, 1739 f.; *Bauer*, PHi 1989, 98 (101).

[409] *Spindler/Klöhn*, VersR 2003, 410 (412); *Spindler*, MMR 1998, 119 (120) *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 441; *Marly*, Softwareüberlassungsverträge, Rn. 1303; *Sodtalbers*, Softwarehaftung im Internet, Rn. 161; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 607; *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 160 ff.; *v. Westphalen*, Vertragsrecht und AGB-Klauselwerke, IT-Verträge, Rn. 92; *Taschner/Frietsch,* § 2 ProdHaftG Rn. 23; Palandt-*Sprau*, § 2 ProdHaftG Rn. 1; Erman-*Schiemann*, § 2 ProdHaftG Rn. 2; MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 15; Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 64.

[410] *Spindler/Klöhn*, VersR 2003, 410 (412); MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 15.

[411] Dazu BGH NJW 1993, 2436 (2437); BGH NJW 1990, 320 (321).

[412] *Taschner/Frietsch,* § 2 ProdHaftG Rn. 23.

[413] *Marly*, Softwareüberlassungsverträge, Rn. 1303; *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 168; *v.Westphalen*, in: v.Westphalen, ProdHaftHdb, § 73 Rn. 39; Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 69; a. A. MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 15.

[414] Stellungnahme der Kommission der Europäischen Gemeinschaften auf die Schriftliche Anfrage Nr. 706/88 von Herrn Gijs de Vries an die Kommission: Produkthaftung für Computerprogramme v. 08.05.1989, ABl. EG Nr. C 114, S. 42.

[415] Dafür *Spindler/Klöhn*, VersR 2003, 410 (412); *Spindler*, MMR 1998, 119 (121); *Wagner*, NJW 1996, 2899 (2904); *Taeger*, CR 1996, 257 (261 f.); *Sodtalbers*, Softwarehaftung im Internet, Rn. 164 ff.; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 607; *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 441; *v. Westphalen*, in: v. Westphalen, ProfHaftHdb, § 73 Rn. 40; MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 16; dagegen Erman-*Schiemann*, § 2 ProdHaftG Rn. 2; Staudinger-*Oechler*, § 2 ProdHaftG Rn. 65, 69a; *Taschner/Frietsch,* § 2 ProdHaftG Rn. 22.

[416] So etwa *v. Westphalen*, in: v. Westphalen, ProdHaftHdb, § 73 Rn. 40 (für online übertragene Software); *Höckelmann*, Die Produkthaftung für Verlagserzeugnisse, S. 141 ff. (für online übertragene Verlagserzeugnisse); für eine Analogie zur Elektrizität *Meyer*, ZUM 1997, 26 (28, 33).

Analogien.[417] Entscheidend ist demnach letztlich die Auslegung des Begriffs der beweglichen Sache in § 2 ProdHaftG. Nach wohl hM ist der Sachbegriff des § 90 BGB aus der Auslegung des § 2 ProdHaftG zugrunde zu legen.[418] Eine Ansicht in der Literatur verneint die Produkteigenschaft online übertragener Software daher auch unter Hinweis auf die fehlende gegenständliche Verkörperung auf einem Datenträger.[419] Ähnlich dürfte dies wohl auch das britische Recht sehen.[420] Diese Argumentation greift indessen zu kurz. Im Hinblick auf den verbraucherschützenden Zweck des ProdHaftG kann die Frage der Anwendbarkeit der verschuldensunabhängigen Haftung nicht davon abhängen, ob bereits die Übertragung in körperlicher Form erfolgte. Entscheidend ist vielmehr, dass zumindest beim Nutzer der Software eine dauerhafte Verkörperung durch Speicherung auf einem Datenträger erfolgt.[421] Für die Anwendbarkeit des ProdHaftG ist demnach danach zu **differenzieren**, ob die Software lediglich zeitweise während der Benutzung der Dienste des Service Providers genutzt werden kann oder ob der Nutzer sie durch Download auf seinen eigenen Rechner dauerhaft verwenden kann.[422] Ein Provider, welcher dem Kunden lediglich **vorübergehend die Nutzung einer Software ermöglicht**, ohne diese auf den Rechner herunter zu laden, unterliegt nicht der Haftung nach dem ProdHaftG, der Provider erbringt hier letztlich nichts anderes als eine Dienstleistung,[423] welche nicht in den Anwendungsbereich des Gesetzes fällt.[424] Bei **dauerhafter Verkörperung** auf dem Rechner findet die Materialisierung erst beim Kunden statt, indem die Software oder die Information auf der Festplatte oder einem anderen Medium gespeichert wird.[425] Eine Verkörperung und damit ein Produkt im Sinne des § 2 ProdHaftG liegt dann vor. Zwar hat hier erst der Kunde durch eigenen Willensentschluss die Körperlichkeit des Produktes herbeigeführt, so dass man an der Herstellung des Produktes im Organisationsbereich des Herstellers zweifeln könnte. Doch liegt das entscheidende Moment der Inverkehrgabe des Produktes „Software“ in der vom Anbie-

[417] *Wagner*, NJW 1996, 2899 (2900); *Spindler*, in: Spindler, Rechtsfragen bei Open Source, Kap. E Rn. 11; *Spindler*, MMR 1998, 119 (120 f.); *Taschner/Frietsch,* § 2 ProdHaftG Rn. 22; Staudinger-*Oechsler,* § 2 ProdHaftG Rn. 12, 67.

[418] *Taschner/Frietsch,* § 2 ProdHaftG Rn. 17; Kullmann/Pfister-*Kullmann*, Kz. 3603 S. 1; Palandt-*Sprau*, § 2 ProdHaftG Rn. 1; Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 11.

[419] Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 11, 66.

[420] S. *Reed* – Annex II – Rn. 1281.

[421] *Wagner*, NJW 1996, 2899 (2900); *Spindler/Klöhn*, VersR 2003, 410 (412); *Spindler*, MMR 1998, 119 (120); *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 441; *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 160 ff.; MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 16.

[422] *Spindler*, in: Spindler, Rechtsfragen bei Open Source, Kap. E Rn. 11 f.; *Spindler*, MMR 1998, 119 (121); MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 16.

[423] MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 16.

[424] Dazu *Taschner/Frietsch,* § 2 ProdHaftG Rn. 8; Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 42.

[425] Abl. daher *Smith/Hamill,* PHI 1988, 85.

ter offerierten Möglichkeit, die Software herunterzuladen.[426] Denn ab diesem Zeitpunkt kann der Kunde das Produkt jederzeit wiederbenutzen, wobei er nicht mehr auf die Netzverbindung angewiesen ist. Die Rechtslage kann hier nicht anders beurteilt werden, als wenn dem Kunden nur noch eine unwesentliche Fertigungshandlung obliegt, um das Endprodukt „herzustellen", etwa bei zusammenschraubbaren Fertigmöbeln.[427]

b) Rechtsgutsverletzung

193 Wie auch der Anspruch aus § 823 Abs. 1 BGB beruht die Haftung nach ProdHaftG auf der Verletzung der dort aufgezählten Rechtsgüter. Der Hersteller ist demnach zum Schadensersatz verpflichtet, wenn durch einen Fehler seines Produkts ein Mensch getötet, Körper oder Gesundheit verletzt oder eine Sache beschädigt werden (§ 1 Abs. 1 Satz 1 ProdHaftG). Primäre Vermögensschäden, welche nicht an eine Rechtsgutsverletzung anknüpfen, werden nicht ersetzt. Hinsichtlich der Haftung für die Verletzung von **Leben, Körper und Gesundheit** durch fehlerhafte IT-Produkte kann auf die Ausführungen zu **Rn. 105 ff.** verwiesen werden.[428]

194 Der Begriff des **Sachschadens** entspricht nach wohl hM dem der Eigentumsverletzung bei § 823 Abs. 1 BGB (ausführlich oben **Rn. 109**).[429] Im Hinblick auf den Wortlaut des Art. 9 lit. a der EG Produkthaftungsrichtlinie wird zum Teil eine Beschränkung auf Substanzverletzungen angenommen.[430] Die abschließende Entscheidung dieser Streitfrage muss letztlich aber einer Klärung durch den EuGH vorbehalten bleiben.[431] Eine bedeutsame Einschränkung erfährt der sachliche Schutzbereich des ProdHaftG im Bereich der Sachschäden durch § 1 Abs. 1 Satz 2 ProdHaftG. Sachbeschädigungen jedoch nur erfasst, wenn eine **andere Sache** als das fehlerhafte Produkt beschädigt (Rn. 109 ff.) und diese anderen Sachen ihrer Art nach gewöhnlich für den **privaten Ge- und Verbrauch** bestimmt und hierzu von dem Geschädigten hauptsächlich verwendet worden ist:

(1) Andere Sache

[426] MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 16.
[427] Ähnlich wohl die österreichische Rechtslage, vgl. *Fallenböck* – Annex II – Rn. 1128.
[428] S. dazu *Taschner/Frietsch*, § 2 ProdHaftG Rn. 22.
[429] Palandt-*Sprau*, § 1 ProdHaftG Rn. 5; MünchKommBGB-*Wagner*, § 823 BGB Rn. 6 f..
[430] *Koch*, Versicherbarkeit von IT-Risiken, Rn. 608.
[431] So zu Recht MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 7.

195 Nach dem ProdHaftG ersatzfähig sind – in **Abgrenzung von der vertraglichen Gewährleistung**[432] – allein Schäden an anderen Sachen als dem fehlerhaften Produkt. Für die Abgrenzung ist die Verkehrsauffassung maßgeblich.[433] Eine „andere Sache" im Sinne der Vorschrift liegt ohne weiteres vor, wenn eine von dem fehlerhaften Produkt **körperlich getrennte Sache** beschädigt wird. Im IT-Bereich ist dies etwa bei einer mechanischen Einwirkung auf eine andere Sache infolge fehlerhafter Steuerungssoftware im privaten Pkw denkbar (z. B. Auffahrunfall). Wird die fehlerhafte Software selbst durch ihren Fehler gelöscht und damit zerstört, kann dieser Schaden nicht über das ProdHaftG liquidiert werden.[434]

196 Streitig ist im Rahmen des ProdHaftG die Behandlung von **Weiterfresserschäden** (dazu bereits Rn. 109),[435] also die Frage, inwieweit ein fehlerhaftes Teilprodukt im Verhältnis zum Endprodukt eine andere Sache sein kann. Unter Hinweis auf §§ 1 Abs. 1 Satz 2, 2 Satz 2, 4 ProdHaftG wird in der Literatur zum Teil vertreten, auch Schäden am Endprodukt ersatzfähig sei.[436] Andere stellen darauf ab, ob das Teilprodukt aus Sicht des Betroffenen im Markt als eigenständige Ware behandelt wird.[437] Die ganz hM lehnt eine Übertragung der Weiterfresser-Rechtsprechung zur deliktischen Produzentenhaftung auf das ProdHaftG indessen ab,[438] da das in Verkehr gebrachte Endprodukt nach der Verkehrsauffassung insgesamt das „fehlerhafte Produkt" sei.[439] Eine Haftung für Eigentumsverletzungen aufgrund von Softwarefehlern scheidet danach auf Grundlage des ProdHaftG jedenfalls dann aus, wenn die **Software in das fertige Endprodukt integriert** war. Nach überwiegender Auffassung gilt dies auch dann, wenn der Hersteller des Endprodukts nicht mit dem Hersteller der Software identisch ist.[440] Nicht nach dem ProdHaftG ersatzfähig sind danach Datenschäden durch fehlerhafte Software, wenn die Software auf einem handelsüblichen Computer vorinstalliert war. Ebenso sind Schäden

---

[432] *Larenz/Canaris*, § 84 I 1 c, S. 646; MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 9.

[433] BT-Drucks. 11/2447 S. 13; *Taschner/Frietsch*, § 1 ProdHaftG Rn. 38.

[434] *Sodtalbers*, Softwarehaftung im Internet, Rn. 317.

[435] Ausführlich zum Streitstand MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 10 ff.; Staudinger-*Oechsler*, § 1 ProdHaftG Rn. 10 ff.

[436] *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 196 f.; *v.Westphalen*, in: v.Westphalen, ProdHaftHdb, § 72 Rn. 7 ff.

[437] *Larenz/Canaris*, § 84 I 1 c, S. 646; Staudinger-*Oechsler*, § 1 ProdHaftG Rn. 20.

[438] *Koch*, Versicherbarkeit von IT-Risiken, Rn. 610; *Sodtalbers*, Softwarehaftung im Internet, Rn. 324 f.; *Tiedtke*, NJW 1990, 2961 (2964); *Taschner/Frietsch*, § 1 ProdHaftG Rn. 38 ff.; Palandt-*Sprau*, § 1 ProdHaftG Rn. 6; Erman-*Schiemann*, § 1 ProdHaftG Rn. 3; MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 14.

[439] BT-Drucks. 11/2447, S. 13; *Sodtalbers*, Softwarehaftung im Internet, Rn. 323.

[440] *Tiedtke*, NJW 1990, 2961 (2964); MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 13.

am privaten Pkw des Nutzers, in den eine fehlerhafte Software (z. B. automatische Fahrabstandsregelung) eingebaut worden ist, nicht ersatzfähig.[441]

197 Anders liegt der Fall, wenn ein Teil einer Sache erst **nachträglich als Ersatz oder Zusatz mit dem Rest- oder Endprodukt verbunden** worden ist.[442] Dies dürfte beispielsweise dann gelten, wenn Software getrennt vom Rechner erworben und auf dem Rechner installiert wurde, wobei es nach Rn. 196 nicht darauf ankommt, ob die Software von einem Datenträger auf den Computer überspielt oder online übertragen wurde.

(2) Privater Gebrauch

198 Durch die Beschränkung des Schutzbereichs auf die Beschädigung privat genutzter Sachen, fällt die Beschädigung **gewerblich**, **beruflich** und **freiberuflich** genutzter Sachen fällt insgesamt **nicht** in den Schutzbereich der verschuldensunabhängigen Produkthaftung.[443] Dies beruht zum einen auf der Erwägung, dass im unternehmerischen Bereich besonders hohe Vermögensfolgeschäden drohen, zum anderen ist einem Unternehmen eher als Privaten zumutbar durch Abschluss einer Versicherung gegen derartige Schäden zumutbar.[444]

c) Verursachung durch einen Fehler des Produkts

199 Ein Produkt ist gemäß § 3 ProdHaftG fehlerbehaftet, wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände, insbesondere seiner Darbietung, des Gebrauchs, mit dem billigerweise gerechnet werden kann und des Zeitpunktes, in dem es in den Verkehr gebracht wurde, berechtigterweise erwartet werden kann. Die Kriterien zur Bestimmung der Fehlerhaftigkeit von IT-Produkten entsprechen insoweit den zur deliktischen Produzentenhaftung gemachten Ausführungen,[445] so dass insoweit auf Rn. 105 ff. verwiesen wird.

d) Haftungsausschlussgründe

200 Die Haftung nach dem ProdHaftG ist ausgeschlossen, wenn einer der Ausschlussgründe des § 1 Abs. 2 ProdHaftG erfüllt ist. Die Beweislast hierfür trägt der Hersteller (§ 1 Abs. 4 Satz 2 ProdHaftG). Hinsichtlich der Herstellung und des Vertriebs von Software

---

[441] So auch *Koch*, Versicherbarkeit von IT-Risiken, Rn. 610; *Sodtalbers*, Softwarehaftung im Internet, Rn. 324 f.

[442] BT-Drucks. 11/2447, S. 13; *Taschner/Frietsch*, § 1 ProdHaftG Rn. 40; Staudiner-*Oechsler*, § 1 ProdHaftG Rn. 20a.

[443] *Hoeren*, in: v. Westphalen, Vertragsrecht und AGB-Klauselwerke, IT-Verträge, Rn. 95; *Taschner/Frietsch*, § 2 ProdHaftG Rn. 33; *Larenz/Canaris*, § 84 I 1 c, S. 647; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 609.

[444] *Larenz/Canaris*, § 84 I 1 c, S. 647.

[445] Dazu auch *Koch*, Versicherbarkeit von IT-Risiken, Rn. 614, 637; Palandt-*Sprau*, § 3 ProdHaftG Rn. 2 ff.; MünchKommBGB-*Wagner*, § 3 ProdHaftG Rn. 29.

kann der Haftungsausschlussgrund des **§ 1 Abs. 2 Nr. 3 ProdHaftG** Bedeutung erlangen, soweit die Software „weder für den Verkauf oder Vertrieb mit wirtschaftlichem Zweck hergestellt noch im Rahmen einer beruflichen Tätigkeit hergestellt oder vertrieben“ wird. Bei unentgeltlicher Überlassung von Software scheidet eine verschuldensunabhängige Haftung folglich von vonherein aus. Dies betrifft zum einen **Freeware** und frei zugängliche **Open Source Software**, welche von Programmieren in ihrer Freizeit erstellt und im Internet zum kostenlosen Download bereitgestellt wird.[446] Dagegen findet das ProdHaftG auf **Shareware** Anwendung, da damit zumindest mittelbar ein wirtschaftlicher Zweck verfolgt wird.[447] Gemäß § 1 II Nr. 5 ProdHaftG wird nach dem Produkthaftungsgesetz zudem nicht für Fehler gehaftet, die nach dem Stand von Wissenschaft und Technik vom Hersteller nicht erkannt werden konnten, als der das Produkt in Verkehr brachte (**Entwicklungsfehler**).[448] Demgemäß kann bei objektiv bei Inverkehrgabe nicht erkennbaren Programmierungsfehlern keine Haftung eingreifen, so daß angesichts der wohl nicht zu erreichenden Fehlerlosigkeit bei Software von vornherein eine Reihe von Softwarefehlern nicht zur Haftung führen.[449] Anders als nach Deliktsrecht besteht nach dem ProdHaftG damit auch keine verschuldensunabhängige Einstandspflicht für Fehler bei der Produktbeobachtung.[450]

e) Beweislast

201 Für die verschuldensunabhängige Produkthaftung gilt, dass sie lediglich dem Geschädigten den Nachweis der Pflichtwidrigkeit des Herstellers abnimmt, indem die Schadensersatzpflicht allein schon beim Vorliegen eines fehlerhaften Produktes, das kausal für die Rechtsgutsverletzung geworden ist, abnimmt. Dem Geschädigten obliegt aber nach wie vor die Darlegungs- und Beweislast dafür, dass das Produkt fehlerhaft war und genau dieser Fehler für die Rechtsgutsverletzung verantwortlich war (Kausalität).[451] Damit treten aber genau diesselben Probleme wie im Bereich der verschuldensabhängigen Produkthaftung auf, insbesondere hinsichtlich des Kausalitätsnachweises. Hinzuweisen ist in diesem Rahmen auf die für das österreichische Recht vertretene Auffas-

[446] *Koch*, Versicherbarkeit von IT-Risiken, Rn. 611; *Marly*, Softwareüberlassungsverträge, Rn. 1306; *Spindler*, in: Spindler, Rechtsfragen bei Open Source, Kap. E Rn. 15.

[447] *Koch*, Versicherbarkeit von IT-Risiken, Rn. 611; *v.Westphalen*, in: v. Westphalen, ProdHaftHdb, § 72 Rn. 56.

[448] *Marly*, Softwareüberlassungsverträge, Rn. 1306.

[449] S., dazu auch das österreichische Recht, dazu *Fallenböck* – Annex II – Rn. 1135.

[450] *Marly*, Softwareüberlassungsverträge, Rn. 1310; Palandt-*Sprau*, § 3 ProdHaftG Rn. 12; MünchKommBGB-*Wagner*, § 3 ProdHaftG Rn. 36, § 1 ProdHaftG Rn. 61.

[451] Palandt-*Sprau*, § 1 ProdHaftG Rn. 9, 25; MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 76 ff.; Bamberger/Roth-*Spindler*, § 823 Rn. 552; ferner OLG Düsseldorf NJW-RR 1997, 1344 (1345).

sung,[452] daß der Hersteller nur darlegen muß, dass das Produkt zur Zeit, zu der es in Verkehr gebracht worden war, wahrscheinlich noch nicht den schadenskausalen Fehler hatte[453]. Dieser erleichterte Beweis soll grundsätzlich mit den getroffenen Feststellungen erbracht sein, dass das Produkt dem Stand der Technik entspricht und etwa das technische Prüfzeichen einer für die Prüfung anerkannten Anstalt aufweist.[454] Dies soll auch den Verweis auf die Einhaltung relevanter Normen und Standards (ISO, ÖNORM etc) umfassen.

f) Rechtsfolgen

202 Der Umfang des zu ersetzenden Schadens richtet sich im Ausgangspunkt nach den §§ 249 ff. BGB. Zu ersetzen sind hierbei entgegen einer in der Literatur vertretenen Meinung auch **Sachfolgeschäden**.[455] Hierbei bestehen gegenüber dem Deliktsrecht jedoch zwei wichtige Einschränkungen. Bei Sachbeschädigungen (also auch Datenschäden[456]) hat der Geschädigte einen **Selbstbehalt** von € 500 selbst zu tragen (§ 11 ProdHaftG). Allgemein beschränkt § 10 Abs. 1 ProdHaftG die Haftung auf einen **Höchstbetrag** von 85 Millionen €. Im Einzelfall kommt eine Kürzung des Schadensersatzanspruchs wegen Mitverschuldens des Geschädigten in Betracht (§§ 6 ProdHaftG, 254 BGB) (siehe dazu oben zur deliktischen Produzentenhaftung Rn.188).

3. Zusammenfassung

203 Eine **verschuldensabhängige** Produkthaftung aufgrund des § 823 Abs. 1 BGB kommt im IT-Bereich in Betracht, soweit ein geschütztes Rechtsgut verletzt wird. Besondere Schwierigkeiten bereitet hierbei noch immer die nicht abschließend geklärte Einordnung von Datenschäden als Eigentumsverletzung. Ebenso von Unsicherheit geprägt ist die Abgrenzung primärer Vermögensschäden von einer die Eigentumsverletzung begründenden Beeinträchtigung der bestimmungsgemäßen Verwendung des Produkts. Im Bereich der Pflichten liegt der Schwerpunkt auf der Abgrenzung von Entwicklungs- zu Konstruktionsfehlern: vor allem die zum Zeitpunkt der Inverkehrgabe nicht bekannten Gefahrenpotentiale aufgrund zukünftiger Entwicklungen führen nicht zu einer Haftung der IT-Hersteller, wohl aber Sicherheitslücken, die zu diesem Zeitpunkt erkennbar ge-

---

[452] S. dazu *Fallenböck* – Annex II – Rn. 1138.

[453] OGH 6 Ob 157/98a.

[454] Dabei handelte es sich um den Zeichengenehmigungsausweis der VDE-Prüfstelle (Verband Deutscher Elektrotechniker) für einen Elektroofen.

[455] *Koch*, Versicherbarkeit von IT-Risiken, Rn. 627; *Taschner/Frietsch*, § 1 ProdHaftG Rn. 42; *v.Westphalen*, in: v. Westphalen, ProdHaftHdb, § 71 Rn. 28 ff.; MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 3 f.

[456] *Marly*, Softwareüberlassungsverträge, Rn. 1307.

wesen wären. Technische Standards wie die Common Criteria und Protection Profiles können hier zur Konkretisierung herangezogen werden, wenngleich sie nur ein Mindestmaß der zu erwartenden Sicherheit darstellen, über die im Einzelfall hinaus zivilrechtlich höhere Anforderungen gestellt werden können, wenn dem Hersteller entsprechende Gefahrenszenarien bekannt sein können. Schließlich kann das Deliktsrecht auch nicht über Rückrufpflichten dazu herangezogen werden, um Pflichten zur nachträglichen Verbesserung der Software zu begründen („Patches") – denn hier ist oftmals das Äquivalenzinteresse berührt, das gerade nicht vom Deliktsrecht erfasst wird.

204 Im Bereich der **verschuldensunabhängigen** Produkthaftung ist die Einordnung von Software als Produkt noch immer von Unsicherheiten gekennzeichnet. Die Reichweite der Haftung wird stark eingeschränkt, indem allein Sachschäden an anderen Sachen als dem fehlerhaften Produkt ersatzfähig sind, und auch dann nur, wenn es sich um privat genutze Sachen handelt; Schäden an gewerblich genutzen Sachen scheiden demnach von vornherein aus. Damit wird der Bereich der verschuldensunabhängigen Produkthaftung erheblich eingeschränkt, da zahlreiche Produkthaftungsfälle sich im B2B-Sektor abspielen.

205 Schließlich ist beiden Bereichen gemein, dass für die Frage der Kausalität keine Beweislastumkehr eingreift, in der Regel auch nicht für das Vorliegen eines Fehlers der Software bei Inverkehrgabe.

IV. Öffentlich-rechtliche Produktsicherheit, insbesondere das GPSG

206 Die zivilrechtliche Regulierung der Produktsicherheit wurde schon seit langer Zeit öffentlich-rechtlich flankiert durch allgemeine und sektorspezifische Normen zur Produktsicherheit. Die bisher im Gerätesicherheitsgesetz (GSG)[457] und im Produktsicherheitsgesetz (ProdSG)[458] nebeneinander geregelten sicherheitsrechtlichen Anforderungen an Produkte wurden mit Inkrafttreten des neuen Geräte und Produktsicherheitsgesetz (GPSG)[459] am 1.5.2004 in einem einheitlichen Gesetz zusammengefasst. Das GPSG dient zugleich der Umsetzung der Richtlinie 2001/95/EG des Europäischen Par-

[457] Gesetz über technische Arbeitsmittel (Gerätesicherheitsgesetz - GSG) vom 14.6.1968, BGBl. I, S. 717.

[458] Gesetz zur Regelung der Sicherheitsanforderungen an Produkte und zum Schutz der CE-Kennzeichnung (Produktsicherheitsgesetz – ProdSG) vom 22.4.1997, BGBl. I, S. 934.

[459] Gesetz über technische Arbeitsmittel und Verbraucherprodukte (Geräte- und Produktsicherheitsgesetz – GPSG) vom 6.1.2004, BGBl. I, S. 2, ber. S. 219.

laments und des Rates vom 3.12.2001 über die allgemeine Produktsicherheit.[460] Neben dieser allgemeinen Produktsicherheitsregelung bestehen nach wie vor sektorspezifische Produktsicherheitsnormen, wie etwa das Medizinproduktegesetz (MPG)[461], die hier nicht näher thematisiert werden können. Zahlreiche dieser Produktsicherheitsnormen gehen zurück auf europarechtliche Vorgaben zur weiteren Integration des Binnenmarktes, die insbesondere den sog. New Approach (dazu unten Rn. 1.c)(1)(b)) umgesetzt haben, um zu einer möglichst flexiblen und aktuellen Harmonisierung im Produktsicherheitsbereich zu gelangen.

207 **Ziel des GPSG** ist es, Schutz vor unsicheren Produkten hinsichtlich des Verbraucher- und Arbeitnehmerschutzes zu gewährleisten und den freien Wahrenverkehr mit sicheren Produkten sicherzustellen.[462] Das GPSG soll insbesondere das gemeinsame „Dach" für alle Verbraucherprodukte im Sinne der Produktsicherheitsrichtlinie bilden und als Auffanggesetz für sonstige Produkte fungieren, für die es keine Spezialnormierung gibt.

1. Anwendungsbereich und Anforderungsprofil des GPSG

208 Gem. § 1 Abs. 1 S. 1 GPSG gilt das Gesetz für das „Inverkehrbringen und Ausstellen von Produkten, das selbständig im Rahmen einer wirtschaftlichen Unternehmung erfolgt." Die private Weitergabe eines Produkts wird folglich nicht vom GPSG erfasst. Das Gesetz statuiert in §§ 4 und 5 GPSG besondere Pflichten beim Inverkehrbringen von Produkten für Hersteller, Importeure, Händler und vom Gesetz gleichgestellte Personen und regelt zusätzlich nachgelagerte Pflichten zum Produktrückruf und zur Beobachtung.

a) Produktbegriff

209 Gefahren die aus der Benutzung **fehlerhafter Hard- und Software** herrühren, könnten prinzipiell vom Schutzumfang des GPSG erfasst sein. Allerdings müsste das GPSG hierzu überhaupt auf Hard- und Software Anwendung finden: Während die Voraussetzung des „Herstellens" und des anschließenden Vertriebs von Hard- und Software im Rahmen einer wirtschaftlichen Unternehmung[463] in aller Regel erfüllt sein werden und

[460] ABl. EG Nr. L 11, S. 4 ff.

[461] Gesetz über Medizinprodukte (Medizinproduktegesetz – MPG) vom 7.8.2002, BGBl. I, S. 2304.

[462] *Runte/Potinecke*, CR 2004, 725; *Wilrich*, Einleitung Rn. 1 ff.; *Littbarski*, VersR 2005, 448 f.

[463] Für Open Source Software kann dies indes fraglich sein.

insofern das Merkmal des Inverkehrbringens i.S.v. § 2 Abs. 8 GPSG vorliegt, ist fraglich, ob es sich bei Hard- und Software um Produkte im Sinne des GPSG handelt.

(1) Grundsätze

210 Weder die Produktsicherheitsrichtlinie noch das GPSG selbst enthalten eine Definition des Produktbegriffes.[464] Beide Regelungen setzen den Begriff des Produkts vielmehr voraus und grenzen ihren Anwendungsbereich auf bestimmte Produktarten ein (Art. 2 Richtlinie 2001/95/EG, § 2 GPSG). Der vom GPSG verwendete Produktbegriff umfasst gemäß der in § 2 Abs. 1 GPSG enthaltenen Begriffsbestimmung technische Arbeitsmittel und Verbraucherprodukte.

211 Nach der in § 2 Abs. 2 GPSG enthaltenen Legaldefinition sind **technische Arbeitsmittel** verwendungsfertige Arbeitseinrichtungen, die bestimmungsgemäß ausschließlich bei der Arbeit verwendet werden, sowie deren Zubehörteile. Da insofern auf die Verwendung zu geschäftsmäßigen Zwecken abgestellt wird, fallen Produkte, die von Verbrauchern in Anlehnung an § 13 BGB weder zur gewerblichen noch zur selbständigen beruflichen Tätigkeit genutzt werden, aus dem Definitionsbereich der technischen Arbeitsmittel heraus.[465]

212 **Verbraucherprodukte** sind demgegenüber gem. § 2 Abs. 3 GPSG „Gebrauchsgegenstände und sonstige Produkte, die für Verbraucher bestimmt sind oder unter vernünftigerweise vorhersehbaren Bedingungen von Verbrauchern benutzt werden können, selbst wenn sie nicht für diesen bestimmt sind“. Insbesondere sind also neben solchen Produkten, die bestimmungsgemäß innerhalb einer Lieferkette an private Endverbraucher abgegeben werden, auch sog. **Migrationsprodukte** in den Anwendungsbereich des GPSG mit einbezogen, also solche, die ursprünglich nicht für Verbraucher bestimmt waren, die jedoch in vorhersehbarer Weise von Verbrauchern benutzt werden.

213 Inwieweit IT-Produkte in den Anwendungsbereich des GPSG fallen, ist weithin ungeklärt. Unter Berücksichtigung der Beschränkung des Anwendungsbereichs des GPSG auf technische Arbeitsmittel und Verbraucherprodukte ist hierbei zwischen Hardware und Software zu unterscheiden.

(2) Hardware

[464] *Klindt*, GPSG, § 2 GPSG Rn. 3.
[465] *Geiß/Doll*, B § 2 GPSG Rn. 12; *Zscherpe/Lutz*, K&R 2005, 499; *Runte/Potinecke*, CR 2004, 725 (726).

214 Hardware-Teile (z.B. Computer, Laptops, Monitore, Drucker, Keyboards und anderes Zubehör) fallen als körperliche Gegenstände unproblematisch unter den Produktbegriff des GPSG.[466] Da auch Migrationsprodukte, also Gebrauchsgegenstände, die nicht zwingend für Verbraucher bestimmt sind, aber deren Verwendung durch Verbraucher vernünftigerweise erwartet werden kann,[467] unter den Begriff der Verbraucherprodukte zu subsumieren sind, ist unbeachtlich, wenn die Hardware auch am Arbeitsplatz Verwendung findet. Handelsübliche Hardware wird daher regelmäßig ein Verbraucherprodukt im Sinne von §§ 2 Abs. 3, 5 GPSG und nicht technisches Arbeitsmittel nach § 2 Abs. 2 GPSG sein.[468] Als technische Arbeitsmittel können im IT-Bereich vor allem computergestützte Steuerungseinrichtungen für Fertigungsprozesse eingestuft werden.[469] Denn diese entsprechen den in der Vorgängerregelung des § 2 Abs. 1 GSG als Arbeitseinrichtungen beispielhaft aufgezählten Werkzeugen, Arbeitsgeräten, usw. Ob auch nicht handelsübliche Hardware, wie etwa bestimmte Arten von Servern oder Hochleistungsrechnern, die bestimmungsgemäß ausschließlich im geschäftlichen Bereich eingesetzt werden, technische Arbeitseinrichtungen sind,[470] ist angesichts der genannten Beispiele zumindest zweifelhaft, soweit von diesen Geräten keine Gefahren aufgrund mechanischer Einwirkung auf Arbeitnehmer oder Dritte ausgehen.[471]

(3) Software

215 Probleme bereitet dagegen die Einordnung von Software als lediglich geistiger Leistung, da für den Produktbegriff – ähnlich wie im ProdHaftG (Rn. 190 ff.) – in der Regel auf die Verkörperung abgestellt wird[472] - anders als etwa im österreichischen Recht, das nicht mehr auf die Körperlichkeit abstellt.[473] Das Abstellen auf die Verkörperung bei technischen Arbeitsmitteln legte im alten Gerätesicherheitsgesetz bereits der Titel „Geräte“ nahe.[474] Die Beispiele im neuen GPSG in der Legaldefinition von technischen Arbeitsmittel in § 2 Abs. 1 GPSG, die sich wiederum ausschließlich auf Geräte beziehen, legen es nahe, auch weiter auf die Verkörperung abzustellen. Ähnliches gilt für den Be-

[466] *Runte/Potinecke*, CR 2004, 725; *Hoeren/Ernstschneider*, MMR 2004, 507; *Zscherpe/Lutz*, K&R 2005, 499 (500); *Wilrich*, § 2 Rn. 4; *Klindt*, GPSG, § 2 GPSG Rn. 13.

[467] *Hoeren/Ernstschneider*, MMR 2004, 507.

[468] *Zscherpe/Lutz*, K&R 2005, 499 (500); *Hoeren/Ernstschneider*, MMR 2004, 507 f.

[469] *Hoeren/Ernstschneider*, MMR 2004, 507 (508).

[470] So *Zscherpe/Lutz*, K&R 2005, 499 (500).

[471] Dazu *Hoeren/Ernstscheider*, MMR 2004, 507.

[472] S. Rn 190 ff.; *Klindt*, GPSG, § 2 GPSG Rn. 13; *Wilrich*, § 2 GPSG Rn. 4; *Runte/Potinecke*, CR 2004, 725; ferner *Hoeren/Ernstschneider*, MMR 2004, 508.

[473] S. den Bericht bei *Fallenböck* – Annex II – Rn. 1115.

[474] S. *Runte/Potinecke*, CR 2004, 726.

griff des Verbraucherprodukts. Dieser kann laut der Gesetzesbegründung alles sein, was aus einem Herstellungsprozess hervorgeht, von technischen Gegenständen bis hin zu Stoffen.[475] Dadurch wird deutlich, dass auch hier die Körperlichkeit klar im Vordergrund steht. Wenn die geistige Leistung daher auf einem Speichermedium verkörpert ist, ist zumindest der Datenträger ein vom GPSG erfasstes Produkt.[476] Darüber hinaus ist allerdings fraglich, ob das geistige Werk selbst – und nicht nur der Datenträger an sich – erfasst wird. Im Unterschied zum **MPG**, in dessen § 3 Nr. 1 MPG ausdrücklich auch Software in den Anwendungsbereich einbezogen wird, enthält das GPSG keine ausdrückliche Regelung. Im Umkehrschluss ließe sich behaupten, dass körperlich nicht fixierte Software nicht vom Geräte- und Produktsicherheitsgesetz erfasst sein soll.[477] Allerdings kann diese Argumentation kaum überzeugen, da aus der Formulierung in § 3 Nr. 1 MPG, nach der Medizinprodukte als „alle einzeln oder verbunden verwendeten Instrumente […] einschließlich der für ein einwandfreies Funktionieren des Medizinproduktes eingesetzten Software“ definiert werden, lediglich ersichtlich ist, dass Software kein „Instrument“ ist.

216 Die Einordnung von Software unter das GPSG bedarf insofern einer differenzierteren Betrachtung, bei der zwischen so genannter „embedded Software“, also solcher, die in ein Endprodukt integriert ist und Steuerungsfunktionen erfüllt, und solcher, die selbständig zu nutzen ist, unterschieden werden muss

(a) Im Endprodukt integrierte Software

217 Soweit die in ein Endprodukt integrierte Steuerungssoftware betroffen ist, nimmt diese als Teil eines ganzen Produkts an der Produkteigenschaft desselben teil.[478] Insofern lässt sich hinsichtlich der **Steuerungssoftware** die Produkteigenschaft bejahen, sofern das Gesamtprodukt entweder technisches Arbeitsmittel oder Verbraucherprodukt im Sinne des GPSG ist. Im Bereich der Verbraucherprodukte wird hierbei in Zukunft wohl der Automobilsektor verstärkt eine Rolle spielen, wenn Steuerungsaufgaben mehr und mehr auf den Computer übertragen werden (z.B. ABS, ESP, automatische Fahrabstandsregelung) und bei Fehlfunktionen Personen (Verwender, Dritte) geschädigt werden können.

---

[475] BT-Drucks. 15/1620, S. 26.

[476] *Hoeren/Ernstschneider*, MMR 2004, 507 (508); *Wilrich,* § 2 Rn. 10.

[477] Hinsichtlich Art. 1 Abs. 2 lit a) Medizinproduktrichtlinie: *Schieble*, Produktsicherheitsgesetz und europäisches Gemeinschaftsrecht, S. 124.

[478] *Runte/Potinecke*, CR 2004, 725 (726); *Zscherpe/Lutz*, K&R 2005, 499 (500).

Gleiches ist im häuslichen Bereich denkbar, wenn Geräte in zunehmendem Maß durch Software gesteuert werden („Vernetztes Haus“).

(b) Selbständige Software

218 Schwieriger ist hingegen die Beurteilung der übrigen **„selbständigen“ Software**. Die Literatur geht in Anlehnung an die zum Produktbegriff des § 2 ProdHaftG entwickelten Grundsätze (dazu oben Rn. 190 ff.) zum Teil davon aus, dass Software zumindest dann in den Anwendungsbereich des GPSG fällt, wenn sie auf einem Datenträger gespeichert und somit verkörpert ist.[479] Mangels Definition des Produktbegriffs in der Richtlinie und dem GPSG hat sich die Auslegung des Gesetzes an Sinn und Zweck des dieser Normen zu orientieren. Ohne Rücksicht auf die engere Definition des Sachbegriffs in § 90 BGB ist folglich entscheidend auf das Ziel der Produktsicherheitsrichtlinie, Verbraucher und Arbeitnehmer vor Gesundheitsschäden durch unsichere Konsumgüter zu schützen, abzustellen. Soweit Software also „gefährlich“ sein kann, wird man sie somit als Produkt im Sinne der Produktsicherheitsrichtlinie und des GPSG einordnen müssen, denn der Hersteller von Software kann grundsätzlich ein vergleichbar hohes Gefährdungspotential schaffen, wie der Hersteller anderer Produkte.[480] Dies gilt auch für online übertragene Software.[481] Unerheblich ist auch, ob es sich um Standard- oder Individualsoftware handelt.[482] Andere Länder in der EU, etwa Großbritannien, qualifizieren indes nur verkörperte Software als Produkt.[483]

219 Während es inzwischen wohl der vorherrschenden (zutreffenden) Auffassung entsprechen dürfte, dass selbständige Software jedenfalls für **Verbraucher** als Produkt im Sinne des GPSG zu qualifizieren ist,[484] ist fraglich, inwieweit von ihr eine vom GPSG erfasste Gefährdungslage für geschützte Rechtsgüter ausgeht (s. Rn. 221 ff.).

220 Zweifelhaft ist die Rechtslage für den Bereich der **technischen Arbeitsmittel**. § 2 Abs. 2 GPSG definiert Arbeitsmittel als „verwendungsfertige Arbeits*einrichtungen*“ und deren „*Teile*“, „Zubehör*teile*“ sowie „Schutzausrüstung“. Der Wortlaut legt somit eine Beschränkung der technischen Arbeitsmittel auf körperliche Gegenstände nahe. Dies wird

---

[479] *Hoeren/Ernstschneider*, MMR 2004, 507 (508); *Zscherpe/Lutz*, K&R 2005, 499 (500); offen lassend *Wilrich*, § 2 GPSG Rn. 10.

[480] *Runte/Potinecke*, CR 2004, 725 (727); *Zscherpe/Lutz*, K&R 2005, 499 (500).

[481] *Klindt*, GPSG, § 2 GPSG Rn. 13.

[482] *Zscherpe/Lutz*, K&R 2005, 499 (500); *Klindt*, GPSG, § 2 GPSG Rn. 13.

[483] S. dazu *Reed* – Annex II – Rn. 1271.

[484] *Zscherpe/Lutz*, K&R 2005, 499 (500); *Hoeren/Ernstschneider*, MMR 2004, 507; zum GPSG *Klindt*, GPSG, § 2 GPSG Rn. 12 f..

auch durch die Vorgängerregelung des § 2 Abs. 1 GSG bestätigt, welcher als Beispiele für Arbeitseinrichtungen Werkzeuge, Arbeitsgeräte, Arbeits- und Kraftmaschinen, Hebe- und Fördereinrichtungen sowie Beförderungsmittel nennt. Der Wortlaut des 1968 erlassenen GSG (früher: „Maschinenschutzgesetz“) orientiert sich indessen weithin an den Gefährdungslagen der industriellen Arbeitswelt und berücksichtigt die Entwicklungen der Computertechnologie und ihren Einfluss auf die Arbeit nicht. Soweit der Einsatz selbständiger Software Sicherheit und Gesundheit von Menschen gefährden kann (Rn. 221 ff.), käme nach Sinn und Zweck des GPSG daher grundsätzlich zumindest eine analoge Anwendung der Bestimmungen über technische Arbeitsmittel in Betracht.

b) Persönlicher und sachlicher Schutzbereich

221 Schutzziel des GPSG ist – neben dem Schutz des Wettbewerbs durch Gewährleistung des Handels mit sicheren Produkten – der Arbeitsschutz und der Schutz der Verbraucher. Der Kreis der vom GPSG geschützten Produktverwender ist danach auf Verbraucher und Arbeitnehmer, die an oder mit technischen Arbeitsmitteln arbeiten, beschränkt.[485] In persönlicher Hinsicht schützt das Gesetz neben dem Produktverwender jedoch auch jeden Dritten (Bystander), der mit den Produkten in Berührung kommt, oder in ihren Gefahrenbereich gelangt, ohne sie selbst zu nutzen (vgl. § 4 Abs. 1, 2 GPSG).[486]

222 Es bezweckt jedoch nur den Schutz vor Gefährdungen der Sicherheit und Gesundheit von Verwendern und Dritten (vgl. § 4 GPSG). **Eigentums- und Vermögensschäden** sind daher grundsätzlich **nicht** vom Schutzumfang des GPSG erfasst.[487] In der Literatur wird zwar vereinzelt vertreten, der Begriff „Sicherheit“ (vgl. § 4 Abs. 1, 2 GPSG) sei nicht auf die Sicherheit von Leib und Leben beschränkt, sondern umfasse auch den Schutz des Eigentums und damit beispielsweise die unberechtigte Löschung von Daten.[488] Sicherheit bezieht sich nach § 4 Abs. 1, 2 GPSG jedoch auf die Sicherheit der Verwender und Dritter und damit auf deren persönliche Integrität.[489] Das Begriffspaar „Gesundheit und Sicherheit“ ist insoweit nicht anders auszulegen, als die gleichlautende

[485] *Wilrich*, Einleitung Rn. 2, 4.
[486] *Wilrich*, Einleitung Rn. 5.
[487] *Wilrich*, Einleitung Rn. 6.
[488] *Runte/Potinecke*, CR 2004, 725 (728). Zur Frage der Eigentumsverletzung bei unberechtigter Löschung von Daten siehe Rn. 110 ff.
[489] *Wilrich*, Einleitung Rn. 6; ebenso zu § 6 ProdSG: *Klindt*, GPSG, § 4 GPSG Rn. 8.

Formulierung in der Vorgängerregelung des § 6 Abs. 1 Satz 1 ProdSG[490]; im gleichen Sinne hatte auch der BGH zum alten § 3 GSG entschieden.[491] Entsprechend ist der Begriff „Gefahr" in der nur für Verbraucherprodukte geltenden Vorschrift des § 5 GPSG auszulegen (vgl. § 5 Abs. 2 GPSG). Allerdings kann der Schutzbereich im europäisch-harmonisierten Bereich auf Grundlage von § 3 Abs. 1 GPSG per Rechtsverordnung auf weitere Rechtsgüter erstreckt werden.[492] Im nicht harmonisierten Bereich ist der Schutzumfang hingegen auf die Abwehr von Personenschäden beschränkt. Das Gesetz bezweckt demnach nicht die Sicherung der Qualität von Produkten allgemein.[493]

223 Damit ergeben sich **im Hinblick auf IT-Produkte bereits wesentliche Einschränkungen**, da in der Mehrzahl der Schadensfälle Eigentum und Vermögen betroffen sein werden, Personenschäden dagegen eher die Ausnahme bilden – wenngleich durch Software verursachte Personenschäden grundsätzlich denkbar sind (s. Rn. 107). Insbesondere der praktisch relevante Bereich der Gefährdung des Eigentums- oder Vermögens (beispielsweise infolge der Vernichtung von Daten oder des Ausfalls von IT-Systemen) von Unternehmen fällt jedoch von vorn herein aus dem Schutzbereich des GPSG heraus. Personenschäden durch Software dürften vor allem im Bereich der Arbeit vorkommen, wenn als **technische Arbeitsmittel** einzuordnende Maschinen aufgrund von Softwarefehlern oder (bei Vernetzung) Sicherheitslücken Arbeitnehmer oder Dritte schädigen. Bei **embedded Software** dürften in Zukunft jedoch auch bei als Verbraucherprodukt einzuordnender Software zunehmend Gefahren für die Sicherheit und Gesundheit von Personen denkbar sein.

224 Beim gegenwärtigen Stand der technischen Entwicklung dürften Gefahren für die Sicherheit und Gesundheit der Produktverwender oder Dritter aufgrund von **selbständiger Software** insbesondere im Verbraucherbereich im Regelfall ausscheiden. Die von Verbrauchern verwendete (selbständige) Software dient größtenteils administrativen (Beispiel: Textverarbeitung, Tabellenkalkulation usw.) oder Unverhaltungszwecken (z.B. Computerspiele), ohne dass mit ihrer Anwendung unmittelbare Einwirkungen auf die reale Welt verbunden wären. Produktfehler werden in diesem Bereich somit kaum jemals in Personenschäden resultieren.

---

[490] MünchKomm-*Wagner*, § 823 BGB Rn. 619; *Wagner*, BB 1997, 2541 (2542); *Klindt*, GPSG, § 6 ProdSG Rn. 5; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 90 Rn. 26, § 91 Rn. 6; Kullmann/Pfister-*Kullmann*, Kz. 2705, S. 8f.

[491] BGH NJW 2006, 1589 (1590); BGH NJW 1983, 812 (813) – Hebebühne; MünchKomm-*Wagner*, § 823 BGB Rn. 618; *Peine*, § 3 Rn. 158.

[492] Hierzu: *Wilrich*, Einleitung Rn. 6, § 3 Rn. 3.

[493] *Wilrich*, Einleitung Rn. 9; noch zum GSG: *Peine*, § 3 Rn. 79.

c) Anforderungen an die Produktsicherheit (§ 4 GPSG)

225 Gem. § 4 GPSG dürfen Produkte nur in Verkehr gebracht und ausgestellt werden, soweit sie den Anforderungen an die Produktsicherheit genügen. Hinsichtlich der Anforderungen ist zu unterschieden zwischen Produkten, welche europäischen Vorgaben entsprechen müssen („harmonisierter Bereich", dazu (1)) und solchen, die lediglich nationalen Anforderungen unterliegen (dazu (2)).

(1) Harmonisierter Bereich (§ 4 Abs. 1 GPSG)

226 § 4 Abs. 1 GPSG bezieht sich auf Produkte, welche einer Rechtsverordnung nach § 3 Abs. 1 GPSG unterfallen und damit einen Teil des europäischen Harmonisierungskonzeptes im Bereich der Produktsicherheit, des so genannten **New Approach** (Neues Konzept)[494], darstellen.

(a) Rechtsverordnungen nach § 3 Abs. 1 GPSG

227 Die in den Harmonisierungsrichtlinien festgelegten europäischen Anforderungen an Produkte werden durch die nach § 3 Abs. 1 GPSG zu erlassenen Rechtsverordnungen in deutsches Recht umgesetzt. Das GPSG dient derzeit der Umsetzung von nicht weniger als 14 Richtlinien des sog. **New Approach** der Europäischen Kommission (dazu ausführlich Teil 2 Rn. 841 ff.).[495] Bei den Richtlinien können die Kategorien sektoral und vertikal unterschieden werden.[496] **Sektorale Richtlinien** enthalten produktbezogene Vorgaben, also Anforderungen an bestimmte Produktgruppen.[497] Demgegenüber sind **vertikale Richtlinien** gefahrbezogen und stellen einheitliche, sektoral übergreifende Anforderungen an Produkte.[498]

228 Für den **IT-Bereich** sind hier insbesondere

- die Erste Verordnung zum Geräte- und Produktsicherheitsgesetz (Verordnung über das In-Verkehr-Bringen elektrischer Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen)[499],
- die Zweite Verordnung zum Geräte und Produktsicherheitsgesetz (Verordnung über die Sicherheit von Spielzeug)[500] und

---

[494] Ausführlich zum New Approach *Klindt*, EuZW 2002, 133 ff.

[495] *Wilrich*, Einl. Rn. 44.

[496] Eingehend *Wilrich*, Einl. Rn. 44 ff.

[497] Abgedeckt sind derzeit: einfache Druckbehälter, Spielzeug, Bauprodukte, Maschinen, persönliche Schutzausrüstung, nicht selbsttätige Waagen, aktive implantierbare medizinische Geräte, Gasverbrauchseinrichtungen, Warmwasserheizkessel, Explosivstoffe für zivile Zwecke, Medizinprodukte, Sportboote, Aufzüge, elektrische Haushaltskühl- und Gefriergeräte, Druckgeräte, In-vitro-Diagnostika sowie Telekommunikationseinrichtungen und Satellitenfunkanlagen.

[498] Dazu gehören derzeit die Niederspannungsrichtlinie, die Richtlinie zur elektromagnetischen Verträglichkeit und die Richtlinie bezüglich Geräten und Schutzsystemen in explosionsgefährdeten Bereichen.

[499] BGBl. I 1979, 629, zuletzt geändert durch Art. 10 des Gesetzes vom 6.1.2004, BGBl. I, 2, 219.

- die neunte Verordnung zum Geräte- und Produktsicherheitsgesetz (Maschinenverordnung)[501]

von Bedeutung. Der Vollständigkeit halber sei aufgrund der offenkundigen Relevanz der Regelwerke für IT-Produkte auch das Gesetz über Medizinprodukte[502] und das Gesetz über die elektromagnetische Verträglichkeit von Geräten[503] erwähnt.

229 Während § 8 Abs. 1 MPG eine eigenständige Vermutungsregel statuiert, ist fraglich, ob das **EMVG** an der in § 4 Abs. 1 GPSG festgesetzten Privilegierung teilhaben kann. Zwar stellt das Gesetz keine Rechtsverordnung nach § 3 Abs. 1 GPSG dar, so dass es gemäß dem Wortlaut von § 4 Abs. 1 GPSG nicht dessen Anwendungsbereich unterliegt. Allerdings setzt das EMVG die EG-Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit in nationales Recht um, so dass hiermit folglich ebenfalls europäisch harmonisiertes Recht vorliegt und unter Berücksichtigung von Sinn und Zweck der Privilegierung Produkte, die in den Anwendungsbereich des EMVG fallen, entsprechend § 4 Abs. 1 GPSG zu beurteilen sind.[504]

230 Indes ist festzuhalten, dass bislang außerhalb von bestimmten Wirtschaftsbereichen **keine speziellen Produktsicherheitsrichtlinien und Verordnungen für den IT-Bereich** gelten. Insbesondere für die Softwareherstellung existieren keine europarechtlich harmonisierten Anforderungen. Demgemäß können insoweit auch keine Vermutungswirkungen im Zusammenhang mit der Einhaltung technischer Regelwerke eingreifen, da hierfür die rechtliche Grundlage bislang fehlt.

(b) Konformitätsvermutung

231 Produkte, welche in den harmonisierten Bereich fallen, dürfen gemäß § 4 Abs. 1 GPSG nur in Verkehr gebracht werden, wenn sie den in den Rechtsverordnungen nach § 3 Abs. 1 GPSG (= GPSGV) vorgesehenen Anforderungen an Sicherheit und Gesundheit und sonstigen Voraussetzungen für ihr Inverkehrbringen entsprechen und Sicherheit und Gesundheit der Verwender oder Dritter oder sonstige in den aufgeführter Rechtsgüter bei bestimmungsgemäßer Verwendung oder vorhersehbarer Fehlanwendung nicht gefährdet werden.

---

[500] BGBl. I 1989, 2541, zuletzt geändert durch Art. 11 des Gesetzes vom 6.1.2004, BGBl. I, 2.

[501] BGBl. I 1993, 704, zuletzt geändert durch Art. 14 der Verordnung vom 23.12.2004, BGBl. I, 3758.

[502] BGBl. I 1994, 1963, neugefasst durch Bekanntmachung vom 7.8.2002, BGBl. I, 3146, zuletzt geändert durch Art. 109 der Verordnung vom 25.11.2003, BGBl. I, 2304.

[503] BGBl. I 1998, 2882, zuletzt geändert durch Art. 3 Abs. 5 des Gesetzes vom 7.7.2005, BGBl. I 1970.

[504] Zustimmend *Hoeren/Ernstschneider*, MMR 2004, 507 (509).

232 Bei einem entsprechend einer harmonisierten Norm hergestellten Produkt wird (widerleglich) **vermutet**, dass es den betreffenden Anforderungen an Sicherheit und Gesundheit genügt (§ 4 Abs. 1 Satz 2 GPSG). **Harmonisierte Normen** in diesem Sinne sind gemäß § 2 Abs. 16 GPSG nicht verbindliche technische Spezifikation, die (1) von einer europäischen Normenorganisation nach den in der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22.6.1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften[505] festgelegten Verfahren angenommen und (2) deren Fundstelle im Amtsblatt der Europäischen Gemeinschaften veröffentlicht wurde.

233 Die Einhaltung der harmonisierten technischen Normen ist für den Hersteller **freiwillig**; er ist an sie nicht gebunden und kann das von der EU-Richtlinie geforderte Sicherheitsniveau auf einem anderen technischen Weg erreichen. Die Vermutungswirkung bildet jedoch einen **Anreiz** zur Einhaltung der technischen Normen.[506] Entscheidet sich der Hersteller nicht nach den Vorgaben einer harmonisierten Norm zu produzieren, trägt er die Beweislast dafür, dass sein Produkt den Vorgaben der einschlägigen Richtlinie entspricht.[507] Diese Kombination von Freiwilligkeit und positiver Vermutungswirkung kann auch als „sanfter Zwang“ zur normgerechten Produktion bezeichnet werden.[508]

(2) Nichtharmonisierter Bereich (§ 4 Abs. 2 GPSG)

234 Außerhalb des durch vertikale und sektorale Richtlinien harmonisierten Bereichs (oben (1)), wenn somit keine Rechtsverordnung nach § 3 Abs. 1 GPSG vorliegen, richtet sich die Zulässigkeit der Inverkehrgabe nach § 4 Abs. 2 GPSG.

(a) Pflichten der IT-Hersteller

235 Nach § 4 Abs. 2 Satz 1 GPSG müssen Produkte so beschaffen sein, dass bei ordnungsgemäßer Verwendung oder vorhersehbarer Fehlanwendung Sicherheit und Gesundheit von Verwendern oder Dritten nicht gefährdet werden. Diese allgemeinen Sicherheitsanforderungen werden in § 4 Abs. 2 Satz 2 Nr. 1 bis 4 GPSG (siehe auch Art. 2 lit. b, 3 Abs. 3 Produktsicherheitsrichtlinie 2001/95/EG) näher konkretisiert. § 4 Abs. 2 Satz 3 GPSG betont ausdrücklich, dass bei der Beurteilung der Produktsicherheit Normen und andere technische Spezifikationen zugrunde gelegt werden können.

---

[505] ABl. EG Nr. L 204 S. 37.
[506] *Wilrich*, § 4 GPSG Rn. 28.
[507] *Wilrich,* Einleitung Rn. 39.
[508] *Spindler*, Unternehmensorganisationspflichten, S. 159.

236 Bei der Bestimmung der Pflichten der IT-Hersteller nach dem GPSG ist zu berücksichtigen, dass die Herstellerpflichten – und daran anschließend die Befugnisse der zuständigen Behörde – grundsätzlich an eine **Gefahr für die Sicherheit und Gesundheit der Produktverwender und Dritter** anknüpfen (§ 4 GPSG). Sie bleiben daher wegen der Ausklammerung von Eigenums- und Vermögensschäden zwangsläufig hinter den zivilrechtlichen Pflichten aus § 823 Abs. 1 BGB (dazu ausführlich oben Rn.119 ff.) zurück, welche auch den Schutz des Eigentums und des Rechts am eingerichteten und ausgeübten Gewerbebetrieb (Recht am Unternehmen) umfassen.[509] Gegenüber einem IT-Hersteller können nach GPSG folglich nur dann behördliche Anordnungen ergehen, wenn dies zur Vermeidung von Personenschäden erforderlich ist.

237 Aus dem GPSG ergeben sich hinsichtlich der Pflichten der Hersteller von Hardware keine wesentlichen Unterschiede gegenüber den Herstellern anderer technischer Geräte. Sie trifft daher insbesondere die Pflicht, dem Produkt eine Gebrauchsanleitung in deutscher Sprache beizufügen (für den nichtharmonisierten Bereich § 4 IV Nr. 2 GPSG).[510] Die Anforderungen an den Schutz der persönlichen Integrität der Verwender und Dritter bilden hierbei – wie in anderem Zusammenhang (oben Rn. 146) bereits ausgeführt – den öffentlich-rechtlich geforderten Mindeststandard ohne die zivilrechtlichen Verkehrspflichten abschließend mitzubestimmen. Besondere Bedeutung aus dem Anforderungskatalog des § 4 Abs. 2 Satz 2 GPSG für die Herstellerpflichten dürfte im Bereich der IT-Hersteller (Hard- und Software) die Einwirkung des Produkts auf andere Produkte, deren Verwendung zu erwarten war (Nr. 2), haben. Insbesondere Softwarehersteller haben daher ggf. etwaige Kompatibilitätsprobleme mit anderen Programmen zu berücksichtigen.

(b) „Nationaler New Approach“

238 In § 4 Abs. 2 Satz 4 GPSG vollzieht der deutsche Gesetzgeber die europäische Konzeption für den nicht harmonisierten Bereich als eine Art **„nationalen New Approach“**[511] nach. Auch im nicht harmonisierten Bereich gilt somit eine Freiwilligkeit der Produktion nach technischen Normen. § 4 Abs. 2 Satz 3 GPSG formuliert lediglich, dass bei der Beurteilung der Produktsicherheit Normen und andere technische Spezifikationen zu-

[509] Dies wird zu wenig berücksichtigt von *Runte/Potinecke*, CR 2004, 725 (728), die beispielsweise auch Informationspflichten zur Datensicherung aus dem GPSG ableiten (die Autoren fassen jedoch – anders als die wohl überwiegende Meinung – unter den Begriff der Sicherheit auch Eigentums- und damit Datenschäden).

[510] *Hoeren/Ernstschneider*, MMR 2004, 507 (510).

[511] *Klindt*, NJW 2004, 465 (466).

grunde gelegt werden können. Aber auch hier gilt die aus dem New Approach stammende Vermutungswirkung zugunsten normkonform hergestellter Produkte. Nationales Gegenstück der europäischen harmonisierten Norm ist hier eine Norm oder sonstige technische Spezifikation, die (1) vom Ausschuss für technische Arbeitsmittel und Verbraucherprodukte (§ 13 GPSG) ermittelt **und** (2) von der beauftragten Stelle[512] im Bundesanzeiger bekannt gemacht wurde (§ 4 Abs. 2 Satz 4 GPSG). Anders als im europäischen Recht wird indes die Normsetzung nicht an private Normungsgremien wie das DIN oder die CEN delegiert, sondern in dem besagten gesetzlich geregelten Ausschuss vorgenommen.

d) Besondere Pflichten bei Verbraucherprodukten (§ 5 GPSG)

239 Soweit Hard- und Software als Verbraucherprodukt im Sinne von § 2 Abs. 3 GPSG einzuordnen sind, treffen den Hersteller die besonderen Pflichten nach § 5 GPSG. Der Hersteller ist daher insbesondere verpflichtet, über von dem Produkt ausgehende Gefahren zu informieren (§ 5 Abs. 1 Nr.1a GPSG), seinen Namen und seiner Adresse auf dem Produkt anzubringen (§ 5 Abs. 1 Nr. 1b GPSG) und Vorkehrungen zu treffen, damit er imstande ist, zur Vermeidung von Gefahren geeignete Maßnahmen zu veranlassen, bis hin zur Rücknahme des Verbraucherprodukts, der angemessenen und wirksamen Warnung und dem Rückruf (§ 5 Abs. 1 Nr.1c GPSG). Gehen von den in Verkehr gebrachten Produkten Gefahren für die Gesundheit und die Sicherheit von Personen aus, hat der Hersteller unverzüglich die zuständige Behörde zu informieren (§ 5 Abs. 2 GPSG).

240 Die genannten Pflichten sind ohne weiteres auf die Hersteller von Hardware anwendbar. Ihre **Übertragung auf Software stößt dagegen auf Schwierigkeiten**. Beispielsweise ist die Informationspflicht nach Nr.1a ist wohl nur schwer auf Software zu übertragen, denn Software weist an sich keine gefährliche Beschaffenheit auf, sondern wird erst infolge eines Programmierfehlers oder nachträglicher Einflussnahme zu einer Gefahr. Die Identifikation des Herstellers (Nr.1b) kann bei online übertragener Software nur durch einen Hinweis im Programm selbst erfolgen.[513] Ein Rückruf von Software erscheint dagegen kaum denkbar. Im Regelfall werden bei erkannten Sicherheitsrisiken unter Ver-

[512] Bundesanstalt für Arbeitsmedizin und Arbeitsschutz, siehe § 2 Abs. 14 und § 12 GPSG.

[513] *Runte/Potinecke*, CR 2004, 725 (729).

hältnismäßigkeitsgesichtspunkten eine Warnung der Verwender und die Zurverfügungstellung eines Updates ausreichen.[514]

2. Normungsverfahren nach dem GPSG

241 Die Vermutungswirkung zugunsten normkonformer Produkte gilt freilich nur für die Konformität mit solchen Normen, die den Anforderungen des GPSG an Normgeber und Verfahren entsprechen. Auch hier wird zwischen harmonisiertem und nicht harmonisiertem Bereich unterschieden.

a) Verfahren im harmonisierter Bereich

242 Gem. § 2 Abs. 16 GPSG gilt die Vermutungswirkung für solche Normen, die von einer **europäischen Normenorganisation** nach dem Verfahren der Richtlinie 98/34/EG (über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften)[515] angenommen und im Amtsblatt der Europäischen Gemeinschaften veröffentlicht worden sind. In concreto handelt es sich bei den Normenorganisationen gemäß Anhang I der Richtlinie 98/34/EG um das CEN (Europäische Komitee für Normung), das CENELEC (Europäisches Komitee für Elektrotechnische Normung) sowie das ETSI (Europäisches Institut für Telekommunikationsstandards). Auch die nationalen Normungsgremien, die in Anhang II der Richtlinie 98/34/EG aufgelistet sind, sind nach Maßgabe von Art. 2, 3 RiLi 98/34/EG in den Normierungsprozess eingebunden. Deutsche Normungsgremien sind gegenwärtig das Deutsche Institut für Normung e.V. (DIN) und die Deutsche Elektrotechnische Kommission im DIN und VDE (DKE). Allerdings kann die Kommission gem. Art. 2 Abs. 4 der Richtlinie 98/34/EG auf Grundlage der Mitteilung eines Mitgliedstaates den Anhang II ändern und gegebenenfalls den Kreis der involvierten nationalen Normungsgremien erweitern.

243 Beschließt ein nationales Normungsgremium die Aufnahme einer neuen Norm in das Normungsprogramm, so hat es die europäischen und nationalen Normungsgremien sowie die Kommission davon zu unterrichten, Art. 2 Abs. 1 Richtlinie 98/34/EG. Über diese nationalen Normungsaktivitäten berät ein ständiger Ausschuss, der aus von den Mitgliedsstaaten ernannten Vertretern besteht, in Zusammenarbeit mit Vertretern der europäischen und nationalen Normungsgremien, Art. 5, 6 Abs. 1 RiLi 98/34/EG. Soweit der Ausschuss dies für sinnvoll erachtet, regt er bei der Kommission die Erarbeitung ei-

[514] *Runte/Potinecke*, CR 2004, 725 (729).
[515] Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22.06.1998, ABl. Nr. L 204, S. 37.

ner europäischen Norm durch ein europäisches Normungsgremium an, Art. 6 Abs. 3 Richtlinie 98/34/EG.

b) Verfahren im nicht harmonisierten Bereich

244 Im nicht harmonisierten Bereich kommt die Vermutungswirkung gem. § 4 Abs. 2 S. 4 GPSG solchen Normen zu, die vom Ausschuss für technische Arbeitsmittel und Verbraucherprodukte ermittelt und von einer beauftragten Stelle im Bundesanzeiger bekannt gemacht worden sind.

245 Dem **Ausschuss für technische Arbeitsmittel und Verbraucherprodukte (AtAV)** obliegt gemäß § 13 Abs. 2 Nr. 2 die Ermittlung von Normen mit Vermutungswirkung im Sinne des § 4 Abs. 2 Satz 4 GPSG. Er ist beim Bundesministerium für Wirtschaft und Arbeit (BMWA) angesiedelt,[516] § 13 Abs. 1 GPSG. Dem Ausschuss gehören „sachverständige Personen aus dem Kreis der zuständigen Behörden für Sicherheit und Gesundheit des Bundes und der Länder, der zugelassenen Stellen (§ 2 Abs. 15 GPSG), der Träger der gesetzlichen Unfallversicherung, des Deutschen Instituts für Normung e.V., der Kommission Arbeitsschutz und Normung, der Arbeitgebervereinigungen, der Gewerkschaften und der beteiligten Verbände, insbesondere der Hersteller und der Verbraucher an- Das BSI als für Sicherheit zuständige Bundesoberbehörde wäre nur dann berechtigt, Vertreter in den Ausschuss zu entsenden, wenn Fragen der Sicherheit und Gesundheit in seine Zuständigkeit fielen (s. § 3 BSIG).

246 Während der alte Ausschuss für technische Arbeitsmittel (AtA) ein reines Beratungsgremium war, ist seit der Einführung des GPSG zum einen die Zuständigkeit für Verbraucherschutz hinzugekommen, zum anderen ist er nunmehr ein **echter Regelungsausschuss,**,[517] wobei sich seine Funktion jedoch in der Ermittlung von Normen und Spezifikationen erschöpft und nicht auch die Aufstellung von Normen umfasst.[518] Grund dafür ist die im Zuge des *nationalen* New Approach eingeführte Vermutungswirkung in § 4 Abs. 2 GPSG.[519]

247 Die Bundesanstalt für Arbeitsmedizin und Arbeitsschutz ist als **beauftragte Stelle** im Rahmen des Normungsverfahrens lediglich für die Bekanntmachung im Bundesanzei-

[516] Laut Gesetz ist dieses zuständig. Allerdings existiert das BMWA durch eine Umstrukturierung nicht mehr. Zuständige Behörde ist nunmehr das Bundesministerium für Arbeit und Soziales (BMAS).

[517] Amtl. Begründung GPSG, BT-Drucks. 15/1620, S. 33 f.

[518] *Klindt*, § 13 GPSG Rn. 5.

[519] *Wilrich*, § 13 GPSG Rn. 4.

ger zuständig. Auch dies ist Voraussetzung für das Eingreifen der Vermutungswirkung. An der Ermittlung der Normen hat sie jedoch keinen Anteil.

3. Zertifizierung

a) CE-Kennzeichen

248 Durch die **CE-Kennzeichnung**[520] (Abkürzung für „Communautés Européenes") erklärt der **Hersteller bzw. Importeur selbst**, dass das Produkt entsprechend der Bestimmungen der auf ihn anwendbaren EU-Richtlinien hergestellt wurde und somit im Europäischen Binnenmarkt in Verkehr gebracht werden darf.[521] Die CE-Kennzeichnung ist obligatorisch, sofern das Produkt einer Richtlinie unterfällt, die eine CE-Kennzeichnung vorschreibt. Es handelt sich dabei indes um kein Zeichen der Qualität oder der Sicherheit des Produkts,[522] sondern allein um eine Kennzeichnung zur Erleichterung des freien Warenverkehrs in der EU und dem EWR (europäischer **„Reisepass" für Produkte**).[523] Die Marktüberwachungsbehören können bei mit dem CE-Kennzeichen versehenen Produkten von der Einhaltung der wesentlichen Sicherheitsanforderungen der EU-Richtlinien ausgehen und müssen Maßnahmen gegen die betreffenden Produkte grundsätzlich unterlassen.[524]

249 Voraussetzung für die CE-Kennzeichnung ist, dass der Hersteller vor dem ersten Inverkehrbringen ein **Konformitätsbewertungsverfahren** nach dem EU-Modulsystem[525] durchführt, an dessen Ende die EG-Konformitätserklärung des Herstellers steht, dass er die grundlegenden Gesundheits- und Sicherheitsanforderungen der betreffenden EU-Richtlinien erfüllt. Welche Module im Einzelnen zur Anwendung kommen, legen die Richtlinien unter Berücksichtigung des Gefahrenpotentials des Produkts fest, wobei

---

[520] Richtlinie 93/68/EWG des Rates vom 22. Juli 1993 zur Änderung der Richtlinien 87/404/EWG (einfache Druckbehälter), 88/378/EWG (Sicherheit von Spielzeug), 89/106/EWG (Bauprodukte), 89/336/EWG (elektromagnetische Verträglichkeit), 89/392/EWG (Maschinen), 89/686/EWG (persönliche Schutzausrüstungen), 90/384/EWG (nichtselbsttätige Waagen), 90/385/EWG (aktive implantierbare medizinische Geräte), 90/396/EWG (Gasverbrauchseinrichtungen), 91/263/EWG (Telekommunikationsendeinrichtungen), 92/42/EWG (mit flüssigen oder gasförmigen Brennstoffen beschickte neue Warmwasserheizkessel) und 73/23/EWG (elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen), ABl. L 220 vom 30.8.1993, S. 1–22 und *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfaßten Richtlinien, abrufbar unter:
http://ec.europa.eu/enterprise/newapproach/legislation/guide/document/guidepublicde.pdf

[521] *Wilrich*, § 6 GPSG Rn. 5.

[522] *Niebling,* DB 1996, 80 (81); *Niebling*, Die CE-Kenzeichnung, S. 23 f.; *Foerste*, in: v.Westphalen, ProdHaftHdb, § 24 Rn. 94; Bamberger/Roth-*Spindler* § 823 BGB Rn. 490.

[523] *Wilrich*, § 6 GPSG Rn. 7.

[524] *Finke*, Die Auswirkungen der europäischen technischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht, S. 89; *Wilrich*, § 4 GPSG Rn. 26.

[525] 93/465/EWG: Beschluß des Rates vom 22. Juli 1993 über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module für die verschiedenen Phasen der Konformitätsbewertungsverfahren und die Regeln für die Anbringung und Verwendung der CE- Konformitätskennzeichnung, ABl. EG Nr. L 220 vom 30.8.1993 S. 23 (Modulbeschluss).

grundsätzlich zwischen Herstellererklärung, Prüfung durch eine benannte Stelle und dem Erfordernis eines zertifizierten Qualitätssicherungssystems[526] unterschieden werden kann.[527] Zuständig für die **Akkreditierung** der benannten Stellen sind in Deutschland die Zentralstelle der Länder für Sicherheitstechnik (ZLS)[528] und die Zentralstelle der Länder für Gesundheitsschutz bei Arzneimitteln und Medizinprodukten (ZLG)[529].

b) GS-Zeichen

250 Das **GS-Zeichen** hat seine gesetzliche Grundlage in § 7 GPSG (vormals § 3 Abs. 4 GSG). Es handelt sich um ein rein nationales Zeichen, welches die hohen deutschen Sicherheitsstandards kenntlich machen soll.[530] Das GS-Zeichen steht für „geprüfte Sicherheit" und wird auf Antrag des Herstellers durch eine von der Zentralstelle der Länder für Sicherheitstechnik (ZLS) **anerkanne GS-Stelle**[531] (§ 11 GPSG) für technische Arbeitsmittel und verwendungsfertige Gebrauchsgegenstände vergeben.

251 Voraussetzung der Zertifizierung ist der Nachweis der Übereinstimmung des geprüften Produkts mit den Anforderungen des GPSG sowie anderer Rechtsvorschriften hinsichtlich der Gewährleistung von Sicherheit und Gesundheit durch eine Baumusterprüfung, sowie der Nachweis, dass die Voraussetzungen eingehalten werden, die bei der Herstellung der technischen Arbeitsmittel und verwendungsfertigen Gebrauchsgegenstände zu beachten sind, um ihre Übereinstimmung mit dem geprüften Baumuster zu gewährleisten (§ 7 Abs. 1 GPSG). In regelmäßigen Abständen führt die Zertifizierungsstelle zudem Fertigungskontrollen durch, wobei überprüft wird, ob das Produkt noch dem geprüften Baumuster entspricht (§ 7 Abs. 2 GPSG).

4. Anordnungsbefugnisse der Marktüberwachungsbehörden

a) Verwaltungsrechtliche Befugnisse

252 Die nach Landesrecht zuständigen Marktüberwachungsbehörden (s. § 8 Abs. 1 Satz 1 GPSG) haben das Inverkehrbringen von Produkten sowie in Verkehr gebrachte Produk-

---

[526] Entspricht ein Qualitätssicherungssystem den Organsationsnormen EN 29000ff. (= ISO 9000ff.), wird vermutet, dass die Anforderungen an ein ordnungsgemäßes Qualitätssicherungssystem erfüllt sind, siehe Modulbeschluss 93/465/EWG (Fn. 525) Modul D, 3.3; Modul E, 3.3.

[527] *Kaufmann*, DB 1994, 1033 (1034); *Roßnagel*, DVBl 1996, 1181 (1183); *Finke*, Die Auswirkungen der europäischen technischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht, S. 90, 206.

[528] Siehe http://www.zls-muenchen.de/.

[529] Siehe http://www.zlg.de/.

[530] *Klindt*, § 7 GPSG Rn. 1.

[531] Z.B. TÜV, VDE. Siehe die Liste der zugelassenen Stellen unter http://www.zls-muenchen.de/.

te aufgrund eines Überwachungskonzeptes zu überwachen (§ 8 Abs. 2 GPSG). Hat die Behörde den begründeten Verdacht, dass ein Produkt nicht den Anforderungen nach § 4 GPSG entspricht, ist sie gehalten, die erforderlichen Maßnahmen zu treffen (§ 8 Abs. 4 GPSG. Die Behörde kann nach GPSG insbesondere:

- Maßnahmen anzuordnen, die gewährleisten, dass ein Produkt erst in den Verkehr gebracht wird, wenn es den Anforderungen nach § 4 Abs. 1 und 2 entspricht,
- anzuordnen, dass ein Produkt von einer zugelassenen Stelle oder einer in gleicher Weise geeigneten Stelle überprüft wird,
- anzuordnen, dass geeignete, klare und leicht verständliche Warnhinweise über Gefährdungen, die von dem Produkt ausgehen, angebracht werden,
- das Inverkehrbringen eines Produkts für den zur Prüfung zwingend erforderlichen Zeitraum vorübergehend zu verbieten,
- zu verbieten, dass ein Produkt, das nicht den Anforderungen nach § 4 Abs. 1 und 2 entspricht, in den Verkehr gebracht wird,
- die Rücknahme oder den Rückruf eines in Verkehr gebrachten Produkts, das nicht den Anforderungen nach § 4 GPSG entspricht, anzuordnen, ein solches Produkt sicherzustellen und, soweit eine Gefahr für den Verwender oder Dritten auf andere Weise nicht zu beseitigen ist, seine unschädliche Beseitigung zu veranlassen,
- anzuordnen, dass alle, die einer von einem in Verkehr gebrachten Produkt ausgehenden Gefahr ausgesetzt sein können, rechtzeitig in geeigneter Form, insbesondere durch den Hersteller, auf diese Gefahr hingewiesen werden.
- selbst die Öffentlichkeit warnen, wenn andere ebenso wirksame Maßnahmen, insbesondere Warnungen durch den Hersteller, nicht oder nicht rechtzeitig getroffen werden.

Bei allen Maßnahmen der Behörden gilt aus Gründen der Verhältnismäßigkeit das Prinzip des **Vorrangs von Eigenmaßnahmen** der für das Inverkehrbringen zuständigen Person (§ 8 Abs. 4 Satz 4 GPSG).

b) Vermutungswirkung von Zertifikaten

253 Gemäß § 8 Abs. 2 Satz 3 GPSG geht die zuständige Marktüberwachungsbehörde bei Produkten, welche einer Verordnung nach § 3 Abs. 1 GPSG unterliegen und mit **CE-Kennzeichen** (Rn. 248 ff.) versehen sind davon aus, dass sie den dort genannten Anfor-

derungen entsprechen. Im Hinblick auf verwaltungsrechtliche Anordnungen bewirkt das CE-Kennzeichen damit eine Vermutung zugunsten der **Verkehrsfähigkeit** des Produkts („Unschuldsvermutung“).[532] Abgesehen von Stichproben dürfen diese Produkte damit nicht Gegenstand einer systematischen Marktkontrolle werden.[533]

254 Das CE-Kennzeichen bewirkt in Verbindung mit § 8 Abs. 2 Satz 3 GPSG indes nur einen formalen Schutz gegen behördliche Anordnungen.[534] Im Rahmen des in den EU-Richtlinien geregelten **Schutzklauselverfahrens** (s. auch Art. 95 Abs. 5 EG) kann die Behörde gegenüber Produkten, welche ihrer Ansicht nach die wesentlichen Anforderungen nicht einhalten, *vorläufige* Maßnahmen treffen.[535] Sie muss dann aber die Europäische Kommission über Maßnahmen, welche den freien Warenverkehr beeinträchtigen informieren, damit die Kommission in die Lage versetzt wird, die Berechtigung er Maßnahmen einzuschätzen und ggf. eine Überprüfung der harmonisierten Normen in die Wege zu leiten.[536]

255 Bei technischen Arbeitsmitteln und verwendungsfertigen Gebrauchsgegenständen, die mit dem **GS-Zeichen** nach § 7 Abs. 1 GPSG versehen sind (dazu Rn. 99 ff.), ist davon auszugehen, dass diese den Anforderungen an Sicherheit und Gesundheit nach § 4 Abs. 1 und 2 GPSG sowie anderen Rechtsvorschriften entsprechen (§ 8 Abs. 2 Satz 4 GPSG). Über § 4 Abs. 2 Satz 4 GPSG hinaus wird damit die Übereinstimmung des Produkts mit *allen* gesetzlichen Anforderungen vermutet.[537] In der Praxis bedeutet ein zu

---

[532] *Europäische Kommission*, Erläuterung zur Maschinenrichtlinie, Rn. 181, 182, S. 50 f., siehe http://ec.europa.eu/enterprise/mechan_equipment/machinery/guide/guide_de.pdf.

[533] Entschließung des Rates vom 7. Mai 1985 über eine neue Konzeption auf dem Gebiet der technischen Harmonisierung und der Normung, ABl. EG Nr. C 136 vom 4.6.1985 S. 1, Anhang II (Modellrichtlinie) B. II. 2; *Wilrich*, § 8 GPSG Rn. 18.

[534] *Wilrich*, § 8 GPSG Rn. 18.

[535] Dazu Entschließung des Rates vom 7. Mai 1985 über eine neue Konzeption auf dem Gebiet der technischen Harmonisierung und der Normung, ABl. EG Nr. C 136 vom 4.6.1985 S. 1, Anhang II (Modellrichtlinie) B. VII; *Finke*, Die Auswirkungen der europäischen technischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht, S. 90; *Wilrich*, § 9 GPSG Rn. 8.

[536] *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfassten Richtlinen, S. 58 ff.: Hält die Kommission die Maßnahmen für gerechtfertigt, setzt sie den betreffenden Mitgliedstaat sowie die übrigen Mitgliedstaaten umgehend davon in Kenntnis, andernfalls fordert sie den betreffenden Mitgliedstaat auf, seine Maßnahmen aufzuheben und unverzüglich das Nötige zu veranlassen, damit die Produkte im Gebiet des betreffenden Staates wieder zum freien Warenverkehr zugelassen werden. Wird die Schutzklausel aufgrund einer Lücke in einer harmonisierten Norm, auf die sich eine Konformitätsvermutung gründet, in Anspruch genommen, leitet die Kommission die Angelegenheit nach Anhörung der betroffenen Parteien an den gemäß Richtlinie 98/34/EG eingerichteten Ausschuss für Normen und technische Vorschriften und ggf. – sofern dies in der den Harmonisierungsrichtlinien vorgesehen ist – spezielle Sektorausschüsse weiter.

[537] *Wilrich*, § 4 GPSG Rn. 44, § 8 GPSG Rn. 19: die Vermutung nach § 4 Abs. 2 Satz 4 GPSG bezieht sich dagegen nur auf die „betreffenden Anforderungen“ der Norm oder technischen Spezifikation.

Recht vergebenes GS-Zeichen damit eine deutliche Erschwernis für behördliches Vorgehen gegen das betreffende Produkt.[538]

5. Zusammenfassung

256 Das öffentliche Produktsicherheitsrecht erfasst sowohl Hard- als auch Softwareprodukte. Für Hardwareprodukte ergeben sich keine grundlegenden Besonderheiten gegenüber anderen elektrischen Geräten. Demgegenüber ist der Anwendungsbereich für Softwareprodukte von vornherin deutlich beschränkt, da der Schutzzweck des GPSG auf Personenschäden beschränkt ist und insbesondere Datenschäden somit nicht erfasst werden.

V. Ergebnis

257 Aus rechtspolitischer Sicht sind insbesondere folgende Defizite zu beklagen:

- die verschuldensabhängige Produkthaftung greift grundsätzlich nur bei Rechtsgutsverletzungen ein; hier bestehen noch zahlreiche Unsicherheiten über die Reichweite. Insbesondere bei Vermögensschäden sowie Betriebsausfallschäden besteht die Gefahr, dass derartige Schäden nicht von der verschuldensabhängigen Produkthaftung erfasst werden.
- das Produkthaftungsrecht sieht grundsätzlich keine Pflichten vor, dass ein IT-Hersteller „Patches“ zur Verfügung stellt; er kann sich mit Warnungen begnügen
- die Verantwortlichkeit für Schnittstellen zu anderen Programmen ist nach wie vor ungeklärt
- Im verschuldensunabhängigen Produkthaftungsrecht ist nach wie vor ungeklärt, ob Software als Produkt überhaupt erfaßt wird. Zudem ist auch hier der Kreis der erfaßten Schäden auf Eigentumsschäden bei Verbrauchern sowie Körperschaden allgemein begrenzt.

258 Im öffentlich-rechtlichen Produktsicherheitsrecht fehlt es bislang vor allem auf europäischer Ebene an entsprechenden sektorspezifischen Richtlinien für den IT-Bereich; auf nationaler Ebene ist die Verengung des GPSG auf Gefahren für Leib und Leben (Gesundheit) zu beklagen, die zahlreiche IT-Risiken unberücksichtigt lässt. Ebensowenig sind allgemeine technische Regeln nach dem nationalen Normungsverfahren im GPSG zu verzeichnen.

D. Verantwortlichkeit der IT-Nutzer

I. Grundsätzliche Überlegungen

1. Die Doppelrolle von IT-Nutzern

[538] *Wilrich*, § 8 GPSG Rn. 19.

259 Den Pflichten der IT-Hersteller, aber auch anderer IT-Verwender in der Wertschöpfungskette, stehen mögliche Pflichten der IT-Nutzer zum Selbstschutz gegenüber. Im Zivilrecht findet dieser Gedanke des zumutbaren Selbstschutzes seinen Niederschlag in erster Linie in § 254 BGB.

260 Damit würde sich indes die Problematik kaum erschöpfen: Denn anders als in klassischen Wertschöpfungsketten, bei denen definitiv von einem Endverbraucher gesprochen werden kann, der ein Produkt „konsumiert", ist die Situation in der IT-Branche anders. IT-Nutzer verwenden typischerweise die IT-Produkte ihrerseits, um andere Produkte herzustellen oder Dienstleistungen zu erbringen. Selbst wenn die IT-Nutzer nicht eigenständig in anderen Wertschöpfungsketten eingeschaltet sind, stehen sie doch in vielfältiger Weise in Interaktion mit anderen IT-Nutzern, oftmals durch ihre Anbindung an entsprechende Netze wie das Internet und die damit gegebenen Kommunikationsmöglichkeiten. Daher wäre es verkürzt, sich nur auf die Selbstschutz- und Schadensminderungspflichten der IT-Nutzer im Verhältnis zu IT-Herstellern oder –Intermediären zu konzentrieren; vielmehr können die IT-Nutzer auch Pflichten gegenüber Dritten treffen, die unmittelbar mit dem Einsatz von IT-Produkten zusammenhängen. Die IT-Nutzer befinden sich daher in einer **Doppelrolle**, die im Folgenden immer im Blickfeld zu behalten ist. Allerdings werden diese Pflichten hinsichtlich ihrer Konkretisierung (Sorgfaltsstandards nach § 276 BGB) oftmals gleichbedeutend sein mit den über § 254 BGB zu definierenden Pflichten.[539] Um den Rahmen der hier vorliegenden Untersuchung nicht zu sprengen, können daher oft die jeweiligen Pflichten gemeinsam behandelt werden, sofern nicht aus besonderen Gründen eine Differenzierung geboten ist.

261 In diesem Rahmen sind **Differenzierungen je nach den Gruppen der verschiedenen IT-Nutzer** geboten, insbesondere ob es sich um private (Rn. 275 ff.) oder kommerzielle IT-Nutzer (Rn 331 ff.) handelt, bei letzteren wiederum nochmals in bestimmte Sektoren mit unterschiedlichen Risikopotentialen unterteilt, etwa für den Finanzsektor (D.III.4.) oder für Berufsgruppen, die besonderen Pflichten unterliegen (D.V.).

262 Die Unterteilung ist sowohl für die zivilrechtliche Pflichtenbestimmung wie für die öffentlich-rechtlichen Vorgaben relevant. Während in der zivilrechtlichen Bewertung häufig Zumutbarkeitserwägungen in wirtschaftlicher Hinsicht betrachtet werden, die regelmäßig nur kommerzielle Anwender wegen ihrer wirtschaftlichen Leistungsfähigkeit und

[539] Objektiver Maßstab (hM) Bamberger/Roth-*Unberath*, § 254 BGB Rn. 10; MünchKommBGB-*Oetker*, § 254 BGB Rn. 35; Palandt-*Heinrichs*, § 254 BGB Rn. 8; Erman-*Kuckuk*, § 254 BGB Rn. 24; *Looschelders*, Schuldrecht AT, Rn. 1023.

den entsprechenden angemessenen Erwartungen der Allgemeinheit treffen, werden auch öffentlich-rechtliche Pflichten meist an bestimmte Mindestkriterien geknüpft. Hier kann als qualifizierendes Merkmal z.B. das Vorliegen eines gewerblichen Handelns oder aber, wie im Datenschutz, die Verarbeitung von Daten über den persönlichen oder familiären Bereich hinaus,[540] was im Ergebnis fast immer nur bei kommerziellen Nutzern der Fall sein wird.

2. Die Abgrenzung der IT-Nutzung (Definition)

263 Zunächst ist zu klären, wer als privater Nutzer anzusehen ist: Als normative Anknüpfungspunkte hierfür könnten zunächst §§ 13, 14 BGB dienen, aber auch europarechtliche Vorgaben sowie Regelungen des Produkthaftungsrechts. Diese Differenzierungen beanspruchen auch für das öffentliche Recht Gültigkeit, sofern dieses zwischen privaten und gewerblichen Abnehmern unterscheidet – auch wenn grundsätzlich die eigenständigen Definitionen der jeweiligen öffentlich-rechtlichen Norm zu berücksichtigen sind. Bereits hier wird die oben (Rn. 259) angesprochene Doppelfunktion deutlich:

a) Privater Nutzer, Verbraucher und Unternehmer

264 §§ 13, 14 BGB regeln die **Verbraucher- bzw. Unternehmereigenschaft**. Hierfür wird grundsätzlich an den Abschluss eines Rechtsgeschäfts, also an eine konkrete rechtlich wirksame Handlung angeknüpft.[541] Unter entsprechender Anwendung wäre demnach privater Nutzer derjenige, dessen schädigende Handlungen in den privaten Bereich einzuordnen sind, der also konkret für den eigenen Bedarf gehandelt hat. In Abgrenzung dazu wäre ein Nutzer als kommerzieller Nutzer einzustufen, sofern seine Handlungen einen Bezug zu seinem Geschäft aufweisen.

265 Allerdings erscheint diese Differenzierung im hier diskutierten Zusammenhang **zunächst nur bedingt zielführend**. Denn die Abgrenzung von privaten und kommerziellen Nutzern wirft vor allem für die Eigenverantwortlichkeit der IT-Nutzer gegenüber Dritten aufgrund der **Heterogenität der Computernutzung** eine Reihe von Problemen auf: Häufig lässt sich eine konkrete Handlung des Nutzers direkt nicht ausmachen, da sein Rechnersystem ohne sein weiteres Zutun etwa schädigende Angriffe auf Dritte durchführen kann. Die Handlung des Nutzers, an die für die Qualifizierung nach §§ 13, 14 BGB angeknüpft würde, müsste also im Augenblick der Beeinträchtigung des eige-

[540] S. dazu näher unten Rn. 404 ff.

[541] Bamberger/Roth-*Schmidt-Räntsch*, § 13 BGB Rn. 5; MünchKommBGB-*Micklitz*, § 13 BGB Rn. 4; rechtsvergleichend zum Verbraucherbegriff *Faber*, ZEuP 1998, 854.

nen Rechnersystems ermittelt werden, obwohl die Schädigung eventuell viel später erfolgt. Grenzt man nach der jeweilig vorliegenden Handlung ab, so hätte dies zur Folge, dass der Nutzer eines einzigen Computersystems **unterschiedlichen Pflichtbereichen** unterworfen wäre. Das System wäre also eventuell in bestimmten Situationen als konform mit eventuellen Sicherungspflichten einzustufen, während dieselbe Rechnereinheit in ihrer Konfiguration auch einen Pflichtverstoß (mangels Sicherheit) darstellen könnte.

266 Diese augenscheinlich widersprüchliche Einordnung ist jedoch hinzunehmen. Zunächst sind viele Pflichten, die dem Nutzer obliegen, **dauerhafter und grundlegender Natur**, die die Person in allen Funktionen und Rollen treffen, etwa die Einrichtung eines Virenscanners und dessen regelmäßiges Update.[542] Darüberhinaus kann darauf abgestellt werden, **in welcher Funktion der Nutzer am Verkehr teilnimmt**: Ist er etwa nicht mit anderen IT-Nutzern verbunden (was indes selten der Fall sein dürfte), reduzieren sich entsprechend seine Pflichten. Wird er seine IT-Produkte dagegen auch gewerblich oder gar in Bereichen mit besonderem Gefahrenpotential einsetzen, so kann er sich nicht darauf berufen, dass eine Schädigung in seinem privaten Bereich seinen Ausgang nahm, etwa durch Befall seines Rechners in seiner Privatsphäre mit einem Virus, dessen schädigende Wirkung sich dann später über den Rechner des IT-Nutzers an andere fortsetzte.

b) Arbeitnehmer

267 Diese Problematik stellt sich insbesondere bei der hier vorzunehmenden Abgrenzung bei **Arbeitnehmern**. Diese handeln regelmäßig im Rahmen des Betriebs und können dabei auch Kundenkontakt haben. Möglicherweise fehlt ihnen jedoch die Berechtigung, Schutzmaßnahmen überhaupt zu ergreifen (Admin-Rechte). Selbst wenn sie die Berechtigung haben, so sind die Pflichten dem Betriebsinhaber zuzuweisen, nicht aber dem einzelnen Arbeitnehmer. Auch ist möglich, dass der Arbeitnehmer an seinem privaten Computer arbeitet und mit diesem dem kommerziellen Betrieb zuzuordnen sein könnte. Fraglich ist, ob die Pflichten, die sie bei der Handlung am Arbeitsplatz haben könnten, auch im rein privaten Bereich weiter gelten müssten. Zwar könnte sich hier die Zurechnung der Gefahrenquellen zum Betriebsinhaber wiederum wegen fehlender Zugriffsmöglichkeiten auf den (privaten) Rechner des Nutzers schwierig gestalten; doch würde damit verkannt, dass der Betriebsinhaber es in der Hand hat, überhaupt den Einsatz von

[542] Dazu sogleich.

privaten Rechnern zuzulassen, einschließlich von Richtlinien zur entsprechenden Konfiguration von Sicherheitsmaßnahmen.

268 Auch hier ist auf den Anknüpfungspunkt einer möglichen Pflicht abzustellen. Der Arbeitnehmer, der nicht an betriebseigenen Systemen arbeitet, kann tatsächlich während seiner Tätigkeit für das Unternehmen nicht gegenüber anderen Mitarbeitern zu Lasten des Geschädigten privilegiert werden. Seine Pflichten bezüglich der IT-Sicherheit des Systems erfolgen aber regelmäßig nicht aufgrund eigenen überlegenen Wissens, sondern weil er im Rahmen des Verantwortungsbereichs des Unternehmens auch besondere Gefährdungen auszuschließen hat. Insofern wird ihm ein überlegenes Wissen bzw. eine Organisationsstruktur des Unternehmens zugerechnet,[543] was wiederum auch die Zuordnung zum Unternehmen ermöglicht. Der Arbeitnehmer muss im Rahmen des Organisationsverbundes seines Unternehmens die notwendigen Anstrengungen zum Schutz seiner Kunden und Dritter treffen; verantwortlich ist indes hierfür der Arbeitgeber als Herrscher über die Gefahrenquellen insgesamt. Diese Organisationsstruktur steht dem Arbeitnehmer dagegen im privaten Umfeld nicht zur Verfügung. Daher kann ihm ein entsprechendes Wissen, das ihm im Rahmen seines Arbeitsumfeldes zur Verfügung steht (oder stünde), nicht zugerechnet werden, so dass Arbeitnehmer auch an mobilen Rechnersystemen (Laptops, PDAs etc.), die sowohl privat als auch beruflich genutzt werden, nicht zwangsläufig als kommerzielle Nutzer einzustufen sind, wenn sie privat handeln.

269 Handelt der Arbeitnehmer dagegen v**on seinem beruflichen Umfeld aus, jedoch in privater Funktion**,[544] profitiert er von den Sicherungsvorkehrungen seines Arbeitgebers und muß sich die entsprechenden Sicherungsmöglichkeiten zurechnen lassen.

270 **Gleiches gilt für Arbeitnehmer**, die **von zu Hause** oder allgemein mit einem eigenen Computersystem arbeiten: Auch sie treffen bei „privater“ Nutzung die gleichen Pflichten wie bei der Nutzung als Arbeitnehmer, sofern sie sich die entsprechenden Sicherungsinfrastrukturen ihrer Arbeitgeber zunutze machen können. Bei sog. **Telearbeitern** wäre schließlich zu überlegen, ob nicht eine Abgrenzung nach dem Umfang der nichtprivaten Nutzung eines Computersystems angebracht wäre, wie sie bereits bei der Un-

[543] BGH NJW 1995, 1339 (1341); BGH NJW 1993, 1066; BGHZ 135, 202 mwN.

[544] Nach Berichten aus der Praxis ist etwa der Einsatz von digitaler Signaturen zum Online-Banking daran weitgehend gescheitert, dass die Kunden das Online-Banking vom Arbeitsplatz aus durchführen wollten – hier aber kein Signaturkarteneinsatz möglich ist, sondern nur das PIN-TAN-Verfahren (LEGAL-IST Workshop zu Privacy, Identity, Management, 17.3.2006, Göttingen). Schon allein diese Tatsache zeigt, dass die private Nutzung am Arbeitsplatz nicht zu unterschätzen ist.

ternehmereigenschaft im Sinne von §§ 13, 14 BGB eine Rolle spielt,[545] und auch im Produkthaftungsrecht angewandt wird.[546] Wenn also ein überwiegender Teil der Rechnernutzung kommerziell erfolgt, wäre der Nutzer als kommerzieller Nutzer anzusehen.

c) Expertenwissen

271 Keine Probleme bei der Einordnung als privater oder kommerzieller Nutzer bereitet das Vorliegen von **Expertenwissen**. Dem IT-Experten können grundsätzlich schon aufgrund vorhandener Verantwortlichkeitsregelungen im Einzelfall weitergehende Pflichten obliegen.

d) Zwischenergebnis

272 Die Pflichten eines Nutzers sind damit nicht einheitlich zu definieren, sondern rollenabhängig; sie können je nach Umfeld und Möglichkeiten erheblich differieren. Als privater Nutzer kann daher unter Zugrundelegung der EG-Produkthaftungsrichtlinie 85/374/EWG nur derjenige definiert werden, „wer die Sache nutzt oder verbraucht, ohne damit seinen Lebensunterhalt zu verdienen oder sonstige Zwecke zu verfolgen, die außerhalb einer privaten Existenz und Tätigkeit liegen."[547] Nicht privat ist demnach zunächst, wer gewerblich oder freiberuflich handelt.[548]

273 Da es sich um die Abgrenzung von privater und kommerzieller Nutzung von Informationstechnik handelt, müsste die kommerzielle Tätigkeit demnach entweder im Erbringen von Diensten *mit* dem System liegen oder die Tätigkeit *mittels* Informationstechnik erbracht bzw. gefördert werden. Auch Handlungen bezüglich Rechnersystemen, die also nicht direkt mit einem eventuell angebotenen Produkt zu tun haben, aber dennoch im weiteren Sinne für die Ausübung der Tätigkeit genutzt werden, sind somit erfasst. Hierzu könnte beispielsweise eine computergestützte Verwaltung, Consumer-Relationship-Management-Systeme u.ä. zählen.

274 Privater Nutzer kann zudem **nur eine natürliche Person** sein, juristischen Personen fehlt es insoweit am „Privatleben".[549] Die Produkthaftungsrichtlinie stellt demnach auf die Nutzung einer Sache ab. Die genutzte Sache wäre vorliegend ein Rechnersystem, auf das sich eventuelle Pflichten beziehen würden. Als privater Nutzer ist demnach ne-

---

[545] OLG Naumburg WM 1998, 2158; Erman-*Saenger*, § 13 BGB Rn. 17; *Pfeiffer,* NJW 1999, 169 (173); aA Bamberger/Roth-*Schmid-/Räntsch*, § 13 BGB Rn. 12.

[546] *Taschner/Frietsch*, § 1 ProdHaftG, Rn. 32 f.; *v.Westphalen*, in: v.Westphalen, ProdHaftHdb, Bd. 2, § 72 Rn. 29.

[547] Schmidt-Salzer/Hollmann-*Schmidt-Salzer*, Art. 9 RL, Rn. 47.

[548] *v.Westphalen*, in: v.Westphalen, ProdHaftHdb, Bd. 2, § 72 Rn. 21 ff.

[549] *Faber*, ZEuP 1998, 854 (883); *Taschner/Frietsch*, § 1 ProdHaftG Rn. 36; ebenso der Verbraucherbegriff in § 13 BGB, MünchKommBGB-*Micklitz*, § 13 BGB Rn. 10.

gativ abgegrenzt anzusehen, wer als natürliche Person ein Rechnersystem nicht (überwiegend) gewerblich oder freiberuflich nutzt. Der Arbeitnehmer unterfällt nur im Rahmen seiner Arbeitnehmertätigkeit den Pflichten für kommerzielle Nutzer.

II. Private IT-Nutzung

275 Private Nutzer treffen im Bereich der IT-Sicherheit regelmäßig keine **vertraglichen Pflichten**. Eine wichtige Ausnahme bildet jedoch die Teilnahme am **E-Commerce**, insbesondere die den Bankkunden treffenden Pflichten beim Online-Banking (dazu ausführlich unten Rn. 280 ff.). Regelmäßig wird es jedoch – gerade imVerhältnis zwischen Privaten – an vertraglichen Beziehungen fehlen, so dass eine Haftung Privater nur auf **außervertragliche Ansprüche** gestützt werden kann. Spezialgesetzlich normierte Pflichten bestehen für Private im IT-Sektor soweit ersichtlich nicht.

1. Vorsätzliche Verletzungshandlungen

276 Als vorsätzliche Schädigungshandlungen kommen im Bereich der IT-Sicherheit vor allem **Hacking**, **Denial-of-Service-Attacken** und die bewusste **Weiterverbreitung von Viren** in Betracht.[550] Gegenüber dem privaten Nutzer als Täter kommen in diesem Fällen Schadensersatzansprüche wegen der Verletzung von Schutzgesetzen (§ 823 Abs. 2 BGB) und wegen vorsätzlich sittenwidriger Schädigung (§ 826 BGB) in Betracht, so dass ohne Rücksicht auf eine Rechtsgutsverletzung im Sinne von § 823 Abs. 1 BGB auch primäre Vermögensschäden ersatzfähig sind. Relevantes Schutzgesetz in diesem Bereich ist neben strafrechtlichen Normen wie beispielsweise § 202a StGB (Ausspähen von Daten) oder § 303a StGB (Datenveränderung) vor allem § 43 Abs. 2 Nr. 4 BDSG. Danach handelt ordungswidrig, wer die Übermittlung personenbezogener Daten, welche nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht.[551] Soweit dem Geschädigten hiernach ein Anspruch zusteht, wird eine Inanspruchnahme des Täters jedoch häufig an praktischen **Durchsetzungsproblemen** scheitern.

2. Sicherheitspflichten privater IT-Nutzer gegenüber Dritten

277 Mangels eines entsprechenden Vorsatzes wird eine Haftung privater Nutzer oftmals nur auf die Verletzung **deliktischer Verkehrspflichten** gestützt werden kann. Der folgende Abschnitt befasst sich mit deliktischen Verkehrspflichten privater Nutzer, die dabei her-

[550] Ausführlich. dazu *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 500 ff., 512 ff.

[551] Dazu *Gola/Schomerus*, § 43 BDSG Rn. 23; *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 502.

ausgearbeiteten Wertungen können jedoch auch im vertraglichen Bereich herangezogen werden (zum Online-Banking unten Rn.542 ff.).[552] Die Sorgfaltspflichten privater Nutzer können in doppelter Hinsicht relevant werden: Zum einen bei Schädigung Dritter infolge unterlassener Sicherungsmaßnahmen (Rn. 278 ff.), zum anderen spiegelbildlich im Rahmen des Mitverschulden (Rn. 314 ff.).

a) Rechtsgutverletzung

278 Die Haftung nach § 823 Abs. 1 BGB beruht auf der schuldhaften Verletzung eines der dort aufgezählten Rechtsgüter oder absoluten Rechte. Hinsichtlich der Verletzung der Rechtsgüter **Leben**, **Körper**, **Gesundheit** und **Freiheit** kann im Wesentlichen auf die zur Produkthaftung gemachten Ausführungen verwiesen werden (oben **Rn. 107**). Ein Eingriff in diese Rechte dürfte bei privaten IT-Nutzern kaum vorkommen, ist aber nicht völlig auszuschließen. Deutlich mehr praktische Relevanz dürfte bei privaten Nutzern eine **Eigentumsverletzung** wegen Störung der Integrität von Daten (z. B. infolge der Weiterverbreitung von Viren) haben (**oben Rn. 108 ff.**).

279 Denkbar ist zudem eine Beeinträchtigung der bestimmungsgemäßen Verwendung eines Computersystems. Problematisch ist in diesem Zusammenhang etwa die Teilnahme an Attacken, die nur die **Funktionsfähigkeit des Systems** beeinträchtigen, aber im Grunde keine Datenveränderung vornehmen. Hierzu gehört beispielsweise die durch unterlassene Sicherungsmaßnahmen ermöglichte Instrumentalisierung des Rechners eines privaten Nutzers für eine Denial-of-Service-Attacke.[553] Zur Eigentumsverletzung wegen Nutzungsstörungen ausführlich oben Rn. 112. Richtet sich der Denial-of-Service-Angriff gegen ein **gewerbliches Unternehmen**, so kommt abgesehen von den genannten Rechten die Beeinträchtigung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb als Auffangrecht[554] in Betracht. Allerdings bestehen hier oftmals Probleme hinsichtlich der notwendigen Betriebsbezogenheit.[555]

b) Verkehrspflichten

280 Der private Nutzer muss die Rechtsgutsverletzung durch zurechenbares und pflichtwidriges **Handeln** oder **Unterlassen** verursacht haben. Eine bewusste Schädigungshand-

---

[552] S. dazu Palandt-*Heinrichs*, § 280 BGB Rn. 28; MünchKommBGB-*Ernst,* § 280 BGB Rn. 104; Bamberger/Roth-*Grüneberg/Sutschet*, § 241 BGB Rn. 92.

[553] Dazu *Möller/Kelm*, DuD 2000, 292; zur Risikoverteilung AG Gelnhausen CR 2006, 209; s.o. Rn. 87 f. (Bedrohungspotentiale Denial-of-Service-Attacks).

[554] *Koch*, NJW 2004, 801 (803) mwN.

[555] Dazu bereits oben Rn. 108; ähnlich für das britische Recht *Reed* – Annex II – Rn. 1318.

lung wird dabei die Ausnahme darstellen. Regelmäßig wird der Privatnutzer entweder fahrlässig zur Schädigung Dritter beitragen, etwa indem er Viren und andere Schadprogramme über seinen Rechner weiter verbreitet. Besondere Bedeutung erlangt zudem die Haftung für Unterlassen, wenn der private Nutzer seinen PC nicht im Rahmen des Zumutbaren gegen Angriffe geschützt hat und Angreifer die Sicherheitslücke zum Schaden Dritter ausnutzen, indem sie seinen Rechner als Werkzeug instrumentalisieren (z. B. aufgrund von Bot-Netzen). Anknüpfungspunkt für die Haftung wird damit im Regelfall entweder eine sog. mittelbare Verletzungshandlung oder ein Unterlassen des Privatnutzers sein, was in den Wertungen eng bei einander liegt.[556] Da der Verletzungserfolg in beiden Fällen nicht unmittelbar durch die Handlung des Schädigers, sondern durch eine Reihe von Zwischenursachen vermittelt werden wird, ist Voraussetzung der Haftung jeweils die Verletzung einer Verkehrspflicht.[557]

(1) Zurechnungskriterien

281 Derjenige, der eine Gefahrenquelle schafft, ist grundsätzlich verpflichtet, die notwendigen und zumutbaren Vorkehrungen zu treffen, um eine Schädigung anderer zu vermeiden. Ihn treffen diesbezüglich Verkehrspflichten.[558] Andererseits gibt es keine allgemeine Rechtspflicht, andere vor Schäden zu bewahren, so dass die Annahme von Verkehrspflichten besonderer Begründung bedarf.[559] Während für IT-Hersteller (Rn.94 ff.) und auch IT-Intermediäre (Rn.660 ff.) weitgehend Einigkeit darüber besteht, dass sie Verkehrspflichten zumindest aufgrund ihrer Herrschaft über Gefahrenquellen treffen, ist die Bestimmung von Inhalt und Umfang der den privaten Nutzer treffenden Pflichten im IT-Bereich noch weitgehend ungeklärt.

282 Eine Zurechnung von Verkehrspflichten kommt grundsätzlich bei der **Beherrschung einer besonderen Gefahrenquelle** sowie bei der Schaffung einer besonderen Gefahrenlage aus **vorangegangenem Tun** in Betracht.[560] Der IT-Nutzer hat als Besitzer die Verfügungsgewalt über sein Computersystem.[561] Ist der Computer durch einen vorheri-

[556] Dazu Bamberger/Roth-*Spindler*, § 823 BGB Rn. 23; *Medicus*, Bürgerliches Recht, Rn. 646; *Larenz/Canaris*, § 75 II 3 c, S. 368, § 76 III 1 c, S. 401 f.

[557] *Kötz/Wagner*, Deliktsrecht, Rn. 108.

[558] BGH NJW-RR 2003, 1459; BGH NJW 1990, 1236; BGH NJW-RR 2002, 525 mwN.

[559] BGH NJW 1987, 2510; Palandt-*Sprau*, § 823 BGB Rn. 46; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 227; *Koch,* NJW 2004, 801 (803); *Libertus,* MMR 2005, 507 (508).

[560] *Larenz/Canaris*, § 76 III 4 b; *Koch,* NJW 2004, 801 (803); ähnl. auch *Libertus,* MMR 2005, 507 (508).

[561] Dabei werden zunächst entsprechende Admin-Rechte unterstellt. Der reine Nutzer ohne Berechtigung, Software zu installieren, hat in der Regel keine Möglichkeit, auf die Konfiguration des Systems Einfluß zu nehmen, damit auch nicht auf dessen Sicherheitsniveau.

gen Angriff kompromittiert und führt selbst entsprechende Angriffe aus, sei es durch Versendung von E-Mails mit Viren oder aber durch die Teilnahme an Denial-of-Service-Attacken,[562] so geht von dieser Computeranlage eine Gefährdung für die Computer und Daten und ggf. weitere Rechtsgüter Dritter aus. Damit besteht hier durchaus ein Anknüpfungspunkt in Gestalt der Beherrschung einer Gefahrenquelle.[563]

283 Allerdings ist zweifelhaft, ob der Nutzer für alle möglichen Schäden einstehen sollte, die von seinem Computer ausgehen, etwa im Rahmen eines Bot-Netzes und davon ausgehenden Denial-of-Service-Attacks oder Virenverbreitung. Denn für den Nutzer ist es im Rahmen des Internets praktisch nicht vorhersehbar, wer durch die jeweiligen Handlungen bzw. Viren geschädigt werden kann. Anders formuliert kann die Haftung hier unabsehbar ausufern – was etwa das britische Recht dazu veranlaßt, hier in der Regel von einer Haftung abzusehen.[564] Im deutschen Recht ergibt sich eine erste Eingrenzung durch die bei gewerblich Geschädigten erforderliche Betriebsbezogenheit des Eingriffs, die bei derartigen Gefährdungen nicht vorliegen wird. Dennoch verbleibt bei Schädigung von Daten ein für den Einzelnen fast unübersehbares Haftungsrisiko, das sich in praxi wohl nur aufgrund des erforderlichen Kausalitätsnachweises relativiert – denn das deutsche Haftungsrecht verlangt ansonsten keinen Vorsatz oder keine Pflichtwidrigkeit hinsichtlich des Schadens selbst bzw. bezüglich des haftungsausfüllenden Tatbestandes.

(2) Sicherheitserwartungen des Verkehrs

284 Grundsätzlich lassen sich gegen die viele Bedrohungen Gegenmaßnahmen ergreifen. Zur genaueren Konkretisierung des Inhalts und Umfangs der Verkehrspflicht ist in erster Linie auf die berechtigten **Sicherheitserwartung der betroffenen Verkehrskreise** abzustellen,[565] zu deren Bestimmung die Möglichkeit und Zumutbarkeit der Gefahrenvermeidung einerseits auf der Versenderseite, andererseits auf der Empfängerseite gegeneinander abzuwägen ist.[566] Für die Bestimmung der Reichweite der Pflichten des Nutzers kommt es auf eine **objektivierte Betrachtung** anhand einer Nutzergruppe an, nicht auf die individuellen Fähigkeiten und Ressourcen des individuellen Nutzers. Angesichts der Entwicklung des Internet zum Massenphänomen wird man sich indes vor

[562] S.o. Rn. 52 ff.; zur Verteilung des Risikos zwischen Serverinhaber und –vermieter bei DoS-Attacken AG Gelnhausen CR 2006, 208.

[563] Ebenso *Koch*, NJW 2004, 801 (803); *Libertus*, MMR 2005, 507 (509); implizit auch *Schmidbauer*, abrufbar unter: http://www.i4j.at/news/aktuell36.htm.

[564] S. dazu *Reed* – Annex II – Rn. 1318.

[565] BGH NJW-RR 2002, 525 (526); BGH NJW 1978, 1629; NJW 1990, 906 (907); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 234; *Schwerdtfeger/Gottschalck,* in: Schwarz/Peschel-Mehner, Kap. 2 Rn. 246.

[566] *Koch,* NJW 2004, 801 (804); *Libertus,* MMR 2005, 507 (509); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 234.

überspannten Sorgfaltsanforderungen an einen vermeintlich „typischen Internetnutzer" hüten müssen, da das Wissen um Einstellungen, Softwareverwendung und Risiken bei privaten Nutzern (insbesondere zwischen den Altersgruppen) zum Teil erheblich variiert.[567] Ebenso ist im schnelllebigen IT-Sektor stets zu berücksichtigen, dass sich die Verkehrserwartungen mit zunehmender Verbreitung eines Risikobewusstseins und der Kenntnis möglicher Gegenmaßnahmen wandeln können.[568]

285 Im Einzelnen ist daher in einem ersten Schritt darauf abstellen, ob das Problem überhaupt weithin **bekannt** ist (dazu Rn. 286 f.).[569] Für die Beurteilung der **Zumutbarkeit** kann in einem zweiten Schritt zwischen der technischen Zumutbarkeit und der wirtschaftlichen Zumutbarkeit unterschieden werden (dazu Rn. 290 ff.).

(3) Bekanntheit des Problems

286 Verkehrspflichten privater Nutzer können nicht mit dem pauschalen Hinweis auf die Komplexität der modernen Informationstechnologie verneint werden. Wenn der BGH in der vielbeachteten **Dialer-Entscheidung** eine Pflicht zur Installation von Dialerschutzprogrammen verneinte,[570] so lag dies vor allem daran, dass Dialer damals noch weitgehend unbekannt (und Schutzvorkehrungen technisch aufwändig) waren.[571] Entgegen zuvor ergangenen instanzgerichlichen Entscheidungen[572] stellte der III. Zivilsenat fest, dass für den Nutzer keine Pflicht zur Überwachung des eigenen Computersystems besteht, solange kein konkreter Hinweis auf einen Missbrauch besteht.[573] Verallgemeinert man diesen Gesichtspunkt, so kommt es grundsätzlich darauf an, ob ein verständiger objektiver Nutzer nicht von einer entsprechenden Gefahr wusste oder zumindest damit rechnen musste.[574] Grund hierfür ist auch, dass der **Bekanntheitsgrad die Verkehrserwartung beeinflusst**. Im zu entscheidenden Fall war für den Nutzer nicht erkennbar, dass eine Beeinträchtigung des Systems stattgefunden hatte bzw. diese nicht einfach beseitigt werden konnte. Hinzu kam, dass der Nutzer auch grundsätzlich nicht

---

[567] Dazu bereits *Spindler*, JZ 2004, 1128 (1129).

[568] *Spindler*, JZ 2004, 1128 (1129).

[569] *Leible/Wildemann*, K&R 2004, 288 (289); vgl. *Schmidbauer*, abrufbar unter: http://www.i4j.at/news/aktuell36.htm; BGH VersR 1972, 70 (71); *Härting/Schirmbacher*, CR 2004, 334 (337); dem hat sich der BGH im Dialer Urteil, NJW 2004, 1590 jedoch nicht angeschlossen, sondern hat im konkreten Fall eine ergänzende Vertragsauslegung vorgenommen.

[570] BGH NJW 2004, 1590 = JZ 2004, 1124 m.Anm. *Spindler*.

[571] So auch *Ernst*, CR 2006, 590 (593).

[572] LG Berlin ZAP 2002, 565; KG Berlin NJW-RR 2003, 637; s. auch AG München JurPC Web-Dok. 391/2002; AG Dillenburg CR 2003, 686.

[573] BGH NJW 2004, 1590 = JZ 2004, 1124 m.Anm. *Spindler*. Dem folgend für Schutzmaßnahmen gegen Trojaner LG Stralsund CR 2006, 487 (489) mit zu Recht krit. Anm. *Ernst*, CR 2006, 590 ff.

[574] Vgl. auch LG Köln NJW 1999, 3206.

misstrauisch sein und demgemäß keine Sicherungsmaßnahmen (z. B. Dialerschutzprogramm) ergreifen musste.[575]

287 Ob allerdings angesichts der weiteren Entwicklung heute noch davon ausgegangen werden kann, dass die Allgemeinheit bzw. ein verständiger Nutzer keine Kenntnis von den Gefahren der Informationstechnologie und den möglichen Schutzmechanismen hat, ist zweifelhaft.[576] Wie die **technische Entwicklung** ist auch der den Nutzer treffende Sorgfaltsmaßstab einer steten Veränderung unterworfen.[577] Gegenwärtig wird man auch vom durchschnittlichen IT-Nutzer zumindest die Kenntnis grundlegender Sorgfaltsmaßnahmen im IT-Verkehr erwarten können. Dazu gehört beispielsweise die Verwendung von Anti-Virus-Programmen (im Einzelnen unten Rn. 295 ff.).

288 **Wann** indes ein Sicherheitsproblem im Einzelfall als **allseits bekannt** unterstellt werden kann, ist bislang wenig geklärt. Ein Problem wird nicht bereits dann weithin bekannt sein, wenn Fachzeitschriften darüber berichten; gerade angesichts der massenweisen Verbreitung von IT-Produkten kann hier etwa nicht auf Computerzeitschriften abgestellt werden, selbst wenn diese sich an einen breiten Leserkreis wenden. Vielmehr muss auch derjenige, der sich nicht direkt und gezielt informiert, die Möglichkeit gehabt haben, von der Problematik Kenntnis zu erlangen, etwa bei umfangreicher Berichterstattung in Print-, Rundfunk- und TV-Medien. Zusätzlich müssen aber auch die generellen Lösungsmöglichkeiten bekannt sein, z.B. durch die Installation entsprechender Abwehrprogramme.

(4) Zumutbarkeit der Schutzmaßnahmen

289 Wirtschaftlich aufwändige, aber auch technisch anspruchsvolle Lösungen, die den Normalnutzer überfordern, nicht verlangt werden. Gerade im Privatbereich muß danach gefragt werden, ob dem potentiell Pflichtigen, also dem Durchschnittsnutzer, die Ergreifung der Sicherungsmaßnahmen überhaupt von seinen Fähigkeiten her möglich ist, etwa wenn technische Lösungen nur durch zahlreiche, teils komplizierte Schritte zu erreichen sind. Fehlbedienungen können z.B. bei Firewalls durchaus gerade den gegenteiligen Effekt hervorrufen und das System anfälliger für Angriffe machen.[578]

---

[575] BGH NJW 2004, 1590 (1592) = JZ 2004, 1124 m.Anm. *Spindler*.

[576] *Leible/Wildemann*, K&R 2004, 288 (289); ähnl. Argumentation für Viren *Schmid*, abrufbar unter: http://www.bwl.tu-darmstadt.de/jus4/lehre/IuD-I_ws_05/ws_0506_vorl_ueb_iud_1_modul_6_060123.pdf, 43.

[577] Dazu schon *Spindler*, JZ 2004, 1128 (1129); zust. *Kind/Werner*, CR 2006, 353 (355).

[578] S.u. Rn. 63 ff.

(a) Technische Zumutbarkeit

290 Technisch zumutbar ist der Einsatz einer Lösung, wenn sie auch für den Nichtfachmann mit geringem Einarbeitungsaufwand installiert werden kann. Die Anforderungen an private Nutzer dürfen hierbei insbesondere im technischen Bereich (z. B. der Konfiguration von Firewalls) nicht übertrieben streng gehandhabt werden (siehe im Einzelnen unten Rn. 294 ff.).[579] Entfernungsanleitungen (Removal tools), die einen Eingriff in Systemkomponenten, z.B. die Beendigung von Systemdiensten oder die Bearbeitung von Systemdatenbanken (registries), erfordern, können durch den Durchschnittsnutzer gerade nicht befolgt werden. Problematisch sind auch Lösungen, die eine ständige Aufmerksamkeit des Nutzers erfordern. Diese kann verlangt werden, sofern auch komplizierte Vorgänge für den Nutzer einfach erklärt werden können, und die Handlungsmöglichkeiten deutlich und eindeutig sind. Sofern allerdings der Nutzer die Bewertung von Systemeinstellungen oder Netzwerkaktionen vornehmen muss, diese häufig notwendig werden, und Entscheidungen bzw. Einstellungen die Sicherheit des gesamten Systems kompromittieren können, also im Grunde ein IT-Experte eingesetzt werden müsste, kann dies nicht von einem Durchschnittsnutzer verlangt werden. Es ist jedoch zumutbar, ein entsprechendes Programm zu installieren, das Schutzmaßnahmen bereitstellt, sofern es die genannten Kriterien der Einfachheit erfüllt.

(b) Wirtschaftliche Zumutbarkeit

291 Zwischen technischer und wirtschaftlicher Zumutbarkeit besteht ein enger sachlicher Zusammenhang. Wirtschaftlich zumutbar ist die Ergreifung von Sicherungsmaßnahmen jedenfalls dann, wenn sie nicht vollkommen außerhalb jedes vernünftigen Verhältnisses zu dem mit der Maßnahme verbundenen Sicherheitsgewinn steht. So können monatlich zu entrichtende Beträge durchaus angemessen sein, sofern sie nicht ein bestimmtes Maß überschreiten, z.B. einer monatlicher Virenscan-Update.

292 Zur Lösung von IT-Sicherheitsproblemen ist stets auch der Einsatz entsprechender **Experten** denkbar. Allerdings sind die Kosten hierfür meist unverhältnismäßig hoch. Der Private wird in aller Regel nur Maßnahmen ergreifen, welche ihm ohne fremde Hilfe möglich sind. Eine Pflicht zur kostenpflichtigen Heranziehung von Fachkräften dürfte bei privaten Nutzern indessen unzumutbar sein.

(c) Allgemeines Lebensrisiko

[579] Dazu auch *Ernst*, CR 2006, 590 (593).

293 Zur Begründung einer Verkehrspflicht müssen von der beherrschten Gefahrenquelle bzw. der geschaffenen Gefahrenlage besondere, über das allgemeine Lebensrisiko hinausgehende Gefahren ausgehen.[580] Bei einem weitverbreiteten und damit auch weithin bekannten Problem könnte man davon ausgehen, die Gefahr einem solchen Angriffs zum Opfer zu fallen, werde bei Nutzung des Internet in Kauf genommen, so dass Schäden in den Verantwortungsbereich des zum Selbstschutz verpflichteten Geschädigten fallen.[581] Zum gegenwärtigen Zeitpunkt wird man so weit allerdings nicht gehen können. Auch wenn bei Internetnutzern ein entsprechendes Selbstverständnis vorhanden sein sollte und ein Virenbefall mithin als „übliches Risiko" der Internetnutzung angesehen würde, kann hierauf keine rechtliche Wertung gestützt werden, so dass Sicherungspflchten privater Nutzer generell zu verneinen wären.

c) Einzelfragen

294 Für die eingangs beschriebenen Bedrohungs- und Abwehrszenarien (oben Rn.52 ff.) ist im Folgenden zu klären, ob eine Verkehrspflicht des privaten Nutzers besteht. Dazu ist im Einzelnen zu prüfen, ob

- die Tatsache, dass es ein Sicherheitsproblem und eine generelle Lösung gibt, weithin bekannt ist,
- die Ergreifung der Lösung technisch
- und wirtschaftlich zumutbar ist.

(1) Virenscanner

295 Eine Gefährdung der IT-Sicherheit durch Viren erfolgt vom Privatnutzer in der Regel durch den unbeabsichtigten Versand mit E-Mails oder durch Weitergabe auf verseuchten Datenträgern.[582] Der virenbefallene Rechner des Privatnutzers stellt hierbei eine besondere Gefahrenquelle dar, welche die Zurechnung einer Verkehrspflicht rechtfertigt.[583] Die Gefahr durch Viren und die erforderlichen Schutzmaßnahmen sind als weithin bekannt anzusehen. [584] Bereits mehrfach wurde über diese Problematik auch in den Medien berichtet.[585] Fachzeitschriften thematisieren diesen Bereich zudem regelmäßig.

---

[580] Erman-*Schiemann*, § 823 BGB Rn. 20; Staudinger-*Hager*, § 823 BGB Rn. 33; vgl. auch BGH NJW 1996, 1533; BGH NVwZ-RR 1994, 400 (401).

[581] Zu Viren *Libertus,* MMR 2005, 507 (509).

[582] *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 516.

[583] *Koch*, NJW 2004, 801 (803); *Libertus,* MMR 2005, 507 (509).

[584] LG Köln NJW 1999, 3206; *Koch*, NJW 2004, 801 (802); *Libertus*, MMR 2005, 507 (509); *Schmidbauer*, abrufbar unter: http://www.i4j.at/news/aktuell36.htm; *Schultze-Melling*, CR 2005, 7; *Schneider/Günther*, CR 1997, 389 (394); *Spindler*, JZ 2004, 1128 (1129); *Tita*, VW 2001, 1781 (1784).

[585] OLG Hamburg MMR 2005, 119 (120); *Göttert*, VW 2001, 1972.

Außerdem wird meist auch darauf hingewiesen, dass mit sogenannten Virenscannern eine relativ einfach zu handhabende Vorsorgemöglichkeit besteht. Der Nutzer muss lediglich ein entsprechendes Programm kaufen oder kostenfrei im Internet herunterladen und installieren. Bei neu erworbenen Computern gehört einvorinstalliertes Virenschutzprogramm zum üblichen Lieferumfang. Die Verwendung eines Antivirenschutzprogramms ist dabei auch dem Durchschnittsnutzer sowohl technisch, als auch wirtschaftlich zumutbar. [586] Technische Vorkenntnisse sind nicht erforderlich, da die Standardprogramme entsprechende Nutzerführungen enthalten. Wirtschaftliche Argumente gegen den Einsatz Virenscannern dürften schon deshalb nicht verfangen, weil solche kostenlos im Internet als Freeware zum Download bereit stehen.[587] Allerdings muß im Einzelfall genau geprüft werden, ob diese Programme weithin bekannt und einfach verfügbar sowie installierbar sind.

296 Problematisch ist indessen, wie häufig der Nutzer seinen Virenschutz **aktualisieren** muss. Hierzu ist zunächst zu beachten, dass auch die aktuellste Virendefinitionsdatei keinen absoluten Schutz bietet. Werden neue Viren erstellt, so brauchen auch die Virenlabore der Antivirensoftwarehersteller einige Zeit, um hierauf zu reagieren. In dieser Zeit ist selbst ein ständig aktuell gehaltenes Computersystem vor dem speziellen Virus ungeschützt.[588] Zudem stellen die Hersteller von Antiviren-Software nicht ständig neue Updates zur Verfügung. Teilweise werden die automatischen Updates z.B. im wöchentlichen Rhythmus bereitgestellt. Weiter bedeutet ein Update regelmäßig den Download größerer Dateien. Zwar nimmt die Verbreitung breitbandiger Internetzugänge zu. Es kann gegenwärtig aber nocht nicht davon ausgegangen werden, dass der Durchschnittsnutzer einen solchen besitzt. Daher dürfte es derzeit überzogen sein, eine ständige Pflicht zur Aktualisierung des privaten Systems zu fordern.[589] Grundsätzlich ist damit **maximal eine wöchentliche Aktualisierung** zumutbar.

297 Im Ergebnis lässt sich danach festhalten, dass dem privaten IT-Nutzer die Pflicht zur Einrichtung, Wartung und wöchentlichen Aktualisierung eines Virenscanners obliegt.[590]

---

[586] *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 516.

[587] *Ernst*, CR 2006, 590 (593).

[588] *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 131.

[589] *Schmidbauer*, abrufbar unter: http://www.i4j.at/news/aktuell36.htm; wöchentlich oder kürzer *Koch*, NJW 2004, 801 (807); ebenso BSI, IT-Grundschutzhandbuch 2005, M 4.3.

[590] Ebenso *Ernst*, CR 2006, 590 (593); *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 516. Abzulehnen LG Stralsund CR 2006, 487 (489).

In ähnlicher Weise stuft etwa auch das österreichische Recht die Pflichten der Nutzer ein, wobei auch hier im Wesentlichen auf die Zumutbarkeit abgestellt wird.[591]

(2) Firewall

298 Ein weiteres Abwehrprogramm ist die sog. Firewall, welche insbesondere der Abwehr von Angriffen aus Netzwerken dient und ist damit wichtig für die generelle Sicherheit des Computers ist.[592] Durch eine Firewall wird einerseits der Zugriff auf Programme und Systemfunktionen von außen bereits im Aufbau blockiert. Andererseits ermöglichen die sog. Personal Firewalls darüber hinaus die Freigabe oder Verweigerung von Netzzugriffsrechten lokaler Programme. So kann z.B. ein Programm, das auf Ressourcen im Internet zuzugreifen versucht, hieran durch entsprechende Regeln gehindert werden. Firewalls dienen damit auch dem Schutz vor Trojanern.

299 Die Unsicherheit des Betriebs von Computern im Internet bzw. die Angreifbarkeit ist weithin bekannt. Dies bezieht sich zwar hauptsächlich auf Viren, aber zumindest die abstrakte Kenntnis des Nutzers von der Gefährlichkeit ohne besondere Kenntnis der Gründe ist vorhanden. Ob daraus allerdings auch darauf geschlossen werden kann, dass auch die Lösung, nämlich die Einrichtung einer Firewall, bekannt ist, ist eher fraglich. Mit aktuellen Betriebssystemen wird meist eine integrierte Firewall geliefert. Beim Einsatz von sogenannten Internetroutern für den breitbandigen Internetzugang ist zudem häufig eine Firewall in die Hardware integriert, die zumindest die größten Gefahren minimiert. Weder dieser Schutz noch die zurzeit beigelegten Firewalls sind allerdings zum absoluten Schutz geeignet, da sie nur eine rudimentäre Funktionalität bieten. So können z.B. die sog. „well-known Ports“ bzw. „trusted Ports“, also die Ports von 0 bis 255 bzw. 1024, offen sein.[593] Wenn hier fehler- oder schadhafte Software auf Verbindungen wartet, so bieten die integrierten Lösungen keinen bzw. kaum Schutz.[594] Programme, die aktive Inhalte ausführen und denen Zugang zum Netz gewährt wurde, bergen die weitere Gefahr, dass selbstverständlich auch die aktiven Inhalte, die für die Firewall nicht vom Programm unterscheidbar sind, die entsprechende Berechtigung zum Netzzugriff haben.[595] Hier bietet die Firewall keinen Schutz.

---

[591] Näher *Fallenböck* – Annex II – Rn. 1162 ff., zusammenfassend die Interessenabwägung in Rn. 1172.

[592] Vgl. LG Köln JurPC Web-Dok. 62/2004, wonach zu einem Sicherheitskonzept auch eine Firewall gehört; *Schneider/Günther*, CR 1997, 389 (394).

[593] *Eckert*, IT-Sichertheit, S. 88; BSI, IT-Grundschutzhandbuch 2005, M 2.76

[594] Zu den Folgen der Überwindung von Firewalls *Quack-Grobecker/Funke*, VW 1999, 157 (158).

[595] Vgl. *Eckert*, IT-Sichertheit, S. 72.

300 Hinzu kommt die schwierige Bedienbarkeit der Programme.[596] Firewalls arbeiten auf der Basis eines bestimmten Regelsatzes. Anhand dieser Regeln entscheiden sie, ob bestimmte Kommunikationsvorgänge erlaubt werden sollen. Da die Kommunikationspartner und –programme vorher nicht bekannt sind, muss hierfür der Nutzer gefragt werden. Die zugehörigen Nachrichten sind jedoch meist kryptisch und unverständlich. Viele Firewalls geben z.B. an, dass von einer bestimmten IP-Adresse aus eine Anfrage an den eigenen Rechner gestellt wurde, oder dass ein lokales Programm Zugriff auf eine entfernte IP-Adresse wünscht. Aufgrund der Vielzahl der Programme und Dienste können Firewalls auch keine direkte Aussage darüber treffen, ob der Zugriff gefährlich ist. Der Nutzer muss also anhand der netzwerkspezifischen Informationen entscheiden. Die Beantwortung ist damit schwierig. Hinzu kommt, dass die Antworten direkt der Regelerstellung dienen. Blockiert der Nutzer also aus Vorsicht eine wichtige Anwendung, so ist diese möglicherweise nicht mehr einsatzfähig bzw. kann erst durch die komplizierte Entfernung der Regel wieder in einen funktionsfähigen Zustand versetzt werden. Durch solche Erfahrungen kann der Nutzer veranlasst sein, auch bei gefährlichen Programmen Zugriffsrechte zu erteilen. Mit der Gewährung von Rechten kann der Nutzer die Firewall sogar vollkommen deaktivieren, ohne dass er dies merkt.[597] Sofern nämlich eine hochpriorisierte Regel den generellen Netzwerkzugriff erlaubt, so greifen auch schützende Regeln nicht mehr. Dennoch signalisiert die Firewall Bereitschaft.

301 Es **fehlt** somit bereits an der **Bekanntheit** unter privaten Nutzern,[598] dass Firewalls als Lösungsmöglichkeit zur Verfügung stehen. Zusätzlich ist die **Benutzung kompliziert** und daher auch technisch dem Durchschnittsnutzer nicht zumutbar, während wegen der geringen Kosten eine eine wirtschaftliche Zumutbarkeit wohl gegeben wäre. Eine grundsätzliche Pflicht zum Einsatz von Firewalls besteht demnach zumindest für Privatnutzer nicht.

(3) System- und Programmupdates

302 Ein weiteres großes Sicherheitsproblem stellen Lücken im Betriebssystem oder Teilen desselben dar. Aufgrund der hohen Komplexität von Betriebssystemen bzw. Program-

[596] „Aufstellen und Aktualisieren der Filterregeln ist keine einfache Aufgabe.“ BSI, IT-Grundschutzhandbuch 2005, M 2.76.

[597] Vgl. zur automatischen Anpassung der Regeln mittels Intrusion Detection-Systemen und der anschließenden Einschränkung von Diensten BSI, IT-Grundschutzhandbuch 2005, M 5.71 (2747); zu den möglichen Folgen von bestimmten Freigaben der Firewall *Klapdor*, VW 2005, 507.

[598] Nur für kommerzielle Nutzer *Schneider/Günther*, CR 1997, 389 (394).

men sind Fehler nicht auszuschließen.[599] Einerseits können lokal ausgeführte Programme solche Lücken nutzen, um ihre Zugriffsrechte auf dem Computersystem unbefugt zu erhöhen, andererseits können solche Lücken durchaus auch von außen über ein Netzwerk bzw. das Internet ausgenutzt werden. Damit sind System- und Programmupdates eine Abwehrmaßnahme auch gegen Trojaner. Indem z.B. Webseiten speziell präpariert werden und einen Fehler in einem Programm auslösen, können sie eigene Computeranweisungen ausführen, die z.B. ein Virus oder andere Malware installiert. Schließlich besteht die Möglichkeit, dass eine nicht ausführbare Datei, beispielsweise ein Bild oder eine Musikdatei so präpariert wird, dass ein Fehler im Programm hervorgerufen wird, der ebenso ausgenutzt wird. Das angreifende „Programm" erwirbt damit automatisch die Rechte des aktuellen Benutzers und kann weitere Programme nachinstallieren, die in dessen Benutzerkontext und mit seinen Rechten laufen. Falls auf der Anlage dann sogar noch Systemlücken bestehen, kann das Programm seine Nutzerrechte erhöhen und damit vollen Zugriff erlangen.[600] Zusätzlich kann es sich eventuell sogar vor Abwehrprogrammen verbergen.

303 Auch hier stellt das kompromittierte System eine Gefahrenquelle dar, die nur der Nutzer beherrschen kann. Es ist somit zu klären, ob dem Nutzer die Verkehrspflicht obliegt, solche Angriffe anzuwehren, indem er wichtige Systemupdates und Programmupdates beschafft und installiert. Während das Wissen über Viren relativ verbreitet ist, ist das Bewusstsein, dass auch ein gegen Viren geschütztes System durchaus verwundbar ist, beim durchschnittlichen privaten Nutzer noch kaum vorhanden. Anderes wird man aber dann annehmen müssen, wenn ein auf dem System laufender Dienst an Updates erinnert bzw. diese sogar automatisch oder halb-automatisch herunterlädt und installiert.[601] In diesem konkreten Fall kann von einer Bekanntheit und ebenso der technischen Zumutbarkeit ausgegangen werden.[602]

304 Aus Nutzersicht ist es zum Teil jedoch gar nicht erwünscht, dass jedes Programm, das er installiert hat, nach Updates fragt, da dadurch grundsätzlich auch die Gefahr besteht, dass Daten über das Nutzerverhalten oder ähnliches übertragen wird. Man könnte dann

---

[599] OLG Hamburg CR 1986, 83 (84); LG Heidelberg CR 1989, 197 (198); *Gorny*, CR 1986, 673 (675); *Engel*, CR 1986, 702 (708); *Bömer*, CR 1989, 361; *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, 1995, S. 37, 40 f.; MünchKommBGB-*Wagner*, § 3 ProdHaftG Rn. 15; *Heussen*, CR 2004, 1 (3); mit Einschränkungen auch *Kilian*, CR 1986, 187 (190).

[600] Zu sog. Root-Kits, die eben diese Techniken verwenden, *Kühnhauser*, DuD 2003, 218 f.

[601] Zu automatisierten Software-Updates *Probst*, DuD 2003, 508.

[602] Ähnl. *Probst*, DuD 2003, 508: „Im Bereich der Endanwender kann die Automatisierung, dass die [...] aus Unwissenheit [...] unterbliebene Systemwartung überhaupt erfolgt."

zwar eine Pflicht des Nutzers anzunehmen, sich selbst über vorhandene Updates zu informieren. Dies kann jedoch bei der Vielzahl der Programme nicht geleistet werden, zumal er häufig gar nicht weiß, dass eine Firewall oder ein ähnliches Programm den Internetzugriff des Programms unterdrückt.

305 Die wirtschaftliche Zumutbarkeit ist besonders bei größeren Updates schwierig zu beantworten, da diese über langsame Internetanbindungen bzw. Telefonleitungen auch hohe Kosten verursachen können.[603] Aus diesem Grunde sind auch größere Systemupdates durchaus wirtschaftlich zumutbar. Allerdings kann sich hier im Einzelfall durchaus eine Unzumutbarkeit ergeben, etwa wenn die Updates von Programmen derart umfangreich sind, dass sie mit einer (zu dem entsprechenden Zeitpunkt) verkehrsüblichen Datenverbindung nicht zu bewältigen sind, wie dies etwa noch für den Service Pack 2 für das Betriebssystem Windows XP der Fall war.

306 Im Ergebnis wird man unter Einbeziehung der durch ungesichterte private Rechner drohenden Schäden (Multiplikatorwirkung[604]) zumindest die Zumutbarkeit von wichtigen System-und Programmupdates bejahen müssen, die automatisiert oder halbautomatisch, also durch einen im System verankerten Update-Dienst, installiert werden können.

(4) Nutzung von Nutzerkonten mit eingeschränkten Rechten

307 Eine weitere Möglichkeit, die Gefahren zumindest zu minimieren, ist die Arbeit unter einem Benutzerkonto mit eingeschränkten Rechten.[605] Als Folge könnte ein erfolgreicher Angriff diejenigen eingeschränkten Nutzerrechte erlangen, sofern er nicht andere Lücken zur Erhöhung ausnutzt.[606] Damit kann eine dauerhafte Verankerung des Schadprogramms im System verhindert oder zumindest erschwert werden. Während bei Unix-Systemen die Arbeit als Nutzer die Regel ist, und nur in Ausnahmefällen Administratorrechte genutzt werden, ist dies bei Windows-Betriebssystemen anders. Hier arbeitet der Hauptnutzer regelmäßig mit Administratorrechten. Viele Programme sind auch ohne diese Rechte gar nicht lauffähig, so dass der Betrieb nur eingeschränkt möglich ist,

---

[603] Als Beispiel habe ein Update eine Größe von ca. 50 MB, der Nutzer hat ein normales Modem und überträgt damit ca. 5 KByte/s, wobei er bei seinem Internetprovider 3 Cent/min bezahlt. Die Übertragung wird ca. 3 Stunden benötigen und damit ca. 5 € kosten.

[604] *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 516.

[605] S. dazu *Endres*, c't Archiv 23/2005, 112.

[606] S.o. Rn. 85.

wenn der Nutzer nicht ständig zwischen dem Administratorkonto und dem eingeschränkten wechseln will.

308 Diese Möglichkeit ist jedoch **keineswegs als weithin bekannt** einzustufen. Der Durchschnittsnutzer ist sich dieser Möglichkeit gar nicht bewusst und kann deshalb auch die entsprechenden Maßnahmen, die auch spezielle Anleitungen oder Expertenwissen und einigen Aufwand erfordern und damit auch technisch nicht zumutbar wären, nicht ergreifen. Es besteht somit keine Verkehrspflicht für private Nutzer, im Regelfall mit eingeschränkten Rechten zu arbeiten.

(5) Intrusion Detection-Systeme

309 In Erweiterung zu Firewalls dienen Intrusion Detection-Syteme der Erkennung von Angriffen, die auch aus dem internen Netzwerk unterstützt werden.[607] Sie überwachen den Netzwerkverkehr sowie die Systemkonfiguration und melden dem Nutzer verdächtige Aktionen oder Veränderungen.[608] Intrusion Detection-Systeme sind allerdings bereits ihrer Bestimmung nach nur für größere Netzwerke geeignet. Die Anpassung an das jeweilige System sowie die entsprechende Überwachung erfordern jedenfalls Expertenwissen bzw. Kenntnis von der Funktionsweise der Kommunikation in Netzwerken. Beim Einsatz von Intrusion Detection-Systemen fallen in der Regel personenbezogene Daten an, die datenschutzrechtlichen Vorgaben sind demnach einzuhalten.[609] Unabhängig davon, ob diese Sicherungswerkzeuge also dem Durchschnittsnutzer bekannt sind, ist dem privaten Nutzer der Einsatz von Intrusion Detection-Systemen jedenfalls nicht technisch zumutbar.

(6) Malware-Entfernungsprogramme

310 Verfügbar sind auch Programme zur Entfernung von sog. Malware,[610] die sich bereits im System tatsächlich eingenistet hat. Dadurch kann insbesondere Schadensfällen bei Dritten – z. B. durch die Weiterverbreitung von Viren – vorgebeugt werden. Der Einsatz der entsprechenden Programme ist durchaus anwenderfreundlich. Zudem sind die Entfernungsprogramme meist kostenlos erhältlich. Zweifelhaft ist jedoch, ob die Existenz dieser Programme bereits so bekannt ist, dass auch dem normalen Nutzer der Ein-

---

[607] *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 133.

[608] S.o. Rn. 65.

[609] Dazu eingehend BSI-Studie „Einführung von Intrusion-Detection-Systemen – Rechtliche Aspekte“, abrufbar unter: http://www.bsi.bund.de/literat/studien/ids02/dokumente/Rechtv10.pdf.

[610] Zum Begriff s.o. Rn. 63, 68.

satz zuzumuten ist. Mangels der notwendigen Bekanntheit ist der private Nutzer nicht verpflichtet, Malware-Entfernungsprogramme einzusetzen.

(7) Verhalten im E-Mail-Verkehr

311 Von den Verkehrspflichten des privaten Nutzers im technischen Bereich zu unterscheiden sind Verhaltenspflichten bei der Nutzung von E-Mail und Internet. So enthalten Spam-E-Mails häufig Anhänge, welche beim Öffnen unbemerkt ein Virusprogramm oder ein trojanisches Pferd auf dem Rechner des Nutzers installieren. Neben der Gefahr für den eigenen Datenbestand besteht hierbei die Möglichkeit der Weiterverbreitung des Schadprogramms auf andere Nutzer. Immer stärker in den Vordergrund tritt zudem gegenwärtig der Identitätsmissbrauch im Internet unter Verwendung von heimlich auf dem Rechner des Privatnutzers installierten Trojanern (s. dazu die Ausführungen zum Online-Banking Rn. 485 ff.).

312 Auch der private Nutzer ist daher verpflichtet, **unbekannte und verdächtige Anhänge** im Zweifelsfall **ungeöffnet zu löschen** bzw. nur nach Verifizierung des Absenders zu öffnen. Das Wissen um die Bedrohungen durch E-Mail-Anhänge darf heute zum allgemeinen Kenntnisstand des durchschnittlichen Internetnutzers gezählt werden. Besondere IT-Kenntnisse sind zur Durchführung der Maßnahme nicht erforderlich. Eine allgemeine Pflicht, präventiv alle **E-Mails mit unbekanntem Absender zu löschen**, wird man demgegenüber **nicht** annehmen können, denn sie würde die E-Mail-Korrespondenz auf Bekannte beschränken und damit in ihrer Reichweite erheblich beschneiden. Auch wenn sich pauschale Aussagen verbieten, da Unternehmen im E-Mail-Verkehr mit privaten Nutzern Adressen durchaus wechseln, etwa wenn eine neue Domain erworben wurde, oder auch private Nutzer (als Korrespondenten) häufig ihre Adresse wechseln können, dürften doch meist bei privaten Nutzern seriöse E-Mails unbekannter Herkunft eher die Ausnahme und Spam-E-Mails die Regel bilden.

(8) Ergebnis

313 Zum jetzigen Zeitpunkt sind lediglich der Einsatz von Virenscannern sowie entsprechende Aktualisierungen als eine grundsätzliche Verkehrspflicht des Nutzers einzuordnen. Hinzu kommen grundlegende Verkehrspflichten im E-Mail-Verkehr.

3. Schadensminderungs- und Selbstschutzpflichten

314 Schließlich ist für die Verteilung der Verantwortungsbereiche das Ausmaß an Selbstschutz und Schadensabwendungspflichten des Geschädigten im Rahmen von § 254 BGB relevant,[611] für die die zuvor erörterten Pflichten quasi spiegelbildlich herangezogen werden können. Schädiger und Geschädigter im Grunde der gleichen Risikosituation ausgesetzt sind. Setzen beide keine entsprechenden Schutzmaßnahmen ein, so hängt es lediglich vom Zufall ab, welches System zuerst infiziert wird. Während also grundsätzlich eine Verkehrspflicht zum Einsatz von Virenscannern besteht, liegt eine gleichartige Pflicht nach § 254 BGB vor.[612]

a) Warnpflichten des Geschädigten

315 § 254 Abs. 2 Satz 1 BGB hält ausdrücklich dazu an, den Schuldner (bzw. Schädiger) auf die Gefahr eines ungewöhnlich hohen Schadens aufmerksam zu machen, die der Schuldner weder kannte noch kennen musste, damit dieser in die Lage versetzt wird, dem Schaden seinerseits zu begegnen.[613] Die Pflicht zur Warnung entsteht für den Geschädigten aber nur dann, wenn er selbst Schädigung und Schadenshöhe vorhersehen kann[614] und er bessere Erkenntnismöglichkeiten als der Schädiger hat.[615] Für IT-Sicherheitslücken kommt dies vor allem dann zum Tragen, wenn allgemein erhältliche, anwendungsneutrale Software, wie Office- oder Betriebssysteme, zum Einsatz in Bereichen mit Gefährdungspotential für hochrangige Rechtsgüter kommen. Denn einerseits hat der Hersteller (nicht der Händler!) oftmals keine Kenntnis von dem jeweiligen Gefährdungspotential seines Produktes; andererseits sind grundsätzlich die Gefahren durch einem breiten Publikum[616] bekannt gewordene IT-Sicherheitslücken dem Nutzer erkennbar. Stets aber muss die Verletzung der Warnpflicht nach § 254 Abs. 2 Satz 1 BGB ursächlich für die Entstehung des Schadens und der Schadenshöhe sein; hätte der Schä-

---

611 Dabei kann die an sich von Gesetzes wegen vorgesehene Unterscheidung zwischen dem Mitverschulden des Geschädigten nach § 254 Abs. 1 BGB und seiner Schadensabwendungs- und -minderungspflicht nach § 254 Abs. 2 BGB offen bleiben, da insoweit Einigkeit darüber herrscht, dass § 254 Abs. 2 BGB nur einen besonderen Anwendungsfall des allgemeineren § 254 Abs. 1 BGB darstellt, vgl. MünchKommBGB-*Oetker*, § 254 BGB Rn. 68; Palandt-*Heinrichs,* § 254 BGB Rn. 32; *Lange/Schiemann*, Schadensersatz, § 10 X 1; der Streit um die dogmatische Einordnung des § 254 BGB (näher dazu *Greger*, NJW 1985, 1130 ff.) spielt hier keine Rolle.

612 *Spindler*, CR 2005, 741 (744); *Schneider/Günther*, CR 1997, 389 (394); *Libertus*, MMR 2005, 507 (511); *Koch*, NJW 2004, 801 (804); *Schmidbauer*, abrufbar unter: http://www.i4j.at/news/aktuell36.htm; iE *Mankowski*, in: Ernst, Hacker, Cracker und Computerviren, Rn. 530 f.

613 So BGH VersR 1960, 526 (527).

614 Vgl. BGH VersR 1964, 950 (951); Staudinger-*Schiemann*, § 254 BGB Rn. 76; MünchKommBGB-*Oetker*, § 254 BGB Rn. 70.

615 BGH VersR 1953, 14; *Lange/Schiemann,* Schadensersatz, § 10 IX 2.

616 Hier gelten spiegelbildlich die Anforderungen wie zu den Warnpflichten des Herstellers. Allein das Bekanntwerden in einschlägigen Fachkreisen oder EDV-Zeitschriften genügt nur bei Nutzern mit einschlägigen Kenntnissen oder EDV-Abteilungen.

diger die Warnung nicht beachtet[617] oder keine Maßnahmen ergreifen können, trifft den Geschädigten auch nicht der Vorwurf nach § 254 Abs. 2 Satz 1 BGB. Die Beweislast hierfür obliegt dem Geschädigten.[618]

b) Selbstschutzpflichten

316 Der Pflicht zur Erfassung der Risiken und der Einleitung von Maßnahmen zur Problembewältigung entspricht die allgemeine Pflicht des Softwarebenutzers zum Selbstschutz.[619] So könnte der IT-Anwender gehalten sein, die allgemein üblichen Vorkehrungen zum Viren- und Wurmschutz zu treffen, indem er Virenscanner bei sich einsetzt und auf dem Laufenden hält.[620] Die Missachtung dieser etwaigen Pflichten würde folgerichtig ein Mitverschulden gemäß § 254 BGB begründen.

317 Zur Feststellung einer solchen Pflicht zum Selbstschutz sind die eingangs dargestellten Kriterien bzgl. der Pflichtenbestimmung im IT-Bereich maßgeblich. Demnach sind die berechtigten Sicherheitserwartungen des Verkehrs und der zumutbare Aufwand für die Bestimmung der Selbstschutzpflichten entscheidend. Es ist eine wertende Interessenabwägung vorzunehmen, bei der das Ausmaß der drohenden Gefahr, sowie die Möglichkeit und Zumutbarkeit der Gefahrenvermeidung auf Seiten des Gefahrverursachers und des Selbstschutzes auf Seiten des Gefährdeten unter Berücksichtigung von Vertrauensschutzgesichtspunkten gewichtet werden müssen.[621] Unter Berücksichtigung dieses Maßstabs wird angesichts des allgemein bekannten Risikos von Computerviren und der geringen Kosten für die Einrichtungen eines aktuellen Virenschutzprogramms teilweise ausdrücklich auch für Privatpersonen die Zumutbarkeit von Selbstschutzmaßnahmen bejaht und eine Schadensbegrenzungspflicht angenommen.[622]

318 Für eine solche Verpflichtung privater IT-Nutzer spricht insbesondere der Umstand, dass das Ausmaß des drohenden Schadens entscheidend von der dem IT-Hersteller regelmäßig unbekannten Tatsache abhängt, welche Daten sich auf der verwendeten

---

[617] BGH NJW 1989, 290 (292).
[618] BGH VersR 1996, 380 (381).
[618] BGH DB 1956, 110 f.; Palandt-*Heinrichs,* § 254 BGB Rn. 74.
[619] Ähnl. *v.Westphalen*, PHI 1998, 222 (223)
[620] *Burg/Gimnich*, DRiZ 2003, 381 (384 f.); *Günther*, Produkthaftung für Informationsgüter, 303 f.; *Schneider/Günther,* CR 1997, 389 (394); *Koch,* NJW 2004, 801 (804 ff .); *Schmidbauer*, Schadensersatz wegen Viren, abrufbar unter http://www.i4j.at/news/aktuell36.htm (zuletzt abgerufen am 22.2.2006).
[621] Vgl. *Koch*, NJW 2004, 801 (804); *Libertus*, MMR 2005, 507 (509).
[622] So bezüglich der Risiken im E-Mail-Verkehr: *Koch*, NJW 2004, 801 (807): In Anlehnung an die Rechtsfigur der Betriebsgefahr im Straßenverkehr will der Autor einen Mitverschuldensanteil von 25 % bei ungenügenden Virenschutzvorkehrungen veranschlagen.

Hardware befinden und wofür diese benutzt werden.[623] Der IT-Anwender kann folglich das Schadensrisiko wesentlich besser abschätzen und durch entsprechende Vorkehrungen auffangen. Richtigerweise ist allerdings unter Bezugnahme auf das Kriterium der Zumutbarkeit der Gefahrenvermeidung zwischen den verschiedenen IT-Anwendern zu differenzieren: Während professionellen IT-Anwendern bei entsprechenden Kenntnissen und Ressourcen derartige Selbstschutzmaßnahmen zumutbar sind,[624] sind die Voraussetzungen bei privaten IT-Nutzern höher. Der Einsatz von Virenscannern ist ihnen aber zuzumuten (oben Rn. 297).

319 Neben dem Zumutbarkeitskriterium kann hier als maßgeblicher Anknüpfungspunkt für diese Differenzierung auch der Gedanke der **Vorteilsziehung** herangezogen werden: Nicht alle IT-Anwender nutzen Softwareprodukte in gleichem Maße und profitieren dementsprechend davon. Der Gedanke der Vorteilsziehung ist in Rechtsprechung und Lehre gleichermaßen als Anknüpfungspunkt zur Bestimmung von Art und Ausmaß der Verkehrspflichten, sowie als Rechtfertigungsgrund zur haftungsrechtlichen Ungleichbehandlung von Privaten und Unternehmern anerkannt.[625] Letztere profitieren in besonderem Maße vom Einsatz von Software und erlangen somit nicht unerhebliche betriebswirtschaftliche Vorteile. Insofern ist unter Berücksichtigung des Gedankens der Vorteilsziehung bzgl. der Bestimmung der Selbstschutzpflichten des Softwarebenutzers folgerichtig zwischen professionellen IT-Anwendern und privaten IT-Anwendern zu unterscheiden. Privaten Softwarebenutzern ist demnach eine Pflicht zu Selbstschutzmaßnahmen unter anderen Voraussetzungen aufzuerlegen.

320 Diese Rechtsauffassung hat der BGH auch in seinem Urteil zu Mehrwertdiensten hinsichtlich einer Pflicht zum Einsatz von Dialerschutz-Programmen deutlich zum Ausdruck gebracht, indem er ausgeführt hat, dass privaten IT-Nutzern eine routinemäßige Überprüfung auf Dialer ohne besondere Verdachtsmomente sowie die Überwachung des Aufbaus von Verbindungen ins Internet nicht obliege.[626] Des Weiteren hat er klargestellt, dass privaten IT-Nutzern keine Pflicht zur Verwendung und Aktualisierung ei-

[623] *Koch*, NJW 2004, 801 (804 f.); *Libertus*, MMR 2005, 507 (509).

[624] S. unten Rn. 375 ff.

[625] BGHZ 5, 378 (384) = NJW 1952, 1050; BGH LM Nr. 10 zu § 823 (Db) BGB; *v. Bar*, Verkehrspflichten, S. 126 mwN.; s. auch *Raab*, JuS 2002, 1041 (1044 f.).

[626] BGH NJW 2004, 1590 (1592) = JZ 2004, 1124 (1127) m. Anm. *Spindler*; s. auch die parallelen Erwägungen des BGH im Fall der R-Gespräche, BGH NJW 2006, 1971 Tz. 22 ff. = MMR 2006, 453, 456, in concreto Zumutbarkeit von Eigenschutzmaßnahmen abgelehnt.

nes Dialerschutzprogramms treffe.[627] Anders ist dies aber zu beurteilen, wenn die Gefahr sowie die Lösung allgemein bekannt sind. Demgemäß entfällt die Pflicht zu Selbstschutzmaßnahmen zumindest bei privaten Softwarenutzern, wenn nicht Problem und Lösung bekannt und die Ergreifung technisch und wirtschaftlich zumutbar ist.[628]

321 Bei Programmen mit bekannten Sicherheitslücken muss der Nutzer, insbesondere ein Unternehmen, dieses Programm sperren und darf es nicht mehr einsetzen. Benutzt es dennoch sehenden Auges die fehlerhafte Software und entstehen hierdurch aufgrund Hackerangriffe Schäden, kann sich ein völliger Ausschluss des Schadensersatzanspruchs ergeben.[629]

322 Schließlich sind Nutzer grundsätzlich auch zum Einspielen von kostenlos zur Verfügung gestellten **Patches** verpflichtet,[630] so daß sich der Hersteller (bzw. Pflichtige) in der Regel auf ein Mitverschulden des Geschädigten berufen kann, wenn dieser einen Patch nicht verwandt hat. Allerdings kann dies nicht uneingeschränkt gelten, da manche Patches einen derartigen Umfang haben, das sie selbst bei breitbandigen Internet-Zugängen kaum herunterladbar sind, etwa das Service Pack 2 für Windows XP. Stellt hier der Hersteller aber kostenlos eine CD zur Verfügung, greifen die entsprechenden Beschränkungen für die Pflichten des Herstellers ebenfalls.

c) Schadensabwendungspflichten

323 Eher die Ausnahme sind Pflichten des Softwarenutzers, insbesondere gewerblicher, etwaigen Schäden durch eine eigenständige Bearbeitung des Programms zuvorzukommen, da ihnen oftmals nicht der Quellcode bekannt ist, und sie zudem das Risiko eingehen, mit urheberrechtlichen Beschränkungen durch den Softwarehersteller konfrontiert zu sein. Zwar darf nach § 69d I UrhG der Nutzungsberechtigte Bearbeitungen am Programm im Rahmen einer bestimmungsgemäßen Nutzung vornehmen, worunter auch die Fehlerbeseitigung fällt.[631] Doch kann aus dieser Erwägung nicht generell die Pflicht des Softwarebenutzers abgeleitet werden, auf eigenes Risiko hin Fehler im Programm zu

---

627 Zust.: *Spindler*, JZ 2004, 1128 (1128 ff.); *Rösler,* NJW 2004, 2566 (2566 ff.); *Mankowski,* MMR 2004, 312 (312 f.); *ders.* CR 2004, 185 (188).

628 S. o. Rn. 275 ff.

629 *Bartsch*, Software und das Jahr 2000, S. 86.

630 Ebenso das britische Recht, vgl. Reed – Annex II – Rn. 1287.

631 OLG Karlsruhe NJW 1996, 2583 (2584); Schricker-*Loewenheim*, § 69d UrhG, Rn. 9; *Schneider,* Handbuch des EDV-Rechts, C Rn. 200 ff.; *Haberstumpf*, in: Lehmann, Rechtsschutz und Verwertung von Computerprogrammen, Kap. II Rz. 159, 169; für das schweizerische Recht *Rigamonti*, SJZ 1998, 430 (433).

632 Zum Vorteilsausgleich, wenn der Hersteller dem Nutzer ein verbessertes Paket mit erweiterter Funktionalität zur Verfügung stellt, um den Fehler zu beheben, s. näher *Spindler,* NJW 1999, 3737 (3744) mwN.

beheben. Eine Ausnahme wäre nur dann gegeben, wenn die drohenden Schäden in keinem Verhältnis mehr zu den möglichen Risiken einer Urheberrechtsverletzung stehen, der Geschädigte über dem Hersteller gleichwertige Kenntnisse verfügt und das Programm nicht ohne weiteres ausgetauscht werden kann.

324 **Ebenso wenig** ist dem Softwarenutzer zuzumuten, zur Schadensabwendung die **neueste Version einer Software zu kaufen**, die keine IT-Sicherheitslücken mehr aufweist. Eine solche Pflicht zum Update-Kauf würde letztlich die Verantwortung für einen Schaden von der Entscheidung des Herstellers abhängig machen, ein neues, verbessertes Produkt auf den Markt zu bringen.[632] Anders ist dies nur zu beurteilen, sofern eine starke Gefährdungslage besteht und dem Nutzer keine andere Möglichkeit verbleibt, als die Software zu ersetzen.

325 Ein in der Praxis offenbar weit verbreitetes Phänomen ist die **zeitliche Verzögerung,** mit der Firmennetzwerke durch das Einspielen **von Patches** gesichert werden, und die Dritten in der Zwischenzeit entsprechende Angriffe ermöglichen. Auch hier ist zu berücksichtigen, dass gerade Unternehmen eine Organisationspflicht trifft, auftretende Sicherheitsprobleme möglichst schnell zu bewältigen, um den Schaden gering zu halten. Natürlich können Sicherheitspatches nicht in jedem Fall unbesehen einfach auf alle PCs eines Netzwerkes aufgespielt werden; dennoch muss der unternehmerische Nutzer von Software seinerseits alles Zumutbare veranlassen, um Sicherheitslücken mit Hilfe von Sicherheitsupdates zu stopfen. Dies umfasst auch die durch den Einsatz von ungesicherten Laptops drohende Gefahr für Netzwerke; hier sind Netzwerkbetreiber gehalten, entsprechende Vorkehrungen gegen den Anschluss nicht gesicherter Notebooks zu treffen, sei es durch Kontrollen oder Sicherung solcher Geräte oder des Netzwerks.

d) Schadensminderung

326 IT-Sicherheitslücken und dadurch bedingte Angriffe durch Hacker mit der Folge von Datenverlusten werfen die Frage auf, zu welchen Schadensminderungsmaßnahmen der Nutzer verpflichtet ist. Dies läßt sich pauschal kaum beantworten, hängt es doch wiederum vom Gefahrenpotential, dessen Wahrscheinlichkeit und dem Rang der betroffenen Rechtsgüter ab,[633] ob etwa der Nutzer, z.B. ein Krankenhaus, gehalten ist, Reservesys-

[632] Zum Vorteilsausgleich, wenn der Hersteller dem Nutzer ein verbessertes Paket mit erweiterter Funktionalität zur Verfügung stellt, um den Fehler zu beheben, s. näher *Spindler,* NJW 1999, 3737 (3744) mwN.

[633] Für den Jahr-2000-Fehler: *Wohlgemuth*, MMR 1999, 59 (65); allg. und zu den sich in der Rechtsprechung herausgebildeten Fallgruppen: MünchKommBGB-*Oetker*, § 254 BGB Rn. 76 ff.; Bamberger/Roth-*Unberath*, § 254 Rn. 30 ff., jeweils mwN.

teme vorzuhalten. Oftmals entsteht aber auch bei diesen Systemen das Problem, dass sie dieselben Programme verwenden (müssen), so dass auch hier die IT-Sicherheitslücke fortbesteht. In der Regel wird der Hersteller daher nicht den Nutzer auf den Einsatz von Reservesystemen bei IT-Sicherheitsproblemen[634] verweisen können. Für Daten ist indes inzwischen anerkannt, dass eine regelmäßige Datensicherung der gebotenen Pflicht zur Schadensminderung entspricht, bei deren Verletzung ein Schadensersatzanspruch vollständig entfallen kann.[635]

4. Beweisfragen

327 Nach allgemeinen Grundsätzen trägt der Geschädigte die Darlegungs- und Beweislast für die haftungsbegründenden Voraussetzungen, im Rahmen des § 823 Abs. 1 BGB also insbesondere für Verkehrspflichtverletzung und Verschulden.[636] Die Rechtsdurchsetzung im Schadensfall hängt zunächst davon ab, die **Person des Schädigers** eindeutig zu identifizieren, was im Internet indessen unter Umständen auf erhebliche Schwierigkeiten stößt.[637] Auch wenn der Schädiger bekannt sein sollte, wird dieser seinen Wohnsitz oftmals im Ausland haben, so dass eine Rechtsverfolgung in der Praxis häufig unterbleiben wird. Bei Weiterverbreitung von Viren im E-Mail-Anhang eines Bekannten, Freundes oder Geschäftspartners mag der Nachweis gelingen. Der Absender von Spam-E-Mails oder die Initiatoren von Denial-of-Service-Attacken können demgegenüber im Regelfall nicht ohne weiteres ermittelt werden, da fremde E-Mail-Adressen und Rechner benutzt werden. Allgemeine Auskunftsansprüche privater Nutzer oder Unternehmen gegen Telekommunikationsunternehmen oder Internet-Provider zur Ermittlung des Absenders bestehen derzeit nicht.[638] Auskunftsberechtigt sind die Strafermittlungsbehörden, so dass bei strafbaren Handlungen im Einzelfall eine Akteneinsicht durch den Anwalt des Geschädigten (§ 147 StPO) und eine Beiziehung staatsanwaltlicher Ermittlungsakten im Zivilprozess in Betracht kommt. Oftmals wird die Inanspruchnahme privater Nutzer jedoch schon an der Identifikation der Person des Schädigers scheitern.

---

[634] Anders natürlich bei Hardware-Problemen, s. etwa OLG Hamm NJW-RR 1998, 380 (381) für einen ausgefallenen Drucker.

[635] OLG Hamm JurPC Web-Dok. 165/2004 Abs. 2, 14; OLG Karlsruhe NJW 1996, 200 (201); OLG Karlsruhe NJW-RR 1997, 554 (554 f.); *Erben/Zahrnt,* CR 2000, 88 f.; *Günther*, Produkthaftung für Informationsgüter, 303 f.; *Meier/Wehlau*, NJW 1998, 1585 (1590) mwN; zur Frage, ob Vertrauensschutz entsprechende Pflichten aufgrund vorherigen Handelns begründen kann, die dann auch Stillstandskosten umfassen würden, BGH NJW 1998, 456 (458), übertragen auf Datensicherung im IT-Bereich könnte also bei entsprechendem Vertrauen aufgrund vorhergegangener ständiger Datensicherungen ein entsprechendes Mitverschulden wegen Unterlassung der Schadensminderung in Form der Datensicherung angebracht sein. Da bei der Haftung nach § 823 Abs. 1 BGB jedoch regelmäßig kein vorheriger Kontakt besteht, kann auch kein solches Vertrauen vorliegen.

[636] Palandt-*Sprau*, § 823 BGB Rn. 80; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 280.

[637] S. dazu auch *Mankowski* in: Ernst, Hacker, Cracker & Computerviren, Rn. 510, 513.

[638] Für die Verletzung von Immaterialgüterrechten enthält § 14 Abs. 2 TMG eine Sonderregelung.

328 Auch wenn ein privater Nutzer eindeutig als Verursacher des Schadens identifiziert ist, hat der Geschädigte den Beweis einer **Pflichtverletzung** durch den Nutzer zu führen. Hierbei handelt es sich um Vorgänge, welche sich in der Sphäre des privaten Nutzers abspielen, in welche der Geschädigte keinen Einblick hat. Der Nachweis, dass ein privater Nutzer unter Verletzung von Sorgfaltspflichten einen E-Mail-Anhang geöffnet und so die Installation eines Virus oder Trojaners ermöglicht hat, wird daher nur schwer zu führen sein. Möglich wäre hier aber eine Untersuchung des Computers des Schädigers auf dem sich die E-Mail noch befindet. Hierzu kann das Gericht die Vorlage des Computers zur Einnahme des Augenscheins und sowie zur Begutachtung durch einen Sachverständigen anordnen (§§ 144 Abs. 1 Satz 2, 371 Abs. 2 ZPO). Ebenso kann so im Einzelfall das Vorhandensein und die regelmäßige Aktualisierung des Virenschutzes überprüft werden. Dies hilft aber dann nicht weiter, wenn der Rechner neu aufgesetzt wurde oder gar keine Protokolle über die Aktualisierung des Betriebssystems oder des Virenschutzes geführt wurden. Nur in Fällen der Beweisvereitelung kann die Behauptung des Geschädigten gemäß § 371 Abs. 3 ZPO als bewiesen angesehen werden.[639] Beim Beweis des **Mitschuldens des Geschädigten** stellen sich spiegelbildlich dieselben Probleme, denn die h.M. und ständige Rechtsprechung bürden dem Schädiger die Beweislast für das Mitverschulden auf.[640]

5. Ergebnis

329 Für private Nutzer lassen sich zwar Pflichten hinsichtlich der Ergreifung von Sicherungsmaßnahmen herleiten. Diese sind mangels der Bekanntheit von Problem und Lösung allerdings stark bzw. auf die Einhaltung allseits bekannter Schutzmaßnahmen eingeschränkt. Standards oder Regelwerke, anhand derer für private IT-Nutzer diese Pflichten konkretisiert werden könnten, sind – soweit ersichtlich – nicht vorhanden. Auch wenn sich begrenzte Verkehrspflichten privater Nutzer entwickeln lassen, ergeben sich in der Praxis zum Teil erhebliche Probleme die Person des Schädigers zu identifizieren und die Pflichtverletzung zu beweisen.

330 Insbesondere mit den aufgezeigten Durchsetzungsproblemen mag zusammenhängen, dass bislang keine Fälle der Inanspruchnahme privater Nutzer bekannt geworden sind. Zu Recht wird daher darauf hingewiesen, dass die Ansprüche des Geschädigten oftmals

---

[639] Dazu Zöller-*Greger*, § 371 ZPO Rn. 5; Musielak-*Huber*, § 371 ZPO Rn. 20.

[640] BGH NJW-RR 2001, 1542 (1543); BGH NJW 2000, 664 (667); BGH NJW 1998, 3706 (3707); BGHZ 90, 17 (32 f.); BGHZ 91, 243 (260); RGZ 159, 257 (261); *Lange/Schiemann,* Schadensersatz, § 10 XIX ; MünchKommBGB-*Oetker*, § 254 BGB Rn. 145.

nur auf dem Papier bestehen.[641] Für geschädigte Private gehen die Beweisschwierigkeiten mit dem Prozeßkostenrisiko (insbesondere Sachverständigenkosten) einher, welche oftmals zudem in keinem vernünftigen Verhältnis zum Schaden stehen werden. Im Zusammenhang mit Viren usw. dürfte hinzukommen, dass private Nutzer diese Erscheinungen als letztlich nicht vollständig vermeidbares Risiko der Internetnutzung hinnehmen, ohne gegen den Verursacher vorzugehen. Bei geschädigten Unternehmen drohen regelmäßig hohe Schadenssummen, jedoch wird dann neben den Schwierigkeiten der prozessualen Rechtsdurchsetzung die mangelnde Beitreibbarkeit der Schadenssumme eine Rechtsverfolgung häufig nicht lohnen.[642] Gleichfalls werden Unternehmen die mit der Rechsverfolgung verbundene Offenbarung von Sicherheitslücken scheuen.[643] Umgekehrt wäre eine Belastung der Nutzer mit praktisch kaum vorhersehbaren – und damit auch kaum versicherbaren Haftungsrisiken – wenig effizient. Eine Haftung privater Nutzer wegen Verletzung von Sorgfaltspflichten erscheint gegenwärtig im Rahmen von Vertragsverhältnissen im Bereich des E-Commerce am wahrscheinlichsten. Siehe dazu ausführlich unten zum Online-Banking Rn. 529 ff.

III. Einsatz von IT bei kommerziellen Unternehmen als Nutzer

1. Überblick

331 Bei kommerziellen Nutzern von IT-Anlagen stellt sich die Lage anders dar. Als kommerzielle Nutzer können – negativ abgegrenzt – alle diejenigen gelten, die nicht privater Nutzer sind, wobei auch hier eine rollenspezifische bzw. funktionale Betrachtungsweise maßgeblich ist. Für bestimmte Bereiche existieren ausdrückliche Regelungen bzw. Regelungen, die die IT-Nutzung unter Auslegung der Norm erfassen könnten. Hinzu können deliktische Ansprüche bei Nichtergreifung der geregelten Pflichten kommen, sofern sie als Schutzgesetz i.S.d. § 823 Abs. 2 BGB einzuordnen sind. Weiter können auch im Rahmen der Haftung nach § 823 Abs. 1 BGB bei kommerziellen Nutzern allgemeine Verkehrssicherungspflichten bestehen, wobei sich der Pflichtenmaßstab von demjenigen bei privaten IT-Nutzern durchaus unterscheiden kann. Diese Pflichten gelten wiederum spiegelbildlich im Bereich der nach § 254 BGB den kommerziellen IT-Nutzern ab-

[641] *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 510.
[642] So auch *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 510.
[643] *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 513.

zuverlangenden Selbstschutzpflichten, die oftmals im Bereich der Organisation besonders konkretisiert sind.

2. Gefahrenpotential und Gegenmaßnahmen

332 In der Regel liegen bei kommerziellen Nutzern unternehmenswichtige Daten vor, die entweder den Betrieb selbst bzw. dessen Organisation oder Umstände der Beziehungen zu den Kunden betreffen. Verlust oder Manipulation dieser Daten können demnach auch das gesamte Unternehmen bedrohen. Hinzu kommt, dass mit der zunehmenden Vernetzung gerade in größeren Unternehmen viele Akteure die Kommunikation bestimmen. Die Angriffsfläche ist damit häufig größer als bei einzelnen Privaten. Dementsprechend aufwändiger ist dann auch die Ergreifung von Gegenmaßnahmen.

3. Anforderungen an die kommerziellen Unternehmen

333 IT-Riskmanagementpflichten können sich sowohl aus allgemeinen gesellschafts- und wirtschafts- wie zivilrechtlichen Vorschriften als auch aus datenschutzrechtlichen Regelungen ergeben. Im Folgenden werden zunächst die relevanten Einzelvorschriften dargestellt. Dabei sind der Hintergrund der Regelung, die daraus resultierenden Pflichten und der Adressat, die möglichen Rechtsfolgen und die Anhaltspunkte für IT-Konkretisierung von Interesse. Anschließend erfolgt eine Gesamtbetrachtung der Vorschriften.

a) Gesellschafts-, wirtschafts- und allgemein zivilrechtliche Anforderungen

334 Praktisch für (fast) alle kommerziellen IT-Nutzer können Pflichten verallgemeinert werden, die aus allgemeinen handels- und gesellschaftsrechtlichen Pflichten abgeleitet werden. Allerdings gelten diese Pflichten zunächst allein im Innenverhältnis zwischen den Organen und der juristischen Person; sie können nicht ohne weiteres auf das Außenverhältnis übertragen werden (sei es für Schädigungen Dritter, sei es für die Konkretisierung von § 254 BGB). Dennoch geben sie wichtige Anhaltspunkte auch für entsprechende Selbstschutzpflichten, da oftmals organisatorische Anforderungen in Rede stehen, die quasi vom Innen- auf das Außenverhältnis übertragen werden. Als Reaktionen auf verschiedene Firmenzusammenbrüche sowohl in den USA als auch in Deutschland sind zudem seit 1998 die Anforderungen an das unternehmensinterne Management gesetzlich verankert, teilweise auch verschärft worden - was auch Auswirkungen auf das IT-Management im Unternehmen hat. Neben den deutschen Vorschriften zum Riskmanagement sind hier in erster Linie der von den beiden US-Kongressabgeordneten Paul

Sarbanes und Michael Oxley angeregte amerikanische Sarbanes-Oxley-Act (SOX) ebenso wie die Regelwerke zur Prüfung von Fremdkapital (Basle II) zu nennen. Demgemäß werden zunächst die im Rahmen der Corporate Governance entwickelten IT-Riskmanagementpflichten betrachtet (Rn 335 ff.), einschließlich der mittelbar aus den neuen Fremdkapitalvergabevorschriften (Basel II) folgenden Vorgaben (Rn 357 ff.), anschließend dann die jeweiligen Selbstschutz- bzw. Verkehrssicherungspflichten (Rn. 375 ff.).

(1) IT-Riskmanagement als Geschäftsleiterpflicht

(a) Hintergrund

335 Die Steuerung von Risiken beim Softwareeinkauf und -einsatz war seit jeher ein Thema überwiegend der Betriebswirtschaft. Softwarepflege, gemeinsame Projektrealisierung[644] und -implementierung dominier(t)en die Themenpalette.[645] Erst mit Einführung des § 91 Abs. 2 AktG durch das KonTraG 1998 ist die rechtlich verbindliche Pflicht der Geschäftsleitung – auch der GmbH[646] – zur Einrichtung eines Risikomanagements für alle Geschäftsfelder deutlicher in das Bewusstsein gerückt,[647] aber nicht nur in Deutschland, sondern auch in anderen Staaten, wie etwa Österreich, teilweise noch durch eine – dem deutschen Recht bislang fremde und nur in § 130 OWiG verankerte - Unternehmensstrafbarkeit für Organisationsmängel.[648] Damit gehören im Prinzip auch der Einkauf und die Implementation von Software zu dem Bereich, dessen Risikopotentiale abgeschätzt und gesteuert werden müssen.

(b) Pflichten und Adressat

336 Die allgemeinen Anforderungen des § 91 Abs. 2 AktG verpflichten den Vorstand dazu, für eine Organisation und ein Managementsystem zu sorgen, das möglichst frühzeitig Risiken zu erkennen vermag, die die Existenz des Unternehmens bedrohen können.[649] Entsprechende Vorkehrungen müssen sowohl durch Festlegung von Zuständigkeiten als

---

[644] S. etwa *Müller-Hengstenberg,* CR 2005, 385 ff., *Schneider,* CR 2000, 27 ff., *Karger,* ITRB 2004, 208 ff. zu entsprechenden Vertragsgestaltungen bei der Projektsteuerung und Projektrisiken.

[645] Vgl. hierzu *Schneider*, Handbuch des EDV-Rechts, Kap. E Rn. 29 ff.; sowie im Zusammenhang mit AGB Kap. E II.

[646] Zwar fehlt es hier an einer entsprechenden Regelung in §§ 35, 43 GmbHG, doch ist es allg. M., dass § 91 Abs. 2 AktG jedenfalls sinngemäß darauf angewandt werden kann, s. dazu *Drygala/Drygala,* ZIP 2000, 297 (301); *Hommelhoff,* in: FS Sandrock, 373 ff.; *Altmeppen,* ZGR 1999, 291 (300 ff.); *Bockslaff,* NVersZ 1999, 104 (109).

[647] Schon zuvor bestanden in zahlreichen Einzelgebieten Pflichten zur ordnungsgemäßen Organisation und zum Risikomanagement, umfassend dazu *Spindler*, Unternehmensorganisationspflichten, 2001, passim.

[648] S. *Fallenböck* Annex II – Österreich - Rn. 1191 ff.

[649] *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 8 ff.; *Seibert*, in: FS Bezzenberger, 427 (437); *Fleischer,* AG 2003, 291 (298); *Zimmer/Sonneborn*, in: Lange/Wall, § 1 Rn. 180 f.; *Becker/Janker/Müller,* DStR 2004, 1578 (1579); *Hauschka,* AG 2004, 461 (467 f.); *Becker/Janker/Müller,* DStR 2004, 1578 (1579); *Schwintowski,* NZG 2005, 200 (201); *Roth/Schneider,* ITRB 2005, 19; MünchKommAktG-*Hefermehl/Spindler,* § 91 AktG Rn. 14 ff. mwN.

auch durch Verfahren getroffen werden. So müssen eindeutig Verantwortlichkeiten und Berichtswege bestimmt werden, um zu verhindern, dass keiner sich für bestimmte Risiken zuständig fühlt; ebenso muss klargestellt werden, wann und wie die Geschäftsleitung von bedeutsamen Vorfällen erfährt, um rechtzeitig darauf reagieren zu können.[650] Verfahrensmäßige Vorkehrungen bestehen oftmals aus Checklisten, die einzuhalten sind, um typische Risiken aufzufangen und um sich ihrer bewusst zu werden, oder aus Abstimmungsverfahren mit anderen Abteilungen, damit nach einem Vier-Augen-Prinzip eine gegenseitige Kontrolle gewährleistet wird.[651]

337 Der Bereich der IT-Sicherheit ist nicht ausdrücklich vom Wortlaut des § 91 Abs. 2 AktG erfasst. Insofern kommt der Auslegung der Norm entscheidende Bedeutung zu. Um die inhaltlichen Anforderungen richtig zu erfassen, ist insbesondere auch der Hintergrund der Herausbildung von Risk Management Systemen im Bereich des Kreditwesens (§ 25a KWG) zu beachten.[652] Insbesondere beinhaltet § 91 Abs. 2 AktG demnach eine einfache Organisationsanforderung und schreibt nicht etwa ein allgemeines Risikomanagement vor.[653] Zu überwachen sind etwa risikoträchtige Zustände oder Entwicklungen und die Einhaltung der eingeleiteten Maßnahmen, ob also das Veranlasste umgesetzt wird und Innenrevision und Controlling die von ihnen gewonnenen Kenntnisse zeitnah dem Vorstand weiterleiten. Die Vorstandsmitglieder der AG haften insofern gesamtschuldnerisch gem. § 93 Abs. 2 S. 1 AktG für die Einrichtung geeigneter Maßnahmen, „insbesondere“ eines Überwachungssystems, zur Früherkennung bestandsgefährdender Entwicklungen.

338 **Entwicklungen** sind hier Veränderungen und Prozesse,[654] wobei zur Erkennung von Veränderungen die Erfassung des Ist-Zustandes und eine **Risikoabschätzung** unerlässlich sind. Nicht jede nachteilige Entwicklung muss frühzeitig erkannt werden. Vielmehr bezieht sich § 91 Abs. 2 AktG lediglich auf besondere, bestandsgefährdende Entwicklungen, also auf solche Veränderungen, die sich auf die Vermögens-, Ertrags- oder Finanzlage der Gesellschaft wesentlich auswirken können.[655] Schließlich bedeutet „früh-

[650] Begr RegE BT-Drucks. 13/9712, 15; *Zimmer/Sonneborn*, in: Lange/Wall, § 1 Rn. 181; *Hüffer,* § 91 AktG Rn. 7; *Stober,* DÖV 2005, 333 (334).

[651] Ausführlicher dazu *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 25, 47; *Spindler*, Unternehmensorganisationspflichten, 2001.

[652] MünchKommAktG-*Hefermehl/Spindler*, AktG, 2. Aufl. 2004, § 91 AktG Rn. 14 ff.

[653] Zur Unterscheidung eingehend: *Hüffer*, AktG, 6. Aufl. 2004, § 91 AktG Rn. 9; MünchKommAktG-*Hefermehl/Spindler*, AktG, § 91 AktG Rn. 23 f.

[654] MünchKommAktG-*Hefermehl/Spindler*, § 91 AktG Rn. 14 ff.

[655] BegrRegE BT-Drucks. 13/9712, 7.

zeitiges Erkennen", dass nachteilige Entwicklungen noch verhindert werden können und der Bestandsgefährdung noch effektiv entgegengewirkt werden kann.[656] Insgesamt ist somit dafür Sorge zu tragen, dass sowohl bestehende, als auch zukünftige, d.h. potentielle Risiken kontrollierbar und kalkulierbar sind, was die möglichst vollständige Identifizierung von Ursachen und Ausmaß der Risiken impliziert.[657]

339 In diesem Zusammenhang sind ergänzend die auf europäischer Ebene unterbreiteten Vorschläge zur Stärkung der Überwachung der Directors bzw. des Vorstands zu erwähnen,[658] insbesondere der Vorschlag der Europäischen Kommission zur Modernisierung der Achten Gesellschaftrechtlichen Richtlinie („Prüferrichtlinie")[659], der insbesondere die Einrichtung eines **Audit Committees** vorsieht. Das Audit Committee soll insbesondere zuständig sein für die Überwachung des Risikomanagements, sowie der Innenrevision und des internen Kontrollsystems. In Deutschland verfügen bereits fast alle börsennotierten Gesellschaften über Audit Committees in Form von Ausschüssen des Aufsichtsrates. Allerdings bezieht sich der Richtlinienvorschlag darüber hinaus auch auf sonstige Unternehmen des öffentlichen Interesses wie Banken und Versicherungen[660], so dass auch in diesen Branchen die Einrichtung eines solchen Gremiums vonnöten wäre. Der im Vorschlag der Kommission verankerte Aufgabenkatalog stimmt ansonsten im Wesentlichen mit den Vorgaben des Abschnittes 5.3.2 DCGK überein, geht aber in Art. 39 mit der Statuierung der Überwachung des internen Kontrollsystems und der Innenrevision darüber hinaus. Zudem konkretisiert der Richtlinienvorschlag die Vorgaben des § 91 Abs. 2 AktG. Explizit ergibt sich daraus als IT-relevanten Anknüpfungspunkt allein die Pflicht des Vorstandes zur Einrichtung eines Risikomanagementsystems, so dass dem Aufsichtsrat im Rahmen seiner allgemeinen Überwachungstätigkeit auch die Kontrolle des Risk-Managements obliegt. Die Einrichtung eines internen Kontrollsystems kommt ihm hingegen nach deutschem Recht nur aus allgemeinen Pflichten zu, weshalb der europäische Richtlinienvorschlag diese allgemeinen Sorgfaltspflichten konkretisieren würde.[661] Allerdings steht die Annahme des Vorschlags der Kommission weiterhin aus, weshalb auch Art. 39 des Richtlinienvorschlags zur Modernisierung der

[656] BegrRegE BT-Drucks. 13/9712, 15.

[657] *Terlau*, CR 1999, 284 (286).

[658] KOM (2003) 286: Mitteilung der Kommission an den Rat und das Europäische Parlament: Stärkung der Abschlussprüfung in der EU.

[659] KOM/2004/0177 endg. Vom 16.3.2004, abrufbar unter: http://www.europarl.eu.int/oeil/file.jsp?id=241922.

[660] *Maul/Lanfermann*, BB 2004, 1861 (1865).

[661] *Maul/Lanfermann*, BB 2004, 1861 (1866).

Prüferrichtlinie gegenwärtig noch nicht zur Konkretisierung der Aufgaben des Aufsichtsrates herangezogen werden kann. Es bleibt insofern vorerst bei der zu § 91 Abs. 2 AktG dargelegten Gesetzesauslegung.

(c) Rechtsfolgen

340 Bei Verstoß gegen die Pflichten aus § 91 Abs. 2 AktG greift zum einen die bereits erwähnte gesamtschuldnerische Haftung der Vorstandsmitglieder gem. § 93 Abs. 2 S. 1 AktG ein. Sorgen die einzelnen Vorstandsmitglieder nicht für die Einrichtung eines Riskmanagements, das auch die IT-Risiken umfasst[662], kann eine entsprechende Haftung auf Schadensersatz gegenüber der Gesellschaft sie persönlich treffen gemäß §§ 93 I AktG. Eine persönliche Haftung gegenüber Dritten ist jedoch selbst unter Zugrundelegung der Rechtsprechung[663] eher die Ausnahme[664]. Zudem kann ein wichtiger Grund zur Abberufung und fristlosen Kündigung vorliegen.[665]

341 Nicht abschließend geklärt ist, ob bei Verstoß gegen die Pflicht aus § 91 Abs. 2 AktG bzw. die Pflicht zur ordnungsgemäßen Buchhaltung gem. § 91 Abs. 1 AktG auch eine deliktische Haftung der Vorstandsmitglieder im Rahmen einer Schutzgesetzverletzung bei § 823 Abs. 2 BGB in Betracht kommt. Dies setzt voraus, dass ein Vorstandsmitglied gegen ein den Schutz eines anderen bezweckendes Gesetz verstoßen hat. Die Einordnung des § 91 Abs. 1 und 2 als Schutzgesetz ist aber abzulehnen. Zum einen ist anerkannt, das § 93 Abs. 1 und 2 kein Schutzgesetz im Sinne des § 823 Abs. 2 darstellt[666]. Es ist nicht ersichtlich weshalb die Organisationspflichten des § 91 Abs. 2 in haftungsrechtlicher Sicht über die Sorgfaltspflichten des § 93 hinausgehen sollten, zumal schon vor Einführung des § 91 Abs.2 AktG nach §§ 76, 93 AktG die Pflicht bestand, für eine angemessene Organisation zu sorgen und gefährdende Entwicklung zu erkennen[667]. Zum anderen geht die h.M. auch im Rahmen des § 91 Abs. 1 davon aus, dass kein Schutzge-

---

662 *Schultze-Melling*, CR 2005, 73 (76); *Roth/Schneider*, ITRB 2005, 19 (19).

663 BGHZ 109, 297, 302 (VI. Zivilsenat) = NJW 1990, 976 – Baustoff II = JZ 1990, 486 m. Anm. *Wagner*; zust. *Brüggemeier*, AcP 191 (1991), 33 (63 ff.); *Foerste*, VersR 2002, 1 ff.; mit anderer, rechtsgeschichtlicher Begründung *Altmeppen*, ZIP 1995, 881 (886 f.); zusammenfassend *Gross*, ZGR 1998, 551 (562 ff.).

664 Zur Kritik an der Rechtsprechung bzgl. des Vorliegens von Verkehrssicherungspflichten bei mittelbarer Verletzungshandlung MünchKommAktG-*Hefermehl/Spindler*, § 93 AktG Rn. 188; MünchKommBGB-*Wagner*, § 823 BGB Rn. 394, mwN; eingehend *Spindler*, Unternehmensorganisationspflichten, 2001, 844 ff.

665 KG, NZG 2004, 1165; s. auch VG Frankfurt/M WM 2004, 2157; MünchKommAktG-*Hefermehl/Spindler*, § 91 AktG Rn. 28 mwN.

666 *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 13 Rn. 41; MünchKommAktG-*Hefermehl/Spindler*, § 91 AktG Rn. 12 mwN.

667 *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 6.

setz begründet wird[668], obwohl die Nähe des Regelungsbereichs zu den Vorschriften und Grundsätzen des Kapitalerhaltungsrechts die Annahme eher begründen könnte.

(d) Anhaltspunkte für IT-Konkretisierung

342 Zu den vom Riskmanagement abzudeckenden Bereichen gehören unter anderem auch der Einkauf, die Implementierung und die regelmäßige Kontrolle von Software, deren Risikopotentiale abgeschätzt und gesteuert werden müssen. Versagt die Software, oder darf sie nicht eingesetzt werden, können einem Unternehmen (aber auch anderen Verwendern, wie Behörden) erhebliche Schäden drohen, die bis hin zur fast völligen Lahmlegung eines Unternehmens gehen können. Unter diesen Umständen droht mithin eine Bestandsgefährdung und der Vorstand hat die Risiken, die sich aus dem IT-Einsatz ergeben, in die Risikoabschätzung zur Erkennung von Veränderungen einfließen zu lassen. Insbesondere der Ausfall von IT-gestützten Steuerungs- oder Buchführungssystemen kann bereits innerhalb weniger Tage zu einem größeren Schaden für das Unternehmen führen.

343 Neben der Pflicht zu einem ausreichenden Risikomanagement aus § 91 Abs. 2 AktG greift hinsichtlich der Buchführungssoftware auch die Pflicht des Vorstands zu ordnungsgemäßer Buchführung aus § 91 Abs.1 AktG, bzw. parallel hierzu aus § 41 Abs. 1 GmbHG und verpflichtet die Geschäftsleitung dazu, angemessene organisatorische Maßnahmen zur Risikominimierung zu treffen. Hierzu gehört nicht allein die Datensicherung, sondern auch die Berücksichtigung alternativer Buchführungssysteme im Falle des EDV-Ausfalls.[669]

344 Eine genaue Zahl der Datensicherungs- und Kontrollabstände lässt sich allerdings nur individuell für jede AG und den jeweils verwendeten IT-Baustein einzeln bestimmen, da ansonsten dem Leitungsermessen des Vorstandes widersprochen würde. Die Unternehmensleitung hat insofern unter den zur Beseitigung des Risikos verfügbaren Maßnahmen im Rahmen des von der Rechtsprechung anerkannten zulässigen Risikos eine Auswahl zu treffen. Exemplarisch führt der BGH in einem obiter dictum zum ARAG/Garmenbeck-Urteil grundlegend aus[670]:

> "[...] Eine Schadensersatzpflicht kann erst in Betracht kommen, wenn die Grenzen, in denen sich ein von Verantwortungsbewusstsein getragenes, ausschließlich am Unternehmenswohl orientiertes, auf

[668] *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 13 Rn. 51 ff.
[669] *Terlau*, CR 1999, 284 (286); *Streitz*, in: v.Westphalen/Langheit/Streitz, Jahr-2000-Fehler, Rn. 238 ff.
[670] BGH ZIP 1997, 883 (885).

sorgfältiger Ermittlung der Entscheidungsgrundlagen beruhendes unternehmerisches Handeln bewegen muss, deutlich überschritten sind, die Bereitschaft, unternehmerische Risiken einzugehen, in unverantwortlicher Weise überspannt worden ist oder das Verhalten des Vorstandes aus anderen Gründen als pflichtwidrig gelten muss."

345 Als Anhaltspunkte für die Erforschung der Gefahren im Unternehmen können die folgenden Punkte dienen:

- die Bedeutung des EDV-Systems für die Geschäftstätigkeit des Unternehmens,
- die Beschaffenheit und Stabilität der eingesetzten EDV-Systeme,
- die Komplexität der Geschäftsprozesse,
- die Abhängigkeit der Funktionsfähigkeit der EDV-Systeme von Dritten (Software-Lieferanten),
- die Gefährdung der Geschäftsabläufe durch den Ausfall einzelner Softwarekomponenten bis hin zum Ausfall des kompletten IT-Systems mit der Aufteilung in Steuerungs- und Datenverarbeitungssoftware, sowie Hardware
- die Abhängigkeit des Geschäftsbetriebs von EDV-Dienstleistern im Falle ausgelagerter Systeme,
- die Abhängigkeit des Geschäftsbetriebs von der Ordnungsmäßigkeit des Geschäftsbetriebes Dritter (Zulieferer, Kunden etc.).

346 Insbesondere in Bereichen sog. „kritischer Infrastrukturen", wie Verkehr, Logistik, Gesundheit, Finanzbereichen, um nur einige zu nennen, spielt die Sicherheit der Informationstechnologie eine entscheidende Rolle.[671] Der befürchtete Jahr-2000-Fehler hatte deutlich vor Augen geführt, wie abhängig Unternehmen und eine ganze Volkswirtschaft von IT-Produkten inzwischen sind.[672] Zu den Pflichten der Geschäftsleitung können dementsprechend auch der Abschluss von Pflegeverträgen und die Schaffung von redundanten Sicherheitssystemen gehören, um dem Ausfall der IT-Steuerungssoftware vorzubeugen.

(e) Riskmanagementpflichten in anderen Rechtsformen

347 Nicht nur in Aktiengesellschaften, sondern auch in anderen Rechtsformen gehört ein Riskmanagement zu den Geschäftsführerpflichten. Dies ergibt sich schon daraus, dass schon bei der Einführung des § 91 II AktG der Gesetzgeber selbst davon ausgegangen

[671] Eingehend dazu die Studien des Bundesamtes für Sicherheit in der Informationstechnologie, „Kritische Infrastrukturen", abrufbar unter: http://www.bsi.bund.de/fachthem/kritis/ (zuletzt abgerufen am 20.02. 2006).

[672] Aus der damaligen Literatur statt vieler: *Bartsch*, CR 1998, 193 ff.; *Spindler*, NJW 1999, 3737 ff.; *v.Westphalen*, DStR 1998, 1722 ff.

ist, dass damit nur allgemeine, aus den Sorgfaltspflichten der Geschäftsführung resultierende Anforderungen kodifiziert werden. Damit ergeben sich aber auch für andere Rechtsformen vergleichbare Pflichten, etwa für die GmbH nach § 43 GmbHG,[673] die indes nach dem Zuschnitt der jeweiligen Gesellschaft (kleine und mittlere Unternehmen) selbstverständlich zu modifizieren sind.

(f) Das IT-Riskmanagementsystem nach ISO 27001

348 Ähnlich den Qualitätsmanagementsystemen liegen inzwischen auch Normungen für das **IT-Riskmanagement** in Gestalt der Ende 2005 verabschiedeten ISO 27001[674] vor. Diese Normung folgt weitgehend dem britischen Ansatz im Qualitätsmanagementsektor, der auf die Steuerung von Geschäftsprozessen abzielt und weniger materielle Vorgaben trifft. In Deutschland wird neben der Zertifizierung nach ISO 27001[675] vor allem die Prüfung nach dieser Norm zuzüglich des vom BSI standardisierten Grundschutzes im IT-Sektor durchgeführt;[676] nur durch letztere wird die Einhaltung materieller Standards gewährleistet, da ein reines Managementsystem ohne jegliche Sicherheitsvorgaben nicht den Anforderungen an die Früherkennung von Risiken im IT-Bereich gerecht werden dürfte.

349 Die Norm ISO 27001 spezifiziert Anforderungen für Erstellung, Einführung, Betrieb, Überwachung und Überprüfung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems.[677] In die Anforderungen werden alle möglichen Risiken in der gesamten Organisation einbezogen, wobei zwischen verschiedenen Organisationsformen differenziert wird. Hierbei werden sämtliche Arten von Organisationen (z.B. Handelsunternehmen, staatliche Organisationen, Non-Profitorganisationen)[678] berücksichtigt.

350 Grundsätzlich wird das Modell des "Plan-Do-Check-Act" (PDCA), also Planung, Implementierung, Überprüfung und Handlung für die Strukturierung des IT-

---

[673] Zur Frage der analogen Anwendung des § 91 Abs. 2 AktG auf den Geschäftsführer einer GmbH Baumbach/Hueck-*Schulze-Osterloh*, § 41 GmbHG Rn. 1; Lutter/Hommelhoff-*Hommelhoff/Kleindiek*, § 43 GmbHG Rn. 19 jeweils mwN.

[674] ISO/IEC 27001, v. 15.10.2005, "Information technology - Security techniques - Information security management systems - Requirements".

[675] Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, Prüfschema für ISO 27001 – Audits, Stand 1.02.2006, abrufbar im Internet unter abrufbar unter: http://www.bsi.bund.de/gshb/zert/Pruefschema06.pdf (zuletzt abgerufen am 20.02.2006).

[676] *Capellaro/Füser,* Die Bank 2005, 68 (70 f.); *Roth/Schneider,* ITRB 2005, 19.

[677] ISO 27001:2005, 4.1.

[678] ISO 27001:2005, 1.1.

Riskmanagementsystems verwendet.[679] Anders formuliert, bedarf das IT-Managementsystem einer initialen Planung und Implementierung und einer anschließenden ständigen Überwachung und Verbesserung.

351 Ein Unternehmen, das ISO 27001 konform arbeitet, muss danach zunächst Zweck und Reichweite des IT-Riskmanagementsystems festlegen, indem wichtige Informationen über das Unternehmen, die wichtigen Einheiten und Technologien zusammengetragen werden. Anschließend müssen diese in einem Rahmenwerk, das auch wirtschaftliche, rechtliche und technische Erfordernisse einbezieht und in das generelle Riskmanagement des Unternehmen eingebettet ist, einbezogen werden, wobei auch Handlungen und Notwendigkeiten mit Hinblick auf IT-Sicherheit benannt werden müssen. Anschließend wird die Methode der Risikobestimmung gewählt und die vorhandenen Risiken sind zu identifizieren, analysieren, evaluieren. Für diese Risiken sind anschließend geeignete Gegenmaßnahmen bzw. Vermeidungsstrategien zu definieren und zu bewerten. Dazu gehört z.B. auch die Versicherung gegen den Eintritt solcher Risiken.[680]

352 Schließlich muss ein Risikobehandlungsplan erstellt werden, der für alle Risiken die im Eintrittsfall zu ergreifenden Maßnahmen enthält. Dieser soll durchgesetzt werden, indem zusätzlich Kontrolleinrichtungen geschaffen werden. Dazu gehören auch Schulungen und Informationsprogramme. Die Überwachung und Überprüfung soll des Weiteren schnell Fehler im IT-Riskmanagement entdecken bzw. ineffektive Maßnahmen identifizieren und die entsprechenden Schlussfolgerungen ziehen und einarbeiten.

353 Zur ISO 27001 gehört auch eine entsprechende Verantwortungsverteilung. So sollen Nachweise für die Einbindung bzw. Verantwortlichkeit des Managements bezüglich des IT-Riskmanagements, z.B. einer entsprechenden Rollenverteilung, erbracht werden. Die verantwortlichen Mitarbeiter sind entsprechend zu informieren und bei Bedarf zu schulen. Zudem müssen notwendige Ressourcen für die verschiedenen Aufgaben des IT-Riskmanagements benannt und zur Verfügung gestellt werden.

354 Zu festgelegten Daten sollte schließlich eine interne unabhängige Überprüfung stattfinden. Zusätzlich soll eine regelmäßige Prüfung durch das Management stattfinden.

355 Es zeigt sich, dass Riskmanagement durch die ISO 27001 spezialisiert auf IT-Risiken übertragen wird. Im Anhang werden spezifische Aufgaben bezüglich wichtiger Risiken

[679] ISO 27001:2005, 0.2.
[680] ISO 27001:2005, 4.2.1.f)4).

für verschiedene Einsatzbereiche, z.B. den Online-Handel oder Telearbeit, im IT-Sektor benannt. Dabei stellen die Anforderungen der ISO 27001 nur einen Teil des Gesamtriskmanagements dar und sind in dieses einzubetten.

356 Die möglichen Rechtsfolgen liegen auf der Hand: Ähnlich wie im Deliktsrecht (oder auch in anderen Rechtsbereichen wie dem Vertragsrecht) sind diese Standards geeignet, als allgemein anerkannte Regeln der Technik die nötige Sorgfalt im Sinne der objektiven Pflicht zu konkretisieren – wenn auch nicht abschließend, sondern nur in dem Sinne, daß vermutet wird, daß sie die vom Gesetz gestellten Anforderungen erfüllen.[681]

(2) Mittelbare Wirkung von Basel II (Kreditwesenaufsichtsrecht)

(a) Hintergrund

357 Diese im Wesentlichen aus dem Gesellschaftsrecht stammenden Pflichten werden in absehbarer Zeit nochmals mittelbar durch das Kreditaufsichtsrecht verschärft – was breitflächige Auswirkungen auch auf kleinere oder mittlere Unternehmen gleich welcher Rechtsform haben wird, da die Fremdkapitalquote in Deutschland nach wie vor beachtlich ist. Denn aufgrund der sog. Basel II-Anforderungen müssen die Banken in qualifizierter Weise das Risiko jeder Gesellschaft per Rating vor jeglicher Fremdmittelvergabe einschätzen.[682] Mit der Neufassung der Richtlinie 2000/12/EG[683] und der Richtlinie 93/6/EWG[684] wird die auf der Grundlage der Baseler Eigenkapitalvereinbarung von 1988 (sog. Basel I) überarbeitete Baseler Eigenkapitalvereinbarung von 2004 (Basel II)[685] auf europäischer Ebene umgesetzt.[686] Im deutschen Recht erfolgte die Umset-

[681] Ausführlich. dazu oben Rn. 174 ff.

[682] *Kümpel*, Bank- und Kapitalmarktrecht, Rn. 19.91; *Fritz-Aßmus/Tuchtfeldt*, ORDO 54 (2003), 267 (270 f.); *Polke*, Die darlehensvertragliche Umsetzung der Eigenkapitalgrundsätze nach Basel II, 73 ff.

[683] Richtlinie 2000/12/EG des Europäischen Parlaments vom 20.03.2000 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute – sog. Bankenrichtlinie, ABl. EG L 126, 1 ff.

[684] Richtlinie 93/6/EWG des Rates vom 15.03.1993 über die angemessene Eigenkapitalausstattung von Wertpapierfirmen und Kreditinstituten - sog. Kapitaladäquanzrichtlinie, ABl. EG L 141, 1 ff.

[685] Basel Committee on Banking Supervision (2004), International Convergence of Capital Measurement and Capital Standards, A Revised Framework, Basel, Juni 2004. Die Baseler Dokumente können von der Website der Bank für Internationalen Zahlungsausgleich heruntergeladen werden unter abrufbar unter: http://www.bis.org.

[686] BegrRegE zum Entwurf eines Gesetzes zur Umsetzung der neu gefassten Bankenrichtlinie und der neu gefassten Kapitaladäquanzrichtlinie vom 15.02.2006, 1; abrufbar unter: http://www.bundesfinanzministerium.de/lang_de/DE/Geld__und__Kredit/Aktuelle__Gesetze/Entwurf__eines__Gesetzes__zur__Umsetzung__Bankenrichtlinie__anl,templateId=raw,property=publicationFile.pdf (zuletzt abgerufen am 20.02.2006). Zu Basel II s. zuletzt *Blöcker/Spielberg,* Die Bank 2005, 56 ff.; *Gaumert/Zattler,* Die Bank 2005, 55 ff.; *Hofmann/Lesko/Vorgrimler,* Die Bank 2005, 48 ff.; *Schöning/Weber,* Die Bank 2005, 47 ff.; *Schubert/Grießmann,* VW 2004, 1399 ff.; *Schulte-Mattler/von Kenne,* Die Bank 2004, 37 ff.; *Capellaro/Füser,* Die Bank 2005, 68 ff.; ausführlich Boos/Fischer/Schulte-Mattler-*Schulte-Mattler,* Basel II Rn. 1 ff.

zung im Kreditwesengesetz,[687] den „Mindestanforderungen an das Risikomanagement (MaRisk) und der Solvabilitätsverordnung (SolvV)[688]. Ziel der Regelungen ist es, die Eigenkapitalanforderungen stärker als bisher vom eingegangenen Risiko abhängig zu machen sowie die allgemeinen und besonderen Entwicklungen an den Finanzmärkten sowie im Riskmanagement der Institute zu berücksichtigen.[689]

(b) Pflichten und Addressat

358 Die genannten Ziele sollen durch einen auf drei Säulen beruhenden Regelungsansatz erreicht werden, wobei die Säule I die Mindestkapitalanforderungen regelt und die bankenaufsichtliche Risikomessung stärker an die Risikosteuerungsmethoden der Banken annähert, während Säule II sich mit der qualitativen Bankenaufsicht und Säule III mit den Offenlegungspflichten befasst.[690] Durch Basel II bzw. die entsprechenden Gesetzesvorschriften zur Umsetzung werden die kreditgewährenden Finanzinstitute verpflichtet, eine individuelle Einschätzung der Bonität bei Unternehmen vor jeder Kreditentscheidung eines Kreditgebers vorzunehmen, welche auf Basis der internen Rating-Systeme der Institute oder durch externes Rating erfolgt.[691] Hierbei sind auch die operationellen Risiken des kreditnehmenden Unternehmens zu beachten, wozu auch die Risiken gehören, die sich aus dem Einsatz von Informationstechnologie in den Unternehmensprozessen ergeben.[692]

(c) Rechtsfolgen

359 Diese Pflichten richten sich allein an die Finanzinstitute, so dass Basel II und die entsprechende Gesetzgebung zur Umsetzung weder eine Pflicht noch eine Obliegenheit für die kreditnehmenden Unternehmen begründen und damit auch keine Rechtsfolgen in Form von Sanktionen oder in Form eines Rechtsverlustes haben können. Allerdings entsteht eine mittelbare Wirkung, da Unternehmen bei fehlendem oder nicht ausreichendem Riskmanagement bei der internen oder externen Risikoeinschätzung der Finanzin-

---

[687] BGBl. I vom 5.01.2007, S. 10, 31, inkraftgetreten am 20.01.2007.

[688] BGBl. I vom 14.12.2006, S. 2926, inkraftgetreten am 1.01.2007.

[689] BegrRegE zum Entwurf eines Gesetzes zur Umsetzung der neu gefassten Bankenrichtlinie und der neu gefassten Kapitaladäquanzrichtlinie vom 15.02.2006, 1 (2); s. auch *Schulte-Mattler/von Kenne,* Die Bank 2004, 37 f.; Boos/Fischer/Schulte-Mattler/*Schulte-Mattler,* Basel II Rn. 11.

[690] Hierzu ausführlich *Schubert/Grießmann,* VW 2004, 1399 ff.; *Fischer,* VW 2002, 237 ff.; *Schulte-Mattler/von Kenne,* Die Bank 2004, 37 ff.; Boos/Fischer/Schulte-Mattler/*Schulte-Mattler,* Basel II Rn. 10 ff.

[691] *Müller-Reichart/Dura/Fischer/Nosty,* VW 2002, 625; *Capellaro/Füser,* Die Bank 2005, 68 (68 f.).

[692] Vgl. BegrRegE zum Entwurf eines Gesetzes zur Umsetzung der neu gefassten Bankenrichtlinie und der neu gefassten Kapitaladäquanzrichtlinie vom 15.02.2006, 1 (2); s. auch *Capellaro/Füser,* Die Bank 2005, 68 (68 f.); *Schultze-Melling*, CR 2005, 73 (78); *Roth/Schneider,* ITRB 2005, 19 f.; Boos/Fischer/Schulte-Mattler/*Schulte-Mattler,* Basel II Rn. 134.

stitute schlechter abschneiden und jene zum Ausgleich der höheren Eigenmittelanforderungen schlechtere Kreditkonditionen bieten werden.

(d) Anhaltspunkte für IT-Konkretisierung

360 Für Zwecke des Ratings eines Unternehmens arbeiten die Banken heute mit branchenspezifischen Risikoprofilen, wobei im IT-Bereich wie in anderen Risikobereichen eine branchentypische Risikodisposition unterstellt wird. Unter dem Gesichtspunkt der IT-Sicherheit kann ein Unternehmen, für das im Ausgangspunkt eine branchentypische Risikodisposition angenommen wird, ein günstigeres Rating, also eine positivere Risikoeinschätzung bezüglich des Unternehmens als hinsichtlich der Branche ingesamt, und damit verbunden günstigere Kreditkonditionen nur erreichen, wenn es gegenüber der Bank nachweist, dass es effektivere IT-Sicherheitsmaßnahmen als der Durchschnitt besitzt.[693] Je mehr das Unternehmen bei seinen Geschäftsabläufen auf eine funktionierende IT angewiesen ist, desto größeres Gewicht haben IT-Sicherheitsrisiken demzufolge bei der Risikovorsorge des Unternehmens. Gefordert ist ein IT-Riskmanagement, welches sich mit allen Aspekten der IT-Sicherheit für das jeweilige Unternehmen befasst; es müssen wichtige IT-Systeme vorhanden und verfügbar sein sowie Angriffe auf diese Systeme wirksam abgewehrt werden können und Notfallpläne vorliegen. Missbrauch der IT durch externe oder interne Mitarbeiter, insbesondere durch Weitergabe von vertraulichen Firmendaten an externe Stellen, Geschäftsunterbrechungen durch IT-Systemausfälle oder Schadensersatzforderungen auf Grund unsicherer IT werden sich daher negativ auf das Risikoprofil des Unternehmens auswirken.[694] Die Relevanz der IT-Risiken als Teil des Geschäftsrisikos sind z.T. aber auch branchenspezifisch; so wird ein Unternehmen, dessen Geschäft ausschließlich auf Online-Handel basiert, ein sehr hohes IT-Risiko besitzen, während bei Finanzdienstleistern die finanziellen Risiken z.B. in Form von Wertberichtigungen überwiegen.[695] Insgesamt werden von der Bonitätsprüfung im Unternehmenskreditgeschäft bezogen auf die Anfälligkeit der IT-Systeme gerade mittelständische Unternehmen betroffen sein.[696]

361 Damit besteht aber indirekt ein breitflächiger **Zwang für diese Unternehmen, ein adäquates Riskmanagement** vorzuweisen, das die für das Controlling essentiellen

---

[693] *Capellaro/Füser,* Die Bank 2005, 68 f.

[694] Beispiele nach *Capellaro/Füser,* Die Bank 2005, 68.

[695] *Capellaro/Füser,* Die Bank 2005, 68 f.

[696] Für die Auswirkungen der Kreditkosten auf den Mittelstand s. *Paul/Stein/Kaltofen,* Die Bank 2004, 342 f.; *Schulte-Mattler/Manns,* Die Bank 2004, 376 ff. mwN.

Elemente des EDV-Einsatzes einschließlich des Rechtemanagements umfasst. Eine Darlehensvergabe ohne jegliche Prüfung der Risikovorsorge, deren Bestandteil auch die Absicherung der IT-Risiken einschließlich der Rechtssituation ist, wird daher nicht mehr möglich sein. Denn als Folge der Relevanz der dargestellten Faktoren kann ein darauf vorbereitetes Unternehmen mit gut dokumentiertem IT-Riskmanagement bei der Kreditvergabe einer Bank für günstigere Konditionen sorgen und umgekehrt können die Kreditbedingungen für einen Kreditnehmer eher schlechter sein, wenn dieser eine anfällige IT-Infrastruktur besitzt. Eine Investition in ein IT-lastiges Unternehmen wird für die Bank dann rentabel sein, wenn das Unternehmen neben den betriebswirtschaftlichen Voraussetzungen insbesondere die IT-relevanten Kriterien erfüllt. Von Vorteil ist es insofern, wenn die Prozesse des Kerngeschäfts durch die eingesetzten Applikationen optimal unterstützt werden. Diese sollten den entsprechenden branchenüblichen Standards entsprechen und auf dem Stand der Technik sein; die Prozesse im IT-Betrieb müssen wirksam und kosteneffizient und die wesentlichen IT-Risiken sollten identifiziert sein sowie geeignete Maßnahmen zu deren Reduktion umgesetzt werden. Zu einem effektiven Risikomanagement gehören auch Schulungen der Mitarbeiter und Aufklärungsmaßnahmen sowie eine im Unternehmen kommunizierte, schriftlich fixierte Sicherheits-Policy.[697] Die Maßnahmen müssen in regelmäßigen Abständen wiederholt werden, um Effektivität zu garantieren. Außerdem muss die IT-Infrastruktur insgesamt robust und geeignet ausgelegt sein, um das aktuelle Transaktionsvolumen zu bewältigen. Hilfreich ist eine flexible Konzeption, so dass durch akzeptable Erweiterungsmaßnahmen auch das zukünftig zu erwartende Transaktionsvolumen bewältigt werden kann. Zudem müssen die Verantwortlichkeiten in der IT klar geregelt sein, der Mitarbeitereinsatz ist insofern an den Erfordernissen auszurichten.[698]

362 In das Rating können durchaus auch andere IT-Zertifikate einbezogen werden.[699] So kann das Zertifikat als Nachweis dienen, dass ein IT-Sicherheitsmanagementsystem vorhanden ist und ein BS 7799-Zertifikat bzw. ein ISO 27001 Einfluss auch auf die Bewertung nach Basel II haben. Allerdings ist im Rahmen eines Ratings darauf zu achten, ob der für die Zertifizierung gewählte Gültigkeitsbereich sich auch mit den Unternehmensbereichen deckt, die wesentlich die Werthaftigkeit oder die Wertschöpfung des

[697] *Haar/Schädler*, Verbaselt, abrufbar unter: http://www.heise.de/ix/artikel/2004/12/099/ (zuletzt abgerufen am 11.5.2006).
[698] Beispiele nach *Capellaro/Füser,* Die Bank 2005, 68 (69 f.).
[699] *Capellaro/Füser,* Die Bank 2005, 68 (69 f.).

Unternehmens widerspiegeln.700 Die für das BSI 7799-2 bzw. ISO 27001 erstellte Risikoanalyse kann hierfür nur bedingt herangezogen werden, da sich diese definitionsgemäß auf den Gültigkeitsbereich der entsprechenden Zertifizierung und nicht auf das Gesamtunternehmen bezieht.701 Eine direkte Übertragbarkeit und damit ein unmittelbarer Nachweis im Sinne von Basel II lässt sich hierin folglich nicht sehen.

363 Beispiel: Hat ein Unternehmen keinerlei Kontrolle im Bereich des Einkaufs von Software bzw. IT-Produkten, und sind diese Produkte kritisch für die Erbringung der Leistungen des Unternehmens, können sich existentielle Risiken für das Unternehmen im Falle des Versagens der Software ergeben. Ein Kreditunternehmen wäre daher u.U. schon von Rechts wegen gehalten, zusätzliche Sicherheiten oder einen höheren Kreditzins zu verlangen. Ein schlechtes IT-Riskmanagement kann sich daher auf die Finanzierungskonditionen eines Unternehmens unmittelbar auswirken.

364 Jedenfalls bezüglich des von dem Zertifikat erfassten Risikobereichs sollte sich das Finanzinstitut aber auf die Vorlage eines Zertifikats berufen können, um den Nachweis zu erbringen, dass im Bereich des IT-Managements des Unternehmens eine ausreichende Risikoeinschätzung stattgefunden hat. Für die Annahme, dass ein Zertifikat eine eigene Risikoeinschätzung durch das Finanzinsitut ersetzt, spricht, dass die Erteilung der genannten Zertifikate an hohe Anforderungen geknüpft ist und jene Anforderungen umfassend sind, so dass kein Raum für zusätzliche Anforderungen seitens der Finanzinstitute besteht. Zwar ist zu bedenken, dass das Verfahren und die Entscheidung zur Zuteilung der Zertifikate fehlerbehaftet sein kann, doch ist es nicht praktikabel und nicht zu erwarten, dass das Finanzinstitut eine Überprüfung des Verfahrens vornimmt. Außerdem würde der Effizienzgewinn durch die Standardisierung stark gemindert, wenn sie keinen Nutzen im Rahmen von Ratingverfahren bringen könnte. Dies gilt vor allem für KMUs, für die Basel II eine besonders hohe Hürde bei der Kreditfinanzierung darstellt. Eine klare Rechtsgrundlage zu diesen Prüfungsverfahren und der Rolle von Zertifikaten ist allerdings bislang im Rahmen des Basle II-Verfahrens nicht ersichtlich.

(3) Anforderungen durch den Sarbanes-Oxley-Act (SOX)

(a) Hintergrund

700 *Capellaro/Füser,* Die Bank 2005, 68 (70).
701 *Capellaro/Füser,* Die Bank 2005, 68 (70).

365 Mit dem US- amerikanischen Sarbanes-Oxley-Act vom 30.07.2002, 15 U.S.C. 7201,[702] werden die Anforderungen an bestimmte Unternehmen bezüglich der Einrichtung eines IT-Riskmanagements und dessen rechtliche Implikationen zukünftig noch erheblich komplexer. Das Gesetz bezweckt nach der Gesetzesbegründung den Schutz von Anlegern durch genauere und verlässlichere wertpapierrechtliche Publizitätspflichten der börsennotierten Unternehmen.[703] Zu diesem Zweck werden die Verantwortlichkeiten der Unternehmensführung und der Wirtschaftsprüfer geregelt und strenge Maßstäbe für die Zusammenarbeit aufgestellt. Das Artikelgesetz, das vor allem Änderungen im Securities und Exchange Act of 1934 („Exchange Act") vorsieht, ist insofern als Reaktion auf die zahlreichen und schwerwiegenden Bilanzskandale mit sich anschließenden Unternehmenszusammenbrüchen, wie z. B. von Enron und WorldCom, zu werten.[704] Es dient nicht zuletzt auch der Wiederherstellung des Vertrauens der Anleger in die Richtigkeit der veröffentlichten Finanzdaten von Unternehmen, die den amerikanischen Rechtsvorschriften hinsichtlich periodischer Berichtspflichten und einzureichender Adhoc Mitteilungen unterliegen.[705] Nach § 13(a) bzw. 15(d) Exchange Act sind dies solche Unternehmen, deren Wertpapiere an einer US-amerikanischen Börse notiert und die insofern gem. § 12 Exchange Act bei der Wertpapieraufsichtsbehörde SEC (Securities and Exchange Commission) registriert sind, oder die Wertpapiere öffentlich in den USA angeboten haben, ohne diese an einer US-amerikanischen Börse notiert zu haben. Die Regelungen betreffen insofern auch eine Vielzahl deutscher Unternehmen, die in den USA Wertpapiere öffentlich anbieten. Damit kommen auch auf viele deutsche Unternehmen spezielle Handlungs- und Sorgfaltspflichten zu, die insbesondere auch im Bereich der IT-Sicherheit berücksichtigt werden müssen.

(b) Pflichten und Adressat

[702] abrufbar unter: http://www.law.uc.edu/CCL/SOact/soact.pdf.

[703] Dem Gesetzestext geht folgender Einleitungssatz voraus: „An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes".

[704] Zum Fall Enron vgl. etwa United Bancruptcy Court Southern District of New York, In re: Enron Corp. et al., First Interim Report of Neal Batson, Court-Appointed Examiner, Sept. 21, 2002; Eine umfassende Dokumentenzusammenstellung zum Fall Enron ist auch abrufbar unter http://news.findlaw.com/legalnews/lit/enron/; zum Fall WorldCom vgl. abrufbar unter: http://lawcrawler.findlaw.com/scripts/lc.pl?entry=WorldCom&sites=news; krit. über den Erfolg des SOX Act *Schwarz/Holland*, ZIP 2002, 1661 ff.; s. auch *Schiessl*, AG 2002, 593 (593 ff.).

[705] *Gruson/Kubicek*, Der Sarbanes-Oxley Act, 1 f., abrufbar unter: http://www.jura.unifrankfurt.de/ifawz1/baums/Bilder_und_Daten/Arbeitspapiere/paper113.pdf; auch AG 2003, 337 (338); Arbeitskreis „Externe und Interne Überwachung der Unternehmen" der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2399); *Schultze-Melling*, CR 2005, 73 (79).

366 Um sicherzustellen, dass Unternehmen richtige und verlässliche Angaben machen, sieht der Sarbanes-Oxley Act in Zusammenhang mit den Ausführungsregeln der SEC[706] eine Vielzahl von Maßnahmen vor, die sich in erster Linie an Mitglieder der Leitungsorgane der registrierten Unternehmen und deren Abschlussprüfer richten. In Bezug auf das interne Kontrollsystem werden zwei Ziele verfolgt[707], deren Umsetzung konkrete Auswirkungen auf Vorstand, interne Revision, Aufsichtsrat und Abschlussprüfung hat[708].

367 Zum einen müssen die CEO und CFO eines Unternehmens nach Section 302 (Disclosure Controls and Procedures) durch die Einrichtung eines internen Kontrollsystems sicherstellen, dass alle relevanten Informationen korrekt erfasst, verarbeitet und fristgerecht veröffentlicht werden und in einer eidesstattlichen Erklärung die korrekte und vollständige Darstellung der finanziellen Situation testieren.[709] Auf diese Weise wird die Verantwortlichkeit des Vorstands für Unternehmensberichte verstärkt und die Einrichtung von Offenlegungskontrollen und Offenlegungsverfahren verlangt.[710]

368 Zum anderen verpflichtet Section 404 (Internal Control over Financial Reporting) das Management, ein internes Kontrollsystem zur Sicherstellung einer effektiven Finanzberichterstattung zu etablieren. DEO und DFO müssen einen Prozess einrichten, der die Ordnungsmäßigkeit der Finanzberichterstattung und somit eine den Rechnungslegungsvorschriften entsprechende Erstellung von Abschlüssen sicherstellt[711], wobei insbesondere die Korrektheit, Nachvollziehbarkeit und Sicherheit der Prozesse geregelt wird.[712] Das so implementierte Überwachungssystem soll dafür sorgen, dass den Mitgliedern der Unternehmensorgane alle relevanten Informationen bezüglich der für den Unternehmensbericht bedeutsamen Teilprozesse und damit auch und gerade hinsichtlich des

[706] Z.B. Auditing standards Nos. 1-3 des Public Company Accounting Oversight Board (PCAOB).

[707] PricewaterhouseCoopers, Sarbanes-Oxley Act – Professionelles Management interner Kontrollen, 2004, passim; *Bülow*, Datenschutz-Berater 10/2005, 13; vgl. auch *Hütten/Stromann*, BB 2003, 2223 (2223 ff.).

[708] Hierzu *Luttermann*, BB 2003, 745 (745 f.); *Gruson/Kubicek*, AG 2003, 337 (337 ff.) und AG 2003, 393 (393 ff.); Arbeitskreis „Externe und Interne Überwachung der Unternehmen" der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2399 ff.), zu den Auswirkungen auf den Berufsstand der Wirtschaftsprüfer ausführlich *Hilber/Hartung*, BB 2003, 1054 (1054 ff.); *Lenz*, BB 2002, 2270 (2270 ff.); *Keller/Schlüter*, BB 2003, 2166 (2166 ff.).

[709] Bzgl. der inhaltlichen Anforderungen der Bestätigungen eingehend *Gruson/Kubicek*, Der Sarbanes-Oxley Act, 46 ff., abrufbar unter: http://www.jura.uni-frankfurt.de/ifawz1/baums/Bilder_und_Daten/Arbeitspapiere/paper113.pdf.

[710] Arbeitskreis „Externe und Interne Überwachung der Unternehmen" der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2400).

[711] *Büssow/Taetzner*, BB 2005, 2437 (3438 f.).

[712] Ausführlich. *Hütten/Stromann*, BB 2003, 2223 (2224 f.); *Taetzner*, BB 2005, 2437 (2437 ff.); *Gruson/Kubicek*, Der Sarbanes-Oxley Act, 37 ff., abrufbar unter: http://www.jura.unifrankfurt.de/ifawz1/baums/Bilder_und_Daten/Arbeitspapiere/paper113.pdf.

verwendeten IT-Systems jederzeit zur Verfügung stehen.[713] Die Verantwortlichkeit des Geschäftsführungsorgans für die Wirksamkeit interner Überwachungsmaßnahmen ist in einem jährlichen Bericht gesondert festzustellen und das Verfahren sowie jede Veränderung der internen Überwachung ist vom Management zu bewerten. Die Mitglieder des Leitungsorgans stehen durch Gewinnabschöpfung persönlich für die Korrektheit von Finanzberichtsabschlüssen ein, indem bei fehlerhaftem Abschluss erhaltene Boni zurückgezahlt und Gewinne aus dem Verkauf von erlangten Aktienoptionen herausgegeben werden müssen.

369 Nach mehrmonatigen Diskussionen hat die SEC nunmehr eine Fristverlängerung für ausländische Unternehmen hinsichtlich der Umsetzung der Regelungen in Section 404 SOX verfügt, wonach die Anforderungen erst für die Geschäftsjahre zu erfüllen sind, die nach dem 15.07.2006 enden.[714] Insofern haben auch die betroffenen deutschen Unternehmen eine letzte Gnadenfrist erhalten, das interne Kontrollsystem den Anforderungen des Sarbanes-Oxley Act anzupassen und ihr IT-Sicherheits-Management entsprechend einzurichten.

370 Schließlich verdient auch die Einrichtung eines **Audit Committees** als Überwachungsorgan gem. Section 301 SOX besondere Beachtung im Zusammenhang mit den vom Sarbanes-Oxley Act geforderten Überwachungsmaßnahmen.[715] Ihm kommt die Aufgabe zu, das Rechnungs- und das Finanzberichtswesen zu überwachen und Unternehmensabschlüsse zu überprüfen.[716] Das Audit Committee ist zudem für die Einrichtung eines **Whistleblowing-Verfahrens** verantwortlich, dass für Emittenten durch Section 301 SOX verbindlich vorgeschrieben ist, um die Gefahr deliktischer Handlungen, die mitunter auch die Existenz der Gesellschaft bedrohen können, zu verringern.[717] Kennzeichnend für den Begriff des Whistleblowings sind drei Merkmale: Ein Organisationsinsider erkennt illegale, illegitime oder unmoralische Praktiken von gleichfalls der

[713] *Pellens*, DBW 2003, 473; *Bülow*, Datenschutz-Berater 10/2005, 13; ausführlich zu Sec. 404 SOX auch *Büssow/Taetzner*, BB 2005, 2437 ff.

[714] SEC Press Release 2005-25 vom 2. 3. 2005; Die Fristverlängerung wird angeordnet durch die SEC Final Rule, Release No. 33-8545, abrufbar unter http www.sec.gov.

[715] Arbeitskreis „Externe und Interne Überwachung der Unternehmen“ der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2402 f.); *Gruson/Kubicek*, Der Sarbanes-Oxley Act, 6 ff., abrufbar unter http: abrufbar unter: http://www.jura.uni-frankfurt.de/ifawz1/baums/Bilder_und_Daten/Arbeitspapiere/paper113.pdf; auch AG 2003, 337 (340 ff.); *Schiessl*, AG 2002, 593 (600); *Hütten/Stromann*, BB 2003, 2223 (2223 f.); *Schwalbach*, AG 2004, 186 (188); zur Stellung des Audit Commitee Financial Experts eingehend *Luttermann*, BB 2003, 745 ff.

[716] Festgelegt in Sec. 3 (a)(58)(A) Exchange Act, eingefügt durch Sec. 205 SOX.

[717] Ausführlich. zum Whistleblowing-Verfahren *Berndt/Hoppler*, BB 2005, 2623; s. auch *Hütten/Stromann*, BB 2003, 2223 (2224).

Organisation angehörenden Personen und meldet diese einer speziellen geeigneten Stelle.[718] Das Merkmal der illegalen Praktiken wird dabei sehr weit verstanden und umfasst insbesondere auch Nachlässigkeiten und Organisationsmängel von Verantwortlichen.[719] Dementsprechend stellt das Whistleblowing-Verfahren auch und gerade hinsichtlich IT-Anwendungen besondere Anforderungen im Rahmen eines Sicherheits-Managements. Die Unternehmen trifft konkret die Pflicht zur Einrichtung interner oder externer Whistleblowing-Stellen, die prinzipiell dazu in der Lage sein müssen, den Hinweisen nachzugehen und ein festgestelltes haftungsrelevantes Verhalten zu unterbinden. Da sich zunächst nicht aufgedeckte deliktische Handlungen von Tochtergesellschaften auch als Gefährdung der Unternehmensfortführung der Muttergesellschaft auswirken können, empfiehlt sich die Einrichtung eines einheitlich geregelten Whistleblowing-Verfahrens für alle Konzernteile, um sich nicht straf- oder zivilrechtlichen Sanktionen ausgesetzt zu sehen.[720]

371 Im Gegensatz zu den besonderen Anforderungen an die Ausgestaltung des internen Überwachungssystems ist schließlich festzuhalten, dass die **interne Revision** nicht explizit im Sarbanes-Oxley Act erwähnt ist. Dennoch ergeben sich Konsequenzen für die Tätigkeit der internen Revision aus den geänderten Regelungen für Vorstand, Aufsichtsrat und Abschlussprüfer.[721] Da die Unternehmensleitung stärker für die Vollständigkeit und Richtigkeit der Finanzberichterstattung einstehen muss, verlagert sich auch für die interne Revision der Schwerpunkt der Prüfung auf die Aspekte der Funktionsfähigkeit und Ordnungsmäßigkeit der Finanzberichterstattung und des internen Kontrollsystems.[722] Um Kontrollschwächen aufzudecken, muss die interne Revision naturgemäß eigene Funktionstests durchführen, von denen auch die IT-Prozesse erfasst sind.

(c) Rechtsfolgen

372 Der SOA schreibt neben zivil- und strafrechtlichen Sanktionen, die das Gesetz selbst anordnet und im Falle von vorsätzlicher Abgabe einer falschen Erklärung Geldbußen bis zu einer Höhe von 5 Mio. Us-Dollar sowie Freiheitsstrafen von bis zu 20 Jahren

---

[718] *Near/Miceli*, Journal of Business Ethics 1985, 4; *Keenan*, Employee Responsibilities and Rights Journal 2000, 200; *Berndt/Hoppler*, BB 2005, 2623 (2624 f.) mwN.

[719] *Grant*, Journal of Business Ethics 2002, 391 f.; *Johnson*, Whistleblowing – When it works and why, 31 ff.; *Leisinger*, Whistleblowing und Coporate Reputation Management, 259 ff.

[720] *Berndt/Hoppler*, BB 2005, 2623 (2625).

[721] Eingehend Arbeitskreis „Externe und Interne Überwachung der Unternehmen“ der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2399 ff.) mwN.

[722] Arbeitskreis „Externe und Interne Überwachung der Unternehmen“ der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2401).

vorsieht, in Section 3 (b)(1) SOX vor, dass jeder Verstoß gegen den Sarbanes-Oxley Act auch als Verstoß gegen den Securities Act 1934 (15 U.S.C. § 78 (a) ff.) zu werten ist; es drohen mitunter zusätzlich durch die SEC erlassene Sanktionen.

(d) Anhaltspunkte für IT-Konkretisierung

373 Im Hinblick auf regulatorische Anforderungen im IT-Bereich sind die Regelungen über strafrechtliche und zivilrechtliche Sanktionen für Sicherheitsverstöße, die Unabhängigkeit der internen und externen Unternehmensprüfungen[723] und die erhöhten Publizitätspflichten bezüglich zu veröffentlichender Unternehmensinformationen von Bedeutung.[724] Da es nur noch selten Geschäftvorgänge gibt, die ohne die Verwendung von IT-Applikationen stattfinden, kommt insofern unter Verlässlichkeitsgesichtspunkten dem IT-Riskmanagement erhöhte Bedeutung zu.

374 So verpflichtet Section 302 SOX die Unternehmensleitung im Hinblick auf den Einsatz von IT-Systemen dazu, die Sicherheit und die Verfügbarkeit der im Zusammenhang mit der Rechnungslegung verwendeten Technik nachzuweisen und zu kontrollieren.[725] . Auch im Hinblick auf Section 404 verschärfen die Anforderungen an die Sicherheit der Prozesse und der Wirksamkeit interner Überwachungsmaßnahmen nicht zuletzt die Anforderungen, die an das IT-Riskmanagement im Unternehmen zu stellen sind. Dabei sollen so genannte „Control Frameworks“ wie die von COSO oder COBIT dazu dienen, dass Gefahren für die Rechnungslegung eliminiert oder wenigstens gemindert werden[726].

b) Allgemeine zivilrechtliche Pflichten

375 Wechselt man die Perspektive und betrachtet die Pflichtenlage der kommerziellen IT-Nutzer im Hinblick auf ihre Sicherungspflichten gegenüber Dritten, ergeben sich erhebliche Unterschiede in den geschuldeten Verkehrspflichten:

376 Ausgangspunkt ist zunächst wiederum, dass derjenige, der eine Gefahrenquelle schafft oder beherrscht, nach § 823 Abs. 1 BGB grundsätzlich verpflichtet ist, die notwendigen und zumutbaren Vorkehrungen zu treffen, um eine Schädigung anderer zu vermei-

---

[723] Ausführlich: Arbeitskreis „Externe und Interne Überwachung der Unternehmen“ der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2399 ff.) mwN.

[724] *Bülow*, Datenschutz-Berater 10/2005, 13 (13); vgl. auch *Gruson/Kubicek*, AG 2003, 337 (337 ff.) und AG 2003, 393 (393 ff.).

[725] *Knolmayer/Wermelinger*, Der Sarbanes-Oxley Act und seine Auswirkungen auf die Gestaltung von Informationssystemen, abrufbar unter: http://www.ie.iwi.unibe.ch/publikationen/berichte/resource/WP-179.pdf, 1.

[726] *Knolmeyer/Wermelinger*, Der Sarbanes-Oxley Act und seine Auswirkungen auf die Gestaltung von Informationssystemen, abrufbar unter: http://www.ie.iwi.unibe.ch/publikationen/berichte/resource/WP-179.pdf, 7 f.

den,[727] wobei – wie bereits dargelegt - zur genaueren Konkretisierung des Inhalts und Umfangs der Verkehrssicherungspflicht in erster Linie auf die berechtigten Sicherheitserwartungen der betroffenen Verkehrskreise abzustellen ist,[728] ferner auf die Möglichkeit und Zumutbarkeit der Gefahrenvermeidung einerseits auf der Versenderseite, andererseits auf der Empfängerseite.[729]

377 Keine Unterschiede ergeben sich hinsichtlich der potentiell bedrohten Rechtsgüter Dritter, von geschützten Daten, Urheberrechten bis hin zum Recht am eingerichteten und ausgeübten Gewerbebetrieb. Auch lässt sich der Angriff des IT-Nutzers auf den Geschädigten jedenfalls mittelbar auf das vorsätzliche Handeln des ursprünglichen Angreifers, z.B. des Virenerstellers bzw. –verbreiters, zurückführen, so dass die Pflicht des Nutzers bestehen bleibt.[730] Die Unterschiede liegen vielmehr in den zumutbaren Verkehrssicherungspflichten für kommerzielle IT-Nutzer:

(1) Herleitung von Pflichten im IT-Bereich

378 Änderungen gegenüber den privaten IT-Nutzern ergeben sich vor allem hinsichtlich des zumutbaren für den Schutz einzusetzenden Aufwandes, den Sicherheitserwartungen des betroffenen Kreise gegenüber kommerziellen IT-Nutzern sowie der Bekanntheit der Problemlage und möglichen Gegenmaßnahmen. Im Gegensatz zu privaten Nutzern, für die der III. Zivilsenat des BGH den Einwand aus § 254 BGB nur bei weitgehender Bekanntheit eines Problems zulässt, kann eine solche Privilegierung für den kommerziellen IT-Nutzer nicht angenommen werden. Zwar ist ihm nicht wie ein IT-Hersteller zuzumuten, jedes Problem umgehend zu erkennen und sich ständig durch Fachzeitschriften oder Expertenberatung zu informieren, es ist jedoch zu verlangen, dass er regelmäßig auch Probleme beim Einsatz von Computern beachtet und, sofern er von Gefahren erfährt, diesbezüglich über die üblichen Informationskanäle, wie eben Fachzeitschriften oder Internetquellen, Erkundungen einholt. Je höherrangiger die Rechtsgüter sind, die in Kontakt mit IT-Produkten des kommerziellen IT-Nutzers kommen, je größer das Vertrauen Dritter in den Einsatz der IT-Produkte durch den IT-Nutzer ist, desto intensiver werden diese Kontrollen und diese Pflicht zur Erkundigung ausfallen. So wird etwa eine Bank, die Online-Banking einsetzt, verpflichtet sein, sich wesentlich schneller und re-

[727] BGH NJW-RR 2003, 1459; NJW 1990, 1236; NJW-RR 2002, 525 mwN.

[728] BGH NJW-RR 2002, 525 (526); BGH NJW 1978, 1629; BGH NJW 1990, 906 (907); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 234; Schwarz/Peschel-*Mehner-Schwerdtfeger/Gottschalck*, Kap. 2 Rn. 246.

[729] *Koch,* NJW 2004, 801 (804); *Libertus,* MMR 2005, 507 (509); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 234.

[730] *Koch*, NJW 2004, 801 (803).

gelmäßiger einen Überblick über Gefahrenlagen aus IT-Produkten zu verschaffen als ein Wertpapierdienstleister, der IT-Produkte lediglich intern oder gar nur sporadisch einsetzt.

379 Diese Maßstäbe entscheiden auch darüber, ob dem IT-Nutzer gar noch weitergehende Pflichten aufzubürden sind, etwa zur **eigenständigen Bewältigung von bekannt gewordenen Sicherheitslücken**. Allerdings kann dies nur besondere Fälle betreffen, da dem IT-Nutzer oftmals enge Grenzen zur Selbsthilfe gesetzt sind, zum einen durch rechtliche Grenzen im Rahmen von §§ 69c, d UrhG, zum anderen durch technische Grenzen der Aufarbeitung komplexer Software. Grundsätzlich ist nach § 69c Nr. 2 UrhG die Bearbeitung oder Umarbeitung von Computerprogrammen nur mit Gestattung des Rechteinhabers möglich. Davon erfasst sind Abänderungen des geschützten Computerprogramms.[731] § 69c Rn 17. § 69d I UrhG stellt klar, dass auch die Fehlerbeseitigung eine Umarbeitung darstellt. Fehler können Bugs, Funktionsstörungen, Programmabstürze, Viren, trojanische Pferde oder ähnliches sein, nicht davon erfasst ist dagegen das Entfernen von Kopierschutzvorrichtungen wie ein Dongle.[732] Fehlerbeseitigungen sind nach § 69d I UrhG aber grds. von der Gestattungspflicht ausgenommen. Allerdings hängt diese Ausnahme wiederum von dem Willen des Rechteinhabers ab.[733] Denn dieser hat nach § 69d I 1. Hs. UrhG („Soweit keine besonderen vertraglichen Bestimmungen vorliegen,[...]“) die Möglichkeit, Ausnahmeregelung des § 69d I UrhG vertraglich abzubedingen oder ihren Umfang einzuschränken, wobei allerdings die Fehlerbeseitung einen sogenannten „abredefesten Kern“ darstellt, der nicht abbedungen werden kann.[734] Schon vom Wortlaut aus sind Wartungen und Programmverbesserungen dagegen nicht von der Ausnahme des § 69d I UrhG erfasst.[735] Insofern bedürfen diese einer Gestattung des Rechteinhabers nach § 69c Nr. 2 UrhG. Daher kann etwa einem kommerziellen IT-Nutzer kein Vorwurf gemacht werden, wenn noch keine Lösung für ein Problem besteht, wie es z.B. häufig bei bekannten Systemlücken ohne entsprechendes Update des Herstellers der Fall ist.

380 Im Rahmen der Zumutbarkeitsprüfung sind allerdings die technischen Grenzen weniger relevant als die wirtschaftlichen Einschränkungen: Denn der kommerzielle IT-Nutzer

[731] Dreier/Schulze-*Dreier*, § 69c Rn. 15.
[732] Schricker-*Loewenheim*, § 69d Rn. 9 f.; Dreier/Schulze-*Dreier*, § 69d Rn. 9.
[733] Dreier/Schulze-*Dreier*, § 69d Rn. 2.
[734] Schricker-*Loewenheim*, § 69d Rn. 13; Dreier/Schulze-*Dreier*, § 69d Rn. 12.
[735] Dreier/Schulze-*Dreier*, § 69d Rn. 9; ferner Schricker-*Loewenheim*, § 69d Rn. 14.

kann immer darauf verwiesen werden, technischen Sachverstand einzukaufen, so dass im Wesentlichen die wirtschaftliche Seite ausschlaggebend ist.

381 Wie schon für private IT-Nutzer, finden sich diese Pflichten quasi spiegelbildlich sowohl hinsichtlich des Schutzes Dritter als auch der zumutbaren Eigenschutzpflichten (§ 254 BGB) wieder – wenngleich für den Schutz Dritter bestimmte besondere Verkehrserwartungen eine andere Rolle spielen mögen, so dass in diesen Situationen die Pflichtenstandards unterschiedlich ausfallen können. Anders formuliert wird der Verkehr generell (nicht nur die Vertragspartner) von einem professionellen IT-Nutzer (Onlinebank) wesentlich höhere Sicherheitsmaßnahmen erwarten.

382 Bislang praktisch kaum geklärt sind etwa die sog. Vorsorgekosten für Schadensfälle im Rahmen von §§ 249, 254 BGB für IT-Systeme. Grundsätzlich können Vorhaltekosten, d.h. solche Kosten, die für eine eigene Betriebsreserve entstehen, vom Schädiger ersetzt werden, wenn diese zur Schadensminderung beitragen.[736] Im IT-Bereich wäre es denkbar, dass die Vorhaltung redundanter Systeme oder die Installation besonderer Sicherheitsmaßnahmen der Schadensminderung beiträgt, insbesondere wenn es sich um umsatzintensive Unternehmen handelt, die auf funktionierende Technik angewiesen sind. Als Beispiel käme der Bereich des Brokering in Frage: steht im Falle eines Ausfalles kein System bereit, können enorme Ausfälle und Schäden entstehen, die durch das Bereitstehen weiterer Systeme wesentlich geringer gehalten werden können. Daher erscheint es in diesen Fällen angemessen, auch Vorhaltekosten geltend machen zu können. Denkbar wäre auch das Geltendmachen von angemessenen „Kopfgeldern“, vergleichbar mit den Fangprämien bei Kaufhausdiebstählen,[737] wenn Unternehmen auf das Finden von Systemcrackern derartige Prämien aussetzen, da dies der Vermeidung von konkreten Schadensfällen entgegenwirkt und das Kopfgeld auch erst im Fall der Aufdeckung fällig wird bzw. die Forderung erst entsteht.[738]

383 Es ist somit für die zu ergreifenden Maßnahmen zu ermitteln,

- ob die Tatsache, dass ein Problem besteht, bekannt ist bzw. bekannt sein muss,

[736] BGH NJW 1976, 286; Erman-*Kuckuk*, § 249 BGB Rn. 71; Bamberger/Roth-*Schubert*, § 249 BGB Rn. 99; MünchKommBGB-*Oetker*, § 249 BGB Rn. 195.

[737] BGH NJW 1980, 119.

[738] S. dazu Bamberger/Roth-*Schubert*, § 249 BGB Rn. 101.

- ferner ob die Ergreifung der Sicherungsmaßnahme wirtschaftlich zumutbar ist, wobei einzubeziehen ist, inwiefern bereits der Eigenschutz derart stark wiegt, dass auch an sich unzumutbare Maßnahme über den kumulativen Effekt des Eigeninteresses doch als zumutbar anzusehen ist,

- sowie wie häufig der Nutzer Aktualisierungen vornehmen muss.

(2) Einzelfragen

384 Diese Punkte sind nun, wie bereits bei den privaten IT-Nutzern, bei den jeweiligen Sicherungsmaßnahmen zu überprüfen.

(a) Virenscanner

385 Der Einsatz von Virenscannern ist bereits Privaten zumutbar. Als Grund, warum den kommerziellen Nutzern von Computersystemen hier geringere Pflichten obliegen sollen, kommen die erhöhten Kosten in Betracht. So sind die Programmlizenzen häufig pro genutztem Computer zu erwerben, so dass bei einer Vielzahl von Rechnern durchaus merkbare Kosten entstehen können. Allerdings ist das Gefahrenpotential durch Viren sehr hoch,[739] auch Leben und Gesundheit können betroffen sein, zudem besteht ein starkes Eigeninteresse hinsichtlich des Schutzes der eigenen Daten und Anlagen. In diesem Rahmen überwiegen die eigenen Schutzinteressen sowie diejenigen Dritter den wirtschaftlichen Aufwand. Eine wirtschaftliche Zumutbarkeit liegt demnach vor. Der Einsatz von Virenscannern ist Teil der Verkehrssicherungspflichten der Nutzer. Nach dem BSI-Grundschutz ist eine permanente Überwachung als Schutz vor Viren absolut notwendig.[740]

386 Eine Änderung könnte sich auch in der notwendigen Aktualisierungsfrequenz ergeben. Allerdings ist eine ständige Aktualisierung auch dem kommerziellen Nutzer nicht zumutbar,[741] solange auch gebräuchliche Standardvirenscanner nur wöchentlich automatische Aktualisierungen anbieten. Sollte sich jedoch das ständige Angebot von Updates durchsetzen, so kann zumindest an Arbeitstagen von einer täglichen Updatepflicht ausgegangen werden.[742]

(b) Firewall

387 Der Einsatz von Firewalls kann von privaten IT-Nutzern nicht generell verlangt werden. Grund hierfür ist einerseits, dass zwar die abstrakte Gefahr „Internet“, aber nicht die

---

[739] Vgl. zum Beispiel heise-online v. 25.4.2006, abrufbar unter: http://www.heise.de/newsticker/meldung/72366.
[740] BSI, IT-Grundschutzhandbuch 2005, B 1.6.
[741] So aber *Schmidbauer*, abrufbar unter: http://www.i4j.at/news/aktuell36.htm.
[742] „Kurze“ Abstände *Tita*, VW 2001, 1781 (1784).

Lösung über eine Firewall bekannt ist. Hinzu kommt der nur unzureichende Schutz sowie als Hauptargument die technische Unzumutbarkeit des Einsatzes. Im Bereich der Haftung der kommerziellen Nutzer besteht dieses letzte Erfordernis jedoch nicht, sondern ist vielmehr nur Teil der wirtschaftlichen Erwägungen.

388 In Firmennetzen werden häufig zentrale Firewalls eingesetzt, die dann auch zentral eingerichtet oder gewartet werden. Aufgrund der Komplexität der Aufgabe[743] wird regelmäßig besonders geschultes Personal oder die Herbeiziehung externen Experten notwendig sein. Für die Wartung und Überwachung, aber auch für die lokale Einrichtung, ist es dem Unternehmen durchaus zuzumuten, Experten heranzuziehen. Diese können z.B. das eigene Personal unterweisen und schulen. Zudem können häufig die elementarsten Sicherungen bereits durch den kostengünstigen Einsatz einer Hardwarefirewall bzw. eines entsprechenden Routers ergriffen werden. Aufgrund der hohen Gefährdung der eigenen und fremden Daten ist die wirtschaftliche Zumutbarkeit des Einsatzes von Firewalls jedenfalls gegeben.

389 Es besteht somit die Pflicht zum Einsatz von Firewalls.[744]

(c) System- und Programmupdates

390 Bereits dem privaten Nutzer ist das Einspielen von Systemupdates zuzumuten, sofern diese automatisch oder halb-automatisch installiert werden. Begründung hierfür ist einerseits die notwendige Bekanntheit, andererseits die leichte technische Umsetzung. Diese Pflichten lassen sich als Mindeststandard ohne weiteres auch auf den Einsatz bei kommerziellen Nutzern übertragen. Nicht verpflichtend für Private sind manuelle Systemupdates sowie Aktualisierungen der installierten Programme. Fraglich ist, ob diese weiter gehenden Pflichten aber dem kommerziellen Nutzer obliegen.

391 Hierfür ist auch die Zweckrichtung der Verwendung von Programmen in kommerziellen Unternehmen zu beachten. Im Idealfall wird ein Softwareprodukt auf einem kommerziell verwendeten Rechnersystem nur dann installiert, wenn es auch tatsächlich für den Betrieb des Unternehmens benötigt wird.[745] Der Unternehmer ist darauf angewiesen, dass diese Programme auch durchgehend funktionieren. Nicht nur durch Systeme entstehen Sicherheitslücken, sondern auch durch Programmfehler. Es besteht also grundsätzlich auch durch sie eine hohe Gefährdung sowohl des eigenen Betriebs als

[743] Vgl. BSI, IT-Grundschutzhandbuch 2005, M 2.76.

[744] Ebenso und sogar für zweistufige Anlage der Firewall *Behnke/Schäffter*, DSB 2002, Heft 7-8, S. 10.

[745] Ähnl. Empfehlung zum „minimalen Betriebssystem“ BSI, IT-Grundschutzhandbuch 2005, M 4.95.

auch mittelbar der Rechtsgüter Dritter. Die Gefährdung durch Viren ist damit auch hier immanent gegeben, was ebenfalls die Möglichkeit des Eintritts der bekannten hohen Schäden impliziert. Der Aufwand für die Aktualisierung der Programme ist jedoch nicht zu unterschätzen. So muss der Unternehmer zunächst Kapazitäten für die ständige oder regelmäßige Überprüfung bereitstellen, die Aktualisierungen vornehmen und dabei auch Behinderungen im Betrieb hinnehmen. Es werden immer wieder neue Sicherheitslücken entdeckt und bekanntgegeben, Programmaktualisierungen folgen ebenso häufig. Die Folge wäre, dass der Unternehmer ständig und immer wieder produktive Einheiten freistellen müsste, was einen enormen wirtschaftlichen Aufwand bedeutet. Dennoch ist er im Rahmen der Abwägung nicht vollständig frei von Pflichten zu stellen.

392 Sind ihm kritische Sicherheitslücken bekannt,[746] so kann davon ausgegangen werden, dass er diese baldmöglichst, z.B. innerhalb von einer Woche zu schließen versucht. Bei anderen Sicherheitsproblemen ist ihm jedenfalls eine regelmäßige Überprüfung und Aktualisierung, z.B. einmal im Monat, bei sensitiven Branchen, wie etwa im Online-Banking durchaus auch kürzer, zuzumuten.

393 Der Nutzer kann jedoch im Sinne einer **Selbstschutzpflicht** (nach § 254 BGB) **nicht gezwungen werden, ein Nachfolgeprodukt** zu erwerben, um den geforderten Sicherheitsstandard zu erreichen.[747] Ansonsten wäre die Pflicht von der Entscheidung des Herstellers, ein neues Produkt herauszubringen, abhängig. Sofern der Nutzer einen Softwarepflegevertrag geschlossen hat, dessen Laufzeit noch nicht beendet ist, stellt sich dieses Problem nicht.[748]

394 Allerdings ergibt sich hier ein **signifikanter Unterschied für die Haftung gegenüber Dritten**, wenn man die Perspektive wechselt und die Pflichten des kommerziellen IT-Nutzers aus Sicht potentiell geschädigter Dritter betrachtet (z.B. durch Versand verseuchter Daten durch Bot-Netze über den kommerziellen, „befallenen“ IT-Nutzer). Denn das letztlich auf das Äquivalenzinteresse abstellende Argument im Verhältnis von IT-Hersteller zu Geschädigten, dass der Geschädigte nicht zu ständigem Neukauf eines Produktes verpflichtet sein kann, verfängt in diesen Konstellationen nicht. Zu berücksichtigen ist hier, dass der Hersteller innerhalb gewisser Grenzen rechtmäßig die Unter-

[746] Ebenso BSI, IT-Grundschutzhandbuch 2005, M 4.83.

[747] *Spindler*, NJW 2004, 3145 (3150); *Spindler*, NJW 1999, 3737 (3744).

[748] Zum Softwarepflegevertrag *Zahrnt*, CR 2000, 205 mwN.

stützung des Produkts vollständig einstellen kann,[749] da er angesichts kurzer Produktzyklen den Support nicht ständig aufrechterhalten will.[750] Er ist zwar für eine gewisse Zeit nach Ablauf des Lebenszyklus zu Pflege- und Wartungsarbeiten am Programm verpflichtet; doch finden auch diese Pflichten eine zeitliche Grenze.[751] Es wäre jedoch nicht angebracht, den kommerziellen IT-Nutzer wegen des mangelnden Supports durch den IT-Hersteller im Verhältnis zu geschädigten Dritten zu entlasten. Denn er verfügt über die Möglichkeiten, die Software entweder zu ersetzen oder die potentiellen Gefahrenquellen zu isolieren („vom Netz nehmen“) und dadurch die Gefahren zu minimieren.[752] Sind die Supportzyklen des Herstellers ausreichend lang,[753] so können dem IT-Nutzer anschließend in entsprechenden Abständen aus dem Blickwinkel des Haftungsrechts durchaus wiederkehrende Kosten auch in Form des Neukaufs aktueller Software, alternativ der Abschluss eines entsprechenden Softwarepflegevertrags,[754] zugemutet werden, sofern dies die einzige Möglichkeit zur Ergreifung notwendiger Sicherungsmaßnahmen ist.

(d) Nutzung von Nutzerkonten mit eingeschränkten Rechten

395 Im Normalbetrieb eines kommerziellen Nutzers werden lediglich die vorhandenen Programme genutzt, Eingriffe in das System durch die Nutzer sind meist sogar unerwünscht. Von daher ist eine organisatorische Aufteilung von Zugriffsrechten, also insbesondere die Vergabe geringer Eingriffsmöglichkeiten an die Nutzer und die Erstellung eines Administratorkontos, durchaus sinnvoll und schützt auch den Betrieb des Unternehmens.[755] Der wirtschaftliche Aufwand ist hierbei gering und damit zumutbar. In sehr kleinen Unternehmen, bei denen allerdings die Nutzer auch die Pflege der IT-Infrastruktur übernehmen, sind somit auch weitgehende Rechte der Nutzer erforderlich. Hier kann diese Pflicht nicht greifen.

(e) Intrusion Detection-Systeme

---

[749] Vgl. z.B. bezüglich der Unterstützung von Windows NT durch Microsoft heise-online, Meldung v. 09.03.2001, abrufbar unter: http://www.heise.de/newsticker/meldung/15958; *Lier*, VW 2004, 554 (556).

[750] *Zahrnt*, CR 2000, 205 f., wobei die Frage, ob ein Softwarepflegevertrag vor Ablauf von 5 Jahren gekündigt werden darf, verneint wird; ebenso LG Köln CR 1999, 218; dazu im Bereich Produktsicherheit AG München NJW 1970, 1852; anders OLG Koblenz CR 2005, 482.

[751] Ca. 5 Jahre, LG Köln CR 1999, 218; eher länger *Jaeger*, CR 1999, 209 (211); 10 Jahre *Bartsch*, CR 1998, 193.

[752] Zur Risikoverteilung bei Angriffen auf Computersysteme (hier DDoS) AG Gelnhausen CR 2006, 208.

[753] Hier ist, unter Verweis auf LG Köln CR 1999, 218, auf 5-10 Jahre abzustellen.

[754] Dazu *Zahrnt*, CR 2000, 205 mwN.

[755] Für Windows NT z.B. IT-Grundschutzhandbuch 2005, M 4.51, M 4.53, allgemein *Bohne,* VW 2004, 1583.

396 Intrusion Detection-Systeme werden insbesondere in größeren Netzwerken eingerichtet.[756] Der Aufwand zu ihrer Einrichtung ist relativ hoch.[757] So muss eine zentrale Komponente des Netzwerks alle durchgeleiteten Pakete analysieren können. Häufig werden auf den einzelnen Rechnern zusätzlich host-basierte Intrusion Detection-Systeme eingerichtet. Ins Gewicht fällt vor allem der Einrichtungs- und Wartungsaufwand, Lizenzkosten fallen hingegen nicht zwangsläufig an.[758] Der Betrieb erfordert jedoch tiefe Kenntnisse von Netzwerken und Netzwerkverkehr, weshalb regelmäßig Experten notwendig sind.

397 Tritt ein Angriff auf, z.B. dadurch, dass ein Virus oder Wurm einen Teil des Systems befallen hat, so kann das Programm einen entsprechenden Alarm auslösen. In der Folge kann die Weiterverbreitung verhindert werden. Ein Großteil der Gefahren kann allerdings schon durch den Einsatz von Firewalls und Virenscanner abgewehrt werden. Intrusion Detection-Systeme sind folglich nachgelagert und dienen der Erkennung, falls die primären Abwehrmechanismen versagt haben.

398 Der hohe Aufwand rechtfertigt den Einsatz nur in Unternehmen mit größeren Netzwerken und entsprechendem Know-How.[759] Eine generelle Pflicht zum Einsatz solcher Systeme besteht nicht.

(f) Malware-Entfernungsprogramme

399 Es besteht weiter die Frage, ob nicht nur Abwehr- sondern auch Vorsorgemaßnahmen im Sinne einer beständigen Beobachtung bzw. Überprüfung durch den Nutzer verlangt werden kann. So können Malware-Entfernungsprogramme zur Erkennung und teilweise auch zur Abwehr von Programmen dienen, die trotz der Ergreifung der Sicherungsmaßnahmen erfolgreich Zugang zum Computer gefunden haben.

400 Häufig sind diese Programme kostenlos verfügbar. Ihr Einsatz kann bei intensiver Beschäftigung damit auch programmiert und wiederholt ablaufen, so dass das Programm so gesteuert wird, dass es die tägliche Arbeit nicht direkt stört. Der wirtschaftliche Aufwand ist damit relativ gering, so dass der Einsatz dieser Programme verlangt werden kann.

---

[756] Zum Erfolg des Einsatzes *Behnke/Schäffter,* DSB 2002, Heft 7-8, 10.

[757] Ebenso *anonymus,* VW 2002, 1050; zur Komplexität solcher Systeme und der Anforderungen BSI, IT-Grundschutzhandbuch 2005, M 5.71.

[758] Als Open Source-Projekt existiert z.B. Snort, abrufbar unter: http://www.snort.org/.

[759] Ebenso *Tita,* VW 2001, 1781 (1784); *Behnke/Schäffter,* DSB 2002 Heft 7-8, 10.

401 Die nachträgliche Kontrolle als zweite Stufe ist nicht so häufig notwendig wie die Aktualisierung der primären Sicherungsprogramme. Ein regelmäßiger Einsatz alle zwei bis vier Wochen dürfte hier ausreichen.

(g) Ergebnis

402 Kommerzielle Nutzer müssen, abhängig auch von der Größe ihrer IT-Infrastruktur, Maßnahmen zur Sicherung ihrer IT-Systeme ergreifen. Dazu gehören die primäre Abwehr, die sekundäre Überprüfung durch Suchprogramme sowie die notwendige Aktualisierung der Programme.

c) Zwischenergebnis: Allg. Verantwortlichkeit kommerzieller Unternehmen als Nutzer

403 Im Ergebnis zeigt sich, dass kommerziellen IT-Nutzern weitgehende Pflichten obliegen. Diese sind jedoch meist mit der einmaligen Einrichtung und entsprechender Konfiguration auch für die Zukunft sicher einzurichten. So kann das Update von Virenscannern, Firewall, Intrusion Detection-Systemen und Malware-Entfernungsprogrammen automatisiert erfolgen. Andere Pflege erfordert durchaus auch personellen Aufwand. Im Rahmen der Abwägung der betroffenen Güter unter Einbeziehung des hohen Eigeninteresses ist jedoch auch dieser angemessen.

4. Der Einfluß des Datenschutzrechts auf die Pflichten von IT-Nutzern (Datensicherheit und Datenschutz)

a) BDSG

(1) Hintergrund

404 Aus öffentlich-rechtlicher Sicht enthält vor allem das Datenschutzrecht allgemeine Vorgaben für kommerzielle IT-Nutzer: Denn die Sicherheit von IT-Systemen bedingt immer auch die Sicherheit der in diesen Systemen kursierenden Daten.[760] Regelmäßig werden die in einem System verarbeiteten Daten in irgendeiner Form personenbezogen i.S.d. § 3 Abs. 1 BDSG sein.[761] Zwar bezieht sich der Datenschutz primär auf den Schutz des durch die Daten Betroffenen in seinen persönlichen Belangen, wohingegen der Begriff der Datensicherung die Sicherheit der Daten an sich betrifft.[762] Allerdings

[760] *Weichert*, in: Killian/Heussen, Kap. 135 Rn. 1; *Reiländer/Weck*, DuD 2003, 692 ff.; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 4.5 Rn. 2; *Opaschowski*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 2.1, Rn. 7 f.

[761] Vgl. dazu BVerfG NJW 1984, 419 (422), wonach es „kein belangloses Datum“ mehr gebe.

[762] Hierunter fallen Maßnahmen zum Schutz von Daten, Programmen und Datenverarbeitungssystemen vor möglichen Gefahren, dazu *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 384.

sind einerseits die Bemühungen um Datensicherheit weitgehend mit denen um Datenschutz deckungsgleich;[763] andererseits betrifft das von der Datensicherheit erfasste Gefährdungspotential in der Folge immer auch den persönlichkeitsorientierten Bereich des Datenschutzes. Sofern sich also datenschutzrechtlich Pflichten zum Schutz der Daten ergeben, umfassen diese regelmäßig auch Pflichten zum Schutz der IT-Systeme.

(2) Kommerzieller IT-Nutzer als Adressat

405 Bezogen auf kommerzielle IT-Nutzer muss zunächst geklärt werden, ob und inwiefern sie dem Anwendungsbereich des BDSG unterfallen. Aufgrund der Verwendung von IT-Systemen greifen Ausnahmen für nicht automatisierte vorliegende Daten wie z.B. Akten vorliegend generell nicht. Das BDSG unterscheidet zunächst zwischen nicht-öffentlichen und öffentlichen Stellen:

(a) Nicht-öffentliche gegenüber öffentlichen Stellen

406 Bei der Einordnung als nicht-öffentliche Stelle kommt es lediglich auf die privatrechtliche Organisationsform an.[764] Der persönliche Anwendungsbereich umfasst sowohl natürliche als auch juristische Personen,[765] aber auch Personenvereinigungen und Personengesellschaften des privaten Rechts, auch wenn ihnen keine eigene Rechtspersönlichkeit zukommt, also z.B. nicht rechtsfähige Vereine.[766]

407 Demgegenüber gehören zu den öffentlichen Stellen i.S.d. BDSG Behörden, Organe der Rechtspflege und andere öffentlich organisierte Einrichtungen, sofern sie nicht als öffentlich-rechtlich organsierte Einrichtungen am Wettbewerb teilnehmen. Ferner sind diejenigen Stellen erfasst, die zwar privatrechtlich organisiert sind, aber hoheitliche Aufgaben wahrnehmen. Öffentlich-rechtlich organisierte Unternehmen, die am Wettbewerb teilnehmen, werden dagegen nach §§ 12, 27 BDSG ebenfalls als nicht-öffentliche Stellen behandelt.[767]

(b) Persönliche Tätigkeiten

---

[763] *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 487; s ferner die Abbildung bei *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 386.

[764] *Gola/Schomerus*, § 2 BDSG Rn. 19; *Wedde*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 4.3 Rn. 32. f.

[765] *Gola/Schomerus*, § 2 BDSG Rn. 19; *Wedde*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 4.3 Rn. 38 f.

[766] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 169 f.

[767] *Gola/Schomerus*, § 2 BDSG Rn. 4.

408 Weiter eingegrenzt wird der Anwendungsbereich durch sachliche Kriterien. Werden Daten nur für persönliche oder familiäre Tätigkeiten erhoben, so findet das BDSG keine Anwendung.[768] Damit verwendet das BDSG zur Abgrenzung letztlich ein ähnliches Kriterium, wie es oben (Rn 259 ff.) im Hinblick auf die rollenspezifische Abgrenzung von IT-Nutzern entwickelt wurde. Ein und dieselbe Person kann daher je nach Tätigkeit dem BDSG unterfallen oder aufgrund rein persönlicher Tätigkeiten aus dessen Anwendungsbereich ausscheiden.

(3) Datenschutzrechtliche Pflichten und IT-Konkretisierung

(a) Die Pflichten zur Organisation und technischen Schutzmaßnahmen (§ 9 BDSG)

(i) Überblick

409 Zentrale Norm für die datenschutzrechtliche Pflicht, Sicherheitsmaßnahmen zu ergreifen, ist § 9 BDSG. Er ist auch deshalb wichtig für alle Stellen, die Daten verarbeiten, weil er fast immer Anwendung findet, sei es kraft einer expliziten Verweisung oder bei fehlenden bereichsspezifischen Regelungen zur Sicherheit von Daten.[769] Durch § 9 BDSG wird IT-Sicherheit „in den Dienst“ des Datenschutzes gestellt.[770]

410 Nach § 9 BDSG sind „technische und organisatorische“ Maßnahmen zu treffen, um die gesetzlichen Anforderungen zu gewährleisten.[771] Ziel der Norm ist, den ordnungsgemäßen Ablauf der Datenverarbeitung durch Sicherung von Hard- und Software sowie von Daten vor Verlust, Beschädigung, aber eben auch Missbrauch, Diebstahl und Verfälschung zu treffen.[772] Hierzu gehören insbesondere regelmäßige Datensicherungen, auch Maßnahmen zur Abwehr von Viren.[773] Grundsätzlich dürfen keine Verfahren oder Techniken eingesetzt werden, die zu einer erheblichen Gefährdung der grundrechtlich geschützten Rechte des Betroffenen führen,[774] die Maßnahmen müssen sich zusätzlich

---

[768] Simitis-*Dammann*, § 1 Rn. 228.

[769] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 388; Sinitis-*Ernestus*, § 9 Rn. 4 ff.

[770] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 644.

[771] Dazu auch *Schöttle*, Anwaltliche Rechtsberatung via Internet, S. 39 ff.; *Kersten*, CR 2001, 576; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rm. 21.

[772] Simitis-*Ernestus*, § 9 Rn. 2; *Gola/Schomerus*, § 9 BDSG Rn. 2 f.

[773] *Gola/Schomerus*, § 9 BDSG Rn. 19.

[774] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 384; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 25 ff; Simitis-*Ernestus*, § 9 Rn. 27.

am aktuellen Stand der Technik orientieren.[775] Die zu ergreifenden Sicherungsmaßnahmen müssen der Sensitivität der Daten vielmehr angemessen sein.[776] Nach § 9 Satz 2 BDSG orientiert sich der notwendige Aufwand auch an der Erforderlichkeit vor dem Hintergrund von wirtschaftlichen Erwägungen als Ausprägung des Verhältnismäßigkeitsgrundsatzes.[777] § 9 Satz 2 BDSG erlaubt jedoch nicht das Unterlassen von Sicherungsmaßnahmen, sondern regelt nur die Schutzintensität.[778] Wichtig ist hier ein angemessenes Verhältnis zum Schutzzweck. Dies zeigt sich auch an der Anlage zu § 9 BDSG, nach der „auf die Art der zu schützenden [...] Daten" eingegangen werden muss. Art. 17 Abs. 1 UAbs. 2 der Datenschutz-Richtlinie 95/46/EG (DS-RL) stellt sogar generell auf den aktuellen Stand der Technik ab.[779]

411 Notwendig ist also jeweils eine Analyse des Gefahrenpotentials, insbesondere konkreter Missbrauchsgefahren.[780] Die Analyse ist kein einmaliger sondern vielmehr ein dauerhafter Prozess, da eine ständige Beobachtung der Risiken erforderlich ist.[781]

412 Die Anknüpfung des Schutzes an die personenbezogenen Daten bewirkt aber auch, dass Rechensysteme, die nicht zur Verarbeitung personenbezogener Daten verwendet werden, diesem Schutz nicht automatisch unterliegen. Wenn allerdings bei einem erfolgreichen Angriff auf diese Systeme auch andere, vom BDSG wiederum erfasste Systeme bedroht werden, liegt natürlich auch der Schutz des zunächst nicht datenrelevanten Systems im Pflichtenbereich des BDSG, wenn die andere Systeme nicht anders geschützt werden können.

413 § 9 BDSG wird durch eine Anlage bereits im Rahmen des BDSG konkretisiert. Diese enthält allgemeingültige Beschreibungen professioneller Standards, insbesondere zu Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskon-

---

[775] *Weichert*, in: Killian/Heussen, Computerrechts-Handbuch Kap. 135 Rn. 2; *Hermeler*, Rechtliche Rahmenbedingungen der Telemedizin S. 83.

[776] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 389; Simitis-*Ernestus*, § 9 Rn. 28; Aufhauser/Hindinger-Back, 117; *Heibey*, in: Roßnagel Handbuch Datenschutzrecht Kap. 4.5 Rn. 32.

[777] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 389; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 25 ff.; Simitis-*Ernestus*, § 9 Rn. 23.

[778] *Wohlgemuth/Gerloff*, Datenschutzrecht, S. 158; *Gola/Schomerus*, § 9 BDSG Rn. 8.

[779] Ebenso § 5 Abs. 1 Satz 2 BerlinDSG.

[780] *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 492; eingehend dazu *Ernestus*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.2 Rn. 29 ff.

[781] *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 504; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 629 f.

trollen,[782] wobei die Aufzählung jedoch nur beispielhaft ist.[783] § 9 BDSG und seine Anlage regeln zwar grundsätzlich das „Ob" der Ergreifung von Sicherungsmaßnahmen. Sie bieten auch Anhaltspunkte für die zu ergreifenden Maßnahmen, indem sie bestimmte Sicherheitsbereiche aufstellen. Die konkrete Ausfüllung ist jedoch eine Frage des Einzelfalls, wobei allerdings die Sensitivität der vorhandenen personenbezogenen und durch das BDSG geschützten Daten und die Gefährdungslage zu berücksichtigen sind.

414 Um den Anforderungen von § 9 BDSG nachzukommen, sind grundsätzlich mehrere wichtige Punkte zu beachten bzw. einzuhalten:

(ii) IT-Sicherheitskonzept

415 Am Anfang jeder Sicherheitsmaßnahme steht die Aufstellung eines gewissen IT-Sicherheitskonzepts. Durch die Erfassung auch organisatorischer Maßnahmen ist grundsätzlich ein solches erforderlich.[784] Neben der Analyse der Sensitivität der Daten im Rahmen des § 9 Satz 2 BDSG werden die konkreten Risiken beleuchtet sowie deren Minimierung oder Ausschaltung.[785] Hierbei können formalisierte Methoden und Dokumente wie das IT-Grundschutzhandbuch des BSI angewandt werden.[786] Zur Erstellung des Sicherheitskonzepts gehört jedenfalls auch die entsprechende Dokumentation bereits im Rahmen der Planung.[787]

(iii) Datensicherung (Backup)

416 Bereits aus der Anforderung der Verfügbarkeitskontrolle ergibt sich, dass eine bestimmte Form der Datensicherung in Form von Kopien (Backup) oder ähnlich zu erfolgen hat - was von der zivilrechtlichen Rechtsprechung als „Selbstverständlichkeit" bezeichnet wird.[788] Hierbei kann eine regelmäßige Sicherung auf externen Datenträgern, Sicherungen auf anderen Rechnern oder auch die jederzeitige Verdopplung von Daten (sog.

---

[782] Eingehend dazu Spindler, Unternehmensorganisationspflichten, 269 ff.

[783] *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 490.

[784] *Wohlgemuth/Gerloff*, Datenschutzrecht, S. 158; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 4.5 Rn. 135 ff.; *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 499; *Bizer*, DuD 2006, 5; *Spindler*, Unternehmensorganisationspflichten, 273.

[785] *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 4.5 Rn. 135; *Spindler*, Unternehmensorganisationspflichten, 270.

[786] *Wohlgemuth/Gerloff*, Datenschutzrecht, S. 162.

[787] LG Köln CR 2003, 724 (725) = JurPC 62/2004, Rn. 38.

[788] BGH NJW 1996, 2924 (2926); OLG Karlsruhe NJW-RR 1997, 554; krit. zur teilweise widersprüchlichen Rechtsprechung zur vertraglichen Risikoverteilung *Erben/Zahrnt*, CR 2000, 88.

RAID-Systeme) verwendet werden.[789] Grundsätzlich empfiehlt sich insbesondere bei hochsensitiven Daten eine Kombination dieser Methoden.

(iv) Erkennung und Abwehr externer Angriffe

417 Insbesondere die unter den Begriffen Zugangs-, Zugriffs- und Weitergabekontrolle erfassten Sicherungsmaßnahmen können bei Angriffen von außen relevant sein. Danach soll gewährleistet werden, dass Dritte nicht auf Daten zugreifen, diese manipulieren oder zerstören können,[790] wovon auch der externe Zugriff durch unbefugte Dritte erfasst ist.[791]

418 Die Pflicht kann hier die Verwendung sicherer Authentifizierungsmethoden, also insbesondere Passwörter, aber auch den Schutz vor dem Zugang von außen durch eine Firewall umfassen.[792] Auch der Einsatz von Virenscannern zählt zum Stand der Technik und wird daher von § 9 BDSG gefordert.[793] Ob auch bereits Intrusion Detection Systeme[794] zum Stand der (Sicherheits-) Technik gehören, lässt sich nicht ohne weiteres entscheiden.[795] Je gebräuchlicher und je leichter handhabbar diese Systeme jedoch werden, desto eher wird eine Pflicht zum Einsatz bestehen.

(v) Schaffung verbindlicher Regelungen

419 Um den Anforderungen des § 9 BDSG sinnvoll nachkommen zu können, müssen die Vorgaben unternehmensintern insgesamt und überall eingeführt sowie eingehalten werden. Der Datenschutzpflichtige kann sich nicht auf reine Empfehlungen beschränken; auch muß den Unternehmensangehörigen verdeutlicht werden, dass an die Verletzung derartiger Regeln Sanktionen geknüpft werden können.

(vi) Dokumentation

420 Bereits als Teil der Risikoanalyse, aber auch, um die Durchsetzung zu ermöglichen bzw. zu erleichtern, empfiehlt sich die Dokumentation der vorgenommenen Maßnahmen sowie der dazu führenden Gründe. Hierzu gehört, die Art der Daten, Speicherung,

---

[789] *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 4.5 Rn. 123 ff.

[790] *Ernestus*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 3.2 Rn. 25.

[791] *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 4.5 Rn. 42, 68.

[792] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 662; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 4.5 Rn. 131.

[793] *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 4.5 Rn. 131.

[794] Vgl. *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 650.

[795] Dafür *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 4.5 Rn. 133 f.

Speicherort, Gefährdungspotentiale und technisch-organisatorische Maßnahmen. Für öffentliche Stellen bestehen durch die Rechnungshöfe des Bundes und der Länder festgelegte Mindestanforderungen.[796]

(vii) Datenschutzbeauftragter

421 Ein weiteres Instrument der unternehmensinternen Kontrolle ist die Pflicht zu Bestellung eines Datenschutzbeauftragten: Nach § 4f BDSG ist sowohl in öffentlichen als auch in nicht-öffentlichen Stellen ein Datenschutzbeauftragter zu bestellen.[797] Im öffentlichen Bereich gibt es auch entsprechende Regelungen der Länder.[798] Mit der Wahl der Verpflichtung zur Bestellung wurde eine Regelung geschaffen, die zwischen staatlicher Aufsicht und wirtschaftlicher Eigenkontrolle liegt.[799] Entsprechend § 4g BDSG wirkt der Beauftrage auf die Einhaltung des BDSG sowie anderer datenschutzrechtlicher Bestimmungen hin. Er ist somit auch verantwortlich für die durch § 9 BDSG sowie die zugehörige Anlage normierten Pflichten.[800] Mittelbar übernimmt er folglich für alle Anlagen und Daten, für die das BDSG Anwendung findet, auch die Aufgabe des IT-Sicherheitsbeauftragten. Zu beachten gilt, dass der Datenschutzbeaufragte weder als betrieblicher Beauftragter noch als Unternehmensbeauftragter einzuordnen ist, was bedeutet, dass GmbH & Co., KG, OHG und AG nicht für jeden ihrer Betriebe einen gesonderten Datenschutzbeauftragten bestellen müssen, sondern nur für jede rechtlich selbstständige Einheit.[801]

422 Sofern der Datenschutzbeauftragte nicht selbst fahrlässig oder vorsätzlich seinen Pflichten nicht nachgekommen ist, ist vertragsrechtlich nicht er, sondern der Rechtsträger des Unternehmens verantwortlich. Der Datenschutzbeauftragte haftet somit grundsätzlich nicht persönlich, sondern ist nur intern verantwortlich gegenüber der nach außen verpflichteten Stelle.[802] Denkbar sind Schadensersatzansprüche der verantwortlichen Stelle gegen den Datenschutzbeauftragten bei Pflichtverletzungen.[803] Eine Haftung nach § 823

---

[796] IuK-Mindestanforderungen 2001, abrufbar unter http://www.bsi.de/gshb/deutsch/hilfmi/extern/IuKMindestanforderungen.pdf.

[797] Ausführlichich *Spindler*, Unternehmensorganisationspflichten, 283 ff.

[798] *Abel*, in: Roßnagel, Handbuch Datenschutzrecht Kap 5.6 Rn. 5.

[799] *Königshofen*, in: Roßnagel, Handbuch Datenschutzrecht Kap 5.5 Rn. 3 f.

[800] *Gliss*, DSB 1996, Heft 5, 1; *Königshofen*, in: Roßnagel, Handbuch Datenschutzrecht Kap 5.5 Rn. 27; *Spindler*, Unternehmensorganisationspflichten, 286; *Breinlinger*, RDV 1995, 7 (8).

[801] Simitis-*Simitis*, § 4f BDSG Rn. 34 f.

[802] *Königshofen*, in: Roßnagel, Handbuch Datenschutzrecht Kap 5.5 Rn. 17.

[803] Näher dazu Simitis-*Simitis*, § 4g BDSG Rn. 97 ff.

Abs. 1 oder Abs. 2 BGB iVm den §§ 4f, g BDSG gegenüber Dritten dagegen kommt grds. nicht in Betracht, da der Beauftragte selbst keine Maßnahmen durchführen und veranlassen kann, weil er weder Entscheidungs- noch Anordnungsbefugnisse besitzt,[804] und sich weiter der schützenswerte Personenkreis nicht derart abgrenzen lässt, wie es für ein Schutzgesetz nach § 823 Abs. 2 BGB erforderlich ist.[805] Eine Haftung des Datenschutzbeauftragten selbst nach § 823 BGB wäre daher nur denkbar, wenn die verantwortliche Stelle ihm derartige Kompetenzen zum Treffen von Maßnahmen erteilt hätte, so das eine persönliche Haftung des Datenschutzbeauftragen einen absoluten Ausnahmefall darstellt.[806] Denkbar sind auch Ansprüche der Betroffenen nach §§ 824 826 BGB, wenn der Datenschutzbeauftragte seine Verschwiegenheitspflichten verletzt.[807] Allerdings bestehen gerade hinsichtlich der Haftung der Beauftragten nach wie vor Unsicherheiten. Seine organisatorische Stellung sowie die Aufgabenwahrnehmung unterliegen jedenfalls indirekt der behördlichen Aufsicht. So kann die Aufsichtsbehörde bei Fehlen entsprechender Fachkunde oder wegen anderer wichtiger Gründe nach § 38 Abs. 5 Satz 3 BDSG bzw. § 36 Abs. 3 Satz 4 BDSG, § 626 BGB den Widerruf seiner Bestellung verlangen.[808]

(viii) Datenschutzaudit, § 9a BDSG

423 Noch relativ neu ist die Einführung eines Datenschutzaudits in § 9a BDSG. Das Vorbild hierzu entstammt dem Bereich des Umweltrechts[809] und dessen Umweltauditvorgaben im BImSchG bzw. der EG-Öko-Audit-VO. Ziel des Audits ist die Verbesserung des Datenschutzes in einem kontinuierlichen und auch wirtschaftlich motivierten Prozess. Die Norm wendet sich an öffentliche wie nicht-öffentliche Stellen, welche personenbezogene Daten unter Einsatz von IT-Systemen verarbeiten.[810] Regelungen zum Datenschutzaudit finden sich mit jeweils unterschiedlichem Normadressat auch an anderer Stelle, so z.B. in § 78c SGB X. Einige **Landesdatenschutzgesetze** enthalten ebenfalls entsprechende Regelungen zu Datensschutzaudits[811] für die öffentliche Stellen des Landes, die

---

[804] Simitis-*Simitis*, § 4f BDSG Rn. 127 f.; *Gola/Schomerus*, § 4f Rn. 48.

[805] Simitis-*Simitis*, § 4g BDSG Rn. 103 ff.; allgemeinen zur Haftung des Beauftragten *Spindler*, Unternehmensorganisationspflichten, 940.

[806] Siehe dazu Simitis-*Simitis*, § 4g BDSG Rn. 104.

[807] Simitis-*Simitis*, § 4g BDSG Rn. 107.

[808] *Spindler*, Unternehmensorganisationspflichten, 287 f. mwN.

[809] *Roßnagel*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 3.7 Rn. 83.

[810] *Voßbein*, DuD 2004, 92 (93).

[811] § 11c BdgDSG, § 10a DSG NW, § 4 Abs. 2, 43 Abs. 2 LDSG SH, s. dazu *Bäumler*, DuD 2004, 80; Simitis-*Bizer*, § 9a BDSG Rn. 32.

ihr Datenschutzkonzept und ihre technischen Einrichtungen einer Prüfung unterziehen können.

424 Durch ein Audit wird eine externe und neutrale Begutachtung des vorhandenen Datenschutzkonzepts durchgeführt.[812] Das Audit ist nach der Fassung des § 9a BDSG nicht obligatorisch.[813] Entsprechende Zertifikate sollen insbesondere wirtschaftliche Vorteile hervorrufen. Allerdings ist die Zertifizierung finanziell aufwändig und damit vor allem für kleinere Unternehmen praktisch nicht finanzierbar.[814] Das Verfahren der Prüfung umfasst die Prüfung und Bewertung der Vorgaben, die die die Prüfung veranlassende Stelle, also das Unternehmen, vorgibt.[815] Das Unternehmen wählt hierfür Produkt oder Verfahren aus,[816] erarbeitet hierzu ein Datenschutzkonzept und legt dem Gutachter die entsprechenden Unterlagen zur Prüfung und Bewertung vor.[817] Dabei umfasst die Prüfung auch eine Rechtmäßigkeitskontrolle, also die Bewertung der Erfüllung der allgemeinen objektiven Vorgaben des BDSG.[818] Zusätzlich werden auch die technischen Einrichtungen und Verfahren durch den Auditor überprüft.[819] Die näheren Anforderungen ergeben sich aus dem nach § 9a Satz 2 BDSG zu erlassenden Ausführungsgesetz, für das allerdings bislang hinsichtlich der Durchführung des fakultativen Audits gemäß § 9a BDSG keinerlei bundeseinheitliche Regelungen bestehen, die die Rahmenbedingungen hinsichtlich der Akkreditierung der Gutachter, die Registrierung und deren Widerruf sowie die Verwendung des Datenschutzauditzeichens abstecken. Maßstab der Bewertung ist die Verbesserung von Datenschutz und Datensicherheit. § 9a BDSG bezieht ausdrücklich nicht nur den Datenschutz sondern auch die Datensicherheit in das Audit ein.[820] Begutachtet werden können demnach auch Konzepte und Umsetzung der Pflichten aus § 9 BDSG sowie der zugehörigen Anlage. Allerdings verlangt § 9a S. 2 BDSG, dass die näheren Anforderungen an das Audit-Verfahren sowie sie Auswahl und Zulassung der Gutachter in einem besonderen Gesetz geregelt werden müssen. Ein sol-

[812] Zur Datenschutzzertifizierung *Reiländer/Weck*, DuD 2003, 692; *Rösser*, DuD 2003, 401.

[813] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 455.

[814] *Gola/Schomerus*, § 9a BDSG Rn. 4.

[815] Simitis-*Bizer*, § 9a BDSG Rn. 69; *Roßnagel*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 3.7 Rn. 93.

[816] *Roßnagel*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 3.7 Rn. 92.

[817] Simitis-*Bizer*, § 9a BDSG Rn. 70; ähnl. *Roßnagel*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 3.7 Rn. 100, 106 f.

[818] *Münch*, RDV 2003, 223 (225); *Roßnagel*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 3.7 Rn. 96.

[819] Simitis-*Bizer*, § 9a BDSG Rn. 70, 58.

[820] Zum Audit nach § 9a BDSG s. auch *Schläger*, DuD 2004, 459; *Bäumler*, DuD 2004, 80; *Bizer*, DuD 2006, 5; *Roßnagel*, Datenschutzaudit, 2000.

ches Ausführungsgesetz existiert aber bislang nicht.[821] Praktisch angewandt wird die Auditierung bislang daher lediglich in Schleswig-Holstein, die in § 43 Abs. 2 LDSG Schleswig-Holstein das Unabhängige Landeszentrum für Datenschutz (ULD) als Begutachter benennen, bei denen öffentliche Stellen ihr Datenschutzkonzept prüfen und beurteilen können. Dabei wird unterschieden zwischen einem Behördenaudit nach § 43 Abs. 2 LDSG SH und einem Produktaudit nach § 4 Abs. 2 LDSG SH. Die zum Datenschutzkonzept verwendeten Produkte können danach dem ULD vorgelegt werden. Das ULD überprüft dann die Produkte und verleiht ihnen gegebenenfalls ein Zertifikat (Gütesiegel).[822] Materielle Standards sind allerdings – soweit ersichtlich – nicht publiziert, nach denen die Auditierungen vorgenommen werden.

425 Die Common Criteria selbst beziehen solche Audits als mögliche Einsatzszenarien entsprechender Zertifikate ein. So sollen nach Nr. 6.3.4 der Common Criteria Teil 1 Auditoren von nach den Common Criteria erteilten Zertifikaten profitieren können. Sofern sich solche Querbezüge durchsetzen, könnte sich dies natürlich auch auf den finanziellen Aufwand für Datenschutzaudits auswirken, sofern die Prüfung nach den Common Criteria tatsächlich auch die Datenschutzanforderungen einbezogen hat.[823] So enthalten die Funktionsklassen der Common Criteria durchaus auch den Schutz von Daten.[824] Das Verfahren der Prüfung regeln die Common Criteria jedoch nicht.[825]

426 Eine staatlich geregelte **Datenschutz-Zertifizierung für IT-Produkte** (Hard- und Softwareprodukte sowie Datenverarbeitungsverfahren) ist derzeit nur im Bundesland Schleswig-Holstein möglich, soweit die Produkte zur Nutzung für öffentliche Stellen geeignet sind.[826] Das Unabhängige Landeszentrum für Datenschutz Schleswig Holstein (ULD)[827] bietet hierzu ein **Datenschutz-Gütesiegel** an, welches nachweist, dass die Vereinbarkeit eines Produktes mit den Vorschriften über Datenschutz und Datensicherheit in einem förmlichen Verfahren festgestellt worden ist.[828] Die Zertifizierung soll vorrangig Behörden die Auswahl datenschutzgerechter Produkte zu erleichtern (s. § 4

---

[821] Simitis-*Bizer*, § 9a BDSG Rn. 76.

[822] Mehr dazu unter: https://www.datenschutzzentrum.de/material/recht/audit/audit.htm.

[823] Ähnl. Überlegungen stellt *Münch*, RDV 2003, 223 (224 f.) an.

[824] Common Criteria Teil 2 Nr. 8.1.

[825] Common Criteria v3.0 Rev. 2 Teil 1, abrufbar unter: http://www.bsi.bund.de/cc/CCMB2005V3T1.pdf, Rn. 6.

[826] Landesverordnung über ein Datenschutzaudit (Datenschutzauditverordnung – DSAVO) vom 3.4.2001, GVOBl. Schleswig-Holstein 4/2001, S. 51. abrufbar unter: http://www.datenschutzzentrum.de/guetesiegel/index.htm. Dazu auch Simitis-*Bizer*, § 9a BDSG Rn. 33 ff.

[827] Abrufbar unter: http://www.datenschutzzentrum.de.

[828] Zum Anforderungskatalog siehe abrufbar unter: http://www.datenschutzzentrum.de/download/anford.pdf.

Abs. 2 LDSG SH), das ULD empfiehlt die Verwendung des Datenschutz-Gütesiegels aber auch als Wettbewerbsvorteil im Privatkundensektor. Es kann auch von Anbietern und Herstellern außerhalb Schleswig-Holsteins erworben werden.[829]

(4) Aufsicht und Durchsetzung

427 Relevant für die weiträumige Verbreitung von sicherer IT-Sicherheitsinfrastruktur sind nicht nur die positiv vorhandenen Pflichten, sondern insbesondere die Durchsetzung in Form von Aufsicht und Sanktionen. Nur anhand dieser lässt sich auch die Effektivität der vorhandenen Regelungen beurteilen (Enforcement).

(a) Aufsicht

428 Die Durchsetzung der datenschutzrechtlichen Pflichten erfolgt grundsätzlich im Rahmen der staatlichen Aufsicht, die ergänzend neben die Selbstkontrolle tritt.[830] Dabei ist wiederum zwischen den öffentlichen und den nicht-öffentlichen Stellen zu unterscheiden:

(i) Nicht-öffentliche Stellen

429 § 38 BDSG enthält eine explizite Aufsichtsregelung nicht-öffentlicher Stellen für den Bereich Datenschutz. Nach den Landesregelungen werden öffentlich-rechtliche Wettbewerbsunternehmen zwar den Pflichten der nicht-öffentlichen Stellen, aber der Aufsicht wie für öffentliche Stellen unterworfen.[831] In den Aufgabenbereich fallen auch die technischen und organisatorischen Maßnahmen nach § 9 BDSG.[832] Die Kompetenzen der Aufsichtsbehörde reichen vom Auskunftsrecht über die Betretung und Besichtigung von Räumen bis hin zur Anordnung von technischen oder organisatorischen Maßnahmen im Rahmen des § 9 BDSG. Die Kontrolle ist gemäß § 38 Abs. 1 Satz 1 BDSG anlassunabhängig. Nach § 38 Abs. 5 Satz 2 BDSG können bei schwerwiegenden Verstößen auch einzelne Verfahren untersagt werden. Im Wege des Verwaltungszwangs können die einzuhaltenden Pflichten auch durchgesetzt werden.[833] Zudem dient sie auch der Kontrolle des Datenschutzbeauftragten. An die Aufsichtsbehörde können sich auch betroffene Dritte wenden, die sich über die Verletzung eigener Rechte durch datenschutzrechtlich nicht erlaubtes Handeln beschweren.

---

[829] Simitis-*Bizer*, § 9a BDSG Rn. 33.

[830] *Hillenbrand-Beck*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 5.4 Rn. 4.

[831] Simitis-*Dammann*, § 27 BDSG Rn. 16; *Hillenbrand-Beck*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 5.4 Rn. 44.

[832] *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 513.

[833] *Auernhammer*, § 38 BDSG Rn. 14; Simitis-*Petri*, § 38 BDSG Rn. 64.

(ii) Öffentliche Stellen

430 Für die Kontrolle der öffentlichen Stellen des Bundes ist nach § 24 Abs. 1 BDSG der Bundesbeauftragte für den Datenschutz zuständig, für die öffentlichen Stellen der Länder liegt die Zuständigkeit bei den Landesdatenschutzbeauftragten. Er nimmt hauptsächlich eine Beraterrolle ein.[834] Dementsprechend beschränken sich seine Kontrollkompetenzen auf ein Auskunfts- und Betretungsrecht, er teilt seine Ansicht bzw. Beanstandungen der öffentlichen Stelle mit. Er kann keine verbindlichen Weisungen erteilen,[835] die Beanstandung ist auch nicht als solche aufzufassen.[836] Zusätzlich kann er Rechtsverletzungen bei der jeweiligen höchsten Aufsichtsbehörde beanstanden, die anschließend im Rahmen ihrer Fach- oder Rechtsaufsicht entsprechende Schritte einleiten kann.[837] Dies gilt ebenso für die Landesdatenschutzbeauftragten, für die das Instrument der Beanstandung insgesamt durch die Länder übernommen wurde. Vom Aufgabenbereich des Bundesdatenschutzbeauftragten sind auch die Sicherungsmaßnahmen des § 9 BDSG erfasst.[838]

(b) Sanktionen

431 Neben dem verwaltungsrechtlichen Zwang enthält das BDSG in §§ 43 f. BDSG Bußgeld- und **Strafvorschriften**. Jedoch werden die Pflichten nach § 9 BDSG nicht von diesen Sanktionen mangels Verweis in § 43 BDSG erfaßt.

432 Neben die Strafvorschriften treten **Haftungsinstrumente**,[839] etwa in Gestalt von § 7 BDSG, der für den Betroffenen einen eigenständigen[840] Schadensersatzanspruch für die unzulässige Erhebung, Verarbeitung oder Nutzung von Daten vorsieht. Nach der Legaldefinition in § 3 Abs. 4 Nr. 1 BDSG erfasst das Verarbeiten von Daten auch das Speichern im Sinne von Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung. Demnach ist jedenfalls auch ein Backup von der Haftungsregelung erfasst.

---

[834] *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 427.

[835] *Heil*, in: Roßnagel, Handbuch Datenschutzrecht Kap. 5.1 Rn. 57; *Gola/Schomerus*, § 25 BDSG Rn. 4.

[836] BVerwG CR 1993, 242.

[837] *Gola/Schomerus*, § 24 BDSG Rn. 7.

[838] *Gola/Schomerus*, § 24 BDSG Rn. 3.

[839] Auf Auskunfts- und Berichtigungsansprüche wird in diesem Rahmen nicht eingegangen.

[840] *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 518 f.

433 Im unternehmerischen Bereich wurde aufgrund des **Wettbewerberschutzes** nach § 1 UWG i.V.m. § 9 BDSG ein Anspruch der Wettbewerber sowie der Verbraucherschutzverbände auf Einhaltung der Pflichten aus § 9 BDSG angenommen. Denn bei Verletzung der datenschutzrechtlichen Pflichten verschafft sich ein Unternehmer einen Wettbewerbsvorteil gegenüber anderen Wettbewerbern.[841] Ob diese Annahme indes auch nach der Novellierung des UWG noch Gültigkeit beanspruchen kann, erscheint mehr als zweifelhaft: Denn schon unter dem alten UWG hatte der BGH einem allgemeinen Anspruch auf Einhaltung der Rechtsnormen (Vorsprung durch Rechtsbruch[842]) eine Absage erteilt und nur solche Normen sanktioniert, die einen Markt- bzw. Wettbewerbsbezug vorsahen[843] – zu denen das BDSG nicht gehören dürfe.[844] Der Gesetzgeber hat diese Rechtsprechung nunmehr in § 4 Nr. 7 UWG kodifiziert.

434 **Mittelbare Wirkung** kann § 9 BDSG sowohl für vertragliche als auch deliktische Ansprüche entfalten, in dem die Anforderungen nach § 9 BDSG den geschuldeten Sorgfaltsstandard bzw. die Verkehrspflichten konkretisieren[845]. Wer die nach § 9 BDSG erforderlichen Sicherungsmaßnahmen nicht ergreift, unterliegt der Haftung.[846] Außerdem kann § 9 BDSG ein Schutzgesetz im Sinne von § 823 Abs. 2 BGB sein[847].

b) TMG

435 Auch das (zukünftige) TMG enthält für Daten, die im Rahmen von Telediensten anfallen, Regelungen zur Datensicherheit, die § 9 BDSG vergleichbar sind. § 13 Abs. 4 TMG enthält eine Aufzählung von bestimmten Schutzzielen, die erreicht werden sollen. Ziel ist auch hier der Systemdatenschutz.[848] Nach § 13 Abs. 4 TMG muss der Dienstanbieter durch technische und organisatorische Vorkehrungen dafür sorgen, dass der Nutzer Teledienste geschützt gegen die Kenntnisnahme Dritter wahrnehmen kann. Wie

---

[841] LG Hamburg NJW-RR 1997, 1407; LG Stuttgart CR 1997, 83; *Weichert*, in: Killian/Heussen, Kap. 134 Rn. 69; *Kahlert*, DuD 2003, 412 (415).

[842] BGHZ 110, 278 (289); BGH GRUR 1973, 146 (147).

[843] BGHZ 110, 278 (289); BGH VersR 1999, 987; BGH WRP 2002, 684; BGH NJW-RR 2002, 1193; dazu auch *Hoeren*, VersR 2005, 1014; *v. Gamm*, GRUR 1996, 574 (577 f.).

[844] *v. Gamm*, GRUR 1996, 574 (578); *Kahlert*, DuD 2003, 412 (415 f.).

[845] *Abel,* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.11 Rn. 28; *Gorny*, CR 1986, 673; *Schneider*, Handbuch des EDV-Rechts, Rn. 498; zur vertraglichen Haftung *Gola/Schomerus,* § 7 BDSG Rn. 16 ff.

[846] *Horns*, in: Abel, Datenschutz in Anwaltschaft, Notariat und Justiz, § 14 Rn. 73; *Holznagel*, Recht der IT-Sicherheit, S. 176.

[847] Palandt-*Sprau*, § 823 BGB Rn. 85.

[848] Spindler/Schmitz/Geis-*Schmitz*, § 4 TDDSG Rn. 1, 24.

die Schutzziele zu erreichen sind, regelt das TMG nicht, es sind jedoch die erforderlichen Maßnahmen zu ergreifen.

436 § 13 Abs. 4 TMG schützt allerdings nicht die Übertragung der Informationen, die bereits durch das TKG erfasst wird, sondern die **interne Datenverarbeitung**, was schon § 11 III TMG klarstellt.[849] § 13 Abs. 4 TMG enthält für bestimmte Teilbereiche das Erfordernis der Ergreifung von Maßnahmen. In diesen Bereichen liegt somit eine bereichsspezifische Spezialregelung vor, die das BDSG verdrängt.[850] Außerhalb dieser Teilbereiche gelten das BDSG und damit die Anforderungen des § 9 BDSG weiter. Insgesamt sind die Anforderungen des § 9 BDSG inklusive der zugehörigen Anlage auch im Rahmen des § 13 TMG anzuwenden, soweit sie nicht den speziellen Regelungen bezüglich der Nutzungsdaten nach § 13 Abs. 4 i.V.m. § 15 TMG widersprechen.[851]

c) TKG

437 Vorgaben für die Datensicherheit werden schließlich auch durch das Telekommunikationsrecht getroffen: Denn durch das Fernmeldegeheimnis werden Inhalt und Umstände der Kommunikation geschützt, so dass die individuelle Nachricht ebenso wie die Verbindungsdaten erfasst werden.[852] Diensteanbieter i.S.d. TKG müssen nach § 109 Abs. 1 TKG **angemessene technische Vorkehrungen** zum Schutz der im Rahmen des Telekommunikationsvorgangs anfallenden Daten treffen. Damit trägt § 109 TKG dem Rang des Fernmeldegeheimnisses sowie des Datenschutzes Rechnung.[853] Normadressat des § 109 Abs. 1 TKG sind auch diejenigen, die an der Telekommunikation lediglich mitwirken, also auch Wiederverkäufer, die für ihren Betrieb Daten erheben.[854] § 109 Abs. 1 Nr. 2 TKG enthält hierbei auch die Verpflichtung zum Schutz vor unbefugten Zugriffen. Allerdings werden die Anforderungen des TKG regelmäßig nur für solche kommerziellen IT-Nutzer relevant werden, die als IT-Intermediäre einzustufen sind, da sie gleichzeitig IT-Dienstleistungen erbringen, etwa als Access-Provider, die die Nutzung von elektronischen Kommunikationsnetzen erst ermöglichen.

---

[849] Spindler/Schmitz/Geis-*Schmitz*, § 4 TDDSG Rn. 34.

[850] BT-Drucks. 14/6098, 14; Roßnagel-*Bizer*, § 4 TDDSG Rn. 78; *Holznagel*, Recht der IT-Sicherheit, S. 188.

[851] Roßnagel-*Bizer*, § 4 TDDSG Rn. 80.

[852] *Weichert,* in: Killian/Heussen, Kap. 136 Rn. 2.

[853] Säcker-*Klesczewski*, § 109 TKG Rn. 1; Scheurle/Mayen-*Zerres*, § 87 TKG a.F. Rn. 1; Beck' scher TKG-Kommentar-*Ehmer*, § 87 TKG a.F. Rn. 1.

[854] Säcker-*Klesczewski*, § 109 TKG Rn. 6.

d) Ergebnis

438 Wie dargelegt, findet das Datenschutzrecht in allen kommerziellen Bereichen Anwendung. Es enthält zudem Regelungen, die insbesondere auch die IT-Sicherheit öffentlich-rechtlich erfassen können. Der Konkretisierungsgrad ist weitaus höher als in anderen relevanten öffentlich-rechtlichen Bereichen, etwa im Produktsicherheitsrecht. Indes besteht auch hier die Notwendigkeit einer Standardisierung, um den sich rasch ändernden Gefahrenpotentialen Rechnung zu tragen.

IV. Besondere Sicherheitsanforderungen im Banken- und Finanzsektor

1. Vorbemerkung

439 Der Banken- und Finanzsektor eignet sich in besonderer Weise für eine Untersuchung der Pflichten der kommerziellen IT-Nutzer, da einerseits inzwischen fast alle Geschäftsvorgänge mittels Informationstechnik abgewickelt werden, andererseits Fehler oder Systemausfälle schnell zu hohen Schadenssummen und schwerwiegenden Folgen für die gesamte Volkswirtschaft führen können. Daher ist es nicht verwunderlich, dass gerade für diesen Sektor spezielle Regelungen existieren, insbesondere im Hinblick auf ein Risikomanagement. Der Finanzsektor kann in drei Sektoren untergliedert werden: den Bankenbereich (KWG, Rn. 440 ff.), den Wertpapierhandel (WpHG, Rn. 459 ff.) sowie schließlich den Versicherungsbereich, wobei die ersten beiden Sektoren einer genaueren Untersuchung unterzogen werden sollen.

2. Anforderungen nach dem KWG

a) Hintergrund

440 Für den Bereich der Bankenaufsicht regelt § 25a KWG als Teil der qualitativen Bankenaufsicht spezielle Organisationspflichten für die beaufsichtigten Kredit- und Finanzdienstleitungsinstitute. Eine ordnungsgemäße Organisation umfasst gemäß § 25a Abs. 1 Satz 3 Nr. 4 KWG ausdrücklich auch angemessene Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung.

441 Zweck des KWG ist es, durch vorbeugende Überwachung allgemein das Entstehen von Schäden im Kreditwesen zu verhindern.[855] Aufgabe der zuständigen Bundesanstalt für Finanzdienstleistung (BaFin) ist es, Missständen im Kredit- und Finanzdienstleistungs-

[855] Boos/Fischer/Schulte-Mattler-*Braun,* Einf. KWG Rn. 61.

wesen entgegenzuwirken, welche die Sicherheit der den Instituten anvertrauten Vermögenswerte gefährden, die ordnungsmäßige Durchführung der Bankgeschäfte oder Finanzdienstleistungen beeinträchtigen oder erhebliche Nachteile für die Gesamtwirtschaft herbeiführen können (§ 6 Abs. 2 KWG). Das KWG dient damit der Schaffung von Vertrauen bei Anlegern und Marktteilnehmern, der Sicherstellung der Solvenz der Unternehmen und dem Schutz der Kunden und leistet einen Beitrag zur Stabilisierung des nationalen und Internationalen Finanzsystems.[856] Das aufsichtsrechtliche Handlungsinstrumentarium der BaFin zur Erreichung dieser Ziele reicht von informellem Handeln (z. B. Anforderung von Informationen, Mitteilung der BaFin zu Vorgängen in den Instituten), Rundschreiben, Anordnungen im Einzelfall bis hin zum Erlass von Rechtsverordnungen.

442 § 25a KWG wurde 1997 durch die 6. Novelle des KWG eingeführt und setzt Art. 10 der Wertpapierdienstleistungs-Richtlinie 1993[857] und Art. 4 Abs. 4 der Kapitaladäquanz-Richtlinie 1993[858] in deutsches Recht um. Durch das Finanzkonglomeraterichtlinie-Umsetzungsgesetz vom 21.12.2004[859] wurde die Vorschrift ohne relevante Auswirkungen auf das Riskmanagement in ihrer gegenwärtigen Form neu gefasst.[860]

b) Pflichten und Adressat

443 § 25 a KWG regelt organisatorische Mindeststandards, welche eine gesetzliche Konkretisierung der allgemeinen Anforderungen an eine ordnungsgemäße Geschäftsführung darstellen.[861] Nach § 25a Abs. 1 Satz 2 KWG sind die Geschäftsleiter (vgl. § 1 Abs. 2 Satz 1 KWG) für die ordnungsgemäße Geschäftsorganisation des Instituts verantwortlich. Die Vorschrift entspricht in ihrer Bedeutung § 91 Abs. 2 AktG und nimmt im Verhältnis zum Aktienrecht eine gewisse „Schrittmacherrolle“ ein.[862] Weitergehend wird nunmehr sogar eine einheitliche Auslegung und Anwendung von § 25a Abs. 1 KWG und § 91 Abs. 2 AktG vertreten.[863]

---

[856] Boos/Fischer/Schulte-Mattler-*Braun,* Einf. KWG Rn. 61.

[857] Richtlinie 93/22/EWG des Rates vom 10. Mai 1993, ABl. Nr. L 141 vom 11. Juni 1993, 27.

[858] Richtlinie 93/6/EWG des Rates vom 15. März 1993, ABl. Nr. L 141 vom 11. Juni 1993, 1.

[859] BGBl. I, 3610.

[860] *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 22.

[861] Boos/Fischer/Schulte-Mattler-*Braun,* § 25a KWG Rn. 2.

[862] *Fleischer*, ZIP 2003, 1 (10); *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 19.

[863] *VG Frankfurt/M* WM 2004, 2157 (2160); *Preußner*, NZG 2004, 303 (305), NZG 2004, 57 (59); *Bürkle*, WM 2005, 1496 (1497); *Witte/Hrubesch*, BB 2004, 725 (730); vorsichtiger *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 19.

444 § 25a Abs. 2 KWG regelt die Anforderungen an die Auslagerung von Bereichen des Instituts auf andere Unternehmen (Outsourcing). Da es sich bei dieser Regelung um einen Bestandteil der allgemeinen organisatorischen Pflichten handelt, orientiert sich die Auslegung nicht nur an den speziellen Risiken eines Outsourcing sondern auch an den allgemeinen aufsichtsrechtlichen Zielen[864] . Das Institut hat den auszulagernden Bereich klar zu definieren, das Auslagerungsunternehmen mit der erforderlichen Sorgfalt auszuwählen und die erforderlichen Weisungsbefugnisse vertraglich zu sichern. Vor allem aber muss der ausgelagerte Bereich in das interne Kontrollsystem des auslagernden Instituts integriert bleiben, als ob die Dienstleistung intern vom Institut selbst erbracht würde[865].

c) Rechtsfolgen

445 Bei Verstößen gegen die Organisationspflichten des § 25a Abs. 1 Satz 3 Nr. 4 KWG kann die BaFin aufsichtsrechtliche Maßnahmen ergreifen. Hierzu gehören informelle, unverbindliche Maßnahmen ebenso wie Anordnungen im Einzelfall (Verwaltungsakte). § 6 Abs. 3 KWG ermächtigt die BaFin gegenüber den Instituten und ihren Geschäftsleitern Anordnungen zu treffen, die geeignet und erforderlich sind, um Verstöße gegen aufsichtsrechtliche Bestimmungen zu unterbinden oder um Missstände in einem Institut zu verhindern oder zu beseitigen, welche die Sicherheit der dem Institut anvertrauten Vermögenswerte gefährden können oder die ordnungsgemäße Durchführung der Bankgeschäfte oder Finanzdienstleistungen beeinträchtigen. Darüber hinausgehend findet sich in § 25a Abs. 1 Satz 4 KWG nunmehr eine besondere Anordnungsbefugnis für die BaFin gegenüber den Instituten (nicht auch den Geschäftsleitern), wenn diese im Einzelfall nicht die adäquaten, internen Maßnahmen zur Erfüllung der Organisationspflichten des § 25a Abs. 1 KWG ergreifen. Die Anordnungsbefugnis dient damit der Gefahrenprävention.[866] Der BaFin stehen zur Durchsetzung der Vorgaben des KWG Zwangsmittel zur Verfügung. Im Extremfall kann dies bis zur Abberufung des Geschäftsleiters (§ 36 Abs. 2 KWG) oder dem Widerruf der Erlaubnis (§ 35 KWG) reichen.[867]

446 Das KWG hat **keine drittschützende Wirkung** zugunsten individueller Gläubiger. Es dient ausschließlich dem Schutz der Allgemeinheit und der Funktionsfähigkeit des Kre-

[864] Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 550.
[865] Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 613 ff.
[866] Boos/Fischer/Schulte-Mattler-*Braun* § 25a KWG Rn. 25.
[867] Boos/Fischer/Schulte-Mattler-*Braun* § 25a KWG Rn. 7.

ditgewerbes.[868] Dies folgt aus § 4 Abs. 4 FinDAG, welcher der BaFin ausdrücklich nur „Aufgaben im öffentlichen Interesse“ zuweist. Bei Verletzung der Aufsichtspflicht durch die BaFin bestehen daher keine Amtshaftungsansprüche nach § 839 BGB i. V. m. Art. 34 GG.[869] Grundsätzlich sind die Vorschriften des KWG auch keine Schutzgesetze im Sinne von § 823 II BGB zugunsten der einzelnen Bankkunden.[870] Aus der Verletzung der IT-spezifischen Organisationspflichten nach § 25a Abs. 1 KWG können daher grundsätzlich keine Schadensersatzansprüche abgeleitet werden. Bei Verletzung eines Rechtsguts oder absoluten Rechts im Sinne von § 823 Abs. 1 BGB kommen Schadensersatzansprüche nach dieser Vorschrift in Betracht. Primäre Vermögensschäden sind danach jedoch nicht ersatzfähig. Zur Konkretisierung der Verkehrspflichten im Rahmen des § 823 Abs. 1 BGB kann auf die Anforderungen des § 25a Abs. 1 KWG zurückgegriffen werden, da sich die Verkehrserwartungen daran ausrichten.[871] Daneben kommt für den Vorstand eines als Aktiengesellschaft organisierten Instituts eine Haftung nach §§ 93, 91 Abs. 2 AktG in Betracht

d) Anhaltspunkte für IT-Konkretisierungen

447 Gemäß § 25a Abs. 1 3 Nr. 4 KWG sind angemessene Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung zu treffen. Hintergrund dieser Regelung ist die Dominanz von IT-Produkten in allen Geschäftsbereichen der Kredit- und Finanzdienstleistungsinstitute. Die wachsende Arbeitsteilung und Vernetzung mit Geschäftspartnern, Kunden, Börsen und anderen Institutionen, wie beispielsweise Aufsichtsbehörden führen zu einer immer stärkeren Abhängigkeit von der Betriebsbereitschaft der IT-Systeme der Institute und der IT-Systeme Dritter.

448 Die **Angemessenheit der erforderlichen Sicherheitsvorkehrungen** ist ein unbestimmter Rechtsbegriff, welcher anhand der Ziele des § 6 Abs. 2 KWG zu konkretisieren ist.[872] Für den IT-Bereich bilden den Beurteilungsmaßstab insbesondere die Sicherung der anvertrauten Vermögenswerte, die Sicherung der ordnungsgemäßen Durchführung der Bankgeschäfte und Finanzdienstleistungen, sowie die Vermeidung von Nachteilen

[868] Boos/Fischer/Schulte-Mattler-*Braun* Einf. KWG Rn. 63.

[869] Boos/Fischer/Schulte-Mattler-*Braun* Einf. KWG Rn. 63; anders die frühere Rechtsprechung des BGH s. BGH WM 1979, 482; WM 1979, 482; allgemein *Schenke/Ruthig*, NJW 1994, 2324.

[870] Boos/Fischer/Schulte-Mattler-*Braun* Einf. KWG Rn. 67 m. w. N.

[871] Für den Bereich der Haftung für die Weiterverbreitung von Viren *Koch*, NJW 2004, 801 (805).

[872] Boos/Fischer/Schulte-Mattler-*Braun,* § 25a KWG Rn. 12, 143.

für die Gesamtwirtschaft durch Missstände im Kredit- und Finanzdienstleistungswesen.[873]

449 **Maßgebliche Kriterien** sind Art und Umfang des Einsatzes von EDV, die eingesetzte Hardware, die Organisation der Datenverarbeitung (zentrale Datenverarbeitung, dezentrale Datenverarbeitung, Datenverarbeitung außer Haus) und die Verarbeitungsform (Stapelverarbeitung, Dialogverarbeitung, Datenbanksystem, Kommunikationssystem).[874] Norminterpretierende und -konkretisierende Wirkung kommt hierbei den Rundschreiben der BaFin zu.[875]

450 **IT-spezifische Vorgaben** enthalten die Mindestanforderungen an das Risikomanagement (MaRisk),[876] welche nunmehr die Einhaltung der BSI-Standards für den IT-Grundschutz fordert. Darüber hinaus sind von der BaFin für die Auslegung des § 25a KWG und die Verwaltungspraxis die Empfehlungen des Basle Committee on Banking Supervision zu beachten.[877] Nach Principle 8 des Rahmenkonzepts zu „Internal Control Systems" ist ein sicheres Management Informationssystem einzurichten. Wegen der mit elektronischen Informationssystemen und dem Einsatz der Informationstechnologie verbundenen Risiken sind hierbei allgemeine Kontrollen und Anwendungskontrollen einzuführen sowie Vorsorge für den Fall des Verlusts oder längeren Ausfalls von Systemen zu treffen.[878] Für den Bereich der IT-Sicherheit finden sich zudem Vorgaben zum Riskmanagement in den Empfehlungen „Riskmanagement for Electronic Banking" vom März 1998[879] und „Risk Management Principles for Electronic Banking" vom Juli 2003.[880]

451 Die **Sicherheitsvorkehrungen** müssen alle IT-spezifischen Sicherheitsrisiken abdecken. Es muss insbesondere sichergestellt sein, dass eingesetzte Programme nachvollziehbar und fehlerfrei arbeiten und Dokumentationen der Programme vorgehalten sind.

---

[873] Boos/Fischer/Schulte-Mattler-*Braun,* § 25a KWG Rn. 143.

[874] Boos/Fischer/Schulte-Mattler-*Braun,* § 25a KWG Rn. 144.

[875] Boos/Fischer/Schulte-Mattler-*Braun,* § 25a KWG Rn. 19; *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 27 ff.

[876] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement" vom 20.12.2005, - sog. Ma-Risk-Rundschreiben, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 20.02.2006). Ausführlichich *Spindler,* in: Fleischer, Handbuch des Vorstandsrechts, 2006, § 19 Rn. 27 ff.

[877] *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 32.

[878] Framework for Internal Control Systems in Banking Organisations, Basle Committee on Banking Supervision, Basel 1998, abrufbar unter http://www.bis.org/pupl/bcbs40de.pdf (zuletzt abgerufen am 10.05.2006); Basel Committee Publication No. 33, S. 19, Rn. 32, 33.

[879] Abrufbar unter http://www.bis.org/publ/bcbs35.pdf (zuletzt abgerufen am 10.05.2006).

[880] Abrufbar unter http://www.bis.org/publ/bcbs82.pdf (zuletzt abgerufen am 10.05.2006).

Die Software muss geprüft sein. Bei Ausfall der eigenen EDV-Anlage muss die Geschäftstätigkeit fortgesetzt werden können; hierzu sind Notfallpläne zu erstellen.[881] Im Einzelnen lassen sich vier Fehlerkategorien unterscheiden: materielles Fehlerrisiko, Formalfehlerrisiko, technisches Ausfallrisiko und Fremdnutzungsrisiko.[882] Materielle Fehler beruhen auf sachlich falschen gespeicherten Daten oder ermittelten Verarbeitungsergebnissen. Formalfehler entstehen durch Nichtbeachtung von Formalvorschriften im Zusammenhang mit der Datenverarbeitung, was regelmäßig auf organisatorische Schwächen zurückzuführen ist. Das technische Ausfallrisiko realisiert sich, wenn Hard- oder Software bzw. Daten nicht oder nicht unversehrt vorhanden sind, oder Softwarefehler zu unkontrollierten Programmabstürzen führen. Nutzen Dritte unberechtigt die Hard- oder Software, oder greifen sie unerlaubt auf Daten zu (Fremdnutzungsrisiko), kann es zu einem Bruch der Vertraulichkeit, Urheberrechtsverletzungen, aber auch zu einem Verlust von Daten oder ganzen Systemen kommen.

452 Die notwendigen Sicherheitsvorkehrungen[883] zur Vermeidung dieser Risiken umfassen Vorkehrungen, um Fehler und Schäden aufzudecken und zu verhindern, Vorsorgemaßnahmen sowie Eventualplanungen. Der Schadensverhinderung und –aufdeckung dienen organisatorische Maßnahmen, wie beispielsweise die Kontrolle der Datenerfassung, Programmfreigabeverfahren und die Kontrolle des Systembetriebs. Daneben sind technische Sicherheitsvorkehrungen zum Schutz des Rechenzentrums (z. B. technische Zugangskontrollen, Feuerschutz usw.) und bezüglich der Hardware (Wartung, Betriebsschloss am Terminal usw.) vorzusehen. Bei der Software sind Ansatzpunkte für technische Sicherheitsvorkehrungen beispielsweise Kennwortverfahren, programmierte Kontrollen sowie systemtechnische Zwangsläufigkeiten. Zu letzteren gehören Zweiterfassungen, Zwangsprotokollierungen u. ä. Vorsorgemaßnahmen dienen der Vorbereitung von Schadensfällen und umfassen Back-Up-Vereinbarungen bei Rechnerausfall, Datenauslagerung für den Fall der Zerstörung des Originaldatenspeichers und Datensicherung für den Fall des Verlustes von Originaldaten. Ebenso sind Eventualplanungen zu erstellen, welche im Schadensfall konkrete Anwendung finden. Hierzu gehören u. a. Datenrekonstruktionsverfahren für gesicherte Daten, Wiederanlaufverfahren nach Systemabbrüchen und Back-Up-Betrieb. Diese Anforderungen entsprechen weitgehend den von

[881] *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 26; C & L Deutsche Revision 6. KWG-Novelle, 246.
[882] Boos/Fischer/Schulte-Mattler-*Braun,* § 25a KWG Rn. 145.
[883] Ausführlich Boos/Fischer/Schulte-Mattler-*Braun,* § 25a KWG Rn. 152 ff.; *Tappert*, EDV-System-Prüfung, 1994.

Principle 8 des Rahmenkonzepts zu „Internal Control Systems“ geforderten Kontroll- und Vorsorgemaßnahmen.[884]

453 Im Hinblick auf ein Outsourcing nach § 25a Abs. 2 KWG ist zu beachten, dass die Sicherheitsanforderungen vertraglich eindeutig festzulegen sind und das auslagernde Institut die Einhaltung dieser Pflichten zu überwachen hat[885]. Außerdem müssen je nach Bedeutung der ausgelagerten Bereiche Notfallpläne für den Ausfall oder die Schlechtleistung des externen Dienstleisters bestehen.[886]

454 Rechtsvergleichend ist in diesem Rahmen auf das österreichische Recht hinzuweisen, das nach § 44a Öst.Nationalbankengesetz ene Aufsicht über die Zahlungssysteme der Österreischen Nationalbank zuweist, in deren Rahmen die A-SIT die Sicherheit der elektronischen Systeme inspiziert.[887]

e) Die MaRisk[888]

455 Durch die Überführung der existierenden Rahmenvorgaben der Mindestanforderungen an die Interne Revision (MaIR),[889] der Mindestanforderungen an das Kreditgeschäft (MaK)[890] und der Mindestanforderungen an das Betreiben von Handelsgeschäften (MaH)[891] in die Mindestanforderungen an das Risikomanagement (MaRisk)[892] wird

[884] Framework for Internal Control Systems in Banking Organisations, Basle Committee on Banking Supervision, Basel 1998, abrufbar unter http://www.bis.org/pupl/bcbs40de.pdf (zuletzt abgerufen am 10.05.2006); Basel Committee Publication No. 33, S. 19, Rn. 32, 33.

[885] Boos/Fischer/Schulte-Mattler-*Braun,* § 25a KWG Rn. 635.

[886] Boos/Fischer/Schulte-Mattler-*Braun,* § 25a KWG Rn. 637.

[887] *Fallenböck* Annex II – Österreich - Rn. 1213 ff.

[888] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, sog. MaRisk-Rundschreiben, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 17.11.2006).

[889] Rundschreiben BaFin Nr. 1/2000 (BA) zu „Mindestanforderungen an die Ausgestaltung der Internen Revision der Kreditinstitute“ vom 17.01.2000 – sog. MaIR-Rundschreiben, (ehemals BaKred)., abrufbar unter http://3a-strategy.de/about/glossary/innenrevision-rundschreiben2000/document_view (zuletzt abgerufen am 17.11.2006).

[890] Rundschreiben BaFin 34/2002 (BA) über "Mindestanforderungen an das Kreditgeschäft der Kreditinstitute", vom 20.12.2002, Az.: I 4 - 44 - 5/2001 – sog. MaK-Rundschreiben, abrufbar unter http://www.bundesbank.de/download/bankenaufsicht/pdf/mak_rs34_2002.pdf (zuletzt abgerufen am 17.11.2006).

[891] BaKred-Verlautbarung über „Mindestanforderungen an das Betreiben von Handelsgeschäften“ vom 25.10.1995 – sog. MaH-Rundschreiben, abrufbar im Internet unter abrufbar unter: http://www.bafin.de/verlautbarungen/minanfhg.htm (zuletzt abgerufen am 05.10.2005). Zur Auslegung der MaH sind insbesondere das Rundschreiben 4/98, abrufbar unter http://www.bafin.de/rundschreiben/96_1998/rs4_98.htm (zuletzt abgerufen am 05.10.2005) und das Rundschreiben 5/2001 vom 12.09.2001, Geschäftszeichen I 4-42-2/2001 zu berücksichtigen, abrufbar unter http://www.bafin.de/rundschreiben/93_2001/rs05_01.htm (zuletzt abgerufen am 05.10.2005).

[892] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, - sog. MaRisk-Rundschreiben, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 20.02.2006). Ausführlichich hierzu, auch zu den Vorgängerrahmenvorgaben, s. *Spindler,* in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 27 ff.

dem Konzept einer einheitlichen Risikobetrachtung Rechnung getragen.[893] In den neuen Rahmenvorgaben werden detailliert Pflichten bezüglich der Ausgestaltung der Leitungs-, Steuerungs- und Kontrollprozesse als elementare Bestandteile des institutsinternen Risikomanagements festgelegt,[894] wobei § 25 Abs. 1 Nr. 1 und 2 KWG als zentraler Anknüpfungspunkt dient[895]. Mit den MaRisk sollen zugleich die an die Kreditinstitute gerichteten qualitativen Anforderungen der zweiten Säule („Qualitative Bankenaufsicht") von Basel II abgedeckt werden.[896]

456 Die modular aufgebaute MaRisk, bestehend aus einem Allgemeinen und Besonderen Teil,[897] greift zum Teil die dargestellten Grundsätze der bestehenden Rahmenvorgaben auf.[898] Insbesondere die allgemeinen Anforderungen an das Risikomanagement wurden jedoch erheblich erweitert. Das Risikomanagement wird verstanden als Teil einer ordnungsgemäßen Geschäftsorganisation und umfasst eine angemessene Strategie und ein angemessenes internes Kontrollverfahren, wobei letzteres aus dem Internen Kontrollsystem und der Internen Revision besteht.[899] Die Geschäftsleitung ist – unabhängig von einer internen Zuständigkeitsregelung – für die ordnungsgemäße Geschäftsorganisation und Weiterentwicklung verantwortlich.[900] Sie hat auf Grundlage einer Risikotragfähig-

---

[893] Vgl. *Angermüller/Eichhorn/Ramke,* Kreditwesen 2005, 396; *dies.,* Kreditwesen 2004, 833; *Pfingsten/Maifarth/Rieso,* Die Bank 2005, 34 (34 f.); *Grabau/Schlee,* Kreditwesen 2005, 392; *Schwirten /Zattler,* Die Bank 2005, 52; *Zimmermann,* BKR 2005, 208 (209).

[894] Vgl. Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement" vom 20.12.2005, AT 4, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 20.02.2006); s. auch *Zimmermann* BKR 2005, 208 (210); *Angermüller/Eichhorn/Ramke,* Kreditwesen 2005, 396, beide allerdings noch zum zweiten Entwurf der MaRisk vom 22.09.2005, abrufbar unter http://www.bafin.de/marisk/marisk2_entwurf.pdf (zuletzt abgerufen am 20.02.2006).

[895] *Wimmer*, BKR 2006, 146.

[896] Vgl. Anschreiben zum Rundschreiben BaFin Nr. 18/2005 vom 20.12.2005 „Veröffentlichung der Endfassung der MaRisk", abrufbar unter http://www.bafin.de/schreiben/89_2005/051220.htm (zuletzt abgerufen am 20.02.2006); *Angermüller/Eichhorn/Ramke,* Kreditwesen 2004, 833; *Zimmermann,* BKR 2005, 208 (209); *Grabau/Schlee,* Kreditwesen 2005, 392. Zu den Anforderungen der Säule II s. Boos/Fischer/Schulte-Mattler-*Schulte-Mattler,* KWG, Basel II Rn. 159 ff

[897] Zur Gliederung der MaRisk näher *Schwirten/Zattler,* Die Bank 2005, 52 (52 f.); *Angermüller/Eichhorn/Ramke,* Kreditwesen 2005, 396; *Grabau/Schlee,* Kreditwesen 2005, 392.

[898] *Angermüller/Eichhorn/Ramke,* Kreditwesen 2005, 396; zust. *Grabau/Schlee,* Kreditwesen 2005, 392; vgl. auch *Schwirten/Zattler,* Die Bank 2005, 52; ausdrücklich *Pfingsten/Maifarth/Rieso,* Die Bank 2005, 34: „diese Bausteine werden in die MaRisk bewusst und explizit aufgenommen." S. auch das Anschreiben der BaFin an die Verbände zum ersten Entwurf vom 02.02.2005, in dem es heißt, dass „der integrierte Ansatz die große Chance zur Entwicklung eines konsistenten und umfassenden Gesamtwerks auf der Basis des § 25a Abs. 1 KWG" eröffnet, abrufbar unter http://www.bafin.de/marisk/050202.htm (zuletzt abgerufen am 05.10.2005); bzgl. der Implementierung der „Mindestanforderungen an das Betreiben von Handelsgeschäften" (MaH) aus dem Jahr 1995 s. auch das Anschreiben der BaFin an die Verbände vom 22.09.2005; abrufbar unter http://www.bafin.de/marisk/marisk2_anschreiben.htm (zuletzt abgerufen am 05.10.2005).

[899] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement" vom 20.12.2005, Vorbemerkung, AT 1, 3 Rn. 1, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 20.02.2006); vgl. auch *Grabau/Schlee,* Kreditwesen 2005, 392; *Zimmermann,* BKR 2005, 208 (210).

[900] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement", vom 20.12.2005, AT 3, 5 Rn. 1, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 20.02.2006); s. zur Gesamtverantwortung der Geschäftsleitung ausführlichich *Zimmermann,* BKR 2005, 208 (209); *Pfingsten/Maifarth/Rieso,* Die Bank 2005, 34 (35).

keit und der Analyse der geschäftspolitischen Ausgangssituation eine Strategie festzulegen, in der Ziele und die entsprechenden Maßnahmen zu definieren sind.[901] Die Festlegung des Inhalts der Strategie liegt allein in der Verantwortung der Geschäftsleitung, d. h. ist nicht Gegenstand von Prüfungshandlungen durch externe Prüfer oder die interne Revision.[902] Im Rahmen eines internen Kontrollsystems sind die Regelungen zur Aufbau- und Ablauforganisation zu treffen sowie Risikosteuerungs- und -controllingprozesse einzurichten.[903] Schließlich ist über eine Interne Revision die Prüfung und Beurteilung sämtlicher Aktivitäten und Prozesse sicherzustellen.[904] Sowohl die besonderen Anforderungen an das interne Kontrollsystem als auch die an die Ausgestaltung der Internen Revision werden in dem Besonderen Teil näher spezifiziert.[905] Die Pflicht, Organisationsrichtlinien, deren Inhalt detailliert geregelt ist,[906] aufzustellen und eine Dokumentationspflicht aller Geschäfts-, Kontroll- und Überwachungsmaßnahmen[907] sollen die Einhaltung der genannten Vorgaben sichern.

457 In diesem Rahmen verlangt die MaRisk jetzt die **Einhaltung der BSI-Standards für den IT-Grundschutz**. Nach AT 4.3.2 der MaRisk hat ein Kreditinstitut bei der Einrichtung eines angemessenen Risikosteuerungs- und -controllingprozesses zunächst die Identifizierung, Beurteilung, Steuerung sowie die Überwachung und Kommunikation der wesentlichen Risiken zu gewährleisten, d. h. die wesentlichen Risiken müssen früh-

---

[901] Vgl. Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 4.2, 6 Rn.1, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 20.02.2006); *Pfinsten/Maifarth/Rieson,* Die Bank 2005, 34 (35).

[902] Anlage 1: MaRisk – Regelungstext mit Erläuterungen vom 20.12.2005, AT 4.2, 8 Rn. 1, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (zuletzt abgerufen am 20.02.2006).

[903] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 4.3, 6 ff.; s. hierbei insbesondere auch die genauen Vorgaben in AT 4.3.1 zur Aufbau- und Ablauforganisation und AT 4.3.2 zu den Risikosteuerungs- und –controllingprozessen; s. hierzu *Zimmermann,* BKR 2005, 208 (210).

[904] Vgl. Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 4.4, 7 Rn. 1-3, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 20.02.2006).

[905] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, BT 1 und BT 2, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 20.02.2006). Näher zur Internen Revision *Pfingsten/Maifarth/Rieso,* Die Bank 2005, 34 (35); *Grabau/Schlee,* Kreditwesen 2005, 392.

[906] Vgl. Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 5, 8 Rn. 3 a) bis d), abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 20.02.2006); näher hierzu *Zimmermann,* BKR 2005, 208 (215).

[907] In dem zweiten Entwurf wurden alle Dokumentationsanforderungen des ersten Entwurf zugunsten einer „Generalklausel“ gestrichen, um den Kreditinstituten breite Spielräume im Hinblick auf erforderliche Dokumentationen zu eröffnen, s. hierzu das Anschreiben der BaFin an die Verbände vom 22.09.2005, abrufbar unter: http://www.bafin.de/marisk/marisk2_anschreiben.htm (zuletzt abgerufen am 05.10.2005). Zu der Regelung im ersten Entwurf s. den ersten Entwurf über die „Mindestanforderungen an das Risikomanagement“, AT 6, 8 Rn. 1 f., abrufbar unter: http://www.bafin.de/marisk/marisk_entwurf.pdf (zuletzt abgerufen am 05.10.2005); krit. hierzu *Grabau/Schlee,* Kreditwesen 2005, 392. Zu der neuen, allgemeiner gefassten Regelung, die auch in der verabschiedeten Endfassung beibehalten wurde und lediglich in dem zweiten Absatz bezogen auf die Begründung konkretisiert wurde s. Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 6, 8 Rn. 1 f., abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 20.02.2006).

zeitig erkannt, vollständig erfasst und in angemessener Weise dargestellt werden können.[908] Operationelle Risiken werden im Modul BTR 4 behandelt, in welchem es um angemessene Risikosteuerungs- und –controllingprozesse geht.[909] Darunter sind Verlustrisiken zu verstehen, die ihre Ursache in inadäquaten und fehlerhaften internen Prozessen, Personen und Systemen oder externen Ereignissen haben.[910] In BTR 4 der MaRisk ist vorgesehen, dass wesentliche operationelle Risiken zumindest jährlich identifiziert und beurteilt werden; bedeutende Schadensfälle sind hingegen unverzüglich hinsichtlich ihrer Ursachen zu analysieren. Es ist zudem jährlich hierüber an die Geschäftsleitung detailliert Bericht zu erstatten, woraufhin entschieden werden muss, welche Maßnahmen zu ergreifen sind. Daneben spielt auch die Interne Revision eine erhebliche Rolle. Ihr ist nach AT 4.4 der MaRisk zur Wahrnehmung der Aufgaben ein vollständiges und uneingeschränktes Informationsrecht einzuräumen; hierfür erhält sie auch das Recht, Einblick in die Aktivitäten und Prozesse sowie in die IT-Systeme des Kreditinstituts zu nehmen.[911] Zwar sind die weiteren besonderen Anforderungen an die Interne Revision in dem besonderen Teil in Abschnitt BT 2 der MaRisk konkretisiert, nähere Regelungen speziell zum IT-Grundschutz sind dort jedoch nicht aufgelistet. Einzelne detaillierte Regelungen zur technisch-organisatorischen Ausstattung finden sich aber in dem allgemeinen Teil der MaRisk,[912] wobei jedoch keine konkreten Anforderungen an bestimmte Systeme gestellt werden, sondern vielmehr die Ziele für ein IT-System vorgegeben werden, um eine möglichst flexible Regelung zu schaffen. Hiernach hat sich gem. AT 7.2 der MaRisk der Umfang und die Qualität der technisch-organisatorischen Ausstattung insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie der Risikosituation zu orientieren. Abzustellen ist grundsätzlich nach AT 7.2 der MaRisk auf gängige Standards, wobei die Eignung regelmäßig zu überprüfen ist. Die IT-Systeme, dh. Hardware- und Software-Komponenten sowie die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertrau-

[908] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“, vom 20.12.2005, AT 4.3.2, 7 Rn. 2, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (zuletzt abgerufen am 20.02.2006).

[909] *Zimmermann,* BKR 2005, 208 (210); s. zum ersten Entwurf der MaRisk *Angermüller/Eichhorn/Ramke,* Kreditwesen 2005, 396.

[910] *Zimmermann,* BKR 2005, 208 (210); Boos/Fischer/Schulte-Mattler-*Schulte-Mattler,* KWG, Basel II Rn. 133.

[911] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 4.4, 8 Rn. 4, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (zuletzt abgerufen am 20.02.2006).

[912] *Pfingsten/Maifarth/Rieso,* Die Bank 2005, 34 (36); *Angermüller/Eichhorn/Ramke,* Kreditwesen 2005, 396; s. auch *Zimmermann,* BKR 2005, 208 (216), der insbesondere auf die finanziellen Herausforderungen des IT-Sektors hinweist.

lichkeit der Daten sicherstellen.[913] Außerdem sind die IT-Systeme nach AT 7.2 der MaRisk vor ihrem erstmaligen Einsatz und auch nach wesentlichen Veränderungen zu testen und von den fachlichen sowie von den technisch zuständigen Mitarbeitern abzunehmen. Für Notfälle in kritischen Aktivitäten und Prozessen ist gem. AT 7.3 der MaRisk ein Notfallkonzept zu treffen, welches geeignet sein muss, das Ausmaß möglicher Schäden zu reduzieren und Geschäftsführungs- sowie Wiederanlaufpläne zu umfassen hat. Die Wirksamkeit und Angemessenheit ist regelmäßig durch Notfalltests zu überprüfen. Innerhalb eines angemessenen Zeitraums müssen die Wiederanlaufpläne die Rückkehr zum Normalbetrieb ermöglichen und die im Notfall zu verwendenden Kommunikationswege sind festzulegen.[914]

458 Demgegenüber verweist das **britische Recht** in seinem FSA (Financial Services Authority) Handbook in der Sektion ***Senior Management Arrangements, Systems and Controls*** **(SYSC**) neben einer Reihe von einzelnen Pflichten vor allem auf die Einhaltung der ISO 17799.[915]

3. Anforderungen nach dem WpHG

a) Hintergrund

459 Das WpHG ist die zentrale Regelung des deutschen vertriebs- und marktbezogenen Kapitalmarktrechts. Es handelt sich hierbei um öffentliches Aufsichtsrecht. Die Marktaufsicht nach dem WpHG steht in engem Zusammenhang mit der Bankenaufsicht nach dem KWG, da Kreditinstitute und Finanzdienstleitungsinstitute sowohl dem KWG, als auch dem WpHG unterfallen. Die Bundesanstalt für Finanzdienstleitungsaufsicht (BaFin) ist neben der Bankenaufsicht nach KWG auch für die Überwachung und Durchsetzung der Vorgaben des WpHG zuständig (§ 4 Abs. 1 Satz 1 WpHG).[916]

b) Pflichten und Adressat

460 Die Vorschriften der §§ 31 ff. WpHG verpflichten die Kreditinstitute und Wertpapierhandelsunternehmen zu anlegerschutz-orientierter Organisation.[917] Nach § 33 Abs. 1 Nr. 1 WpHG sind die Wertpapierdienstleistungsunternehmen verpflichtet, die für eine

---

[913] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 7.2, 9 Rn. 2, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (zuletzt abgerufen am 20.02.2006).

[914] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 7.3, 10 Rn. 1 f., abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (zuletzt abgerufen am 20.02.2006).

[915] SYSC 3A.7.8, dazu *Reed* – Annex II – Rn. 1330 f.

[916] Zur Abgrenzung von Bank- und Marktaufsicht Schwark-*Schwark*, § 1 WpHG Rn. 6.

[917] *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 41.

ordnungsmäßige Durchführung der Wertpapierdienstleistung und Wertpapiernebendienstleistung notwendigen Mittel und Verfahren vorzuhalten und wirksam einzusetzen. Bei der Auslegung dieser Norm kann auf § 25a Abs. 1 KWG zurückgegriffen werden.[918] Wie § 25a Abs. 1 KWG stellt auch § 33 Abs. 1 WpHG eine Umsetzung des Art. 10 der Wertpapierdienstleistungs-Richtlinie von 1993 dar.[919] Die Auslegung orientiert sich daher an den Zielen der Richtlinie, die Anleger zu schützen sowie die Stabilität und das reibungslose Funktionieren der Wertpapiermärkte bzw. des Finanzsystems zu gewährleisten.[920] So müssen die Unternehmen die Risiken und die Art ihrer Bewältigung ständig im Auge behalten und angemessene Vorsorge betreiben[921].

c) Rechtsfolgen

461 Ein Verstoß gegen die Organisationspflichten des § 33 Abs. 1 Nr. 1 WpHG zieht weder straf- noch ordnungswidrigkeitsrechtliche Folgen nach sich.[922] Da es sich um öffentliches Aufsichtsrecht handelt, kann ein Verstoß jedoch aufsichtsrechtliche Konsequenzen haben.[923]

462 Bei der Organisationsvorschrift des § 33 WpHG handelt es sich nicht um ein Schutzgesetz im Sinne von § 823 Abs. 2 BGB924, da die dort geregelten Pflichten zu unbestimmt sind, um aus ihrer Verletzung Individualansprüche ableiten zu können, und es sich lediglich um Hilfspflichten handelt, die der betriebsinternen Durchsetzung der Verhaltenspflichten der §§ 31, 32 WpHG dienen.[925] Deliktische Ansprüche sind allenfalls bei Verletzung eines der Rechtsgüter oder Rechte des § 823 Abs. 1 BGB oder bei vorsätzlich sittenwidriger Schädigung (§ 826 BGB) denkbar[926]. In Betracht kommen im Einzelfall zudem vertragliche Schadensersatzansprüche gegenüber dem Kunden wegen verschuldeter Nichterreichbarkeit des Wertpapierdienstleistungsunternehmens im Falle

---

[918] Schwark-*Schwark*, § 33 WpHG Rn. 6.

[919] *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 42.

[920] Erwägungsgründe 37 und 38 der Richtlinie 93/22/EWG des Rates vom 10. Mai 1993, ABl. Nr. L 141 vom 11. Juni 1993, 27.

[921] Assmann/Schneider-*Koller*, § 33 WpHG Rn. 6.

[922] Schwark-*Schwark*, § 33 WpHG Rn. 4; Assmann/Schneider-*Koller*, § 33 WpHG Rn. 50.

[923] *Balzer*, WM 2001, 1533 (1539); Assmann/Schneider-*Koller*, vor § 31 WpHG Rn. 17.

[924] BGH v. 8.5.2001 – XI ZR 192/00, BB 2001, 1865, 1867; *Kümpel*, Wertpapierhandelsgesetz, S. 162; Schwark-*Schwark*, vor § 31 WpHG Rn. 9; *Lang*, WM 2000, 451 (456); *Balzer*, WM 2001, 1533 (1540); *Hopt*, ZHR 159 (1995), 135 (161); *Spindler*, Unternehmensorganisationspflichten, S. 828; *Arendts*, ÖBA 1996, 775 (780); Assmann/Schneider-*Koller*, § 33 WpHG Rz. 1.

[925] *Balzer*, WM 2001, 1533 (1540); Schwark-*Schwark*, § 33 WpHG Rn. 4; Assmann/Schneider-*Koller*, § 33 WpHG Rn. 1.

[926] Assmann/Schneider-*Koller*, § 33 WpHG Rn. 1.

eines Systemausfalls[927]; allerdings strahlt § 33 WpHG nicht unmittelbar auf die schuldrechtliche Beziehung zwischen Anleger und Wertpapierdienstleistungsunternehmen aus[928].

d) Anhaltspunkte für IT-Konkretisierungen

463 Im Einzelnen verlangt § 33 Abs. 1 Nr. 1 WpHG das Vorhalten von persönlichen und sachlichen Mitteln, soweit diese für die richtige Ordnung des Geschäftsbetriebes erforderlich sind.[929] Die erforderlichen sachlichen Mittel beziehen sich auf die technische Ausstattung, insbesondere somit auch auf EDV-Systeme. Hinsichtlich der notwendigen Verfahren müssen die Wertpapierdienstleistungsunternehmen ausreichende Maßnahmen in Bezug auf die elektronische Datenverarbeitung treffen, so dass Unbefugten der Zugriff auf die Daten des Unternehmens verwehrt wird.[930] Die wertpapierhandelsrechtlichen Organisationsvorschriften verlangen außerdem Vorkehrungen im Hinblick auf Systemausfälle und –störungen.[931] Die Wertpapierdienstleistungsunternehmen haben hierzu Vorkehrungen zu treffen, die eine rasche Behebung technischer Fehler ermöglichen sowie ggf. Ersatzkapazitäten zu reservieren.[932] Auch die **Richtlinie gemäß § 35 Abs. 6 WpHG** zur Konkretisierung der Organisationspflichten von Wertpapierhandelsunternehmen gemäß § 33 Abs. 1 WpHG[933] fordert ausdrücklich Vorkehrungen, um bei Systemausfällen und –störungen Verzögerungen bei der Auftragsausführung oder –weiterleitung möglichst gering zu halten (Nr. 2.2).

4. Die MiFID

a) Hintergrund

464 Mit der Richtlinie über Märkte für Finanzinstrumente[934] und die konkretisierende Durchführungsrichtlinie bzw. -verordnung[935] werden vor allem zwei Ziele verfolgt: die

---

[927] Für Direktbanken *Balzer*, WM 2001, 1533 (1540 f.); *Balzer*, ZBB 2000, 259 (264).

[928] Assmann/Schneider-*Koller*, § 33 WpHG Rn. 1.

[929] *Balzer*, WM 2001, 1533 (1539).

[930] Assmann/Schneider-*Koller*, § 33 WpHG Rn. 9.

[931] Assmann/Schneider-*Koller*, § 33 WpHG Rn. 11a.

[932] *Balzer*, ZBB 2000, 258 (260); *Balzer,* WM, 2001, 1533 (1539); Assmann/Schneider-*Koller,* § 33 WpHG Rn. 11a.

[933] Assmann/Schneider-*Koller*, § 35 WpHG Rn. 8.

[934] Richtlinie 2004/39/EG des Rates und des Europäischen Parlamentes vom 21.4.2004 über Märkte für Finanzinstrumente, zur Änderung der Richtlinien 85/611/EWG und 93/6/EWG und der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 93/22/EWG, ABl. EG Nr. L 141 v. 30.4.2004, 1.

[935] Richtlinie 2006/73/EG der Kommission vom 10.8.2006 zur Durchführung der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates in Bezug auf die organisatorischen Anforderungen an Wertpapierfirmen und die Bedingungen für die Ausübung ihrer Tätigkeit sowie in Bezug auf die Definition bestimmter Begriffe für die Zwecke der genannten Richtlinie, ABl. EG Nr. L 241 v. 2.9.2006, 26; Verordnung (EG) Nr. 1287/2006 der Kommission v. 10.8.2006 zur Durchführung der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates betreffend die Aufzeichnungspflichten für

Verbesserung des Anlegerschutzes und die Förderung der Marktintegrität im Sinne von Fairness, Effizienz und Transparenz. Der Erreichung dieser Ziele dienen vor allem Organisationspflichten[936], die in Art. 13 MiFID, Art. 6, 7 DVO und Artt. 5-20 DRL geregelt sind und die Bereiche Compliance, Risikomanagement und Innenrevision betreffen.[937]

465 Der Referentenentwurf zur Umsetzung der MiFID vom 27.9.2006[938] sieht hinsichtlich der Ausführung von Wertpapiergeschäften Änderungen unter anderem am KWG und am WpHG vor, wobei hier nur die neuen Organisationsanforderungen von Interesse sind. Da die Anforderungen in § 33 WpHG und § 25a KWG zum Teil aber schon einen höheren Konkretisierungsgrad besitzen als die Vorgaben der MiFID, enthält der RefE keine bahnbrechenden Neuerungen[939]. Allerdings ist zu bedenken, dass sich die nationale Umsetzung nicht mit dem Verweis auf die Verwaltungspraxis, wie z.B. durch die MaRisk beeinflusst, begnügen kann, da dies nicht die nötige rechtliche Verbindlichkeit garantiert[940].

b) Pflichten und Adressat

466 Hinsichtlich des ersten Themenbereichs der Compliance enthält Art. 13 Abs. 2 MiFID die generalklauselartige Verpflichtung, angemessene Strategien und Verfahren anzuwenden, die sicherstellen, dass die Anforderungen der Richtlinie eingehalten werden. Eine Konkretisierung erfolgt in Art. 6 DRL in der Form, dass z.B. die Verpflichtung zur Aufspürung und Minimierung von Fehlerrisiken und zur Bestellung eines Compliance-Beauftragten zur Überwachung der Geschäftsprozesse festgeschrieben wird941.

467 Des Weiteren werden effiziente Riskmanagementsysteme vorgeschrieben; Art. 7 Ab. 1a DRL konkretisiert diese Anforderungen durch das Gebot, Risiken zu identifizieren und

---

Wertpapierfirmen, die Meldung von Geschäften, die Markttransparenz, die Zulassung von Finanzinstrumenten zum Handel und bestimmter Begriffe im Sinne dieser Richtlinie, ABl. EG Nr. L 241 v. 2.9.2006, 1. Bereits im Februar 2006 hatte die Kommission für ihre Entwürfe noch zwei begleitende Hintergrundanmerkungen beigefügt, abrufbar unter: http://ec.europa.eu.int/nternal_market/securities/isd/MiFID2_de.htm.

[936] *Spindler/Kasten*, AG 2006, 785; EuGH v. 11.8.1995 – Rs. C-433/93 – Kommission/Deutschland, Slg. 1995, I-2303 Rz. 18 ff.; v. 30.5.1991 – Rs. C-361/88 – Kommission/Deutschland, Slg. 1991, I-2567 Rz. 15 ff. – TA-Luft; *Ruffert* in: Callies/Ruffert, § 249 EGV Rz. 51; EUV/EGV-*Schroeder*, Art. 249 EGV Rz. 93 ff., 95.

[937] Zu allen Aspekten ausführlichich *Spindler/Kasten*, AG 2006, 785 ff.

[938] Abrufbar unter: http://www.bundesfinanzministerium.de/lang_de/DE/Geld__und__Kredit/Aktuelle__Gesetze/005__c,templateId=raw,property=publicationFile.pdf (zuletzt abgerufen am 22.11.2006)

[939] *Spindler/Kasten*, AG 2006, 785 (786).

[940] *Spindler/Kasten*, AG 2006, 785 (787).

[941] Zur weiteren Konkretisierung siehe *CESR*, CESR/05-24c, s. 13 ff.

einer individuellen Bewertung mit Hilfe von sog. Risikotoleranzschwellen zu unterziehen.

468 Zuletzt umfassen die Organisationspflichten auch eine Pflicht zur internen Revision (Art. 8 DRL), die unabhängig die Wirksamkeit der Systeme überprüfen und bewerten und auf dieser Grundlage Empfehlungen aussprechen soll.

469 Wie bereits dargelegt, werden sich die Änderungen an WpHG und KWG in Grenzen halten. Die neuen organisatorischen Anforderungen an die Wertpapierfirmen werden sich aus einem Verweis in § 33 WpHG auf den erweiterten § 25a KWG-RefE und aus spezifischen Vorschriften ergeben.

470 Im Hinblick auf das Outsourcing von Geschäftsprozessen enthält die MiFID kein Verbot, allerdings muss die Auslagerung wichtiger betrieblicher Aufgaben, also des Kernmanagements i.S.d. Art 13 DRL, im Unterschied zu untergeordneten Bereichen den besonderen Anforderungen des Art. 13 Abs. 5 1. Unterabs. Satz 2 MiFID genügen, wonach eine Auslagerung die Qualität der internen Kontrolle oder die Möglichkeit einer aufsichtsrechtlichen Überprüfung nicht beeinträchtigen darf. Der RefE zeichnet diese Unterscheidung nicht nach, sondern unterstellt sämtliche Auslagerungen, ob kritische Arbeitsbereiche betreffend oder nicht, den höheren Anforderungen. Die Möglichkeit der Auslagerung hängt von der Ordnungsmäßigkeit der Geschäftsorganisation, des angemessenen und wirksamen Risikomanagements und der Erhaltung der Verantwortung der Geschäftsleitung ab; im Rahmen des WpHG darf außerdem das Rechtverhältnis zum Kunden nicht verändert werden (Art. 14 Abs. 1 Ziff b) DRL).

471 Nach Art. 13 Abs. 6 MiFID sind Aufzeichnungen über alle Dienstleistungen und Geschäfte der Wertpapierfirmen anzufertigen um die Aufsichtsbehörde in die Lage zu versetzen, die Erfüllung der Verpflichtungen der Wertpapierfirma gegenüber ihrer Kunden überprüfen zu können. Art. 51 DRL sieht eine Archivierung dieser Aufzeichnung für fünf Jahre vor. Der RefE sieht in § 34 Abs. 1 und 2 die Umsetzung dieser Vorgaben vor; dabei sollen sämtliche Wertpapierdienstleistungen und –nebendienstleistungen, also auch die bloße Anlageberatung, erfasst werden.

472 Die MiFID regelt in Art. 18, 13 Abs. 3 explizit die Interessenkonflikte. Wertpapierfirmen haben alle angemessenen organisatorischen Vorkehrungen zu treffen, um Interessenkonflikte zwischen ihnen und ihren Kunden oder zwischen ihren Kunden untereinander zu erkennen und zu verhindern. Nach § 33 Abs. 1 Nr. 3 WpHG-RefE müssen In-

teressenkonflikte durch eine wirksame Organisation vermieden werden. Nur bei Unmöglichkeit müssen sind sie dem Kunden zu offenbaren[942].

c) Rechtsfolgen

473 Da die MiFID keine eigenen Regelungen zur Sanktionierung der genannten Pflichten enthält und auch die nach dem Referentenentwurf geplanten Änderungen des KWG und WpHG nicht die Rechtsfolgen betreffen, bleibt die oben dargestellte Rechtslage von der neueren Entwicklung unberührt.

d) Anhaltspunkte für IT-Konkretisierung

474 Konkrete Anhaltspunkte für die Umsetzung der Organisationspflichten im IT-Bereich sind nur vereinzelt vorhanden. So werden die Wertpapierfirmen etwa in Art. 13 Abs. 5 2. Unterabs. MiFID, das Risikomanagement betreffend, dazu verpflichtet, wirksame Kontroll- und Sicherheitsmechanismen für Datenverarbeitungssysteme einzurichten. Art. 5 Abs. 3 DRL enthält nur die Generalverpflichtung zur Überwachung und Sicherstellung der EDV-Systemsicherheit. Im Vergleich hierzu sind die Vorschriften in § 25a Abs. 1 Nr. 2 KWG zur Sicherheit von IT-Systemen deutlich präziser[943].

475 Die Einführung einer Aufzeichnung- und Archivierungspflicht hat auch für den IT-Bereich Bedeutung. Nach Art. 51 Abs. 2 sind Aufzeichnungen so auf einem Datenträger zu speichern, dass sie der Behörde leicht zugänglich gemacht werden können, wobei diese Aufzeichnungen insbesondere nicht anderweitig manipulierbar oder veränderbar sein dürfen.

5. Zwischenergebnis: besondere Verantwortlichkeit im Banken- und Finanzsektor

476 Im Banken-, Versicherungs- und Finanzsektor ist durch KWG, WpHG, VAG und die entsprechenden Mindestanforderungen, wie z.B. MaRisk, eine starke Aufsicht vorhanden. Die Pflichten sind auch hinsichtlich der Verwendung von Informationstechnik geregelt. Die Aufsichtsbehörde hat zusätzlich auch entsprechende Mittel, um diese Anfor-

---

[942] Zum gesamten Problemkomplex ausführlichich *Spindler/Kasten*, AG 2006, 785 (789 ff.); s. auch zu Interessenkonflikten allgemein Enriques, Conflicts of Interest in Investment Services: the Price and uncertain impact of MiFID's Regulatory Framework, University of Bologna, abrufbar unter http abrufbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id= 782828; dem Problem von Interessenkonflikten und Vermögensverwaltung widmet sich Kruithof, Conflicts of Interest in Institutional Asset Management: Is the EU Regulatory Approach adequate?, Financial Law Institute – Universiteit Gent, Working Paper Series, WP 2005, 07, Dec 2005; *Bolton/Freixas/Shapiro*, NBER, working paper series, No. 10571, abzurufen unter www.nber.org/papers/w10571; Cain/Loewenstein/Moore, J.Leg.Studies, 34 (2005), 1, abzurufen unter www.journals.uchicago.edu/JLS/journal/issues/v34n1/340105/340105.web.pdf.

[943] *Spindler/Kasten*, AG 2006, 785 (786).

derungen durchzusetzen. Zwar sind die Normen nicht als Schutzgesetze i.S.d. § 823 Abs. 2 BGB zu qualifizieren, durch die Möglichkeit, sie zur Konkretisierung der Verkehrssicherungspflichten im Rahmen des § 823 Abs. 1 BGB besteht aber dennoch ein enger Zusammenhang auch zur deliktischen Haftung.

6. Die Verteilung der Risiken bei Online-Bankgeschäften

477 In den letzten Jahren konnte ein stetig ansteigendes Auftreten neuartiger Bedrohungen des E-Commerce durch durch den Missbrauch im Internetverkehr verwendeter Legitimationsmedien beobachtet werden. Waren Angriffe auf die Sicherheit der Informationssysteme bislang meist von dem Wunsch getrieben, Störungen um ihrer selbst Willen zu verursachen (z.B. denial-of-serivce-Attacken), verlagert sich die Motivation zunehmend hin zu bloßem Gewinnstreben.[944] Besonders betroffen waren hierbei bislang die Kunden des Online-Banking,[945] insbesondere der Deutschen Bank, der Postbank sowie der Volks- und Raiffeisenbanken, aber auch die Kunden des Internet-Auktionshauses eBay. Angesichts der fortschreitenden Verlagerung des Wareneinkaufs in der Internet und der vermehrten Online-Abwicklung von Bankgeschäften, dürfte künftig eine Zunahme dieser Fälle zu verzeichnen sein, was – neben hier nicht zu behandelnden strafrechtlichen Konsequenzen[946] – verstärkt Fragen der zivilrechtlichen Haftung aufwirft. Entscheidend sind hierbei die Fragen der Risikoverteilung und Risikobeherrschung im Verhältnis von Unternehmer (hier: Bank) und Kunde beim Geschäftsverkehr im Internet (s. zum Online-Banking Rn. 509 ff.). Probleme bereiten im Haftungsfall vor allem die Beweisführung hinsichtlich einer Identitätstäuschung oder einer Pflichtverletzung des Nutzers.

478 Im Folgenden wird für das Online-Banking zunächst das Gefahrenpotential anhand dreier beispielhafter Szenarien (a)) dargestellt. Darauf folgt eine Untersuchung der Haftungsverteilung zwischen den Beteiligten (b)), welche sich in einem ersten Teil der materiellen Rechtslage (b)(1) bis b)(3)) und in einem zweiten der prozessualen Rechtslage widmet (b)(4)).

---

[944] Vgl. die Einschätzung der Mitteilung der EU-Kommission „Eine Strategie für eine sichere Informationsgesellschaft – ‚Dialog, Partnerschaft und Delegation der Verantwortung'" vom 31.5.2006, KOM(2006) 251 endgültig (abrufbar unter: http://eur-lex.europa.eu/LexUriServ/site/de/com/2006/com2006_0251de01.pdf). Ebenso der Symantec Internet Threat Report für das erste Halbjahr 2006 (abrufbar unter: http://www.symantec.com/specprog/threatreport/entwhitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf).

[945] Frankfurter Allgemeine Zeitung vom 11.7.2005: „Trickbetrüger nehmen Internet-Banking ins Visier" und vom 10.3.2006: „Angriffe auf Online-Bankkunden nehmen sprunghaft zu"; Süddeutsche Zeitung vom 2.8.2006: „Surfen am Abgrund"; Spiegel-Online vom 24.9.2006: „Phishing und Pharming – Die Bedrohung wächst", abrufbar unter: http://www.spiegel.de/netzwelt/technologie/0,1518,438677,00.html.

[946] Dazu *Popp*, NJW 2004, 3517.

a) Gefahrenpotential

(1) Szenario 1: Phishing[947], ohne Trojaner, mit Visual Spoofing

479 Angreifer A schickt dem Nutzer N eine E-Mail mit vorgetäuschter („gespoofter") Absender-Adresse der Hausbank B von N. Es handelt sich um eine HTML-Mail, die dem Layout einer typischen Mail von B entspricht und N auffordert, aus benannten Gründen PIN und TAN einzugeben. Die E-Mail enthält einen Link zum Webserver von A, auf dem das Online-Portal von B nachgebildet wurde. N ist halbwegs versiert und überprüft die einschlägigen Sicherheitsmerkmale der Online-Verbindung: URL im Adress-Feld, Schloss-Symbol und Zertifikatsinformationen (Fingerprint). Alle diese Merkmale werden jedoch mithilfe Aktiver Inhalte dem Original nachgebildet (Visual Spoofing), so dass N die Fälschung nicht bemerkt und seine Zugangsdaten arglos preisgibt. N ist die Freischaltung Aktiver Inhalte gewohnt, da auch das reguläre Portal von B nur mit Aktiven Inhalten nutzbar ist. A nutzt die Zugangsdaten, um eigene Transaktionen auszulösen.

(2) Szenario 2: Man-in-the-middle-Angriff mittels DNS-Spoofing/Pharming i. w. S.

480 Die kriminelle Organisation KO hat eine Schwachstelle in der BIND-Software (die am weitesten verbreitete DNS-Server-Software) entdeckt, bevor sie von den BIND-Entwicklern aufgedeckt wurde. Die Schwachstelle erlaubt, DNS-Server zu korrumpieren, indem der Angreifer DNS-Datensätze mit falschen Zuordnungen zwischen Domain-Namen und IP-Adressen einspielt. Nach erfolgtem Angriff liefert der DNS-Server falsche IP-Adressen als Antwort auf DNS-Anfragen aus.

481 KO gelingt es, den DNS-Server des Providers P so zu manipulieren, dass anstelle der korrekten IP-Adresse die IP-Adresse eines KO-Servers ausgeliefert wird, wenn DNS-Anfragen nach dem Online-Banking-Portal der Bank B eingehen. Auf diese Weise gelangt der Nutzer N des Online-Portals von B nicht auf den Bank-Server, sondern auf den Server von KO, auf dem das Online-Portal von B nachgebildet wurde. B setzt aus-

[947] Der Begriff leitet sich aus dem englichen „Password-Fishing" ab. Zur steigenden Anzahl von Phishing-E-Mails weltweit vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2005, S. 22 ff.(abrufbar unter: http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf). Dem Symantec Internet Threat Report zufolge, wurde im ersten Halbjahr 2006 ein Anstieg der Varianten von Phishing-E-Mails um 81 Prozent auf fast 160.000 Varianten registriert (S. 82 ff., abrufbar unter: http://www.symantec.com/specprog/threatreport/entwhitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf)

schließlich auf das PIN-TAN-Verfahren. N übersendet in bestem Glauben alle Zugangsdaten. Da das Portal die Eigenschaft hat, unmittelbar nach dem Zugang den Konto-Stand an den Kunden zu übermitteln, muss KO mit den Zugangsdaten von N Kontakt zum echten Portal aufnehmen, um die entsprechenden Daten an N übersenden zu können. KO übernimmt also die Rolle eines Man-in-the-middle.

482 Die von N initiierte Transaktion wird von KO manipuliert, d. h. vor allem Höhe und Empfänger der Transaktion werden verändert. An B wird die manipulierte Transaktion übermittelt, an N jedoch eine Bestätigung über die Ausführung der beabsichtigten Transaktion mit dem vermeintlich richtigen Kontostand. N beendet die Verbindung.

483 Der Angriff von KO beginnt Freitag abend in der Hoffnung, dass bei B signifikante Abweichungen möglichst spät entdeckt werden. Z. B. soll B möglichst spät erkennen, dass sich die Verbindungen zu einigen IP-Adressen häufen - nämlich zu den KO-Servern.

484 Dem Angriff lässt sich leicht begegnen, indem die Banken ihren Kunden die festen IP-Adressen der Online-Banking-Portale mitteilen und nicht die URL. Unter dieser Voraussetzung müsste der Angreifer Routing-Tabellen im Internet manipulieren oder Trojanische Pferde einsetzen, um den Online-Kunden auf seinen Server zu lotsen. DNS-Spoofing und die Manipulation des IP-Routing gelten als die Achillesfersen des Internet.

(3) Szenario 3: Pharming i. e. S., mit Trojaner

485 Mithilfe eines Interesse erweckenden E-Mail-Anhangs gelingt es dem Angreifer A, ein Trojanisches Pferd auf dem Rechner des Nutzers N zu platzieren. Der Trojaner ergänzt die „hosts"-Datei auf dem Rechner um den manipulierten Eintrag für das Online-Banking-Portal der Bank B. Daraufhin werden Aufrufe des Bank-Portals auf den Webserver von A geleitet. A übernimmt die Rolle eines Man-in-the-middle. Ansonsten entspricht der Angriff dem Szenario „Pharming im weiteren Sinne".

b) Haftungsverteilung zwischen den am Online-Banking Beteiligten

486 Nachdem die Bankpraxis nach Auftreten der ersten Schadensfälle durch Phishing und Pharming noch dahin ging, Schäden der Kunden (aus Kulanz) vollumfänglich zu ersetzen, stellen sich die Banken zunehmend auf den Standpunkt, der Kunde sei durch die Berichterstattung in den Medien und die Informationsarbeit der Banken hinreichend

über die Risiken des Online-Banking informiert. Schäden seien daher regelmäßig auf mangelnde Sorgfalt des Kunden zurückzuführen. Bislang sind – soweit ersichtlich – zwar noch keine Haftungsfälle vor Gericht gelangt, angesichts der Erfahrungen im Zusammenhang mit ec-Kartenmissbrauch ist jedoch zu erwarten, dass sich diese Linie durchsetzen wird und die Banken dem Kunden das Risiko des Phishing und Pharming zuweisen.

(1) Rechtliche Grundlagen des Online-Banking

487 Die Online-Bankgeschäfte bilden einen Ausschnitt aus dem Bereich des Direktbanking,[948] welcher neben der Abwicklung von Bankgeschäften über die herkömmlichen Kommunikationswege wie Brief, Telefon und Fax auch Online- und Homebanking umfasst.[949] Der Begriff des Online-Banking kann als Überbegriff für alle online abgewickelten Bankgeschäfte verwendet werden (Online-Banking i. w. S.). Von **Online-Banking i. e. S.** (früher: Btx) spricht man, wenn Bankgeschäfte über ein geschlossenes Netz, d.h. eine von einem Telekommunikationsunternehmen (z.B. T-Online, AOL) vermittelte, geschlossene Kunde-zu-Bank-Verbindung abgewickelt werden, für deren Nutzung eine Registrierung und Zulassung des Kunden durch den Netzbetreiber erforderlich ist.[950] **Homebanking** ist dem gegenüber nach gängiger Unterscheidung die Abwicklung von Bankgeschäften über ein offenes Netz wie das Internet.[951]

488 Der Zentrale Kreditausschuss (ZKA) hat für Online-Banking i.e.S. und Homebanking Musterbedingungen entwickelt,[952] welche sich im verwendeten **Sicherungsverfahren** unterscheiden,[953] im Übrigen aber nicht wesentlich von einander abweichen[954]. Die Sonderbedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN („**Online-Bedingungen**“) knüpfen an die Verwendung des PIN-/TAN-Verfahrens an und entsprechend weitgehend den alten Btx-Bedingungen. Daneben wurden für die Verwendung des HBCI-Verfahrens die Bedingungen für die konto-

[948] *Kümpel*, Bank- und Kapitalmarktrecht, 4.733.

[949] Ausführlich zu diesen Unterscheidungen *Bock* in: Bräutigam/Leupold, Kap. VII Rn. 3 ff.

[950] *Bock* in: Bräutigam/Leupold, Kap. VII Rn. 4; *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 1; *Hellner/Escher-Weingart*, in: Hellner/Steuer, Band 3, Teil 6/96; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 806.

[951] Vgl. das Homebanking-Abkommen vom 1.10.1997; *Bock* in: Bräutigam/Leupold, Kap. VII Rn. 4; *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 1, 27; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 806; *Hellner/Escher-Weingart*, in: Hellner/Steuer, Band 3, Teil 6/96.

[952] *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 109.

[953] *Borges*, in: Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bankrecht, § 8 Rn. 1.

[954] *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 27.

/depotbezogene Nutzung des Online-Banking mit elektronischer Signatur[955] („**Homebanking-Bedingungen**“) entwickelt.[956] Die Verwendung des einen oder anderen Sicherungsverfahrens ist gesetzlich nicht vorgeschrieben und folglich auch nicht an den Zugang über ein geschlossenes oder offenes Netz geknüpft. Das PIN-/TAN-Verfahren findet daher gegenwärtig auch im Internet Anwendung.[957] Das Homebanking-Abkommen verpflichtet die Banken jedoch, Online-Banking zumindest auch im HBCI-Dialog durchzuführen.[958] In der Praxis dürfte gegenwärtig das PIN-/TAN-Verfahren noch am weitesten verbreitet sein.[959]

489 Dem Online-Banking liegt im Verhältnis des Kunden zur Bank ein neben dem eigentlichen Girovertrag (und den Allgemeinen Bankenbedingungen) bestehender **Online-Bankingvertrag** zugrunde, welcher durch die Online-Bedingungen bzw. Homebanking-Bedingungen der Banken näher ausgestaltet wird.[960] Hierbei handelt es sich im Grundsatz um einen Geschäftsbesorgungsvertrag nach § 675 BGB.[961] Weist der Kunde die Bank beispielsweise an, einen bestimmten Betrag von seinem Konto auf ein anderes Konto zu überweisen, liegt der einzelnen Transaktion ein **Überweisungsvertrag** (§§ 676a ff. BGB) zugrunde. Ein solcher wird bei einer Online-Überweisung mittels elektronischer Willenserklärung[962] des Kunden durch Eingabe von PIN und TAN und konkludenter Annahme durch die Bank (§ 362 HGB) geschlossen.[963] Die Bank erwirbt aufgrund der Überweisung einen Aufwendungsersatzanspruch (§§ 670, 675 BGB) in Höhe des Überweisungsbetrages und belastet das Konto des überweisenden Kunden.[964]

(2) Vorschlag der EU-Kommission für eine Zahlungsdiensterichtlinie („SEPA“)

[955] Das Homebanking-Computer-Interface-Verfahren (HBCI) auf Grundlage des Homebanking-Abkommens von 1997 soll gegenüber dem PIN-/TAN-Verfahren eine höhere Sicherheit gewährleisten. Ausführlich dazu *Stockhausen*, WM 2001, 605 ff.

[956] Die Online-Bedingungen und Homebanking-Bedingungen sind abgedruckt in WM 2001, 650 ff. und *Gößmann*, in: Bankrechts-Handbuch, Band I, Anh. 6 und 7 zu §§ 52- 55, S. 1147 ff.

[957] *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 16; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 806.

[958] *Stockhausen*, WM 2001, 605 (611).

[959] *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 7; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 14.

[960] *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 30; *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 106; *Borges*, in: Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bankrecht, § 8 Rn. 14; *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 15.

[961] *Karper*, DuD 2006, 215 (216); *Werner*, in: Hoeren/Sieber, Kap. 13.5 Rn. 37.

[962] Zum Begriff *Bock* in: Bräutigam/Leupold, Kap. VII Rn. 43.

[963] Palandt-*Sprau*, § 676a BGB Rn. 11.

[964] *Kind/Werner*, CR 2006, 353; *Borges*, NJW 2005, 3313 (3315); *Karper*, DuD 2006, 215 (216); *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 179; MünchKommBGB-*Casper*, § 676a BGB Rn. 33.

490 Die künftige Rechtslage im Bereich des Online-Banking wird maßgeblich durch den europäischen Gesetzgeber mitbestimmt werden. Nachdem die EU-Kommission bereits 1997 in der – rechtlich nicht verbindlichen – **Empfehlung vom 30. Juli 1997** zu den Geschäften, die mit elektronischen Zahlungsinstrumenten getätigt werden[965] eine gewisse Hilfestellung bei der Ausformung der Rechte und Pflichten der Parteien im Online-Banking gegeben hatte, legte die Kommission Ende 2005 den Vorschlag für eine **Zahlungsdiensterichtlinie** vor.[966]

491 Im Interesse der Rechtssicherheit und eines hohen Verbraucherschutzniveaus strebt die EU eine europaweite **Harmonisierung der Hauptrechte und –pflichten** der Nutzer und Anbieter von Zahlungsdiensten an. Der Anwendungsbereich der Richtlinie erstreckt sich auf alle Zahlungsdienste gemäß Art. 2 Abs. 1 i.V.m. Anhang „Zahlungsdienste" unabhängig von der Art und Weise technischen Durchführung. Erfasst werden demnach ec-Kartensysteme ebenso wie Online-Banking. Gemäß ihrer Zielsetzung bezweckt die Richtlinie zwar die Verbesserung des **grenzüberschreitenden** Zahlungsverkehrs, im Interessen einer einheitlichen Rechtslage wird die auf europäischer Ebene gefundene Lösung jedoch wohl auch auf reine Inlandsfälle ausstrahlen.

492 Der Vorschlag regelt die wesentlichen **Sorgfaltspflichten** des Zahlungsdienstnutzers (Art. 46) und der Pflichten des Zahlungsdienstleisters (Art. 47) in Bezug auf Zahlungsverifikationsinstrumente. Der Nutzer ist danach verpflichtet, bei der Verwendung eines Zahlungsverifikationsinstruments die Bedinungen für dessen Ausgabe und Benutzung einzuhalten (Art. 46 lit. a), sowie dem Zahlungsdienstleister unverzüglich nach Feststellung den Verlust, Diebstahl, die widerrechtliche Aneignung oder die sonstige nicht autorisierte Verwendung des Zahlungsverifikationsinstruments anzeigen (Art. 46 lit. b). Der Zahlungsdienstleister hat hierzu die erforderlichen organisatorischen Vorkehrungen zu treffen (Art. 47 Abs. 1 lit. c). Ebenso muss der Dientleister sicherstellen, dass die personalisierten Sicherheitsmerkmale des Zahlungsverifikationsinstruments keiner anderen Person als dem Inhaber zugänglich sind (Art. 47 Abs. 1 lit. a). Detaillierte IT-spezifische Sorgfaltspflichten enthält der Vorschlag nicht.

---

[965] 97/489/EG: Empfehlung der Kommission vom 30. Juli 1997 zu den Geschäften, die mit elektronischen Zahlungsinstrumenten getätigt werden (besonders zu den Beziehungen zwischen Emittenten und Inhabern solcher Instrumente) (Text von Bedeutung für den EWR), ABl. Nr. L 208 vom 2. August 1997, S. 52 ff.

[966] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt und zur Änderung der Richtlinien 97/7/EG, 2000/12/EG und 2002/65/EG vom 1. Dezember 2005, KOM (2005), 603 endg. (von der Kommission vorgelegt)

493 Ebenso trifft der europäische Gesetzgeber eine ausdrückliche Regelung der **Beweislastverteilung** bei strittiger Autorisierung (Art. 48). Bestreitet der Zahlungsdienstnutzer einen abgeschlossenen Zahlungsvorgang, hat die Bank nachzuweisen, dass der Zahlungsvorgang authentifiziert war, ordnungsgemäß aufgezeichnet und verbucht und nicht durch eine technische Panne oder einen anderen Mangel beeinträchtigt worden ist (Abs. 1). Streitet der Nutzer die Autorisierung der Zahlung auch nach Vorlage dieser Nachweise noch ab, hat er seinerseits Fakten oder Umstände vorzutragen, die die Vermutung zulassen, dass er die Zahlung nicht autorisiert und nicht in betrügerischer Absicht oder grob fahrlässig in Bezug auf die ihm nach Artikel 46 lit. b obliegenden Pflichten (Rn. 492) gehandelt haben kann (Abs. 2). Im Fall des Online-Banking könnte hierzu unter Umständen schon die Anzeige eines Diebstahls der Legitimationsmedien oder Vorliegen einer Phishing-Mail bzw. eines Trojaners auf dem Rechner des Kunden ausreichen. Um diese Vermutung zu widerlegen und nachzuweisen, dass der Zahlungsdienstnutzer die Zahlung autorisiert bzw. in betrügerischer Absicht oder in Bezug auf die ihm gemäß Artikel 46 obliegenden Pflichten grob fahrlässig gehandelt hat, reicht die vom Zahlungsdienstleister aufgezeichnete Nutzung eines Zahlungsverifikationsinstruments allein nicht aus (Abs. 3). Die bloße Verwendung von PIN und TAN könnte danach nicht mehr zur Begründung eines Anscheinsbeweises für Urheberschaft oder pflichtwidriges Handeln des Kunden herangezogen werden.[967]

494 Der Zentrale Kreditausschuss (ZKA) hat die Regelung des Art. 48 Abs. 3 des Entwurfs als unausgewogen kritisiert und hierbei insbesondere auf die Gefahr betrügerischer Handlungen von Kunden unter Ausnutzung der Beweisregel hingewiesen. Der ZKA fordert, die bisherigen Beweislastgrundsätze (im deutschen Recht damit den Anscheinsbeweis) beizubehalten, da andernfalls das Online-Banking-Angebot eingeschränkt oder erheblich verteuert werden müsste. Die vom BGH[968] zu ec-Karten bestätigen Grundsätze zum Anscheinsbeweis sollten durch gesetzgeberische Maßnahmen auf europäischer Ebene nicht angetastet werden.[969]

---

[967] Siehe zu dieser Einschätzung auch *Burgard*, WM 2006, 2065 (2069) zum Anscheinsbeweis bei ec-Kartenmissbrauch.

[968] BGH NJW 2004, 3623 ff..

[969] Anmerkungen des Zentralen Kreditausschusses zum Vorschlag der Europäischen Kommission für eine „Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt und zur Änderung der Richtlinien 97/7/EG, 2000/12/EG und 2002/65/EG“ vom 1. Dezember 2005 (KOM[2005] 603 endgültig), S. 5, 38 f., abrufbar unter http://www.bankenverband.de/pic/artikelpic/022006/sp0602_eu_NLF-ZKA_final_dt.pdf

495 Die Bestimmungen über die **Haftung des Kunden** (Art. 50) sehen eine Haftungshöchstgrenze von € 150 für Schäden vor, die vor Erfüllung der Anzeigepflicht gemäß Art. 46 lit. b aus der Verwendung eines verlorenen oder gestohlenen Zahlungsverifikationsinstruments entstanden sind. Dagegen haftet der Nutzer ohne Haftungshöchstbetrag für alle Schäden die durch nicht autorisierte Zahlungsvorgänge entstanden sind, wenn er sie in *betrügerischer Absicht* oder durch *grobe Fahrlässigkeit* gegenüber den ihm nach Artikel 46 obliegenden Pflichten herbeigeführt hat. Nach Anzeige des Verlusts, des Diebstahls oder der widerrechtlichen Aneignung des Zahlungsverifikationsinstruments beim Zahlungsdienstleister trägt der Zahler keinerlei finanzielle Folgen aus der Verwendung des verlorenen, gestohlenen oder widerrechtlich angeeigneten Instruments, es sei denn, er hat in betrügerischer Absicht gehandelt.

(3) Materiell-rechtliche Rechtslage

496 Bei Fällen der Identitätstäuschung aufgrund Phishing und Pharming stellt sich nach derzeitiger Rechtslage die Frage, ob die Bank vom Kunden die Erstattung des Überweisungsbetrages verlangen kann. Als Anspruchsgrundlagen kommt ein Aufwendungsersatzanspruch (unten (a)) oder ein Schadensersatzanspruch (unten (b)) in Betracht. Eine verschuldensunabhängige Haftung des Bankkunden aufgrund von AGB-Klauseln kommt hingegen nicht in Betracht, dazu unten (d).

(a) Aufwendungsersatzanspruch der Bank

(i) Vertragsschluss

497 Ein Aufwendungsersatzanspruch der Bank gemäß §§ 670, 675, 676a BGB auf Erstattung des überwiesenen Betrages beruht auf vertraglicher Grundlage und setzt damit einen wirksam zustande gekommenen Überweisungsvertrag zwischen dem Kunden und der Bank in Bezug auf die konkret ausgeführte Transaktion voraus. Gelingt einem Angreifer aufgrund einer Phishing- oder Pharming-Attacke die Veranlassung einer Überweisung, so kommt zwischen Kunde und Bank **kein Vertragsschluss** zustande.[970] Die Problematik liegt hierbei in der Praxis im Bereich der Beweislast. Denn die Bank wird sich auf den Standpunkt stellen, dass die Erklärung, welche aufgrund der Verwendung des einschlägige Legitimationsmediums (z.B. PIN und TAN) dem Kunden (objektiv) zuzurechnen ist, auch tatsächlich von diesem oder einem autorisierten Dritten

[970] *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 81; Palandt-*Sprau*, § 676a BGB Rn. 11.

stammt.[971] Verlangt die überweisende Bank nun vom Kunden Aufwendungsersatz, steht sie – wenn der Kunde den Vertragsschluss bestreitet – vor dem Problem im Prozess die anspruchsbegründende Tatsache des Vertragsschlusses beweisen zu müssen (dazu ausführlich unten Rn. 559 ff.).[972] Das Risiko einer gefälschten Überweisung trägt grundsätzlich die Bank.[973] Denkbar wäre jedoch auch mit einem Teil der Literatur eine Rechtsscheinshaftung des Kunden anzunehmen (dazu sogleich).

(ii) Bindung kraft Rechtsscheins

498 Aus Sicht der Bank unterscheidet sich ein gefälschter Online-Überweisungsautrag, welcher unter Verwendung des Legitimationsmediums des Kunden (z.B. PIN/TAN, HBCI, elektronische Signatur) erstellt wurde, nicht von einem vom Berechtigten Kontoinhaber stammenden Auftrag. Es entsteht mithin der **Schein einer ordnungsgemäßen Willenserklärung** des Bankkunden. Ein Teil der Literatur leitet eine Bindung des Bankkunden gegenüber der Bank folglich aus Rechtsscheinsgrundsätzen her.

499 Schon im Rahmen des **Btx-Systems** wurde für den missbräuchlich handelnden Dritten eine Anscheinsvollmacht angenommen und dem Inhaber des Btx-Anschlusses damit die Erklärung des Dritten zugerechnet, wenn er den Mißbrauch von PIN und TAN ermöglich hatte.[974] In den meisten Verfahren, welche eine behauptete missbräuchliche Verwendung von ec-Karten zum Gegenstand hatten, wurde dagegen keine Rechtsscheinshaftung angenommen, sondern nur ein Anscheinsbeweis zugunsten der Tatsache, dass der Karteninhaber oder ein von ihm autorisierter Dritter gehandelt hat (näher Rn. 569).[975] Allerdings ist einzuräumen, dass die Rechtsprechung diese Frage kaum thematisiert hat. Allerdings hat sich der BGH im Rahmen von R-Gesprächen zum Thema der Anscheinsvollmacht geäußert und klargestellt, dass die entwickelten Grundsätze der Anscheinsvollmacht, also eine „gewisse Dauer und Häufigkeit", für ein Greifen unbedingt vorliegen müssen.[976] Für Internet-Auktionen haben Instanzgerichte in neueren Entscheidungen eine Anscheinsvollmacht zwar nicht grundsätzlich abgelehnt, aber die

[971] So auch *Borges*, NJW 2005, 3313 (3316).

[972] *Borges*, NJW 2005, 3313 (3316); *Karper*, DuD 2006, 215 (218).

[973] BGH NJW 2001, 2968 (2969); BGH NJW 1994, 2357 (2358); BGH NJW 1994, 3344 (3345).

[974] So für über Btx getätigte Rechtsgeschäfte: OLG Oldenburg NJW 1993, 1400 (1401); OLG Köln NJW-RR 1994, 177 (178); LG Ravensburg NJW-RR 1992, 111; LG Koblenz NJW 1991, 1360.

[975] Vgl. etwa KG NJW 1992, 1051 (1052); LG Bonn NJW-RR 1995, 815; LG Darmstadt WM 2000, 911 (913 f.); LG Frankfurt WM 1999, 1930 (1932 f.); LG Hannover WM 1998, 1123 f.; LG Köln WM 1995, 976 (977 f.); AG Frankfurt NJW 1998, 687 f.; AG Osnabrück NJW 1998, 688 f.

[976] BGH JZ 2006, 1073 (1074) mit Anm. *Lobinger*.

Zurechenbarkeit des Rechtsscheins und – im Hinblick auf den derzeitigen Sicherheitsstandard des Internet – ein schutzwürdiges Vertrauen des Klägers verneint.[977]

500 Soweit die Literatur zum Online-Banking eine Rechtsscheinshaftung bejaht, verweist sie auf die Grundsätze der Anscheinsvollmacht[978] oder nimmt in Fortbildung dieser Grundsätze eine besondere Rechtsscheinsvollmacht an,[979] wobei sie den Rechtsschein jeweils mit dem hohen technischen Sicherheitsstandard der Online-Banking-Systeme begründet.[980]

(a) Anscheinsvollmacht

501 Eine Bindung des Kunden an eine gefälschte elektronische Willenserklärung kraft Anscheinsvollmacht ist mit der überwiegenden Meinung abzulehnen.[981] Ein „Normalfall" der Anscheinsvollmacht[982] liegt beim Online-Banking schon deshalb nicht vor, da der objektive Rechtsscheinstatbestand nicht auf dem (mehrfachen) Auftreten eines anderen als Vertreter beruht, sondern vielmehr von einem Handeln des Kunden selbst ausgegangen wird.[983]

502 Typisch für die Fälle der Anscheinsvollmacht ist überdies das Handeln eines Dritten, der aus der Sphäre des Vertretenen stammt, etwa aus dessen Unternehmen, und dessen Handlungen grundsätzlich vom Vertretenen kontrolliert werden können.[984] Demgegenüber kennzeichnen sich die Sachverhalte, in denen elektronische Legitimationsmedien mißbräuchlich verwandt wurden, im Wesentlichen durch den (behaupteten) Eingriff Dritter, die nicht dem „Lager" des Kunden entstammen, sondern unbekannt agieren.

---

[977] OLG Hamm NJW 2007, 611; OLG Köln MMR 2006, 321 (322); LG Bonn MMR 2004, 179 (180); LG Bonn MMR 2002, 255 (257) bestätigt von OLG Köln MMR 2002, 813 (814); dazu auch *Wiebe*, in: Spindler/Wiebe, Internet-Auktionen und Elektronische Marktplätze, Kap. 4 Rn. 65 ff.; ebenso *Borges*, NJW 2005, 3313 (3316).

[978] So *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 26; Baumbach/Hopt-*Hopt* (7) Bankgeschäfte F/35; allgemein zur Anscheinsvollmacht Palandt-*Heinrichs*, § 172 BGB Rn. 11 ff.; MünchKommBGB-*Schramm*, § 167 BGB Rn. 54 ff.

[979] Zur „Btx-Rechtsscheinsvollmacht" *Lachmann*, NJW 1984, 405 (408); für Btx im Bankbereich unter Verwendung von PIN und TAN auch *Borsum/Hoffmeister*, NJW 1985, 1205 (1206).

[980] *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 26; zum Btx-System LG Ravensburg CR 1992, 472 (473); *Lachmann*, NJW 1984, 405 (408); *Borsum/Hoffmeister*, NJW 1985, 1205 (1206).

[981] *Borges*, NJW 2005, 3313 (3315); *Kind/Werner*, CR 2006, 353; *Kunst*, MMR Beilage 9/2001, 23 (24); *Wiesgickl*, WM 2000, 1039 (1047); *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 82; *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 145 f.

[982] Eine Anscheinsvollmacht liegt nach den anerkannten Grundsätzen der Rechtsprechung vor, wenn der Vertretene das Handeln des Vertreters nicht kennt, er es aber bei pflichtgemäßer Sorgfalt hätte erkennen können und der andere Teil annehmen durfte, der Vertretene dulde und billige das Handeln des Vertreters.

[983] So auch *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 82.

[984] Paradigmatisch etwa der Fall BGH NJW 1998, 1854; vgl. ferner die Auflistung der einschlägigen Rechtsprechungsfälle bei Soergel-*Leptien*, § 167 BGB Rn. 31 ff.; schließlich MünchKommBGB-*Schramm*, § 167 BGB Rn. 61 („Organisationsmangel") sowie Rn. 64 („Organisationsrisiko"); ausführlich *Recknagel*, Vertrag und Haftung beim Internet Banking, S. 137 f.

503 Weitere Voraussetzung für eine solche Zurechnung qua Anscheinsvollmacht ist aber nach wie vor, daß der Dritte für eine gewisse Dauer und wiederholt für den vermeintlich Vertretenen aufgetreten ist.[985] An beiden Merkmalen läßt sich aber für missbräuchliche Erklärungen im Internet im Bereich des Online-Banking mit Fug und Recht zweifeln: es fehlt bei einem einmaligen oder nur kurzzeitig andauernden Missbrauch an der erforderlichen Dauer, um von einem entsprechend zurechenbaren, gesetzten Rechtsschein ausgehen zu können.[986] Dauert der Missbrauch längere Zeit an, so greifen im Übrigen bereits die entsprechenden Kontroll- und Meldepflichten des Kunden gegenüber der Bank ein, so dass die Bank Schadensersatzansprüche gegen den Kunden wegen Vertragspflichtverletzung geltend machen kann.[987]

504 Aus dogmatischer Sicht kann dieses Unbehagen gegenüber einer Anscheinsvollmacht schließlich damit begründet werden, daß hier statt einer Zurechnung einer Erklärung, die auf einer Handlung und einem Erklärungsbewußtsein beruhen müsste, letztlich eine Haftung auf das positive Interesse für die **fahrlässige Verletzung von rechtsverkehrsbezogenen Sorgfaltspflichten** eingeführt wird, ein Tatbestand, wie er für die Pflichtverletzungen im vorvertraglichen Stadium eher typisch ist.[988] Eine weit verbreitete Lehre möchte die Anscheinsvollmacht daher insgesamt auf den Handelsverkehr beschränken.[989]

(b) Allgemeine Haftung für fahrlässig gesetzte Rechtsscheinstatbestände?

505 Ein Teil der Literatur bejaht eine besondere Rechtsscheinsvollmacht in Fortbildung der Grundsätze zur Anscheinsvollmacht, wobei jedoch auf das Erfordernis der „gewissen Häufigkeit und Dauer“ verzichtet werden soll.[990] Bei R-Gesprächen lehnt der BGH in der Regel den herkömmlichen Anscheinsvollmacht ab. Allerdings komme eine Rechtsscheinshaftung bei R-Gesprächen aber doch in Betracht, wenn ein Minderjähriger wie-

---

[985] BGH NJW 1998, 1854 (1855); BGH NJW-RR 1986, 1169; OLG Dresden NJW-RR 1995, 803 (804); MünchKommBGB-*Schramm*, § 167 BGB Rn. 68; Palandt-*Heinrichs* § 172 BGB Rn. 12; Soergel-*Leptien*, § 167 BGB Rn. 21.

[986] Wie hier *Siebert*, Das Direktbankgeschäft, S. 133; *Langenbucher*; Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 146; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 138 f.

[987] *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 139.

[988] So insbesondere *Flume,* AT II, § 49, 3, 4; dem folgend *Medicus*, Bürgerliches Recht, Rn. 101; *Pawlowski*, Allgemeiner Teil des BGB, Rn. 720; Staudinger-*Schilken*, § 167 BGB Rn. 31; *Erfurth*, WM 2006, 2198 (2200); *Wiesgickl*, WM 2000, 1039 (1047); *Werner*, Bankrecht und Bankpraxis, Rn. 19/349; *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 25; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 138.

[989] *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, S. 48 ff.

[990] Zur „Btx-Rechtsscheinsvollmacht“ *Lachmann*, NJW 1984, 405 (408); für Btx im Bankbereich unter Verwendung von PIN und TAN auch *Borsum/Hofmeister*, NJW 1985, 1205 (1206); im Ergebnis wohl ebenso *Dörner*, AcP 202 (2002), 363 (390 f.).

derholt und über gewisse Dauer R-Gespräche angenommen hat und der Anbieter durch das Begleichen der Rechnung durch den Anschlussinhaber davon ausgehen konnte, dass dieser die Inanspruchnahme dulde.[991] Das bedeutet, dass der BGH gerade nicht auf das anerkannte Merkmal der „gewissen Häufigkeit und Dauer" verzichten will. Gegen die Annahme einer Rechtsscheinshaftung beim Online-Banking spricht indessen, dass die gesetzlich geregelten Fälle der Rechtsscheinshaftung im nicht-kaufmännischen Verkehr[992] für die Zurechnung eines Rechtsscheins grundsätzlich die **bewusste Schaffung des Rechtsscheinstatbestandes** (z.B. §§ 170 ff., 405 BGB) verlangen.[993] Insbesondere im Verbraucherbereich dürften an die Zurechnung fahrlässig gesetzter Rechtsscheine daher hohe Anforderungen zu stellen sein.[994] Die Anscheinsvollmacht durchbricht den genannten Grundsatz insoweit, als sie Fahrlässigkeit als Zurechnungsgrund ausreichen lässt (zur rechtsdogmatischen Kritik oben Rn. 504). Dies lässt sich indessen nur unter Hinweis, wie auch vom BGH bei R-Gesprächen bekräftigt,[995] auf die Anforderungen des objektiven Rechtsscheinstatbestandes – mehrmaliges Auftreten des Vertreters von gewisser Dauer – rechtfertigen. Der Vertretene hat aufgrund der zeitlichen Streckung des Rechtsscheinstatbestandes insbesondere die Möglichkeit das Handeln des Dritten (der noch dazu seiner Sphäre entstammt) zu erkennen und zu verhindern. Versäumt er dies, stellt die Rechtsprechung die fahrlässige Nichtverhinderung des Handelns des Vertreters dem bewussten Dulden gleich.[996]

506 Beim Online-Banking wird im Regelfall nur ein einmaliger Identitätsmissbrauch vorliegen. Der dadurch entstandene Rechtsschein kann dem Kunden auch dann nicht zugerechnet werden, wenn ihm im Einzelfall – etwa bei Beantwortung einer Phishing-E-Mail – eine Sorgfaltspflichtverletzung vorzuwerfen sein sollte. Denn vor dem eigentlichen Missbrauch besteht zwar die abstrakte Gefahr eines Angriffs Dritter. Anders als bei der Anscheinsvollmacht wird der Bankkunde jedoch nicht durch konkrete Anhalts-

---

[991] BGH JZ 2006, 1073 (1074) mit Anm. *Lobinger*.

[992] Nach §§ 56, 362 HGB wird im kaufmännischen Verkehr ein Rechtsschein auch rein objektiv zugerechnet. Dazu *Langenbucher*, die Risikozuordnung im bargledlosen Zahlungsverkehr, S. 25.

[993] *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, S. 51, 477 ff.; *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 25, 146 mwN. Gleiches gilt für die Duldungsvollmacht und den Blankettmissbrauch (§ 172 BGB analog), BGH NJW 1996, 1469 ff.; *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, S. 62. Auch bei der abhanden gekommenen Vollmachtsurkunde genügt die bloße Fahrlässigkeit des Vertretenen nicht, siehe BGH NJW 1975, 2101 (2102).

[994] In diese Richtung auch *Canaris*, Bankvertragsrecht, Rn. 527 ff. Zum Streit um die Anscheinsvollmacht im nicht-kaufmännischen Bereich *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, S. 48 ff.

[995] BGH JZ 2006, 1073 (1074) mit Anm. *Lobinger*.

[996] Die Anscheinsvollmacht entpuppt sich somit als abgeschwächte Duldungsvollmacht. Bei der Duldungsvollmacht begründet bereits das erstmalige Auftreten als Vertreter den Rechtsschein, jedoch nur deshalb, weil der Vertretene das Handeln bewusst duldet, Palandt-*Heinrichs*, § 172 BGB Rn. 8.

punkte für ein Missbrauchsverhalten Dritter für Schutzmaßnahmen sensibilisiert. Somit mag zwar ein punktuelles Fehlverhalten vorliegen (bspw. die sorglose Weitergabe von PIN und TAN im Zusammenhang mit Phishing-Mails), dieses genügt jedoch nicht, um es in der Rechtswirkung dem bewussten Dulden gleich zu stellen; es begründet vielmehr allenfalls eine zum Schadensersatz verpflichtende **Vertragspflichtverletzung**.[997] Eine Gleichstellung mit den Fällen der Anscheinsvollmacht müßte überdies die Beherrschbarkeit des eingesetzen Mediums und des Mißbrauchs Dritter in gleichem Maße wie im Falle des Risikos des in der Organisationsphäre eingesetzten Gehilfen postulieren - woran erhebliche Zweifel bestehen.

507 Gegen eine Lösung nach Rechtsscheinsgrundsätzen spricht im Bereich des E-Commerce und des Online-Banking im Besonderen, dass ein Schadensersatzanspruch **flexiblere Lösungen** erlaubt als eine pauschale Zurechnung kraft Rechtsscheins. Der Vorteil einer Lösung über Schadensersatzregeln liegt hierbei insbesondere die Berücksichtigung eines **Mitverschuldens** der Bank (§ 254 BGB) bei der Bemessung der Schadenshöhe.

(b) Schadensersatzansprüche der Bank

508 Verletzt der Kunde schuldhaft seine Sorgfaltspflichten aus dem Online-Bankingvertrag, haftet er der Bank für entstandene Schäden gemäß **§§ 280 Abs. 1, 241 Abs. 2 BGB**. Die Online- und Homebanking-Bedingungen enthalten keine eigene Haftungsregelung (mehr), vielmehr kommt die Haftungsregelung der Ziffer 3 der AGB-Banken zur Anwendung, welche eine **verschuldensabhängige Haftung** vorsieht.[998] Diese Haftungsklausel entspricht dem gesetzlichen Leitbild und ist mit § 307 BGB vereinbar.[999] Wie nunmehr auch im österreichischen Recht anerkannt,[1000] kann die Bank das Risiko für ein (von ihr nicht verschuldetes) Versagen der Sicherheitssysteme nicht im Wege einer verschuldensunabhängigen Risikohaftung auf den Kunden verlagern. Für die Haftung beim Online-Banking ist dabei entscheidend die Pflichtenverteilung zwischen Kunde und Bank, die gerade im IT-spezifischen Bereich bislang wenig geklärt ist. Gerichtliche Entscheidungen zu den Pflichten im Zusammenhang mit Online-Banking liegen soweit ersichtlich noch nicht vor.

---

[997] Im Ergebnis ebenso *Langenbucher*, Die Risikozuordnung im bargeldosen Zahlungsverkehr, S. 146.

[998] *Borges*, NJW 2005, 3313 (3314); *Kind/Werner*, CR 2006, 353 (354); *Karper*, DuD 2006, 215 (216); *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 81; *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 146.

[999] *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 178.

[1000] OGH 4 Ob 179/02f, s. *Fallenböck* – Annex II – Rn. 1146 ff. mwNachw.

(i) Interessenlage und Zurechnungskriterien

509 Der Bank obliegen als Initiator des Online-Banking Pflichten zur Sicherung der in diesem Verfahren getätigten Bankgeschäfte. Dahinter steht die Wertung, dass die Bank durch die Eröffnung des Online-Verkehrs ein Risiko veranlasst hat,[1001] welches sie mit ihren personellen, finanziellen und technischen Ressourcen besser beherrschen kann als der Kunde.[1002] Hinzu kommt die Möglichkeit der Banken Sicherungsaufwand und Schäden auf durch entsprechende Preisgestaltung umzulegen.[1003] Die Kreditinstitute entscheiden in eigener Verantwortung über das angebotene Sicherungssystem und steuern damit gerade im Hinblick auf neue Formen von Bedrohungen aus dem Internet das beim Kunden verbleibende Restrisiko und die von ihm zu treffenden Sicherungsmaßnahmen. So verwenden einige Banken noch immer Aktive Inhalte in ihren Webangeboten, welche auf der Kundenseite ein großes Angriffspotential eröffnen (näher Rn. 522). Hinzu kommt ein großer Informationsvorsprung der Banken gerade auch im Hinblick auf neu auftretende Bedrohungsformen.[1004]

510 Die Banken ziehen aus dem Online-Banking beträchtliche eigene Vorteile. Diese liegen in der Einsparung von Personal, Filialen und – zeitgeistgerecht – jederzeitiger Erreichbarkeit der Bank für den Kunden und der Möglichkeit einer Marktexpansion ohne größeren Investitionsaufwand.[1005] Man wird zwar zugeben müssen, dass Online-Banking – etwa in Form geringerer Überweisungsgebühren und Unabhängigkeit von Banköffnungszeiten – auch dem Bankkunden Vorteile bietet. Bei wertender Betrachtung liegen die Vorteile indessen überwiegend auf seiten der Bank, die sich überdies an die breite Masse der Bankkunden wendet und nicht nur an den technisch versierten Internet-Nutzer.[1006] Wegen höherer Transaktionskosten beim herkömmlichen Bankgeschäft schafft die Bank zudem selbst Anreize, durch den Abbau von Filialen – etwa in ländlichen Gebieten – aber auch faktischen Zwang zur Inanspruchnahme ihres Online-Angebots.

511 Auch wenn Vorteile und Risiken somit vornehmlich bei der Bank liegen, wird man den Bankkunden nicht aus allen Sorgfaltspflichten entlassen können. Der Kunde verfügt mit

---

[1001] Zu ähnl. Erwägungen im Rahmen der Rechtsprechung zu Dialern s. BGH MMR 2004, 308 (311); LG Stralsund MMR 2006, 487 (488).

[1002] Ebenso *Erfurth*, WM 2006, 2198 (2206).

[1003] *Erfurth*, WM 2006, 2198 (2206).

[1004] Ebenso *Kind/Werner*, CR 2006, 353 (356).

[1005] So auch *Erfurth*, WM 2006, 2198 (2206).

[1006] *Spindler*, in: Hadding/Hopt/Schimansky, S. 179; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 225 f.

seinem privaten Computer über eine **potentielle Gefahrenquelle** (allgemein Rn.282). Hinzu kommt, dass bei Phishing und Pharming der PC des Kunden das primäre Angriffsziel bildet und Sicherheitsvorkehrungen somit notwendig auch beim Kunden (seinem PC) selbst ansetzen müssen. Ein maßgeblicher Gesichtspunkt ist hierbei die **Möglichkeit des Selbstschutzes** (allg. Rn.294 ff.), d.h. inwieweit der Kunde mit einfachen und kostengünstigen Mitteln eigene Schutzvorkehrungen treffen kann, wobei aber insbesondere im technischen Bereich keine überzogenen Anforderungen an die Sorgfalt des Durchschnittsnutzers gestellt werden dürfen (näher unten Rn. 538 ff.).

512 Anders als in den ec-Karten-Fällen, in denen viele Sachverhalte sich dem gesunden Menschenverstand erschließen, etwa die Aufbewahrung einer ec-Karte zusammen mit der PIN in einem Jacket im Büro etc,[1007] ist das Bewußtsein für IT-Risiken wesentlich geringer ausgeprägt, da die technischen Vorgänge komplex und für den überwiegenden Teil der Kunden schwer zu durchschaubar sind. Dies trifft in besonderem Maße auf die neuen Bedrohungslagen des Phishing und Pharming zu, welche den meisten Online-Banking-Kunden nicht oder nur wenig bekannt sind.

513 Um entsprechende Sorgfaltspflichten im Umgang mit den Legitimationsmedien beim Online-Banking anzunehmen, die sich auch auf Risiken des EDV-Einsatzes beziehen, muß ein Mehr an Aufklärung und Information sowie an Sicherungsmaßnahmen seitens der das System einsetzenden Bank verlangt werden. Erst die Weitergabe des nötigen Wissens und die Schaffung eines Risikobewusstseins auf Seiten des Kunden versetzt diesen bei technisch komplexen Dienstleistungen in die Lage, die angemessenen Sicherheitsvorkehrungen zu ergreifen. Die vom Kunden verlangten Pflichten sind daher stets im Lichte der Pflichten, die der Bank obliegen, zu sehen. Ob mangels ausreichender Aufklärung und Instruktion bereits eine Pflichtverletzung des Bankkunden zu verneinen oder der Anspruch der Bank nach § 254 BGB zu kürzen ist, wird sich nur im Einzelfall beurteilen lassen.

514 In ähnlicher Weise formt auch das österreichische Recht die Pflichten der Bank und des Kunden aus, wobei indes auch hier noch viele Einzelheiten anscheinend nicht letztlich geklärt sind.[1008]

(ii) Pflichten der Bank

[1007] S. etwa für den vergleichbaren Fall der gemeinsamen Aufbewahrung von ec-Karte und Scheckvordrucken in einem im Büro aufgehängten Jackett AG Hannover WM 1996, 2013 f.; s. auch LG Köln NJW-RR 2001, 1340 (1341).

[1008] S. *Fallenböck* – Annex II – Rn. 1153 f. mit weiteren Einzelheiten und Nachw.

515 Die Bestimmung der Pflichten der Bank erlangt in zweifacher Hinsicht Bedeutung: zum einen kann die Verletzung der die Bank treffenden Vertragspflichten nach §§ 280 Abs. 1, 241 Abs. 2 BGB eine **Schadensersatzhaftung** gegenüber dem Kunden begründen, zum anderen beeinflussen die Sorgfaltsanforderungen der Bank – quasi spiegelbildlich – die Obliegenheiten der Bank im Rahmen der Prüfung des **Mitverschuldens** (§ 254 BGB) (dazu unten Rn. 555).

(a) Technische Sicherheit

516 Die Bank unterliegt beim Online-Banking dem für ein Unternehmen üblichen Sorgfaltsanforderungen.[1009] Die allgemeinen Organisationspflichten im IT-Bereich ergeben sich hierbei aus § 25a KWG (oben Rn. 440 ff.). Als grundlegende Pflcht obliegt der Bank die Bereitstellung eines **technisch sicheren Online-Banking-Systems**.[1010] Das System muss danach einerseits Schutz vor gegen die Bank selbst gerichteten Angriffen bieten. Genauso hat die Bank durch die technische Gestaltung des Online-Banking-Verfahrens aber auch die technischen Voraussetzungen für eine sichere Benutzung des Online-Banking durch den Kunden zu schaffen und – soweit technisch möglich – Missbräuchen durch Dritte bereits auf technischer Ebene zu begegnen. Schließlich ist durch regelmäßige Überprüfungen die Sicherheit des Systems auch während des Betriebs zu gewährleisten und auf Sicherheitslücken – insbesondere nach Hinweisen von außen[1011] – durch erforderliche Anpassung des Systems zu reagieren.

517 Aus Sicht des Gesetzgebers bestand zumindest vor Auftreten der ersten Fälle von Phishing und Pharming keine Notwendigkeit, einen allgemeinen Sicherheitsstandard gesetzlich, untergesetzlich oder auf freiwilliger Verpflichtung der Banken einzuführen.[1012] Maßgeblich für die Sicherheitserwartungen des Verkehrs ist gegenwärtig der jeweilige **Stand der Technik**.[1013] Hierbei ist anerkannt, dass normative Standards[1014] wie der „Stand der Technik“ den Pflichteninhalt nicht nur dort konkretisieren, wo eine Vorschrift des technischen Sicherheitsrechts eine ausdrückliche Regelung vorsieht.

[1009] *Spindler*, in: Hadding/Hopt/Schimansky, S. 178; zust. *Erfurth*, WM 2006, 2198 (2201).

[1010] *Kind/Werner*, CR 2006, 353 (357 f.); *Karper*, DuD 2006, 215 (217); *Koch*, Versicherbarkeit von IT-Risiken, Rn. 812; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 151, 206; *Göβmann*, in: Bankrechts-Handbuch, § 55 Rn. 19.

[1011] Vgl. etwa zu den Sicherheitsmängeln der Online-Banking-Portale der Sparda-Bank und der DAB-Bank durch sog. Cross-Site-Scripting-Lücken (XXS) abrufbar unter: http://www.heise.de/newsticker/meldung/76258.

[1012] Antwort der Bundesregierung vom 4.7.2000 auf die Kleine Anfrage der Abgeordneten Rainer Funke, Dr. Edzard Schmidt-Jortzig, Dr. Max Stadler, weiterer Abgeordneter und der Fraktion der F.D.P. – Drucksache 14/3603 –, BT-Drucks. 14/3757, S. 3.

[1013] So auch *Kind/Werner*, CR 2006, 353 (359); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 207, 225.

[1014] Zur Unterscheidung zwischen anerkannten Regeln der Technik, Stand der Technik und Stand von Wissenschaft und Technik grundlegend *Marburger*, Die Regeln der Technik im Recht, S. 121 ff.; .

Vielmehr umschreiben technische Standards auch außerhalb dieses Bereichs die zur Gefahrsteuerung objektiv geeigneten Maßnahmen.[1015] Der erforderliche Sicherheitsstandard bestimmt sich nach dem **Gefährdungspotential** des technischen Systems,[1016] welches im Online-Banking durch das Risiko beträchtlicher Vermögensschäden und die Offenbarung personenbezogener Daten des Kunden gekennzeichnet ist. Im Bereich des Online-Banking muss zudem berücksichtigt werden, dass sich die Online-Dienstleistung der Banken gerade auch an den **technisch nicht versierten Nutzer** wendet.

518 Die Unterhaltung und der Betrieb technischer Systeme stellen Dauertatbestände dar, die eine Pflicht zur **Anpassung der Systeme** an den jeweils verbesserten technischen Standard nach sich ziehen, wobei jedoch der mit einer Anpassung verbundene Sicherheitsgewinn mit dem wirtschaftlichen Aufwand in Relation zu setzen ist.[1017] Hier lassen sich Parallelen zum Recht der Anlagensicherheit, aber auch zum Produkthaftungsrecht ziehen: der Hersteller eines Produkts haftet zwar nicht für im Zeitpunkt des Inverkehrbringens nach dem Stand von Wissenschaft und Technik nicht erkennbare Fehler (Entwicklungsfehler), doch ist er verpflichtet seine künftige Produktion auf die neu aufgetretene Gefahrenlage einzustellen.[1018] Diese Wertung ist auf die Bank als IT-Dienstleister übertragbar, so dass sie zur Behebung von Sicherheitslücken ihres Systems bzw. Umstellung des Online-Banking-Sicherungsverfahrens verpflichtet ist,[1019] wenn sich herausstellt, dass das verwendetete PIN/TAN-Verfahren nach geltendem Stand der Technik nicht mehr sicher ist. Man wird der Bank für die Umstellung ihrer Systeme aber eine **Übergangszeit** einräumen müssen.

519 Gegenwärtig dürfte aufgrund der Erfahrungen mit Phishing und Pharming davon auszugehen sein, dass ein **konventionelles PIN-/TAN-Verfahren** nicht mehr dem Stand der Technik entspricht, da es für Angriffe Dritter aus dem Netz – insbesondere durch Schadprogramme, die den PC unbemerkt kontrollieren – eine erhöhte Anfälligkeit aufweist.[1020] Die - für Btx wohl noch gültige - Annahme, dass die TAN Sicherheit verspricht, da sie zwar ausgespäht werden kann, aber schon während des Ausspähens ver-

---

[1015] *Marburger*, Die Regeln der Technik im Recht, S. 439.

[1016] *Marburger*, Die Regeln der Technik im Recht, S. 126 f.

[1017] Dazu *Marburger*, Die Regeln der Technik im Recht, S. 162, 437 f.; allgemein dazu: MünchKomm.-*Wagner*„§ 823 BGB Rn. .

[1018] BGH NJW 1990, 906 (907 f.); BGH NJW 1994, 517 (519 f.); BGH NJW 1994, 3349 (3350 f.); *Kullmann*, in: Kullmann/Pfister, Kz. 1520, Bl. 60 f.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 580, 602.

[1019] So auch *Kind/Werner*, CR 2006, 353 (359); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 47 f.

[1020] So wohl auch *Kind/Werner*, CR 2006, 353 (357).

braucht ist,[1021] hilft nicht weiter. Denn die TAN, die eingesetzt wird, gelangt in den oben Rn. 479 ff. beschriebenen Angriffsszenarien überhaupt nicht bis zur Bank, sondern wird vorher quasi „abgesogen“ und gesammelt werden, so daß sie dann für einen Einsatz durch Dritte zusammen mit der PIN-Nummer zur Verfügung steht.

520 Ein Teil der Banken hat auf die neue Bedrohungslage bereits reagiert und neue Varianten des PIN-/TAN-Verfahrens eingeführt. Nach Einschätzung des BSI sind für das Online-Banking allein Verfahren geeignet, bei welchen ein **Medienbruch** durch den Einsatz zusätzlicher Hardware erfolgt. Von den gegenwärtig im Einsatz befindlichen PIN/TAN-Sicherungsverfahren entsprechen diesen Anforderungen einzig Verfahren mit **TAN-Generator** und Verfahren bei welchen eine Bestätigung der übermittelten Transaktionsdaten auf das Mobiltelefon des Kunden erfolgt (**mTAN**). Beide Verfahren ermöglichen es, dass Manipulationen der Transaktionsdaten durch ein Schadprogramm vom Kunden (mTAN) bzw. der Bank (TAN-Generator) sofort erkannt werden können (näher die technische Beschreibung unter Rn. **Error! Reference source not found.**).

521 Das **HBCI-Verfahren** mit Chipkarte und elektronischer Signatur gilt derzeit als das wohl sicherste Verfahren beim Online-Banking.[1022] Eine **Pflicht zum Systemwechsel** von PIN-/TAN auf ein Verfahren mit elektronischer Signatur (z.B. HBCI) – so die Forderung von Verbraucherschutzverbänden[1023] – wird man zum gegenwärtigen Zeitpunkt nicht annehmen können. Zwar ist ein Verfahren mit Chipkarte und elektronischer Signatur äußerst sicher gegenüber Missbräuchen. Neuere Varianten des PIN-/TAN-Verfahrens (z.B. mTAN der Postbank, Sm@rtTAN plus der Volksbanken) haben sich aber als durchaus leistungsfähig erwiesen, so dass gegenwärtig kein zwingendes sicherheitstechnisches Bedürfnis zum Umstieg auf HBCI erkennbar ist.[1024] Überdies ist zu bedenken, dass Verfahren mit Chipkarte vom Bankkunden – insbesondere wegen der höheren Kosten für die Anschaffung und die weniger komfortable Bedienung (z. B. keine Nutzungsmöglichkeit am Arbeitsplatz) – bislang nur zögerlich angenommen werden.

[1021] So für das Btx-Banking *Hellner*, FS Werner, S. 251, 270.

[1022] Selbst das HBCI-Verfahren hat sich bei einem gestellten Angriff durch den Chaos Computer Club in Zusammenarbeit mit dem Hessischen Rundfunk als nicht völlig sicher gegenüber Trojanern erwiesen, wenn der Bankkunde seine Chipkarte im Lesegerät stecken lässt, vgl. abrufbar unter: http://www.heise.de/newsticker/meldung/9349. Sofern der Kunde darüber instruiert war, die Chipkarte nach Beendigung des Online-Banking aus dem Lesegerät zu entfernen, wird man hier eine Pflichtverletzung des Kunden annehmen können.

[1023] Vgl. *Stockhausen*, WM 2001, 605 (606).

[1024] Im Ergebnis ebenso *Kind/Werner*, CR 2006, 353 (359). Dazu auch *Spindler*, in: Hadding/Hopt/Schimansky, S. 212 f.

522 Die Sicherheit des Online-Banking kann auf einfache Weise auch bei der Gestaltung des Web-Portals der Bank erhöht werden. Die **Verwendung Aktiver Inhalte** in sensiblen Webangeboten wie dem Online-Banking entspricht nicht dem Stand der Technik. Durch die Verwendung Aktiver Inhalte auf den Seiten der Bank wird der Kunde gezwungen Aktive Inhalte in seinem Browser freizuschalten um das Online-Banking-Angebot überhaupt nutzen zu können. Die Freischaltung Aktiver Inhalte führt auf der Kundenseite jedoch zugleich zu einer deutlich erhöhten Gefährdung, da Aktive Inhalte wichtige Hilfsmittel für mehr oder weniger aufwändige Angriffe Dritter sind. Alternative Möglichkeiten zur ansprechenden Gestaltung von Webseiten ohne Aktive Inhalte sind verfügbar und mit nur geringem Aufwand auch noch nachträglich umsetzbar. Verwendet die Bank auf ihren Webseiten dennoch Aktive Inhalte, wird man im Schadensfall eine eigene Pflichtverletzung, zumindest aber ein Mitverschulden der Bank annehmen müssen.

(b) Beobachtungspflichten

523 Neben der fortlaufenden Überwachung der eigenen Systeme trifft die Bank auch die Pflicht die Sicherheit des Online-Banking insoweit zu beobachten, als nicht die Bank selbst, sondern der Kunde Angriffsziel ist. Maßgebliche Wertung ist hierbei, dass die Bank als **überlegene Systembeherrscherin** über das spezifische Wissen um Risiken verfügt oder sich dieses zumindest leichter aneignen kann als der Kunde.[1025] Übertragen auf Phishing und Pharming bedeutet dies, dass die Bank Vorkehrungen treffen muss, um neu auftauchende Formen von Bedrohungen aus dem Internet zu erkennen und durch entsprechende Reaktionen zu beseitigen oder zumindest zu minimieren.

524 Entsprechend der Produktbeobachtungspflicht des Herstellers[1026] kann hierbei eine **passive** und **aktive** Beobachtungspflicht unterschieden werden. Die Bank hat daher Hinweisen auf Missbräuche aufgrund von bekannt gewordenen Missbrauchsfällen und Kundenbeschwerden nachzugehen. Ebenso ist die Bank aber auch gehalten, aktiv im Internet, einschlägigen Fachpublikationen usw. Informationen über neue Risiken zu beschaffen. Die Beobachtungspflichten der Bank dürfen hierbei nicht überspannt werden. Es genügt daher, wenn die Bank sich auf die Beobachtung marktüblicher und von Kunden üblicherweise eingesetzter Betriebssysteme und Software beschränkt. Organisatorisch ist sicherzustellen, dass diese Informationen an den Kunden (z.B. auf der Website

[1025] *Wiesgickl*, WM 2000, 1039 (1049); *Karper*, DuD 2006, 215 (217).
[1026] Ausführlich dazu Bamberger/Roth-*Spindler*, § 823 BGB Rn. 511.

der Bank, durch Informationsbriefe und Flyer) auch weiter gegeben werden (zur Warnpflicht unten Rn. 525).

(c) Aufklärungs-, Instruktions- und Warnpflichten

525 Die Bank trifft gegenüber dem Kunden eine Aufklärungs- und Instruktionspflicht bereits im Vorfeld der erstmaligen Benutzung.[1027] Gerade für technisch unerfahrene Kunden besteht in dieser Situation der größte Informationsbedarf. Mit Abschluss des Online-Bankingvertrages ist der Kunde daher in die **Benutzung** des Systems[1028] und das **Missbrauchsrisiko**[1029] im Besonderen einzuweisen.[1030] Sofern verschiedene Sicherungsverfahren (z.B. PIN-/TAN und HBCI) angeboten werden, kann von der Bank auch erwartet werden, dass der Kunde vor die **Wahl zwischen den verschiedenen Systemen** gestellt wird. Dem Kunden sind hierzu die Vor- und Nachteile der einzelnen Systeme zu erläutern und – insbesonder im Fall von HBCI – die (höheren) Kosten dem Nutzen gegenüber zu stellen. In der Praxis der Banken erfolgt derzeit oftmals keinerlei Hinweis auf Verfahren mit Chipkarte und elektronischer Signatur – dies dürfte jedoch mit dem Umstand zusammenhängen, dass viele Kunden sich für das bequemere PIN-/TAN-Verfahren entscheiden und die Kosten für die Anschaffung von HBCI scheuen. Erlangt die Bank Kenntnis von neuen Risiken (zur Beobachtungspflicht oben Rn. 523), hat sie ihre Kunden unverzüglich zu **warnen**. Soweit aufgrund der neuen Risikolage erforderlich, hat die Bank ihre Benutzerinformation entsprechend **umzustellen**.[1031]

526 Die Information des Kunden kann in in einem persönlichen Beratungsgepräch, einer gesonderten **schriftlichen Bedienungsanleitung** sowie den **Online- bzw. Homebanking-Bedingungen** (s. Rn. 488), einer **Benutzerführung auf dem Bildschirm** und durch eine auffällige Information auf der **Website** des Kreditinstituts (insbesondere in der Nähe des Login-Buttons) erfolgen.[1032] Nicht empfehlenswert ist hierbei die Ver-

---

[1027] *Kind/Werner*, CR 2006, 353 (356); *Karper*, DuD 2006, 215 (218); *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 65 ff.; *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 167; *Canaris*, Bankvertragsrecht, Rn. 527 ff; *Göβmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 19 ff.; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 220 ff.

[1028] *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 66.

[1029] *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 220 f.; *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 67; *Göβmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 20.

[1030] Ebenso für das Btx-System schon *Hellner*, FS Werner, S. 251, 260 f.; *Siebert*, Das Direktbankgeschäft, S. 125; allgemein für automatisierte Einrichtungen bereits *Köhler,* AcP 182 (1982), 126, 129 ff.

[1031] Ebenso *Kind/Werner*, CR 2006, 353 (357). Zur Parallelproblematik der Umstellung der Instruktion durch den Hersteller MünchKommBGB-*Wagner*, § 823 BGB Rn. 602.

[1032] *Kind/Werner*, CR 2006, 353 (357); *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 67 f.; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 220; *Göβmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 21.

wendung von Po-Up-Fenstern, da diese von vielen Browsern geblockt werden.[1033] Ob die Anordnung von Sorgfaltspflichten in den AGB der Banken für sich alleine ausreicht,[1034] erscheint zweifelhaft, da das „Kleingedruckte" vom Kunden erfahrungsgemäß kaum gelesen wird.[1035] Überdies taugen AG kaum um dem Kunden die Benutzung eines komplexen technischen Systems anschaulich zu erläutern.[1036] Erforderlich und empfehlenswert erscheint daher dem Kunden in jedem Fall eine gesonderte Benutzerinformation zukommen zu lassen und eine eine Benutzerführung am Bildschirm vorzusehen. Dagegen sollten die Banken von Informationen per **E-Mail** absehen. Empfehlenswert ist es als Schutz gegen Phishing gegenüber dem Kunden von vornherein ausdrücklich klarzustellen, dass die Bank mit ihm unter keinen Umständen per E-Mail in Kontakt treten wird (s. auch Rn. 545).[1037]

527 Die Informationen müssen jeweils auch für einen **Durchschnittskunden** ohne größere technische Fähigkeiten leicht verständlich sein.[1038] Die Anforderungen der Rechtsprechung zur Klarheit und Verständlichkeit von Produktinformationen können hier herangezogen werden.[1039] Im IT-Bereich stößt die Informationspflicht an die **Grenzen des technischen Verständnisses** des Durchschnittskunden. Unbedenklich sind in diesem Zusammenhang Hinweise zur Verwahrung und Geheimhaltung der Legitimationsmedien selbst (z.B. sichere Verwahrung von PIN und TAN oder der Chipkarte bei HBCI). Anders wäre dies zu beurteilen, wenn die Bank dem Kunden Informationen beispielsweise zu komplizierten Einstellungen von Browser oder Firewall zukommen lässt, die zwar erhöhte Sicherheit gewährleisten, einen Großteil der Bankkunden aber überfordern und für sie ohne fremde Hilfe nicht zu bewerkstelligen sind (ausführlich zu den Sorgfaltsanforderungen an private Nutzer im IT-Bereich oben Rn. 280 ff., zu Firewalls Rn.298). Die Bank kann die Risiken des Online-Banking nicht durch Übererfüllung ihrer Aufklärungs- und Instruktionspflicht auf den Kunden abwälzen. Denn es würde ein Risiko auf den Kunden verlagert, welchem dieser durch eigene Maßnahmen nicht zu begegnen vermag.

[1033] *Kind/Werner*, CR 2006, 353 (357).
[1034] So aber *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 67; ebenso *Hellner*, FS Werner, S. 251, 260 f., allerdings für das Btx-Banking, das geringere Probleme als das Internet aufwies.
[1035] So zutreffend *Canaris*, Bankvertragsrecht, Rn. 527 q; *Fervers*, WM 1988, 1037 (1041); aA *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 220 mit dem Argument, eine derartige Nachlässigkeit dürfte nicht zu Lasten der Bank gehen.
[1036] *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 167.
[1037] *Kind/Werner*, CR 2006, 353 (357).
[1038] *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 167.
[1039] Näher Bamberger/Roth-*Spindler*, § 823 BGB Rn. 502 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 588 ff.

(d) Organisationspflichten

528 Erlangt die Bank Kenntnis von missbräuchlichen Transaktionen, hat sie dafür Sorge zu tragen, dass keine weiteren unberechtigten Transaktionen erfolgen können.[1040] Daneben hat die Bank Vorkehrungen dahingehend zu treffen, dass der Kunde den Zugang zum Online-Banking bei Kenntnis oder Verdacht eines Missbrauchs jederzeit **sperren** lassen kann.[1041]

(iii) Pflichten des Kunden

529 Die **vertraglichen Schutzpflichten** nach §§ 280 Abs. 1, 241 Abs. 2 BGB entsprechen inhaltlich weitgehend den **deliktischen Verkehrspflichten**[1042] (zu den deliktischen Verkehrspflichten des privaten Nutzers ausführlich oben Rn. 275 ff.). Schutzmaßnahmen, welche vom privaten IT-Nutzer nach deliktsrechtlichen Grundsätzen verlangt werden können, bilden im vertraglichen Bereich grundsätzlich zugleich den Mindestgehalt der vertraglichen Schutzpflichten nach § 241 Abs. 2 BGB. Im Einzelfall können die vertraglichen Sorgfaltsanforderungen angesichts der bestehenden Sonderverbindung und der damit verbundenen verstärkten Einwirkungsmöglichkeit auf die Rechte und Rechtsgüter des Vertragspartners über die deliktischen Pflichten hinausgehen. Die Pflichten des Kunden werden konkretisiert durch die Online- und Homebanking-Bedingungen.

(c) Allgemeine Geschäftsbedingungen der Banken

530 Auch wenn die Online-Bedingungen und Homebanking-Bedingungen keine ausdrückliche Haftungsregelung vorsehen, sind sie insoweit für die Haftung des Kunden von Bedeutung, als sie die Pflichten des Kunden näher ausgestalten.

(i) Online-Banking-AGB in der Praxis

531 Die im Bereich des Online-Banking derzeit verwendeten Sonderbedingungen für Online- und Homebanking sehen ausdrückliche Regelungen der Pflichten des Kunden vor. So regeln die **Online-Bedingungen**[1043]:

> 7. Geheimhaltung der PIN und TAN
>
> Der Teilnehmer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN und den TAN erlangt. Jede Person, die die PIN und - falls erforderlich - eine TAN kennt, hat die

[1040] *Karper*, DuD 2006, 215 (218).
[1041] Vgl. auch Art. 47 des Vorschlags der EU-Kommission für eine Zahlungsdiensterichtlinie.
[1042] Palandt-*Heinrichs*, § 280 BGB Rn. 28; MünchKommBGB-*Ernst,* § 280 BGB Rn. 104; Bamberger/Roth-*Grüneberg/Sutschet*, § 241 BGB Rn. 92.
[1043] Abgedruckt in WM 2001, 650 f.

Möglichkeit, das Online-Banking-Leistungsangebot zu nutzen. Sie kann z. B. Aufträge zu Lasten des Kontos/Depots erteilen. Insbesondere Folgendes ist zur Geheimhaltung der PIN und TAN zu beachten:

PIN und TAN dürfen nicht elektronisch gespeichert oder in anderer Form notiert werden;

die dem Teilnehmer zur Verfügung gestellte TAN-Liste ist sicher zu verwahren;

bei Eingabe der PIN und TAN ist sicherzustellen, dass Dritte diese nicht ausspähen können.

Stellt der Teilnehmer fest, dass eine andere Person von seiner PIN oder von einer TAN oder von beidem Kenntnis erhalten hat oder besteht der Verdacht einer missbräuchlichen Nutzung, so ist der Teilnehmer verpflichtet, unverzüglich seine PIN zu ändern bzw. die noch nicht verbrauchten TAN zu sperren. Sofern ihm dies nicht möglich ist, hat er das Kreditinstitut unverzüglich zu unterrichten. In diesem Fall wird das Kreditinstitut den Online-Banking-Zugang zum Konto/Depot sperren. Das Kreditinstitut haftet ab dem Zugang der Sperrnachricht für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

532 Ähnlich bestimmen die **Homebanking-Bedingungen**[1044]:

IV. Legitimationsverfahren/Geheimhaltung

(1) Der Nutzer ist verpflichtet, die mit dem Kreditinstitut vereinbarten Sicherungsmaßnahmen durchzuführen.

(2) Mit Hilfe der mit dem Kreditinstitut vereinbarten Medien identifiziert und legitimiert sich der Nutzer gegenüber dem Kreditinstitut. Der Nutzer hat dafür Sorge zu tragen, dass kein Dritter in den Besitz der Identifikations- und Legitimationsmedien kommt sowie Kenntnis von dem zu deren Schutz dienenden Passwort erlangt. Denn jede Person, die im Besitz der Medien ist und das Passwort kennt, kann die vereinbarten Dienstleistungen nutzen. Insbesondere Folgendes ist zur Geheimhaltung der Identifikations- und Legitimationsmedien zu beachten:

Die den Nutzer identifizierenden Daten dürfen nicht außerhalb der Sicherheitsmedien, z. B. auf der Festplatte des Rechners, gespeichert werden;

die Identifikations- und Legitimationsmedien sind nach Beendigung der Online-Banking-Nutzung aus dem Lesegerät zu entnehmen und sicher zu verwahren;

das zum Schutz der Identifikations- und Legitimationsmedien dienende Passwort darf nicht notiert oder elektronisch abgespeichert werden;

bei Eingabe des Passwortes ist sicherzustellen, dass Dritte dieses nicht ausspähen können.

533 Die Bedingungen stellen weitgehend allgemeine Pflichten hinsichtlich der Geheimhaltung der Legitimationsmedien auf, sehen jedoch keine IT-spezifischen Pflichten wie et-

[1044] Abgedruckt in WM 2001, 650.

wa die Installation von Anti-Virensoftware, Firewalls usw. oder Verhaltenspflichten in Bezug auf Phishing-E-Mails vor.

534 Die deutschen Banken haben auf die neuartigen Bedrohungsszenarien durch Phishing und Pharming nunmehr mit einer **Anpassung der Allgemeinen Bankbedingungen** reagiert. So bestimmen nunmehr beispielsweise die AGB der Deutsche Bank AG[1045]:

- Anfragen außerhalb der bankseitig zur Verfügung gestellten originären Zugangswege, in denen nach vertraulichen Daten wie Geheimzahl oder Passwort/Online-TAN gefragt wird, dürfen nicht beantwortet werden.
- Der Aufforderung per elektronischer Nachricht (z.B. E-Mail), eine damit übersandte Verknüpfung zum (vermeintlichen) Online-Banking der Bank anzuwählen und darüber persönliche Zugangsdaten einzugeben, darf nicht gefolgt werden.
- Auf einer Login-Seite (Startseite) zum (vermeintlichen) Online-Banking der Bank darf keine TAN eingegeben werden.
- Der Kunde hat sich regelmäßig über aktuelle Sicherheitshinweise zum Online-Banking auf der Website der Deutschen Bank zu informieren.
- Der Kunde hat vor seinem jeweiligen Zugang zum Online-Banking sicherzustellen, dass auf seinem verwendeten System handelsübliche Sicherheitsvorkehrungen (wie Anti-Viren-Programm und Firewall) installiert sind und diese ebenso wie die verwendete Systemsoftware regelmäßig aktualisiert werden. Beispiele handelsüblicher Sicherheitsvorkehrungen kann der Kunde der Website der Deutschen Bank entnehmen.

535 Die AGB der comdirect bank[1046] enthalten unter anderem die Regelung

> Die Sicherheitsvorkehrungen gem. Nr. 4 sollten nicht abgespeichert werden, insbesondere ist im Internet der Cache des verwendeten Browsers zu deaktivieren oder nach der Nutzung zu löschen (vgl. Sicherheitshinweise im Internet).

536 Die Vereinbarkeit vieler derzeit gebräuchlicher Bedingungen für die Online-Nutzung mit den Vorschriften der §§ 307 ff. BGB, war bislang noch nicht Gegenstand gerichtlicher Entscheidungen. Angesichts der oben entwickelten Kriterien für Sorgfaltspflichten des privaten IT-Nutzers, sind die Grenzen des für den Kunden technisch und wirtschaftlich Zumutbaren zu beachten (allgemein Rn. 289 ff., zum Online-Banking unten Rn.

[1045] Vgl. A II Nr. 8. der AGB der Deutsche Bank AG. Besondere Bestimmungen im Hinblick auf Angriffe aus dem Internet sehen auch die AGB der citibank (C I Nr. 11) vor. Entsprechende Hinweise zur Sicherheit beim Online-Banking stellt auch der Bundesverband Deutscher Banken (BDB) in seinen Empfehlungen zur Verfügung, abrufbar unter: http://www.bankenverband.de/pic/artikelpic/072005/br0507_rb_phishing.pdf und abrufbar unter: http://www.bankenverband.de/pic/artikelpic/062005/0506_OnlineBankingSicherheit.pdf.

[1046] Siehe A. II. Nr. 9, abrufbar unter: http://www.comdirect.de/static/pdf/corp0058.pdf.

538 ff.). Hier könnten sich zumindest Teile der Sorgfaltsanforderungen an den Kunden im Online-Banking-Bereich als zu streng und mit dem Verbot den Kunden entgegen den Geboten von Treu und Glauben unangemessen zu benachteiligen (§ 307 Abs. 1, 2 BGB), unvereinbar erweisen.[1047]

(ii) Inhaltskontrolle

(a) Geheimhaltung und sichere Verwahrung der Legitimationsmedien

537 Die den Kunden treffenden Sorgfaltspflichten sind insoweit unproblematisch, als es um die **Geheimhaltung** und **sichere Verwahrung** von PIN und TAN bzw. der Chipkarte bei HBCI geht.[1048] Hier liegen Vergleiche zur ec-Karte nahe. Der Kunde darf die Legitimationsmedien nicht an Dritte weitergeben und die PIN nicht auf einem am Bildschirm befestigten Zettel zu notieren oder auf dem PC abspeichern. Bei der Eingabe von PIN und TAN muss sichergestellt sein, dass Dritte diese nicht ausspähen können. Hierbei handelt es sich um Vorgänge, die auch in der Laiensphäre leicht nachzuvollziehen sind und die jeder Kunde in ihrer Bedeutung für die Geheimhaltung und Funktionsfähigkeit des Gesamtsystems unschwer erkennen und befolgen kann. Die Bedeutung der Geheimhaltung der Legitimatonsmedien ist überdies von der ec-Karte und Kreditkarte dem Bankkunden vertraut. Die von der Rechtsprechung zur ec-Karte entwickelten Grundsätze der dürften insoweit auch übertragbar sein.[1049]

(b) IT-spezifische Pflichten des Bankkunden beim Online-Banking

(i) Grundsätze

538 Weitgehend ungeklärt ist, welche **IT-spezifischen** Sorgfaltspflichten (insbesondere Umgang mit Phishing-E-Mails, Installation von Virenschutz, Firewalls usw.) dem Kunden zumutbar auferlegt werden können. Auszugehen ist hierbei von den allgemeinen Pflichten privater IT-Nutzer (Rn. 275 ff.). Denn Pflichten, welche den privaten Nutzer aufgrund deliktischer Verkehrspflichten gegenüber Dritten treffen, sind grundsätzlich auch im Rahmen einer vertraglichen Sonderverbindung zu beachten (§ 241 Abs. 2

[1047] S. dazu auch *Erfurth*, WM 2006, 2198 (2201 f.).

[1048] *Kind/Werner*, CR 2006, 353 (354).

[1049] Vgl. etwa zu den Sorgfaltsanforderungen an die Verwahrung der ec-Karte und PIN in der Wohnung BGH NJW 2001, 286 ff.: keine grobe Fahrlässigkeit bei Aufbewahrung von ec-Karte und PIN in einer Wohnung; OLG Frankfurt NJW-RR 2001, 1341 (1342): keine grobe Fahrlässigkeit bei Aufbewahrung der PIN in einem anderen Stockwerk des Hauses. Ausführlich auch *Werner*, in: Hellner/Steuer, Band 3, 6/1386 ff.

BGB).[1050] Im Rahmen des Vertragsverhältnisses zwischen Bank und Kunde ist daher jedenfalls kein gegenüber den deliktischen Sorgfaltspflichten geringerer Maßstab anzusetzen.

539 Gewichtiger ist indes die Frage, ob den Bankkunden beim Online-Banking gegenüber den allgemeinen Grundsätzen **erhöhte Sorgfaltspflichten** treffen.[1051] Hierfür mag zwar sprechen, dass sich der Kunde der höheren Sensibilitat von Online-Bankgeschäften bewusst sein dürfte und die Risiken durch Phishing-E-Mails und Trojaner aufgrund von Medienberichten und der Informationsarbeit der Banken einem breiten Publikum bekannt geworden sind (allg. Rn. 479).[1052] Die bloße Kenntnis von der Bedrohungslage darf indessen nicht darüber hinwegtäuschen, dass dem Großteil der Internet-Nutzer und Online-Bankkunden zum gegenwärtigen Stand spezielle Computer- und Internet-Kenntnisse fehlen, um allen diesen Phänomenen wirksam zu begegnen.

540 Anders als die Pflichten zur Geheimhaltung und sicheren Verwahrung der Legitimationsmedien, erschließen sich die im IT-spezifischen Bereich erforderlichen Maßnahmen dem Durchschnittskunden nicht ohne weiteres. Die Anpassung oder Änderung der Sicherheitseinstellungen des eigenen PC, werden normale Nutzer häufig überfordern. Die technische Fähigkeiten des Durchschnittsnutzers müssen aber Grenze der zu fordernden Sorgfaltspflichten markieren, da sich daran die Sicherheitserwartungen des Verkehrs ausrichten (allg. Rn.277 ff.).[1053] Realisiert sich eine Gefahr, welche nur für einen technisch versierten Nutzer beherrschbar ist, trägt dieses Risiko die Bank. Dies rechtfertigt sich aber aus der Erwägung, dass sich die Banken mit ihrem Online-Banking-Angebot nicht nur an technisch versierte Nutzer, sondern gerade auch an die breite Masse der Kunden wenden.[1054]

541 Bei der Bestimmung der Sorgfaltspflichten wird man ausgehend vom Maßstab des Durchschnittskunden anhand des konkreten Bedrohungsszenarios, sowie der Bekanntheit des betreffenden Problems und der (wirtschaftlichen und technischen) Zumutbar-

---

[1050] Palandt-*Heinrichs*, § 280 BGB Rn. 28; MünchKommBGB-*Ernst,* § 280 BGB Rn. 104; Bamberger/Roth-*Grüneberg/Sutschet*, § 241 BGB Rn. 92.

[1051] So etwa *Karper*, DuD 2006, 215 (217). Nach *Kind/Werner* sollen die Sorgfaltanforderungen an den Kunden wegen der Gefahren des Online-Banking zwar besonders hoch anzusetzen sein. Dennoch verneinen die Autoren sogar eine Pflicht zur Einrichtung von Virenschutzprogrammen, s. CR 2006, 353 (355).

[1052] *Karper*, DuD 2006, 215 (217).

[1053] Ebenso *Spindler*, in: Hadding/Hopt/Schimansky, S. 178 f.; *Erfurth*, WM 2006, 2198 (2201); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 225.

[1054] *Spindler*, in: Hadding/Hopt/Schimansky, S. 179; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 225 f.; im Ergebnis ebenso *Erfurth*, WM 2006, 2198 (2201).

keit möglicher Schutzmaßnahmen zu unterscheiden haben. Soweit es zur Abwehr von Phishing-Versuchen darum geht, keine verdächtigen E-Mails zu beantworten, keine in E-Mails eingebetteten Link anzuklicken, keine unbekannte Anhänge zu öffnen usw., wird man ein entsprechendes Nutzerverhalten nach gehöriger Aufklärung durch die Bank als zumutbar ansehen können (unten Rn. 545). Problematischer ist es dagegen den Kunden zu bestimmten Einstellungen des Browsers oder der Firewall zu verpflichten (unten Rn. 542). In der Praxis wird sich eine Pflichtverletzung des Kunden nur durch eine **Gesamtwürdigung aller Umstände im Einzelfall** feststellen lassen.

(ii) Pflicht zur Sicherung des privaten Computers

542 Hinsichtlich der Sicherung des privaten Computers wird man auch beim Online-Banking-Kunden gegenüber den oben Rn. 280 ff. entwickelten allgemeinen Pflichten zum Einsatz von **Virenscannern** und **Systemupdates** kein „Mehr" verlangen können. Der BGH hatte in seiner **Dialer-Entscheidung** eine Pflicht des privante Nutzer zur Verwendung eines Dialerschutzprogrammes noch verneint,[1055] was indessen auf das Vorhalten eines allgemeinen Virenschutzes nicht übertragbar ist (s. oben Rn.295 ff.). Zu weitgehend ist es aber aus den dargelegten Gründen (Rn. 538 ff.), dem Online-Banking-Kunden darüber hinaus unter Berufung auf die Sensibilität des Bankgeschäfts beispielsweise eine Pflicht zur Konfiguraton einer Firewall oder zur Vornahme bestimmter Browsereinstellungen aufzuerlegen.[1056]

543 Die Sicherung des privaten Computers läuft als Präventionsmaßnahme indessen leer, wenn – wie häufig – **Online-Bankgeschäfte vom Arbeitsplatz** aus getätigt werden und hierzu (erlaubt oder unerlaubt[1057]) die Hard- und Software des Arbeitgebers verwendet wird. Nutzt der Kunde das Online-Banking am Arbeitsplatz, bedarf es keiner großen Anstrengungen für einen einigermaßen versierten Computerspezialisten, ein Programm auf dem Rechner im Hintergrund zu installieren, das die Vorgänge auf dem Computer aufzeichnet, insbesondere die eingegebenen Kennwörter oder Internet-Adressen. Dem Kunden kann hier allenfalls vorgeworfen werden, seine Kennwörter auf dem Arbeitsplatzrechner zu gebrauchen, wenn er davon ausgehen musste, daß dieser auch Dritten

[1055] BGH MMR 2004, 308 (311); ausführlich *Spindler*, JZ 2004, 1128 ff.; vgl. auch LG Stralsund MMR 2006, 487 (489) mit zu Recht krit. Anm. *Ernst*, CR 2006, 590 ff.

[1056] So aber *Karper*, DuD 2006, 215 (217)

[1057] Die arbeitsrechtliche Zulässigkeit der privaten Nutzung des Internet am Arbeitsplatz ist heute meist im Arbeitsvertrag oder Betriebsvereinbarungen geregelt. Ausführlich zur arbeitsrechtlichen Problematik, *Hanau/Hoeren*, Private Internetnutzung durch Arbeitnehmer.

zugänglich ist und keine besonderen Sicherheitsvorkehrungen bestanden. Aber auch hier ist eine Aufklärung über die Risiken erforderlich, da vielen Kunden nicht bewusst ist, welche technischen Möglichkeiten des Ausspähens am Computer bestehen.

(iii) Pflichten bei der Teilnahme am E-Mail-Verkehr

544 Bei der Durchführung von Online-Bankgeschäften kann vom privaten Bankkunden die Einhaltung gewisser grundlegender Verhaltensstandards verlangt werden. Hierzu gehört etwa PIN und TAN nicht auf dem Computer **abzuspeichern**[1058] und bei der Verwendung von HBCI die Chipkarte nach Abschluss der Transaktion aus dem Lesegerät zu entfernen, um ein Ausspähen durch Trojaner zu verhindern.[1059] Ebenso gelten die unter Rn. 311 f. beschriebenen Pflichten im **Umgang mit unbekannten E-Mail-Anhängen**.

545 Nach gehöriger Aufklärung durch die Bank wird man von Teilnehmern am Online-Banking auch erwarten können, dass er **Phishing-E-Mails** mit (vermeintlichem) Bankabsender nicht beantwortet (Szenario 1). Insbesondere darf der Kunde auf E-Mail-Anfrage keine PIN und TAN auf vermeintlichen Login-Seiten eingeben.[1060] Hierbei handelt es sich um einfache und jedem Internet-Nutzer heute ohne weiteres verständliche Vorsorgemaßnahmen, welche keine speziellen IT-Kenntnisse erfordern. Bei der Feststellung der Pflichten des Bankkunden wird man zudem berücksichtigen müssen, dass Phishing-E-Mails mit Bankabsender aufgrund der Aufklärungsarbeit der Banken und Medienberichten in der Masse der Spam-E-Mails eine gewisse Bekanntheit auch unter privaten Nutzern erlangt haben. Besondere Vorsicht ist zudem geboten, wenn bereits der äußere Anschein oder die sprachliche Aufmachung der E-Mail (z.B. gebrochenes Deutsch) Zweifel an der Urheberschaft der Bank begründen.[1061] Eine Pflichtverletzung wird aber zu verneinen sein, wenn die Bank selbst E-Mails zur Kommunikation mit dem Kunden nutzt und der Kunde davon ausgehen durfte, es handele sich um eine Nachricht seiner Bank.[1062] Viele Banken stellen mittlerweile in ihren Informationsmaterialien klar, dass sie den Kunden unter keinen Umständen per E-Mail kontaktieren oder gar zur Preisgabe von PIN und TAN auffordern werden.

[1058] *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 221.

[1059] Vgl. abrufbar unter: http://www.heise.de/newsticker/meldung/9349.

[1060] *Karper*, DuD 2006, 215 (217); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 222 f.

[1061] So auch *Erfurth*, WM 2006, 2198 (2202).

[1062] *Borges*, NJW 2005, 3313 (3314 f.); jedenfalls stünde ein Mitverschulden der Bank im Raum.

(iv) Pflichten bei der Durchführung von Online-Bankgeschäften

546 Ob der Durchschnittskunde zur **Überprüfung der Sicherheitsmerkmale der Online-Verbindung** (URL im Adress-Feld, Schloss-Symbol und Zertifikatsinformationen[1063]) verpflichtet ist,[1064] erscheint fraglich.[1065] Zum gegenwärtigen Zeitpunkt stellt das Wissen um diese – eigentlich einfach zu bewerkstelligenden – Schutzmaßnahmen noch kein Allgemeingut des durchschnittlichen Internet-Nutzers dar. Jedenfalls wird man deshalb eine intensive Informationsarbeit der Banken verlangen müssen, um eine entsprechende Kundenpflicht bejahen zu können. Keine Pflichtverletzung des Bankkunden wird man zudem annehmen können, wenn die Bank wechselnde URLs verwendet.[1066] Wie Szenario 1 (Rn. 479) zeigt, versagen diese Sicherheitsmaßnahmen bei der Verwendung von Visual Spoofing (eine andere Frage ist dann, ob bereits das Öffnen und Beantworten der Phishing-E-Mail eine Pflichtverletzung begründet, s. Rn. 544).[1067]

(v) Verhaltenspflichten im Missbrauchsfall

547 Der Kunde ist verpflichtet, bei Kenntnis oder Verdacht von Unregelmäßigkeiten seiner Bank Mitteilung zu machen und den Online-Zugang seines Kontos **sperren** zu lassen.[1068] Unterlässt der Kunde eine ihm mögliche Mittelung und hätte die Bank die Transaktion bei unverzüglicher Meldung noch verhindern oder rückgängig machen können, haftet der Kunde gegenüber der Bank.

548 Zur Vermeidung einer Vergrößerung des Schadens ist der Kunde nach einem erkannten Missbrauch gehalten, seine **PIN zu ändern**.[1069] Eine weitergehende, verdachtsunabhängige Pflicht zur Änderung der PIN in regelmäßigen Abständen ist dagegen abzulehnen, da der Durchschnittskunde infolge der wachsenden Zahl von im Alltag verwendeten Identifikationsnummern und Passwörtern schnell überfordert wäre.[1070]

[1063] Das Sicherheitszertifikat kann durch Doppelklick auf das Schlosssymbol eingesehen werden.

[1064] So *Karper*, DuD 2006, 215 (216).

[1065] So auch *Kind/Werner*, CR 2006, 353 (356); *Erfurth*, WM 2006, 2198 (2202).

[1066] *Erfurth*, WM 2006, 2198 (2202).

[1067] Ausführlich zu den Manipulationsmöglichkeiten *Erfurth*, WM 2006, 2198 (2202 f.).

[1068] *Borges*, NJW 2005, 3313 (3314); *Werner*, MMR 1998, 338 (339); *Werner*, in: Hellner/Steuer, Band 6, 19/68; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 223.

[1069] *Werner*, in: Hellner/Steuer, Band 6, 19/68; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 224.

[1070] *Spindler*, in: Hadding/Hopt/Schimansky, S. 218; *Werner*, in: Hellner/Steuer, Band 6, 19/70; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 224.

(iii) Zusammenfassende Bewertung der Bedrohungsszenarien

(a) Szenario 1

549 Der Kunde hat (wenn man so weitgehende Sorgfaltspflichten überhaupt bejahen kann, s. Rn. 546) durch Überprüfung der Online-Verbindung sorgfaltsgemäß gehandelt. Die URL im Adress-Feld, das Schloss-Symbol und die Zertifikatsinformationen waren durch Visual Spoofing für den Kunden nachgebildet und als Täuschung nicht erkennbar. Die Verwendung von Aktiven Inhalten stellt eine Pflichtverletzung auf Seiten der Bank dar (Rn. 522). Da der Bankkunde schon zur Nutzung des regulären Online-Banking-Angebots Aktive Inhalte in seinem Browser freischalten musste, kann darin seinerseits keine Pflichtverletzung gesehen werden.

550 Davon zu trennen ist die Frage Pflichtverletzung durch bloße Antwort auf eine Phishing-E-Mail. Bei entsprechender Aufklärung des Kunden durch die Bank wird man hier eine Pflichtverletzung seitens des Kunden bejahen können, wenn keine besonderen Umstände vorliegen auf Grund derer er auf eine E-Mail seiner Bank vertrauen durfte. Eine Pflichtverletzung scheidet regelmäßig aus, wenn die Bank selbst zum Kunden per E-Mail in Kontakt getreten ist.

(b) Szenario 2

551 Der Angriff mittels DNS-Spoofing richtet sich gegen den Server des Providers, nicht gegen den PC des Bankkunden. Der Kunde handelt unter keinem Gesichtspunkt sorgfaltswidrig, da der Angriff für ihn nicht erkennbar, noch verhinderbar ist.[1071] Das Risiko für den Kunden besteht hier darin, ob es ihm überhaupt gelingt den von der hM bejahten Anscheinsbeweis für seine Urheberschaft zu erschüttern (unten Rn. 586 ff.).

(c) Szenario 3

552 Beim Pharming i.e.S. kommt eine Pflichtverletzung des Bankkunden zunächst unter dem Gesichtspunkt des Öffnens des E-Mail-Anhangs in Betracht. Hierbei wird man darauf abstellen müssen, ob die E-Mail von einem bekannten und vertrauenswürdigen Absender stammte. Das Öffnen von Spam-E-Mail als solches begründet grundsätzlich zwar noch keine Pflichtverletzung, jedoch hat auch der private Nutzer beim Umgang mit Anhängen unbekannter Herkunft besondere Sorgfalt walten zu lassen. Kann dem Kunden nicht vorgeworfen werden kann, er habe fahrlässig einen unbekannten E-Mail-

[1071] So auch *Kind/Werner*, CR 2006, 353 (356); *Erfurth*, WM 2006, 2198 (2202); *Borges*, NJW 2005, 3313 (3315).

Anhang geöffnet, kommt eine Pflichtverletzung wegen mangelnder Sicherung des eigenen PC mit Anti-Virus-Software und Systemupdates in Betracht. Die Sorgfaltsanforderungen an den privaten Nutzer und Bankkunden sind dabei in oben dargelegten Umfang beschränkt.

(iv) Vertretenmüssen des Kunden, § 280 Abs. 1 Satz 2 BGB

553 Die von den Banken für das Online-Banking entwickelten AGB enthalten keine spezielle Haftungsregelung. Anders als nach den ec-Bedingungen[1072] haftet der Kunde somit nicht nur für grobe, sondern bereits für **einfache Fahrlässigkeit** (§ 276 Abs. 1, 2 BGB),[1073] wobei vermutetet wird, dass der Kunde ein pflichtwidriges Verhalten auch zu vertreten hat (§ 280 Abs. 1 Satz 2 BGB). Für die Reichweite der Haftung des Bankkunden kommt es daher ganz entscheidend darauf an, wie eng oder weit die Pflichten des Kunden gefasst werden.

(v) Schaden der Bank

554 Überweist die Bank einen Geldbetrag an einen Angreifer, welcher sich Zugang zum Legitimationsmedium des Kunden verschafft hat, so besteht ein Schaden der Bank grundsätzlich in Höhe des Überweisungsbetrages. Während bei einer Bargeldabhebung am Geldautomaten mittels EC-Kartenmissbrauchs der Täter im Regelfall nicht mehr ermittelt werden kann und der Abhebungsbetrag somit (vorbehaltlich eines etwaigen Mitverschuldens der Bank) meist identisch mit dem Schaden der Bank ist, liegt die Situation bei einer Online-Überweisung insoweit anders, als eine Rückverfolgung der Überweisung technisch möglich ist.[1074] Geht man davon aus, dass die Überweisung dem Kunden nicht zurechenbar ist und es mithin keine wirksame Anweisung des Kunden gegenüber der Bank vorliegt,[1075] steht der Bank ein Anspruch aus § 812 Abs. 1 Satz 1 Fall 2 BGB (Direktkondiktion) gegen den Zahlungsempfänger[1076] und unter Umständen Schadensersatzansprüche gegen den Täter zu. Ein liquidationsfähiger Schaden entsteht

---

[1072] Vgl. III Nr. 1.4 der ec-Bedingungen der Privatbanken, abgedruckt bei *Werner*, in: Heller/Steuer, Band 3, 6/1763a.

[1073] *Kind/Werner*, CR 2006, 353 (354).

[1074] *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 148.

[1075] Dazu *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 175. Liegt dagegen – etwa wegen Bejahung einer Rechtsscheinshaftung – eine wirksame Anweisung des Kunden vor, sind auch die Voraussetzungen für einen Aufwendungsersatzanspruch der Bank nach §§ 670, 675, 676a BGB erfüllt. Der Kunde kann in diesem Fall nur Bereicherungs- und Schadensersatzansprüche gegen den Täter geltend machen.

[1076] OLG Hamburg WM 2006, 2078; *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 176; *Oechsler*, in: Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bankrecht, § 37 Rn. 40; *Schimansky*, in: Bankrechts-Handbuch, Band I, § 50 Rn. 3 f..

demnach erst, wenn die Durchsetzung dieser Ansprüche scheitert oder von vornherein aussichtslos ist, weil der Täter beispielsweise vom Ausland aus gehandelt hat und nicht greifbar ist.[1077] Der Schaden wird in diesen Fällen dem Überweisungsbetrag entsprechen. Im Einzelfall wird eine Kürzung des Anspruchs wegen Mitverschuldens der Bank (§ 254 BGB) in Betracht kommen.

(vi) Mitverschulden der Bank, § 254 BGB

555 Im Schadensersatzprozess der Bank gegen den Kunden, könnte sich der Kunde auf **Mitverschulden** (§ 254 BGB) der Bank berufen, wenn die mangelnde Sicherheit des *mitursächlich* für den Missbrauch wurde.[1078] Eine Obliegenheitsverletzung der Bank wird beispielsweise vorliegen, wenn sie dem Kunden das Erkennen manipulierter Websites durch häufig wechselnde Designs der Login-Seite oder unklare oder nicht nachvollziehbare URLs erschwert. Ebenso kann ein Mitverschulden der Bank in Betracht kommen, wenn das SSL-Zertifikat nicht auf den Namen der Bank ausgestellt ist und dem Kunden hierdurch die Überprüfung der Authentizität der Website erschwert wird. Die Beweislast für ein Mitverschulden der Bank liegt nach allgemeinen Grundsätzen beim Kunden.[1079]

(d) Verschuldensunabhängige Haftung des Kunden aufgrund AGB?

556 Da Internet-Banking trotz aller Sicherungsvorkehrungen Risiken aufweist, wäre es aus wirtschaftlicher Sicht verständlich, daß in Allgemeinen Geschäftsbedingungen das Risiko von trotzdem auftretenden Mißbrauchsfällen dem Kunden zugewiesen wird. In den **Btx-Bedingungen** war in Ziffer 9 eine verschuldensunabhängige Haftung des Kunden für Schäden vorgesehen, welche durch sorgfaltswidrigen Umgang mit PIN und TAN entstehen[1080]; eine vergleichbare Regelung enthielten bis 1989 die **ec-Bedingungen**.[1081] Nach dem **Sphärengedanke**[1082] sollte das Missbrauchsrisiko bei der Verwendung von PIN und TAN von demjenigen getragen werden, in dessen Verantwortungsbereich der sichere Umgang mit diesem Legitimationsmedium gehörte. Die Zulässigkeit solcher

---

[1077] *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 148; wohl auch *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 81.

[1078] *Karper*, DuD 2006, 215 (219); *Borges*, NJW 2005, 3313 (3315); *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 81.

[1079] *Kind/Werner*, CR 2006, 353 (360); BGH NJW 1994, 3102 (3105); Bamberger/Roth-*Unberath*, § 254 BGB Rn. 68 mwN.

[1080] Dazu *Canaris*, Bankvertragsrecht, Rn. 527 ff, 527 hh.

[1081] Zur Unwirksamkeit dieser Klausel nach § 9 Abs. 2 Nr. 1 AGBG (jetzt § 307 Abs. 2 Nr. 1 BGB) s. BGHZ 135, 116 (121 ff.); ausführlich *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 171 ff.

[1082] *Canaris*, Bankvertragsrecht, Rn. 527 ff; *Borsum/Hofmeister*, NJW 1985, 1205 ff.; *Werner*, in: Hellner/Steuer, Band 6, Rn. 19/82; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 141 f.

verschuldensunabhängig formulierter Klauseln ist umstritten,[1083] die Frage war jedoch nicht Gegenstand einer gerichtlichen Entscheidung. Für das Online-Banking wäre eine Übertragbarkeit des Sphärengedankens denkbar, da auch hier der Kunde nach Überlassung der Legitimationsmedien das Risiko eines Missbrauchs letztlich besser beherrschen kann. Dagegen spricht aber bereits, dass es sich beim Btx um ein geschlossenes System handelte und Bedrohungen wie Phishing und Pharming zur damaligen Zeit noch unbekannt waren; die Missbrauchsursachen beim Btx waren stets am Anschluss des Kunden zu suchen.[1084]

557 Für den Bereich des Online-Banking ist mit der heute wohl herrschenden Meinung die Anordnung einer verschuldensunabhängigen Haftung in AGB als gemäß § 307 BGB unwirksam anzusehen.[1085] Nach § 307 Abs. 2 Nr.1 BGB besteht eine gesetzliche Vermutung („im Zweifel") der Unwirksamkeit einer Klausel bei Abweichung vom **Leitbild des dispositiven Gesetzesrechts** in AGB, die nur dann widerlegt ist, wenn eine Gesamtwürdigung aller Umstände unter Abwägung der beiderseitigen Interessen ergibt, dass die Klausel den Kunden nicht unangemessen benachteiligt.[1086] Maßgeblich ist hierbei zu berücksichtigen, dass das in § 280 Abs. 1 BGB zum Ausdruck kommende **Verschuldensprinzip** nicht nur auf Zweckmäßigkeitserwägungen beruht, sondern eine Ausprägung des Gerechtigkeitsgebots darstellt.[1087] Eine Abweichung vom Verschuldensprinzip kann nur dann wirksam vereinbart werden, wenn sie durch höhere Interessen des Verwenders der AGB gerechtfertigt oder durch Gewährung rechtlicher Vorteile ausgeglichen wird.[1088] Ein besonderes Interesse der Bank an der alleinigen Risikotragung durch den Kunden besteht beim Online-Banking indessen nicht, da die Bank durch Eröffnung des Online-Banking-Verkehrs das Risiko geschaffen hat[1089] und sie die Sicherheit des Online-Banking entscheidend durch die Auswahl der technischen Systeme

[1083] Für zulässig hielten wegen unübersehbarer Schadensrisiken solche Klauseln: *Hellner*, FS Werner, S. 251, 273 ff.; *Reiser*/*Werner*, WM 1995, 1901 (1907); letztlich auch *Blaurock,* CR 1989, 561 (566), da der Kunde jederzeit die PIN-Nummern ändern könne; dagegen bereits *Borsum*/*Hoffmeister*, BB 1983, 1441 (1443); *Canaris*, Bankvertragsrecht, Rn. 527 ff.

[1084] *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 142.

[1085] *Kind/Werner*, CR 2006, 353 (354); *Erfurth*, WM 2006, 2198 (2200); *Wiesgickl*, WM 2000, 1039 (1050); *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 85; *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 176; *Spindler*, in: Hadding/Hopt/Schimansky, S. 216 f.; *Hartmann*, in: Hadding/Hopt/Schimansky, S. 319; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 141 f.; *Werner*, in: Hellner/Steuer, Band 6, 19/82.

[1086] BGH NJW 2003, 1447 (1448); Palandt-*Heinrichs*, § 307 BGB Rn. 25.

[1087] BGHZ 135, 116 (121); BGHZ 114, 238 (242 f.).

[1088] BGHZ 135, 116 (121); BGHZ 114, 238 (242 f.).

[1089] *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 142.

mitbestimmt.[1090] Eine alleinige Risikozuweisung an den Kunden ist auch deshalb abzulehnen, weil Möglichkeiten des Kunden zur Gefahrbeherrschung maßgeblich durch die Instruktion und Aufklärung seitens der Bank mitbestimmt werden. Da die Risikoabwälzung auch nicht durch Vorteile des Kunden ausgeglichen wird, ist eine Klausel, welche ohne Rücksicht auf schuldhafte Pflichtverletzungen das Missbrauchsrisiko dem Kunden zuweist, als nach Treu und Glauben unangemessene Benachteiligung zu werten (§ 307 Abs. 1, 2 Nr. 1 BGB).[1091]

(e) Zwischenergebnis

558 In materiell-rechtlicher Hinsicht kommen in den Fällen des Missbrauchs der Legitimationsmedien beim Online-Banking Ansprüche der Bank gegen den Kunden aus § 670 BGB bzw. §§ 280 Abs. 1, 241 Abs. 2 BGB in Betracht. Eine verschuldensunabhängige Haftung kann zu Lasten des Kunden kann nicht AGB nicht wirksam vereinbart werden. Sofern die Bank keinen Vertragsschluss beweisen kann (zum Anscheinsbeweis s. unten), kann sie ihre Forderung allein auf eine Sorgfaltspflichtverletzung des Kunden im Umgang mit den Legitimationsmedien stützen. Entscheidend ist hierbei die Pflichtenabgrenzung zwischen Bank und Kunde, wobei sich eine enge Wechselbeziehung zwischen den Pflichten der Bank (insbesondere Informations- und Warnpflichten) und den Pflichten des Kunden zeigt. Den Bankkunden treffen beim Online-Banking keine gegenüber dem normalen Internetverkehr erhöhten Sorgfaltsanforderungen. Die Sicherheitserwartungen des Verkehrs orientieren sich insbesondere im IT-spezifischen Bereich an den technischen Fähigkeiten des Durchschnittsnutzers. Sofern im Einzelfall ein Schadensersatzanspruch gegen den Kunden bejaht werden kann, kommt eine Kürzung wegen Mitverschuldens der Bank etwa wegen unzureichender Aufklärung in Betracht.

(4) Prozessuale Rechtslage, insbesondere Anscheinsbeweis

559 Nach allgemeinen Beweislastgrundsätzen trägt die **Bank die Darlegungs- und Beweislast** dafür, dass zwischen ihr und dem Kunden ein Überweisungsvertrag zustande gekommen ist oder – wenn ein Missbrauchsfall ist – dass der Kunde die ihm obliegende Sorgfalt verletzt hat (die Beweislastumkehr des § 280 Abs. 1 Satz 2 BGB gilt nur hin-

[1090] *Werner*, MMR 1998, 338 (340); *Wiesgickl*, WM 2000, 1039 (1050); *Janisch/Schartner*, DuD 2002, 162 (167); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 142. Zu verschuldensunabhängigen Abwälzung des Fälschungsrisikos auf den Kunden in den ec-Bedingungen 1989 s. BGHZ 135, 116 (122) und ausführlich *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 171 ff.; zur Kundenkreditkarte BGHZ 114, 238 (245).

[1091] *Kind/Werner*, CR 2006, 353 (354).

sichtlich des Vertretenmüssens).[1092] Bestreitet der Kunde Urheber des elektronischen Überweisungsauftrages zu sein, wird die Bank im Regelfall nicht beweisen können, dass gerade der Kunde oder ein von ihm bevollmächtigter Dritter die für die Überweisung erforderlichen Eingaben getätigt und das Legitimationsmedium verwandt hat.[1093] Angesichts der Beweisnot der Bank kommen **Beweiserleichterungen** in Form entweder einer Umkehr der Beweislast ((a)) oder eines Anscheinsbeweises ((b)) zu Lasten des Kunden in Betracht.

(a) Umkehr der Beweislast

560 Eine Beweislastumkehr zugunsten der Bank, so dass der Kunde nachweisen müßte, dass er nicht die elektronische Willenserklärung abgegeben hat, findet keine Grundlage im Gesetz[1094] und wäre auch nicht sachgerecht, da sie dem Kunden den Vollbeweis aufbürden würde. Der Kunde ist selbst unter Zugrundelegung von Gedanken aus der **Gefahrenkreis- bzw. Sphärentheorie**[1095] nicht in der Lage, Risiken zu beherrschen, die nicht aus seinem Bereich stammen; gerade durch diese nicht auszuschließende Möglichkeit charakterisiert sich jedoch das Internet-Banking, da Kommunikationskanäle, die weder vom Kreditinstitut noch vom Kunden beherrschbar sind, benutzt werden.[1096]

561 Die oben beschriebene Bedrohungslage (Rn. 479 ff.) beim Online-Banking unterscheidet sich auch wesentlich von den **Btx-Fällen**,[1097] in denen Instanzgerichte wohl eine Beweislastumkehr zu Lasten des Anschlussinhaber bejaht haben.[1098] Dort war nur fraglich, ob der Anschlussinhaber selbst oder ein Familienangehöriger bzw. Dritter den häuslichen Btx-Anschluss benutzt hatte. Die missbräuchliche Nutzung hatte daher jedenfalls im Einflussbereich des Anschlussinhabers stattgefunden, was eine Beweislastverteilung nach Risikosphären nahe liegend erscheinen ließ. Überdies handelte es sich

---

[1092] *Borges*, NJW 2005, 3313 (3316); *Erfurth*, WM 2006, 2198 (2203); *Karper*, DuD 2006, 215 (218); *Wiesgickl*, WM 2000, 1039 (1047); *Werner*, in: Schwarz/Peschel-Mehner, Recht des Internet, Teil 2, Kap. 2 A Rn. 2 f.

[1093] *Kind/Werner*, CR 2006, 353 (359); *Karger*, DuD 2006, 215 (218); *Langenbucher*, Die Risikoverteilung im bargeldlosen Zahlungsverkehr, S. 147.

[1094] Zur Beweislastumkehr als Rechtsfortbildung Musielak-*Foerste*, § 286 ZPO Rn. 37; MünchKommZPO-*Prütting*, § 286 ZPO Rn. 117, 119, 121; *Stodolkowitz*, VersR 1994, 11 (13 f.); für strenge Voraussetzungen *Prütting*, RdA 1999, 107 (110 f.); Zöller-*Greger*, Vor § 284 ZPO Rn. 17 f.

[1095] Grundlegend *Prölss*, Beweiserleichterungen im Schadensersatzprozeß, S. 65 ff.; krit. *Musielak*, AcP 176 (1976), 465 (470 ff.).

[1096] *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 145. Ebenso verneint die Rechtsprechung eine Beweislastumkehr bei Internet-Auktionen OLG Naumburg NOZ 2005, 2222 (2224); OLG Köln MMR 2002, 813; LG Bonn MMR 2004, 179 (180); LG Bonn MMR 2002, 255 (256); LG Konstanz MMR 2002, 835 (836).

[1097] OLG Oldenburg NJW 1993, 1400 ff.; OLG Köln VersR 1993, 840 ff.; OLG Köln VersR 1998, 725 ff.

[1098] Das OLG Oldenburg spricht bspw. von einer „tatsächlichen Vermutung“, was trotz Bezugnahme auf den Sphärengedanken auf einen bloßen Anscheinsbeweis hindeutet, s. OLG Oldenburg NJW 1993, 1400 (1401).

bei Btx um ein geschlossenes System.[1099] Auf die technischen Möglichkeiten des Phishing oder Pharming lässt sich dieser Gedanke nicht übertragen, da hierbei Angriffe aus dem Internet als einem offenen Netz erfolgen, welches der Kontrolle des Bankkunden entzogen ist.

562 Die Ablehnung einer Beweislastumkehr rechtfertigt sich auch im Hinblick auf **technische Weiterentwicklungen** oder Durchbrechungen des technischen Schutzes: Bei Annahme einer Beweislastumkehr würde dem vermeintlich Erklärenden stets der Vollbeweis aufgebürdet, dass die Erklärung nicht von ihm stammt. Der jeweilige technische Standard und sein Schutzniveau könnten nicht angemessen berücksichtigt werden.[1100] In vergleichbarer Weise und aus guten Gründen wendet die ständige Rechtsprechung bei technischen Regeln (z.B. DIN) stets nur einen Anscheinsbeweis bei Verletzung technischer Standards an.[1101] Eine Beweislastumkehr wäre der besonderen Situation beim Online-Banking nicht angemessen.[1102]

(b) Beweis des ersten Anscheins

(i) Voraussetzungen des Anscheinsbeweises

563 Die überwiegende Ansicht in der Literatur belässt es bei der Beweislast der Bank, spricht sich in Anlehnung an die Rechtsprechung und hM zur ec-Karte (dazu Rn. 569) jedoch für einen alternativen **Anscheinsbeweis**[1103] zugunsten der Bank aus.[1104] Der Beweis des ersten Anscheins spricht nach Ansicht des Schrifttums demnach für die Tatsache, dass

- derjenige, der das Legitimationszeichen verwandt hat, entweder der Kunde selbst ist oder zumindest von diesem autorisiert wurde, die Willenserklärung abzugeben,
- hilfsweise für die Tatsache, daß der Kunde den Mißbrauch der Legitimationszeichen schuldhaft ermöglicht hat.

[1099] *Trapp*, WM 2001, 1192 (1195).

[1100] Ähnl. *Sieber/Nöding*, ZUM 2001, 199 (208 f.): Flexibilität für künftige technische Entwicklungen erforderlich.

[1101] S. etwa BGH NJW 1991, 2021; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 22 ff.

[1102] Dies verkennt *Trapp*, WM 2001, 1192 (1200 f.), der hier eine gesetzliche Spezialregelung des Beweismaßes annehmen will; ähnl. wie hier aber *Melullis*, MDR 1994, 109 (111); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 144 f.; s. auch *Roßnagel*, MMR 2000, 451 (459).

[1103] So *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 146.

[1104] *Borges*, NJW 2005, 3313 (3316); *Karper*, DuD 2006, 215 (218 f.); *Kunst*, MMR Beilage 9/2001, 23 (25); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 149 ff.; *Werner*, MMR 1998, 232 (235); *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 83; *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 180; *Kümpel*, Bank- und Kapitalmarktrecht, 4.752; *Werner*, in: Hellner/Steuer, Band 6, 19/84; *Werner*, in: Schwarz/Peschel/Mehner, Recht des Internet, Teil 2, Kap. 2 A Rn. 24 f.; *Borges*, in: Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bankrecht, § 8 Rn. 79; einschränkend *Wiesgickl*, WM 2000, 1039 (1050).

564 Gerichtliche Entscheidungen zur Beweislast beim Online-Banking stehen soweit ersichtlich noch aus.[1105]

565 Für das PIN-/TAN-Verfahren und das HBCI-Verfahren ist anders als in **§ 371a Abs. 1 Satz 2 ZPO/§ 292a ZPO aF** für die qualifizierte elektronische Signatur nach dem Signaturgesetz (SigG) kein Anscheinsbeweis für die Echtheit der Erklärung im Gesetz angeordnet. Dies schließt indessen nicht aus, aufgrund der allgemeinen Grundsätze des Beweisrechts einen Anscheinsbeweis auch für diese Sicherungsverfahren zu bejahen.[1106] Für Sicherungsverfahren auf Basis einer elektronischen Signatur wie beispielswiese HBCI liegt eine Parallele zu der gesetzlichen Regelung in § 371a Abs. 1 Satz 2 ZPO/§ 292a ZPO nahe.[1107]

566 Grundlage des Anscheinsbeweises ist, dass sich unter Berücksichtigung aller unstreitigen und festgestellten Einzelumstände und besonderen Merkmale des Sachverhalts ein für die zu beweisende Tatsache nach der Lebenserfahrung **typischer Geschehensablauf** ergibt.[1108] Ein typischer Geschehensablauf setzt voraus, dass ein bestimmter Sachverhalt feststeht, der nach der allgemeinen Lebenserfahrung auf eine bestimmte Ursache oder auf einen bestimmten Ablauf als maßgeblich für den Eintritt eines bestimmten Erfolgs hinweist.[1109] Die aus dem Sachverhalt zu ziehende Schlussfolgerung muss sich dem Betrachter gleichsam aufdrängen, so dass individuelle Kennzeichen des Einzelfalles zurücktreten und bedeutungslos erscheinen.[1110] Es handelt sich hierbei um keine Umkehr der Beweislast, sondern die Berücksichtigung von Erfahrungssätzen[1111] durch den Richter im Rahmen der freien Beweiswürdigung (§ 286 Abs. 1 ZPO),[1112] wobei die dem Erfahrungssatz zugrunde liegenden Tatsachen entweder unstreitig sein müssen oder ihrerseits des Vollbeweises bedürfen.[1113]

[1105] Das LG Bonn begründet seine Ablehnung des Anscheinsbeweises bei Internet-Auktionen jedoch ausdrücklich auch mit dem Unterschied zwischen dem bloßen Passwortschutz und der Verwendung von PIN und TAN, s. MMR 2004, 179 (181).

[1106] Gegen einen Umkehrschluss zu § 292a ZPO (jetzt § 371a Abs. 1 Satz 2 ZPO nF) im Zusammenhang mit Internet-Auktionen auch *Mankowski*, CR 2003, 44 (47); *Ernst*, Vertragsgestaltung im Internet, Rn. 28.

[1107] *Stockhausen*, WM 2001, 605 (618); *Wiesgickl*, WM 2000, 1039 (1050); *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 84; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 150.

[1108] BGH NJW 2004, 3623 - ec-Karte; BGH NJW 2001, 1140 (1141); BGH NJW 1987, 2876; Musielak-*Foerste*, § 286 ZPO Rn. 23.

[1109] BGH NJW 2004, 3623 - ec-Karte; BGH NJW 2001, 1140 (1141); BGH WM 1997, 1493 (1496); BGHZ 100, 31 (33).

[1110] S. BGHZ 100, 241 (216).

[1111] Ausführlich MünchKommZPO-*Prütting*, § 286 ZPO Rn. 55 ff.; Stein/Jonas-*Leipold*, § 286 ZPO Rn. 90.

[1112] MünchKommZPO-*Prütting*, § 286 ZPO Rn. 47; Zöller-*Greger*, Vor § 284 ZPO Rn. 29.

[1113] Zöller-*Greger*, Vor § 284 ZPO Rn. 29.

567 Die Typizität des Geschehensablaufs erfordert nicht, dass die Ursächlichkeit einer bestimmten Tatsache für einen bestimmten Erfolg bei allen Sachverhalten dieser Fallgruppe notwendig immer vorhanden ist. Die Ursächlichkeit einer bestimmten Tatsache für einen bestimmten Erfolg muss aber so häufig gegeben sein, dass die **Wahrscheinlichkeit**, einen solchen Fall vor sich zu haben, **sehr groß** ist.[1114] Die bloß abstrakte Möglichkeit eines anderen Geschehensablaufs steht der Annahme einem Erfahrungssatz nicht entgegen.[1115]

568 Bei der Prüfung des Anscheinsbeweises sind zwei Fragen strikt zu trennen[1116]: als Vermutungsgrundlage ist zunächst zu prüfen, ob beim Online-Banking überhaupt ein Erfahrungssatz bejaht werden kann. Wird ein Erfahrungssatz bejaht, stellt sich weiter die Frage, ob die **Vermutungsfolge** im Einzelfall dadurch erschüttert werden kann, dass die ernsthafte Möglichkeit eines Phishing- oder Pharming-Angriffs und damit ein atypischer Geschehensablauf dargelegt wird.

(ii) Rechtslage bei ec-Karten und Internet-Auktionen

(a) ec-Karten

569 Für den Einsatz von **ec-Karten** bejaht die obergerichtliche Rechtsprechung seit langem einen Anscheinsbeweis dafür, dass bei Einsatz der PIN tatsächlich auch der Verfügungsberechtigte die ec-Karte benützt oder jedenfalls grob fahrlässig den Mißbrauch ermöglicht hat.[1117] Die hM nimmt hierbei an, dass die bei den Banken verwendeten Sicherheitssysteme für ec-Karten und Geldautomaten Manipulationen durch Dritte mit sehr hoher Wahrscheinlichkeit ausschließen oder zumindest nachträglich erkennbar machen.[1118] Im Einzelfall dürfte zwar nach wie vor Streit über die Verschlüsselungsgüte des Systems bestehen.[1119] Auch lässt die Rechtsprechung zunehmend die Möglichkeiten des Ausspähens oder Abfangens der PIN als Erschütterung des Anscheinsbeweises ge-

---

[1114] BGH NJW 2004, 3623 - ec-Karte; BGH VersR 1991, 460 (462); Zöller-*Greger*, Vor § 284 ZPO Rn. 29.

[1115] BGH NJW 2004, 3623 (3624); Stein/Jonas-*Leipold*, § 286 ZPO Rn. 90.

[1116] S. auch *Karger*, DuD 2006, 215 (219).

[1117] St. Rspr. der meisten Instanzgerichte: s. etwa KG NJW 1992, 1051 (1052); LG Bonn NJW-RR 1995, 815; LG DarmstadtWM 2000, 911 (913 f.); LG Frankfurt WM 1999, 1930 (1932 f.); LG Hannover WM 1998, 1123 f.; LG Köln WM 1995, 976, (977 f.); AG Frankfurt NJW 1998, 687 f.; AG Osnabrück NJW 1998, 688 f.; aA OLG Hamm NJW 1997, 1711 (1712 f.): wegen mangelnder Schlüsselsicherheit; LG BerlinWM 1999, 1920 f.: wegen Möglichkeit des Ausspähens.

[1118] *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 181; *Werner*, MMR 1998, 338 (339) mwN aus der Rechtsprechung der Instanzgerichte.

[1119] Charakteristisch das Urteil des OLG Hamm NJW 1997, 1711 (1712 f.); dieses Urteil ist jedoch vereinzelt geblieben. Außerdem haben die Banken die Verschlüsselungstiefe der EC-Karten verbessert, so daß diese Rechtsprechung jedenfalls von ihrem Ausgangspunkt her nicht mehr anwendbar sein dürfte.

nügen.[1120] Sie fragt dann aber häufig nach Einhaltung der gebotenen Sorgfalt zur Abschirmung der PIN-Eingabe,[1121] denn es liegt weitgehend im Macht- und Einflußbereich des Kunden, ob Dritte Kenntnis von der PIN erhalten, etwa indem er bei der Eingabe der PIN diese verdeckt hält etc.[1122] Da beim Online-Banking ebenfalls mit PIN gearbeitet wird, liegt eine Übertragung dieser Grundsätze nahe. Der BGH hatte die Frage des Anscheinsbeweises beim ec-Kartenmissbrauch bislang offen gelassen.[1123] In der Entscheidung vom 5. Oktober 2004 hat das Gericht nunmehr die bisherige Rechtsprechungslinie der Instanzgerichte bestätigt.[1124]

(b) Internet-Auktionen

570 Ganz anders ist die Rechtslage im Bereich der Internet-Auktionen. Die Vergabe von Passwörtern begründet nach der Rechtsprechung der Instanzgerichte und dem wohl überwiegenden Teil der Literatur **keine Vermutung** für die Verwendung durch den Inhaber.[1125] Anders als bei ec-Karten und dem Online-Banking trägt somit bei Internet-Auktionen der Erklärungsempfänger die volle Beweislast für den Vertragsschluss. Die Durchsetzung vertraglicher Ansprüche wird mithin regelmäßig ausscheiden, wenn der registrierte Nutzer behauptet, er habe die Erklärung nicht abgegeben, was in der Literatur als „Widerrufsrecht kraft Beweislast“ kritisiert wird.[1126]

571 Die instanzgerichtliche Rechtsprechung verneint unter Hinweis auf den derzeitigen **Sicherheitsstandard** der im Internet verwendeten Passwörter und das Fehlen einheitlicher Maßstäbe für die Verschlüsselung den für die Annahme eines Anscheinsbeweises typischen Geschehensablaufs. Der Sicherheitsstandard für Passwörter sei nicht ausreichend, um aus der Verwendung eines geheimen Passworts auf denjenigen als Verwender zu schließen, dem dieses Passwort ursprünglich zugeteilt worden ist.[1127] Die Tatsache, dass weltweit tagtäglich Millionen von Rechtsgeschäften per Internetauktion klag-

---

[1120] So etwa AG München NJW-RR 2001, 1056 (1057).

[1121] S. LG Halle WM 2001, 1298 (1299).

[1122] Allerdings mag man darüber streiten, welches Ausmaß an Sorgfalt angesichts der Realität im Einsatz von PIN-Eingabegeräten dem Kunden abverlangt werden kann. Oftmals sind diese Geräte für jedermann einsehbar, so daß die Geheimhaltung durch verdeckte Eingabe an den Kunden in zahlreichen Situationen überspannte Anforderungen stellen würde.

[1123] BGHZ 145, 337 (342).

[1124] BGH NJW 2004, 3623 (3624).

[1125] OLG Köln MMR 2002, 813 (814); LG Bonn MMR 2004, 179 (180); LG Bonn MMR 2002, 255 (256); LG Konstanz MMR 2002, 835 (837); ebenso *Borges*, NJW 2005, 3313 (3317); *Borges*, in: Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bankrecht, § 8 Rn. 80; *Mehrings*, in: Hoeren/Sieber, Kap. 13.1 Rn. 270 ff.; *Wiebe*, in: Spindler/Wiebe, Internet-Auktionen und Elektronische Marktplätze, Kap. 4 Rn. 61.

[1126] *Mankowski*, CR 2003, 44; *Ernst*, Vertragsgestaltung im Internet, Rn. 26.

[1127] OLG Köln MMR 2002, 813 (814); LG Bonn MMR 2002, 255 (256); LG Bonn MMR 2004, 179 (180).

los abgewickelt werden, lasse den Schluss auf die Verlässlichkeit des Mediums Internet im Allgemeinen und der Kommunikationsplattform Internet-Auktion im Besonderen nicht zu.[1128] Hervorgehoben wird dabei der Unterschied der Verwendung eines bloßen Passwortes – welches noch dazu online ohne Identitätsprüfung vergeben wird – gegenüber den Sicherungsverfahren bei ec-Karten mit PIN und Online-Banking mit PIN und TAN.[1129] Für die hM lässt sich hierbei die gesetzgeberische Wertung des § 371a Abs. 1 Satz 2 ZPO/§ 292a ZPO aF anführen, wonach erst eine qualifizierte elektronische Signatur den Anscheinsbeweis rechtfertigt (zur Bedeutung dieser gesetzlichen Wertung für das Online-Banking unten Rn. 565).[1130] Soweit diese Beweislastverteilung für den Käufer im Einzelfall ein Reuerecht begründen sollte, wird dies in der Rechtsprechung hingenommen, weil der Verkäufer dieses Risiko bei der Nutzung einer Internet-Auktion in Kenntnis der Missbrauchsmöglichkeiten eingehe.[1131]

572 Ein Teil der Literatur argumentiert dagegen, für die Authentizität einer unter einer E-Mail-Adresse abgebenen und durch Passwort geschützen E-Mail spreche die **allgemeine Lebenserfahrung**, was bereits (unabhängig von einem technischen Sicherheitsstandard) einen Anscheinsbeweis rechtfertige.[1132] Das Ausspähen des Passwortes sei wegen der zu überwindenden technischen Hürden nicht jedermann möglich, sondern verlange besondere Fachkenntnisse.[1133] Die Wahrscheinlichkeit einer Manipulation sei folglich trotz der mangelnden Sicherheit des Passwortsystems im Verhältnis zum Gesamtumfang des E-Mail-Aufkommens denkbar gering.[1134] Wertungsmäßig wird überdies darauf hingewiesen, der Nutzer habe das Missbrauchsrisiko zu tragen, weil er sich des Internets in Kenntnis seiner Risiken bediene.[1135]

[1128] LG Bonn MMR 2004, 179 (180).

[1129] LG Bonn MMR 2002, 255 (257); LG Bonn MMR 2004, 179 (181); *Borges*, NJW 2005, 3313 (3317); *Wiebe*, MMR 2002, 257 (258); *Wiebe*, in: Spindler/Wiebe, Internet.Auktionen und Elektronische Marktplätze, Kap. 4 Rn. 61. Gegen die Zugrundelegung bestimmter technischer Sicherheitsstandards, weil es sich hierbei um eine „normative Überhöhung" handele, s. *Mankowski*, CR 2003, 44 (45).

[1130] *Mehrings*, in: Hoeren/Sieber, Kap. 13.1 Rn. 290; *Wiebe*, MMR 2002, 257 (258); *Wiebe*, in: Spindler/Wiebe, Internet-Auktionen und Elektronische Marktplätze, Kap. 4 Rn. 62.

[1131] OLG Naumburg NJOZ 2005, 2222 (2224); LG Bonn MMR 2004, 179 (180). Abweichend davon möchte *Wiebe*, in: Spindler/Wiebe, Internet-Auktionen und Elektronische Marktplätze, Kap. 4 Rn. 68; das Missbrauchsrisiko nicht einem der beiden Vertragspartner des Kaufvertrags, sondern als Betreiber des elektronischen Marktplatzes und Nutznießer des Geschäftsverkehrs dem (dritten) Auktionshaus auferlegen.

[1132] So *Mankowski*, CR 2003, 44 (45).

[1133] *Mankowski*, CR 2003, 44 (45); *Hoffmann*, in: Leible/Sosnitza, Versteigerungen im Internet, Teil 3 Kap. B Rn. 176; *Ernst*, Vertragsgestaltung im Internet, Rn. 29.

[1134] *Mankowski*, MMR 2004, 182 ff.; *Mankowski*, CR 2003, 44 (45); *Krüger/Büttner*, MDR 2003, 181 (186); *Hoffmann*, in: Leible/Sosnitza, Versteigerungen im Internet, Teil 3, Kap. B, Rn. 184; *Ernst*, Vertragsgestaltung im Internet, Rn. 26 ff.

[1135] *Mankowski*, CR 2003, 44 (46).

(iii) Bestehen eines Erfahrungssatzes beim Online Banking

(a) Ausgangspunkt der hM: Technische Sicherheit des Online-Banking

573 Grundlage für beide Formen des Anscheinsbeweises (Urheberschaft für die Erklärung und Sorgfaltspflichtverletzung) ist, dass für das Online-Banking überhaupt entsprechende Erfahrungssätze formuliert werden können. Als Vermutungsgrundlage des Anscheinsbeweises hat die **Bank** daher die technische Sicherheit ihres Online-Banking-Systems gegen Eingriffe Dritter zu **beweisen** (Rn. 566). Die **hM bejaht** für das Online-Banking einen Anscheinsbeweis mit dem mehr oder minder pauschalen Hinweis auf den **hohen technischen Sicherheitsstandard** der verwendeten PIN-/TAN-Sicherungssysteme. Diese könnten nur mit einem Aufwand überwunden werden, welcher unter technischen oder wirtschaftlichen Gesichtspunkten unwahrscheinlich erscheine.[1136] Die Annahme hinreichender technischer Sicherheit beim Online-Banking bildet somit die tatsächliche Basis für den die erforderliche hohe Wahrscheinlichkeit, dass die Erklärung vom Kunden selbst oder einem autorisierten Dritten abgesandt wurde oder aber, dass sich ein unbefugter Dritter die Legitimationsmedien nur aufgrund einer Sorgfaltspflichtverletzung des Kunden zunutze machen konnte.

574 Der Anscheinsbeweis ist jedoch nur solange und nur insoweit gerechtfertigt, als ein technisches Sicherheitsniveau gewährleistet werden kann, welches auch im Hinblick auf die technische Fortentwicklung und aktuelle Bedrohungen noch als weitgehend unüberwindlich angesehen werden kann.[1137] In Bezug auf die Sicherheit des PIN-/TAN-Verfahrens ist der hM im Ausgangspunkt zumindest soweit zuzustimmen, als PIN und TAN durch **Ausrechnen** oder bloßes **Ausprobieren** nur unter völlig unwahrscheinlichen Umständen erlangt werden können.[1138] Genauso wird man den Anscheinsbeweis für die Urheberschaft des Bankkunden für einen Transaktionsauftrag nicht schon deshalb verneinen können, weil der Bankkunde – unter Verletzung seiner Pflichten aus dem Online-Bankingvertrag – die Verwendung der Legitimationsmedien durch Dritte

[1136] *Werner*, MMR 1998, 338 (339); *Wiesgickl*, WM 2000, 1039 (1047, 1050); *Trapp*, WM 2001, 1192 (1199); *Bock,* in: Bräutigam/Leupold, Kap. VII Rn. 83; *Kunst*, MMR Beilage 9/2001, 23 (24 f.); *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 183; *Werner*, in: Hoeren/Sieber, Kap. 13.5. Rn. 37; *Werner*, in: Hellner/Steuer, Band 6, 19/ 17, 84; *Werner*, in: Schwarz/Peschel-Mehner, Recht des Internet, Teil 2, Kap. 2 A Rn. 25; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 150. Im Ergebnis wohl ebenfalls auf die technische Sicherheit abstellend *Karper*, DuD 2006, 215 (218 f.).

[1137] *Werner*, in: Schwarz/Peschel-Mehner, Recht des Internet, Teil 2, Kap. 2 A Rn. 73.

[1138] *Kind/Werner*, CR 2006, 353 (369); *Wiesgickl*, WM 2000, 1039 (1047). Ebenso die Antwort der Bundesregierung vom 4.7.2000 auf die Kleine Anfrage der Abgeordneten Rainer Funke, Dr. Edzard Schmidt-Jortzig, Dr. Max Stadler, weiterer Abgeordneter und der Fraktion der F.D.P. – Drucksache 14/3603 –, BT-Drucks. 14/3757, S. 2.

ermöglichen kann.[1139] Denn während bei Internet-Auktionen die **Weitergabe des Passwortes** etwa im Familienkreis – nicht unüblich sein dürfte,[1140] werden die Legitimationsmedien für das Online-Banking regelmäßig auch im Familienkreis (und erst recht im Bekanntenkreis) vertraulich behandelt.

575 Bei der Frage des Anscheinsbeweises vielfach unberücksichtigt bleiben indes die in neuerer Zeit aufgetretenen Möglichkeiten des **„Ausspähens"** der Legitimationsmedien durch Phishing-E-Mails und Trojaner. Für ec-Karten hat der BGH die Möglichkeit des Ausspähens der PIN mit Hilfe optischer oder technischer Hilfsmittel bzw. Manipulation des Geldautomaten zwar als Möglichkeit zur Kenntnis genommen. Das Gericht sah den Anscheinsbeweis aufgrund solcher Phänomene aber nicht generell in Frage gestellt.[1141] Diese Erwägungen können aufgrund der völlig anders gelagerten Möglichkeiten die Legitimatonsmedien auszuspähen jedoch nicht unbesehen auf das Online-Banking übertragen werden. Zwar kann auch beim Online-Banking das Ausspähen „konventionell" durch Verschaffung der auf einem Zettel notierten PIN und einer TAN-Karte erfolgen – die Situation unterscheidet sich dann nicht wesentlich von der ec-Kartenproblematik. Weitaus relevanter sind indessen die hier interessierenden neuen Erscheinungen der Phishing-E-Mails oder trojanischen Pferde. Gerade im Hinblick auf diese Gefahren bieten viele der derzeit verwendeten PIN-/TAN-Sicherungsverfahren nicht die erforderliche Sicherheit um von einer faktischen Unüberwindbarkeit sprechen zu können. Nach dem derzeitigen Stand der Technik wird man zwischen Verfahren mit Medienbruch (unten (b)) und solchen ohne Medienbruch (unten (c)) zu unterscheiden haben:

(b) Sicherungsverfahren ohne Medienbruch

576 Angesichts der neuen „elektronischen" Bedrohungsformen muss die vor einigen Jahren wohl noch zutreffende Annahme, die Überwindung der PIN-/TAN-Sicherungsverfahren sei nur mit unvertretbarem Aufwand möglich und liege daher außerhalb jeder Wahrscheinlichkeit, heute zumindest für **Systeme ohne Medienbruch** (Rn. 519) als obsolet angesehen werden. Wie oben beschrieben (Rn. 519) liegt der Nachteil dieser PIN-/TAN-Verfahren in der **Möglichkeit, PIN und TAN auf rein elektronischem Wege**

[1139] *Wiesgickl*, WM 2000, 1039 (1047) verneint aus diesem Grund einen Anscheinsbeweis für die Urheberschaft.

[1140] So auch *Hoffmann*, in: Leible/Sosnitza, Versteigerungen im Internet, Teil 3, Kap. B, Rn. 175, 185.

[1141] Vgl. BGH NJW 2004, 3623 (3624). Im Fall verneinte der BGH eine Erschütterung des Anscheinsbeweises, da die Klägerin am Tag des Diebstahls der ec-Karte keine Abhebung vorgenommen hatte. Nach Auffassung des BGH bestand bei diesem Geschehensablauf keine Möglichkeit des „Ausspähens" der PIN ohne Sorgfaltswidrigkeit der Kundin.

(im Zweifel damit auch aus dem weit entfernten Ausland) beispielsweise durch Trojaner **auszuspähen**.

577 Für die unberechtigte Nutzung von Nutzer-Accounts bei Internet-Auktionen stellte das LG Konstanz auf der Grundlage eines Sachverständigengutachtens fest, das Ausspähen des Passworts durch Trojaner usw. sei eine „reale Gefahr".[1142] Die vielfältigen Manipulationsmöglichkeiten im Internet ließen damit keinen sicheren Rückschluss auf die Person des Erklärenden zu.[1143] Das OLG Köln verneinte für Internet-Auktionen trotz der Schwierigkeiten bei der Entschlüsselung des Passworts den für die Annahme eines Anscheinsbeweises typischen Geschehensablauf, weil ein Missbrauch auch ohne vorherige Entschlüsselung des Passwortes durch bloßes Ausspähen möglich sei.[1144]

578 Gegenüber dem bloßen Passwortschutz bei Internet-Auktionen bieten Verfahren mit PIN und TAN zwar einen deutlich höheren Schutz gegen Entschlüsselung. Auch dieses System hilft indessen nicht, wenn ein Angreifer aufgrund einer Phishing-E-Mail oder Pharming Zugriff auf PIN und TAN selbst erhält. Auf die von der hM angeführten technischen und finanziellen Hindernisse bei der Entschlüsselung kommt es aber nicht an, wenn PIN und TAN abgefangen und das **Sicherheitssystems des Internet-Banking** somit **umgangen** werden kann. Mit der Begründung des OLG Köln und des LG Koblenz lässt sich im Ergebnis auch der Anscheinsbeweis beim Online-Banking mit PIN-/TAN-Verfahren ohne Medienbruch in Zweifel ziehen.[1145] Angesichts der beschriebenen Anfälligkeit von Sicherungsverfahren ohne Medienbruch für Identitätsmissbrauch (vgl. die Bedrohungsszenarien und oben Rn. 519) und der Vielzahl der technischen Möglichkeiten des Ausspähens der Legitimationsmedien durch Phishing-E-Mails und Pharming lässt sich ein **Anscheinsbeweis für die Urheberschaft** bei Verwendung dieser Systeme **nicht** mehr begründen.[1146]

[1142] LG Konstanz MMR 2002, 835; dazu auch *Winter*, MMR 2002, 836.

[1143] LG Konstanz MMR 2002, 835.

[1144] Das OLG Köln MMR 2002, 813 (814) führt hierzu aus: „Auf die vom Kl. dargestellten Probleme einer „Entschlüsselung" des Passworts kommt es in diesem Zusammenhang nicht an. Ein Missbrauch setzt nämlich eine vorherige Entschlüsselung gar nicht voraus. Vielmehr kann jemand, der mit Abläufen im Netz ausreichend vertraut ist, was heute schon bei einer Vielzahl der Jugendlichen gegeben ist, ohne allzu großen Aufwand das Passwort „lesen". Von einer für einen Anscheinsbeweis ausreichenden Typizität wird man möglicherweise bei der Verwendung einer elektronischen Signatur ausgehen können, nicht aber bei einem ungeschützten Passwort."

[1145] Ebenso *Erfurth*, WM 2006, 2198 (2205). Anders *Karper*, DuD 2006, 215 (219) der zufolge die Einschätzung des LG Koblenz auf das Verfahren unter Nutzung von PIN und TAN wegen dessen höheren Schutzniveau nicht übertragen werden könne. Dies lässt indes außer Betracht, dass die Verschlüsselungsgüte keinen Schutz gegen ein Ausspähen des Passworts bietet.

[1146] Ebenso, jedoch ohne Ausnahme der Sicherungsverfahren mit Medienbruch *Kind/Werner*, CR 2006, 353 (359); *Erfurth*, WM 2006, 2198 (2205).

579 Ebensowenig ist eine Vermutung für eine **Pflichtverletzung** des Kunden gerechtfertigt. Gegen Bedrohungen durch Phishing und Pharming ist ein wirksamer Schutz durch den Kunden selbst schon wegen mangelnder IT-Kenntnisse regelmäßig nur in sehr begrenztem Umfang möglich (zu den Pflichten des Kunden im Einzelnen oben Rn. 281 ff.). Insbesondere bei der zunehmend zu beobachtenden Verwendung von Trojanern kann selbst dann Zugriff auf die Zugangsdaten erlangt werden, wenn der Kunde alle zumutbaren Sicherheitsvorkehrungen getroffen hat.[1147] Zum Teil werden eigene Sicherheitmaßnahmen des Kunden auch durch Maßnahmen der Bank konterkarriert – so etwa bei Verwendung aktiver Inhalte auf den Websites der Bank (Rn. 522). Keine Pflichtverletzung des Kunden ist beispielsweise auch dann anzunehmen, wenn der Identitätsmißbrauch durch eine lückenhafte Webanwendung ermöglicht wurde. Beispielhaft hierfür sind etwa Sicherheitslücken im Internet Explorer von Microsoft[1148] oder anderer Programme.[1149] Keineswegs kann gegenwärtig somit davon ausgegangen werden, die missbräuchliche Verwendung von PIN und TAN beruhe typischerweise auf einer Pflichtverletzung des Bankkunden.

580 In Zukunft ist zu erwarten, dass sich die Methode der „Online-Betrügereien" zunehmend von einfachen Phishing-E-Mails weg, hin zur Verwendung von **immer ausgefeilteren Schadprogrammen** verlagern wird.[1150] Im selben Maße verringern sich damit aber zugleich die Möglichkeiten des Bankkunden diesen Bedrohungen durch eigene Sorgfalt wirksam zu begegnen und somit die Risiken des Online-Banking zu beherrschen. Gerade in den die Fällen des Pharming (Szenarien 2 und 3) sind schon nach gegenwärtigem Stand der Informatik eine Vielzahl von Fallgestaltungen denkbar, in denen dem Kunden keine Pflichtverletzung vorgeworfen werden kann. Daraus muss gefolgert werden, dass der dem Anscheinsbeweis zugrundeliegende **Erfahrungssatz**, ein Missbrauch durch Dritte beruhe typischerweise auf einer Sorgfaltspflichtverletzung des Bankkunden, jedenfalls **für PIN-/TAN-Verfahren ohne Medienbruch zu verneinen** ist, da die zu fordernde Typizität angesichts der neuen Bedrohungsformen nicht (mehr) gegeben ist.[1151] Beließe man es bei der gegenwärtigen hM, würden die Risiken der künftigen Entwicklung von Schadprogrammen letztlich in weiten Teilen beweisrecht-

[1147] *Kind/Werner*, CR 2006, 353 (359).

[1148] Vgl. dazu abrufbar unter: http://www.heise.de/security/news/meldung/78372.

[1149] Ebenso mit weiteren Beispielen *Erfurth*, WM 2006, 2198 (2202).

[1150] *Erfurth*, WM 2006, 2198 (2206).

[1151] So auch *Kind/Werner*, CR 2006, 353 (359); *Erfurth*, WM 2006, 2198 (2206); Zweifel auch bei *Borges*, NJW 2005, 3313 (3317).

lich einseitig dem Kunden aufgebürdet, obwohl die Banken durch den Einsatz besserer technischer Systeme schon heute Abhilfe schaffen können.

581 Der Anscheinsbeweis kann bei Verwendung von PIN-/TAN-Verfahren ohne Medienbruch auch nicht auf das häufig – insbesondere in Bankenkreisen – verwendete Argument gestützt werden, erfolgreiche Phishing und Pharming-Attacken stellten **nur Einzelfälle** dar, so dass die ordnungsgemäße Transaktion der typische Geschehensablauf sei.[1152] Diese Behauptung entbehrt angesichts sich häufender Meldungen über Missbräuche beim Online-Banking allerdings einer gesicherten tatsächlichen Grundlage.[1153] Die Banken dürften über aussagekräftiges Zahlenmaterial verfügen, halten sich diesbezüglich jedoch bedeckt. Im Hinblick auf die Rechtsprechung der Instanzgerichte zu Internet-Auktionen ist die Tragfähigkeit des Arguments insgesamt zweifelhaft. Denn diese misst der weit überwiegenden Zahl der fehlerfrei durchgeführten Online-Geschäfte wegen der Unsicherheit des Passwortschutzes keine entscheidende Bedeutung bei.[1154] Da – wie ausgeführt – auch das PIN-TAN-Verfahren ohne Medienbruch in erheblichem Umfang anfällig für Ausspähen ist, dürften hier keine anderen Grundsätze gelten.

(c) Sicherungsverfahren mit Medienbruch

582 Gegenwärtig kann der erforderliche hohe Sicherheitsstandard zur Bejahung eines Anscheinsbeweises allenfalls dort bejaht werden, wo **Sicherungssysteme mit Medienbruch** (s. Rn. 520) Verwendung finden. Bei Verwendung eines TAN-Generators kann eine ausgespähte TAN wegen deren Verknüpfung mit der konkreten Transaktion des Bankkunden technisch nicht für eine andere (missbräuchliche) Transaktion verwendet werden. Bei Übermittlung der TAN und Bestätigung der übermittelten Transaktionsdaten durch eine SMS auf das Mobiltelefon des Bankkunden (mTAN) gelangt die gültige TAN stets nur auf das Mobiltelefon des Kunden. Ein Identitätsmißbrauch ist bei Verwendung von Systemen mit Medienbruch damit von vornherein nur dann denkbar, wenn neben der PIN auch die zugehörige Hardware (TAN-Generator, Mobiltelefon) in den Besitz des Täters gelangt, was dann aber die Vermutung einer unsorgfältigen Verwahrung dieser Geräte nahelegt (unten Rn. 583). Ein **Ausspähen der TAN auf *rein***

[1152] So im Ergebnis *Borges*, NJW 2005, 3313 (3317); *Karper*, DuD 2006, 215 (219).

[1153] Frankfurter Allgemeine Zeitung vom 11.7.2005: „Trickbetrüger nehmen Internet-Banking ins Visier“ und vom 10.3.2006: „Angriffe auf Online-Bankkunden nehmen sprunghaft zu“; Süddeutsche Zeitung vom 2.8.2006, S. 2: „Surfen am Abgrund“; Spiegel-Online vom 24.9.2006: „Phishing und Pharming – Die Bedrohung wächst“, abrufbar unter: http://www.spiegel.de/netzwelt/technologie/0,1518,438677,00.html.

[1154] LG Bonn MMR 2004, 179 (180).

elektronischem Wege durch Trojaner uä. ist dagegen ***nicht*** **möglich**, was insbesondere ein Handeln vom Ausland aus praktisch unmöglich macht.

583 Da eine authentifizierte Transaktion durch unbefugte Dritte bei Verwendung von Sicherungsverfahren mit Medienbruch regelmäßig nur denkbar ist, wenn der Täter erstens die PIN kennt und zweitens auch in den Besitz der Hardware, d.h. des TAN-Generators oder des Mobiltelefons, gelangt ist, ist hier auch der **Anscheinsbeweis für ein pflichtwidriges Handeln** des Bankkunden gerechtfertigt. Selbst wenn die PIN auf elektronischem Wege „abgefischt" werden konnte, müsste sich der Täter zusätzlich den TAN-Generator bzw. das Mobiltelefon des Bankkunden (nebst der PIN des Mobiltelefons) verschaffen. Hier ist dann aber – anders als bei Verfahren ohne zusätzliche Hardware – die **Parallele zur ec-Kartenproblematik** tatsächlich gerechtfertigt, da dem Kunden letztlich nichts anders abverlangt wird, als TAN-Generator bzw. Mobiltelefon – also körperliche Gegenstände – sicher und von der PIN getrennt zu verwahren. Dies entspricht weitgehend den Anforderungen, welche die Rechtsprechung für die sichere und getrennte Verwahrung von PIN und ec-Karte aufgestellt hat. Der Fall, dass die PIN auf elektronischem Wege (noch dazu wie häufig aus dem Ausland) durch einen Trojaner usw. ausgespäht, der Aufenthalt des Bankkunden ermittelt und dann noch die Hardware entwendet wird, dürfte bloß theoretische Relevanz besitzen. Entsprechend der Rechtsprechung zu ec-Karten (Rn. 569) erscheint daher eine tatsächliche Vermutung für die Weitergabe oder unsorgfältige Verwahrung der PIN und der Hardware gerechtfertigt.

(d) Zwischenergebnis

584 Nach derzeit **hM** im juristischen Schrifttum wird es der Bank regelmäßig gelingen, die technische Sicherheit der PIN-/TAN-Systeme als Grundlage des Anscheinsbeweises zu beweisen. Insbesondere die Gefahr des Ausspähens trifft damit beweisrechtlich den Kunden, da dieser die Legtimationsmedien geheim halten müsse und folglich eine tatsächliche Vermutung dafür spreche, dass der Kunde den Mißbrauch von PIN und TAN zumindest fahrlässig ermöglicht habe.[1155] Wegen des vermeintlich hohen technischen Sicherheitsstandards wird angenommen, die Ursache eines Mißbrauchs könne nur aus der Sphäre des Kunden kommen.[1156] Phishing und Pharming werden damit nicht als

[1155] *Karger*, DuD 2006, 215 (219); *Borges*, NJW 2005, 3313 (3316); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 127.

[1156] Dazu *Werner*, MMR 1998, 232 (235); *Wiesgickl*, WM 2000, 1039 (1050); *Gößmann*, in: Bankrechts-Handbuch, § 55 Rn. 26. Auch der Trojaner-Angriff auf das HBCI-Verfahren wurde nicht als Angriff auf die Sicherungssysteme des Online-

Frage der (mangelnden) Sicherheit des Online-Banking gesehen, sondern einseitig dem Verantwortungsbereich des „Unsicherheitsfaktors Benutzer“ zugewiesen, der nun seinerseits den Anscheinsbeweis erschüttern muss.

585 Verfahren **ohne Medienbruch** weisen indessen keine hinreichende technische Sicherheit gegenüber Manipulationen Dritter auf, welche die Vermutung zuließe, der Kunde selbst habe die Transaktion initiiert oder aber seine Pflichten verletzt (s. Rn.519 ff.). Anders ist dies bei Sicherungsverfahren **mit Medienbruch bzw. einem zweiten unabhängigen Kommunikationskanal (Zwei-Kanal-Verfahren)**, da bei diesen Eingriffe von außen mit an Sicherheit grenzender Wahrscheinlichkeit auszuschließen sind. Nur bei diesen – bislang nur vereinzelt eingesetzten Verfahren – kommt daher ein Anscheinsbeweis in Betracht.

(iv) *Erschütterung des Anscheinsbeweises*

(a) Grundsatz

586 Soweit man den Anscheinsbeweis bejaht, liegt es am Bankkunden, den Anscheinsbeweis zu erschüttern, voraussetzt, dass der Gegner (hier der Bankkunde) Tatsachen behauptet und beweist, aus denen sich die **ernsthafte Möglichkeit eines abweichenden (atypischen) Geschehensablaufs** im konkreten Einzelfall ergibt.[1157] Die Tatsachen aus denen die Möglichkeit eines abweichenden Ablaufs abgeleitet werden sollen, bedürfen des Vollbeweises.[1158] Die Erschütterung des Anscheinsbeweises ist nicht mit dem strengeren Anforderungen des Beweises des Gegenteils gleich zu setzen.[1159]

587 Für den oben (Rn. 563) formulierten alternativen Anscheinsbeweis bedeutet dies, dass der Bankkunde den Anscheinsbeweis für die Urheberschaft erschüttern kann, indem er die ernsthafte Möglichkeit einer Veranlassung des Bankgeschäfts durch einen unbefugten Dritten darlegt und erforderlichenfalls beweist. Gelingt dem Kunden die Erschütterung des Anscheinsbeweises für die **Urheberschaft**, bedeutet dies indessen nicht notwendig, dass es der Bank nunmehr verwehrt ist, das Konto des Kunden zu belasten. Vielmehr wird angenommen, dass der Kunde die Transaktion des Unbefugten durch die Verletzung eigner **Sorgfaltspflichten** ermöglich hat. Hier zeigt sich, dass die Festle-

Banking, sondern als Angriff auf den Computer des Kunden gewertet, s. *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 183.

[1157] BGH NJW 1991, 230 (231); *Borges*, NJW 2005, 3313 (3317); *Karper*, DuD 2006, 215 (218); Musielak-*Foerste*, § 286 ZPO Rn. 23; MünchKommZPO-*Prütting*, § 286 ZPO Rn. 64; Thomas/Putzo-*Reichold*, § 286 ZPO Rn. 13; Zöller-*Greger*, Vor § 284 ZPO Rn. 29; *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 180, 184 ff.

[1158] BGH NJW 1991, 230 (231); Zöller-*Greger*, Vor § 284 ZPO Rn. 29; Stein/Jonas-*Leipold*, § 286 ZPO Rn. 98.

[1159] MünchKommZPO-*Prütting*, § 286 ZPO Rn. 64.

gung der Sorgfaltspflichten des Kunden zugleich mitbestimmend für die Erschütterung des Anscheinsbeweises ist. Kann der Kunde diesen Anscheinsbeweis nicht erschüttern, haftet er nach §§ 280 Abs. 1, 241 Abs. 2 BGB gegenüber der Bank auf Schadensersatz.[1160]

588 Welche **Anforderungen** die Rechtsprechung an die Erschütterung des Anscheinsbeweises stellt, bleibt der freien richterlichen Beweiswürdigung im Einzelfall überlassen.[1161] Denkbar ist, dass die Rechtsprechung die Anforderungen an die Erschütterung des Anscheinsbeweises wegen der andauernden Diskussion über die Sicherheit des Online-Banking relativ niedrig ansetzen wird.[1162] Dies erscheint zumindest dann interessengerecht, wenn man entgegen der hier vertretenen Auffassung einen Anscheinsbeweis bei **Sicherungssystemen ohne Medienbruch** befürwortet. Das LG Stralsund sah den Anscheinsbeweis für die Richtigkeit einer Telefonrechnung dadurch als erschüttert an, dass sich ein Virus mit Namen „Backdoor-Explorer 32-Trojan" auf dem Rechner des Telefonkunden befunden hatte.[1163] Beim Phishing soll man zumindest den Anscheinsbeweis für die Urheberschaft durch eine noch vorhandene Phishing-E-Mail erschüttern können.[1164] In der Literatur wird darüber hinaus zum Teil die Ansicht vertreten, die ernsthafte Möglichkeit eines atypischen Geschehensablaufs könne bereits mit Hilfe von Medienberichten und einschlägiger Fachliteratur über Pharming-Angriffe bewiesen werden.[1165] Bejaht man jedoch den Erfahrungssatz, genügen allein abstrakte Berichte über mögliche Bedrohungen ohne Bezug zum konkreten Einzelfall nicht, um den Anscheinsbeweis zu entkräften. Gerade beim Pharming werden aber oftmals greifbare Anhaltspunkte für eine Manipulation durch Dritte fehlen, da diese Angriffe nachträglich kaum feststellbar sind.[1166] Ebenso kann dem Kunden entgegen gehalten werden, er habe die Installation eines Schadprogramms oder lückenhafter Software nachträglich in manipulatorischer Absicht bewirkt, was diesen zum Vollbeweis des atypischen Geschehensablaufs zwingt. Zu strenge Anforderungen an die Erschütterung des Anscheinsbeweises und tatsächliche Nachweisprobleme können im Ergebnis einer Beweislastumkehr oder

[1160] *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 184 f.

[1161] BGH NJW 1969, 277; Stein/Jonas-*Leipold*, § 286 ZPO Rn. 98.

[1162] So auch die Einschätzung von *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 186; *Kind/Werner*, CR 2006, 353 (359).

[1163] LG Stralsund MMR 2006, 487 (488 f.). Eine Pflichtverletzung wegen unterlassenen Virenschutzes verneinte das Gericht unter Berufung auf die Dialer-Rechtsprechung des BGH.

[1164] *Borges*, NJW 2005, 3313 (3317); *Karper*, DuD 2006, 215 (219).

[1165] So *Kind/Werner*, CR 2006, 353 (360).

[1166] *Borges*, NJW 2005, 3313 (317); *Karper*, DuD 2006, 215 (219).

gar einer (in AGB unzulässigen) verschuldensunabhängigen Haftung des Bankkunden gleichkommen.[1167]

589 Bei **PIN-/TAN-Verfahren mit Medienbruch** wird man dagegen in Anlehnung an die Rechtsprechung zu ec-Karten strengere Anforderungen anlegen können, da ein Missbrauch praktisch nur dann möglich ist, wenn der Täter Zugriff auf die Hardware (TAN-Generator, Mobiltelefon) und zugleich auf die PIN erlangt.

(b) Erörterung der Beweislage bei den einzelnen Bedrohungsszenarien

590 Bejaht man mit der bislang vorherrschenden Ansicht den Anscheinsbeweis auch bei Verwendung von PIN-/TAN-Verfahren ohne Medienbruch, ergeben sich im Einzelfall erhebliche Beweisschwierigkeiten und Prozessrisiken, die insbesondere beim Einsatz von Trojanern oftmals nicht überwindbar sein werden. Im Einzelnen stellt sich die Beweislage in den eingangs geschilderten Bedrohungsszenarien wie folgt dar:

(i) Szenario 1

591 Das Phishing per E-Mail und Visual Spoofing ist auf die aktive Mitwirkung des Bankkunden angewiesen, der die E-Mail öffnen, dem angegebenen Link folgen und schließlich PIN und TAN eingeben muss. Am Kunden ist es zunächst den Anscheinsbeweis für die Urheberschaft der Erklärung zu erschüttern, was beim Phishing wohl gelingen wird, sofern die Pishing-E-Mail noch nachweisbar vorhanden ist.[1168]

592 Auch wenn der Nachweis eines Angriffs Dritter erfolgreich geführt wird, steht der Kunde vor dem Problem, auch den Anscheinsbeweis einer Pflichtverletzung zu erschüttern. Er wird dann darzulegen haben, dass er gutgläubig auf die Absenderschaft der Bank für die (Phishing-)E-Mail vertraut hat und deshalb PIN und TAN übermittelt hat. Die Anforderungen an die Erschütterung des Anscheinsbeweises sind dabei abhängig davon, welche Sorgfaltsanforderungen dem Bankkunden auferlegt werden. Sofern bereits die bloße Beantwortung einer Phishing-E-Mail eine Pflichtverletzung begründet, wird die Erschütterung des Anscheinsbeweises in der Regel wohl ausscheiden.

(ii) Szenario 2

593 Der Bankkunde kann den Beweis des ersten Anscheins für seine Urheberschaft für eine Transaktion erschüttern, wenn er die ernsthafte Möglichkeit einer Manipulation darlegt.

[1167] So zutreffend *Erfurth*, WM 2006, 2198 (2206).
[1168] *Karper*, DuD 2006, 215 (219).

Hierbei wird es entscheidend darauf ankommen, ob die Rechtsprechung beispielsweise die gehäufte Verbindung zu einigen IP-Adressen als Erschütterung des Anscheinsbeweises ausreichen lässt. Gelingt dem Bankkunden schon der Nachweis einer Manipulation des Provider-Servers nicht, wird besteht der Anscheinsbeweis seiner Urheberschaft fort.

(iii) Szenario 3

594 Beim Pharming i.e.S. mit Trojaner obliegt dem Bankkunden als erste Hürde die Erschütterung des Anscheinsbeweises für seine Urheberschaft für die Transaktion. Diese wird gelingen, wenn sich der Trojaner auf dem PC des Kunden noch nachweisen lässt.[1169] Andernfalls kommt es auf die Frage der Pflichtverletzung nicht mehr an, da der Bankkunde als Urheber des Auftrags an die Bank gilt.

595 Für die Erschütterung des Anscheinsbeweises für eine Sorgfaltswidrigkeit wird man hinsichtlich einzelner Pflichtverletzungen unterscheiden müssen: Im Hinblick auf die Sicherung des eigenen PC kann sich der Bankkunde entlasten, wenn er die Durchführung der ihm zumutbaren Sicherungsmaßnahmen (Virenschutz, regelmäßige Systemupdates) nachweist. Dieser Nachweis lässt sich bei beim Betriebssystem Windows und den meisten Anti-Virus-Programmen durch eine automatisch protokollierte Liste der Updates führen. Konnte die Installation des Trojaners trotz dieser Sorgfaltsmaßnahmen nicht verhindert werden, ist der Anscheinsbeweis für eine Pflichtverletzung des Kunden dennoch erschüttert. Bejaht man eine Pflichtverletzung wegen des Öffnens eines E-Mail-Anhangs, kommt es darauf an, ob der Bankkunde darlegen kann, dass er auf die Seriosität des Inhalts vertrauen durfte.

(c) Zwischenergebnis

596 Entgegen der wohl hM kann beim – derzeit überwiegend im Einsatz befindlichen - Authentisierungsverfahren mittels PIN/TAN **ohne Medienbruch** kein Anscheinsbeweis dafür bejaht werden, dass entweder der Bankkunde selbst gehandelt oder aber den Missbrauch durch Dritte pflichtwidrig ermöglicht hat. Angesichts der neuen und nur schwer beherrschbaren Bedrohungen insbesondere durch Schadprogramme fehlt die hierfür erforderliche Typizität des Geschehensablaufs. Eine entsprechende Typizität ließe sich allein bei den nach dem – gegenwärtigen Stand der Technik – als sicher zu be-

[1169] Vgl. auch LG Stralsund MMR 2006, 487 (488) zur Erschütterung des Anscheinsbeweises für die Richtigkeit der Telefonrechnung bei bloßem Vorliegen eines Trojaners auf dem PC des Kunden. Kritisch zu dieser Entscheidung *Ernst*, CR 2006, 590 ff.

wertenden Verfahren bejahen, die auf einem **Medienbruch** bzw. der Verwendung eines zweiten, unabhängigen Kommunikationskanals (Zwei-Kanal) beruhen.

597 Nach gegenwärtig hM hängt die Risikoverteilung beim Online-Banking dagegen – auch bei Einsatz des PIN/TAN-Verfahrens – davon ab, wie streng die Gerichte die Erschütterung des Anscheinsbeweises handhaben. Für den Bankkunden birgt die Annahme eines Anscheinsbeweises das beweisrechtliche Risiko selbst dann haften zu müssen, wenn alle Sorgfaltsanforderungen beachtet wurden, wenn die Erschütterung des Anscheinsbeweises (etwa bei Pharming-Angriffen) nicht gelingt.

c) Haftung weiterer Akteure

598 Die aufgezeigten Gefahren beim Online-Banking werfen die Frage nach den Rückgriffsmöglichkeiten des von seiner Bank in Anspruch genommenen Kunden auf. Da die eigentlichen Täter entweder nicht identifizierbar oder – etwa bei Wohnsitz im Ausland – nur schwer greifbar sind, kommen als mögliche Anspruchsgegner meist nur die Hersteller fehlerhafter IT-Produkte sowie Internet-Provider und private Nutzer in Betracht:

(1) IT-Hersteller

599 Nutzt ein Trojaner eine Sicherheitslücke in einer vom Bankkunden verwendeten Software (beispielsweise seinem Betriebssystem, Internet-Browser usw.), stellt sich im Schadensfall die Frage einer Haftung des IT-Herstellers gegenüber dem Kunden. Mangels Eigentumsverletzung (Rn. 108 ff.)) kommen gegen den IT-Hersteller regelmäßig nur vertragliche Ansprüche in Betracht. Wurde aber die Installation des Trojaners durch einen Fehler der Software ermöglicht, ist im Ausgangspunkt zunächst festzuhalten, dass kein Schadensersatzanspruch der Bank gegen den Kunden besteht, da dieser nicht pflichtwidrig gehandelt hat. Gleichfalls entfällt mangels Schaden ein produkthaftungsrechtlicher Regressanspruch des Kunden gegen den Hersteller.

600 *Soweit* man den Anscheinsbeweis bejaht (s. oben Rn. 563), lautet die praktisch relevante Frage in diesem Zusammenhang, ob es dem Kunden überhaupt gelingt, die Ursächlichkeit der Softwarelücke für die Installation des Trojaners zu beweisen. Schlägt die Erschütterung des Anscheinsbeweises (oben Rn. 586 ff.) fehl und haftet er gegenüber der Bank in Höhe des Überweisungsbetrages, dürfte die anschließende Inanspruchnahme des Herstellers der Software kaum größere Erfolgsaussichten haben. Wegen des Beweis- und Kostenrisikos wird die Bedeutung der Produkthaftung wird im vorliegenden Zusammenhang damit eher gering sein. Ansprüche der Bank gegen den IT-Hersteller scheitern bereits an der fehlenden Vertragsbeziehung und Rechtsgutsverletzung. Die

engen Voraussetzungen einer Drittschadensliquidation werden im Verhältnis zwischen Bank und Kunde regelmäßig nicht vorliegen.[1170]

(2) Intermediäre

601 Eine Haftung von Intermediären gegenüber dem Bankkunden erscheint zumindest auf vertraglicher Grundlage möglich, wenn der Provider eine ihn selbst treffende Sicherungspflicht schuldhaft verletzt hat (ausführlich zu den Sicherungspflichten der Intermediäre unten Rn. 668 ff.). Sofern sich aber nachweisen lässt, dass die Identitätstäuschung durch einen Angriff auf den Provider des Bankkunden verursacht wurde (vgl. beispielsweise Szenario 2 zu DNS-Spoofing, Rn. 480), haftet der Kunde mangels eigener Pflichtverletzung nicht gegenüber seiner Bank. Eine Inanspruchnahme des Providers durch den Kunden scheitert wiederum am fehlenden Schaden des Bankkunden. Konnte dagegen die Verantwortlichkeit des Intermediärs schon gegenüber der Bank nicht nachgewiesen (d.h. der Anscheinsbeweis erschüttert) werden, dürfte auch hier eine Inanspruchnahme des Intermediärs regelmäßig aus Beweisnot unterbleiben. Eigene vertragliche Ansprüche der Bank gegen den Provider des Kunden bestehen ebenso wie deliktische Ansprüche regelmäßig nicht.

(3) Private Nutzer

602 Hat ein privater Nutzer (etwa ein Freund oder Bekannter) den Trojaner in einem E-Mail-Anhang an den Bankkunden gesandt, stellen sich im Schadensfall die oben erwähnten Probleme zur Haftung privater Nutzer (s. Rn. 275 ff.). Mangels Vertragsverhältnis und Eigentumsverletzung infolge der Installation des Trojaners (Rn. 114), wird ein Schadensersatzanspruch gegen den Versender aber allenfalls bei Verstoß gegen ein Schutzgesetz (§ 823 Abs. 2 BGB) oder vorsätzlich sittenwidriger Schädigung zu bejahen sein (§ 826 BGB).

d) Ergebnis

603 Zum gegenwärtigen Zeitpunkt muss davon ausgegangen werden, dass das Online-Banking über Internet-Verbindung unter Verwendung eines normalen PC keine hinreichende Sicherheit zu bieten vermag. Primär obliegt es der das Online-Banking anbietenden Bank, ein dem Stand der Technik entsprechendes Sicherungsverfahren vorzuhalten. Die Schwachstellen des Online-Banking bilden derzeit zum einen Sicherheitslücken in den Online-Banking-Systemen und die mangelnde Sicherung seines privaten Compu-

[1170] Dazu Palandt-*Heinrichs*, Vorb v § 249 BGB Rn. 112 ff.; Bamberger/Roth-*Schubert*, § 249 BGB Rn. 153.

ters. Eine strenge Risikoverteilung nach Gefahrenbereichen kommt hierbei jedoch nicht in Betracht. An den durchschnittlichen privaten Nutzer können beim Online-Banking insbesondere im technischen Bereich nur begrenzte Sorgfaltsanforderungen gestellt werden (z.B. Virenschutz, Systemupdates). Soweit ein Restrisiko im Bereich der privaten Nutzung verbleibt, ist dieses wertungsmäßig der Bank zuzurechnen. Wegen des von der hM angenommenen Anscheinsbeweises kann dieses Restrisiko aber nach gegenwärtiger Rechtslage im Einzelfall beweisrechtlich auf den Bankkunden verlagert werden, wenn eine Manipulation der Online-Transaktion – insbesondere im Falle eines Pharming-Angriffs – nicht nachweisbar ist.

7. Zwischenergebnis: besondere Verantwortlichkeit im Banken- und Finanzsektor

604 Im Banken-, Versicherungs- und Finanzsektor ist durch KWG, WpHG, VAG und die entsprechenden Mindestanforderungen, wie z.B. MaRisk, eine starke Aufsicht vorhanden. Die Pflichten sind auch hinsichtlich der Verwendung von Informationstechnik geregelt. Die Aufsichtsbehörde hat zusätzlich auch entsprechende Mittel, um diese Anforderungen durchzusetzen. Zwar sind die Normen nicht als Schutzgesetze i.S.d. § 823 Abs. 2 BGB zu qualifizieren, durch die Möglichkeit, sie zur Konkretisierung der Verkehrssicherungspflichten im Rahmen des § 823 Abs. 1 BGB besteht aber dennoch ein enger Zusammenhang auch zur deliktischen Haftung.

V. Besondere Risikopotentiale für Experten und beratende Berufe (Rechtsanwälte etc.)

1. Vorbemerkung

605 Bestimmte Berufsgruppen unterliegen weitergehenden Pflichten als andere, sei es aufgrund ihrer besonderen Vertrauensstellung im Rechtsverkehr oder sei es aufgrund bestimmter volkswirtschaftlich besonders wichtiger Funktionen, die sie übernehmen. Wenn sich solche berufsbezogenen Pflichten auf die Vorhaltung oder Behandlung von Daten beziehen, so können auch spezielle Pflichten im Hinblick auf IT-Sicherheit normiert oder den vorhandenen Regelungen zu entnehmen sein. Besonders betrachtet werden sollen hier insbesondere Rechtsanwälte und Ärzte, aber auch Steuerberater, für die spezielle Pflichten im Hinblick auf den Umgang mit Informationen bestehen.

2. Gefahrenpotential und Gegenmaßnahmen

606 Grundsätzlich unterscheidet sich das technische Gefahrenpotential nur wenig von den Gefahren bei anderen kommerziellen Nutzern – nicht indes das Schädigungspotential.

Daten, die in einem besonderen Vertrauensverhältnis wie zwischen Anwalt und Mandant oder Arzt und Patient preisgegeben werden, sind häufig existenziell wichtig und/oder höchstpersönlich. Das Bekanntwerden bzw. die Einsicht Fremder in diese Informationen kann einen hohen vermögensrelevanten Schaden hervorrufen, ist aber auch geeignet, in so weitgehendem Maße in (höchst-)persönliche Rechtsgüter einzugreifen, dass eine Schädigung meist nicht vermögensrelevant einzuordnen bzw. aufzuwiegen ist, und die Daten bereits deshalb eines maximalen Schutzes bedürfen. Darüberhinaus können vermehrte Verstöße zu einer Erschütterung des Vertrauens des Rechtsverkehrs in diese spezifischen Berufe führen, was insgesamt zu Marktstörungen führen kann. Aus diesem Grunde sind allgemein das Rechtsverhältnis zwischen Klienten und Berufsträger[1171] sowie spezifisch die hierbei offenbarten Informationen einem auch strafrechtlich abgesicherten strengen Schutzregime unterworfen.[1172]

3. Rechtsanwälte

607 Ein solches Vertrauensverhältnis besteht insbesondere für Rechtsanwälte in ihrer Beziehung zu Mandanten. Dementsprechend sind für Daten, die einem Anwalt anvertraut sind, neben den Vorschriften des BDSG und des StGB die Bundesrechtsanwaltsordnung (BRAO) und die Berufsordnung für Rechtsanwälte (BORA) zu beachten.

a) § 43a Abs. 2 BRAO (Verschwiegenheitspflicht)

608 Nach § 43a Abs. 2 BRAO ist der Anwalt zur Verschwiegenheit verpflichtet, wobei sich diese Pflicht auf „alles“ bezieht, was ihm in Ausübung seines Berufs bekannt geworden ist. Verletzt der Anwalt vorsätzlich seine Pflicht aus § 43a Abs. 2 BRAO, so ist regelmäßig auch § 203 Abs. 1 Nr. 3 StGB verwirklicht.

609 In diesem Rahmen ist etwa fraglich, ob ein Anwalt verpflichtet ist, elektronische Informationen nur verschlüsselt zu übertragen.[1173] So wird die Frage aufgeworfen, ob dast das Versenden von unverschlüsselten **E-Mails** an den eigenen Mandanten der offenen Versendung von Postkarten gleichkommt und aus diesem Grunde eine Verletzung von § 43a Abs. 2 BRAO und § 203 Abs. 1 Nr. 3 StGB vorliegen kann.[1174] Dies wird man jedoch zu verneinen haben, da die E-Mails nur an den Mandanten gerichtet sind und E-

[1171] Für das anwaltliche Vertrauensverhältnis *Henssler,* NJW 1994, 1817 (1818); für das ärztliche Vertrauensverhältnis *Hermeler*, Rechtliche Rahmenbedingungen der Telemedizin, 45.

[1172] Dazu BVerfG NJW 2005, 1917 (1919); *Henssler,* NJW 1994, 1817 (1818).

[1173] Dazu *Härting,* NJW 2005, 1248 (1248 ff.) mwN.

[1174] So mit guten Gründen *Backu*, ITRB 2003, 251 (251); *Jungk*, AnwBl 2001, 170 (172); *Lapp*, BRAK-Mitt 1997, 106 (107); *Streitz*, NJW-CoR 2000, 208 (209); *Wagner/Lerch*, NJW-CoR 1996, 380 (384); differenzierend *v. Lewinski*, BRAK-Mitt 2004, 12 (13).

Mailkonten regelmäßig durch Passwörter geschützt sind.[1175] Fraglich ist, ob dies auch dann gilt, wenn der **Kommunikationsverkehr** mittels Funktechniken unverschlüsselt oder nicht ausreichend gesichert übertragen wird. Während es relativ komplex ist, Daten eines kabelgebundenen Kommunikationsvorgangs abzufangen und auszulesen, stellt dies im Fall von drahtlosen Übertragungsformen, wie etwa WLAN kein Problem dar. Wird ein Funknetz ohne Verschlüsselung genutzt und werden hierbei E-Mails oder andere Daten übertragen, so kann diese jeder in einem gewissen Umkreis ohne besondere technische Schwierigkeiten abfangen und einsehen.[1176]

610 Nach derzeit wohl h.M. geht eine Verpflichtung zu aktiven T-Sicherheitsmaßnahmen jedoch über den Wortlaut des § 43a Abs. 2 BRAO, der sich auf die Pflicht zur Verschwiegenheit beschränkt, und das tradierte Verständnis des Anwaltsgeheimnisses hinaus.[1177] Jedenfalls im Falle der Verwendung von drahtlosen Übermittlungsformen wird man jedoch die Verwendung gängiger Verschlüsselungsstandards – etwa dem Wired Equivalent Privacy (WEP)-Standard – fordern müssen, um eine Basissicherheit zu gewährleisten.

611 Weitere Konkretisierungen enthält **§ 2 BORA**,[1178] der in Abs. 4 alle Personen, die bei der Berufstätigkeit des Anwalts mitwirken, ebenfalls zur Verschwiegenheit verpflichtet, so dass etwa auch outgesourcte Tätigkeiten des Anwalts, z.B. die externe Pflege der IT-Komponenten des Anwalts, erfasst werden können.

b) BDSG

(1) Rechtsanwälte als nicht-öffentliche Stellen

612 Rechtsanwälte erheben, speichern und verarbeiten Daten im Sinne des BDSG, wenn sie Daten ihrer Mandanten im Rahmen ihrer IT-Systeme verwenden. In diesem Rahmen sind sie als nicht-öffentliche Stellen zu qualifizieren, auch wenn sie nach § 1 BRAO als Organe der Rechtspflege gelten,[1179] da sie keine Stelle des Bundes oder der Länder sind.[1180]

[1175] So *Härting,* NJW 2005, 1248 (1249); *Härting*, MDR 2001, 61 (62); *v. Lewinski*, BRAK-Mitt 2004, 12 (16).

[1176] Dazu näher *Dornseif/Schumann/Klein*, DuD 2002, 1; zur strafrechtlichen Beurteilung *Ernst,* CR 2003, 898.

[1177] *Härting*, NJW 2005, 1248 (1249); *Härting*, MDR 2001, 61 (62); *v. Lewinski*, BRAK-Mitt 2004, 12 (16); aA. *Eylmann*, in Henssler/Prütting, BRAO, 2. Aufl. (2004), § 43a BRAO Rn. 64.

[1178] *Eylmann*, in: Henssler/Prütting, § 43a BRAO Rn. 28 ff.; *Feuerich/Weyland*, § 43a BRAO Rn. 12 ff.; *Hartung*, in: Hartung/Holl, § 43a BRAO Rn. 25 ff. und § 2 BORA Rn. 1 ff.

[1179] *Zuck,* in: Abel, Datenschutz in Anwaltschaft, Notariat und Justiz, § 2 Rn. 27; vgl. *Wedde*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.3 Rn. 34.

[1180] *Gola/Schomerus*, § 2 BDSG Rn. 12.

(2) Verhältnis des BDSG zur BRAO

613 Da sowohl das BDSG als auch die BRAO Pflichten zum Datenschutz bzw. Verschwiegenheit regeln, liegt es auf der Hand, dass das Verhältnis zwischen beiden Regelungen Probleme bereitet. In Rede stehen sowohl die Verdrängung des BDSG durch die BRAO als lex specialis als auch die Subsidiarität des BDSG (§ 1 Abs. 3 BDSG),[1181] die allerdings nur dann greifen würde, wenn die BRAO besondere Regelungen bereithält. Dieser grundsätzliche Streit kann hier nur ansatzweise gestreift werden, da er für hier interessierenden Fragen der IT-Sicherungspflichten letztlich nicht entscheidend ist: So decken sich die Ziele des § 9 BDSG weitgehend mit denen des Berufsrechts,[1182] ohne dass dies speziell kodifiziert wäre. Im Rahmen der Selbstverwaltung unterliegt der Anwalt nach § 73 Abs. 2 Nr. 4 BRAO einer gewissen Kontrolle durch die Rechtsanwaltskammern.[1183] Diese können auf die Einhaltung des Berufsrechts achten und im Verletzungsfall berufsrechtliche Schritte bis hin zum Entzug der Anwaltszulassung nach § 114 BRAO gerichtlich erwirken. Dem Anwalt obliegt demnach auch auf Basis des Berufsrechts der sorgsame Umgang mit den Daten; allerdings lassen sich diese Pflichten tatsächlich nicht konkret benennen. Sie dürften, zumindest was z.B. die regelmäßige Datensicherung sowie den Einsatz von allgemein bekannten Sicherungssystemen betrifft, ähnlich den durch § 9 BDSG und der zugehörigen Anlage geregelten Pflichten sein.[1184] Die Anlage zu § 9 Satz 1 BDSG enthält eine allgemeingültige Beschreibung professioneller Standards, deren Nichtbeachtung sowohl standes- als auch strafrechtlich relevant wäre.[1185] Durch das besondere Schadenspotential, das durch den Verlust oder die Entwendung von Daten aus dem Verhältnis zwischen Mandant und Anwalt verwirklicht werden kann, sind bei der Verwendung von Rechnersystemen in der anwaltlichen Tätigkeit dem Anwalt jedenfalls die Sicherungsmaßnahmen zuzumuten, deren Gefahr allgemein bekannt ist und die ohne spezielles Fachwissen eingesetzt werden können. Dies zeigt sich auch an der Anlage zu § 9 BDSG, nach der „auf die Art der zu schützenden [...] Daten" eingegangen werden muss. Im Einzelfall, also z.B. bei Gefahren, die sich bereits im

[1181] S. dazu Stellungnahme der Bundesrechtsanwaltskammer (BRAK) zu der Frage der Bestellung eines Beauftragten für Datenschutz in Rechtsanwaltskanzleien, abrufbar unter: http://www.brak.de/seiten/pdf/Stellungnahmen/2004/StnBDSinKanzleien.pdf, S. 3 unter Verweis auf BAG NJW 1998, 2466; ebenso *Rüpke*, AnwBl 2004, 552 (552 f.).

[1182] *Abel,* in: Roßnagel, Handbuch Datenschutzrecht, 7.11 Rn. 28 f.; *Rüpke,* AnwBl 2004, 552, (555); die BRAK hat Vorschläge zur Konkretisierung des § 43a Abs. 2 BRAO zur Erweiterung auch auf technische Organisationspflichten gemacht.

[1183] Stellungnahme der BRAK, abrufbar unter: http://www.brak.de/seiten/pdf/Stellungnahmen/2004/StnBDSinKanzleien.pdf, 6; Feuerich/Weyland-*Feuerich*, § 73 BRAO Rn. 42; *Abel,* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.11 Rn. 38.

[1184] Dazu auch *Schöttle,* Anwaltliche Rechtsberatung via Internet, S. 39 ff.

[1185] *Abel,* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.11 Rn. 28.

konkreten Fall gezeigt haben, wird dem Anwalt aber auch die Beiziehung von Fachpersonal zur Absicherung abverlangt werden können. Der Anwalt muss allerdings nicht „mit Kanonen auf Spatzen schießen“;[1186] für äußerst unwahrscheinliche Bedrohungsszenarien müssen keine aufwändigen und dementsprechend kostspieligen Maßnahmen ergriffen werden.

614 Demgemäß sind die grundsätzlichen Pflichten des § 9 BDSG auch aus dem Berufsrecht herleitbar. Insofern ist bisher der einzige relevante Unterschied, was die Pflicht zur Ergreifung von Sicherungsmaßnahmen im Bereich der IT-Sicherheit angeht, dass im einen Fall die Aufsichtsbehörde nach § 38 BDSG die Einhaltung der Voraussetzungen des § 9 BDSG im speziellen, im anderen Fall die Rechtsanwaltskammern die Einhaltung der vermutlich kongruenten Pflichten nach Berufsrecht kontrollieren. Zwar enthält § 38 Abs. 3 Satz 2 BDSG ein Auskunftsverweigerungsrecht über alle diejenigen Daten, deren Herausgabe dem Auskunftspflichtigen unter Androhung von Strafe verboten ist. Gestützt auf diese Ausnahme kann der Anwalt somit jegliche inhaltlichen Daten zurückhalten. Hinzu kämen die Schranken der §§ 43a Abs. 2, 56 Abs. 1 BRAO.[1187] Diese würde natürlich nicht für Daten gelten, die schon von Anfang an voll dem BDSG unterfallen. Auskunft erteilen müsste der Anwalt aber z.B. über die grundsätzlichen Rahmenbedingungen seiner Datenverarbeitung wie die Umstände der regelmäßigen Datensicherung. Allerdings ist gerade die Auskunftspflicht im Rahmen der BRAO sehr differenziert ausgestaltet. Aus diesem Grunde tritt § 38 BDSG jedenfalls vollständig zurück.[1188]

(3) Ergebnis

615 Insofern kann offen bleiben, ob das BDSG insgesamt subsidiär ist oder nur im Einzelfall als allgemeineres Gesetz zurücktritt. Der Pflichtenmaßstab richtet sich an § 9 BDSG sowie der zugehörigen Anlage aus. Die Prüfung der jeweiligen Pflichtenerfüllung erfolgt nicht nach dem BDSG, sondern wird durch die Rechtsanwaltskammern durchgeführt.

c) Vertragliche Nebenpflichten

616 Unabhängig davon, ob gesetzliche Pflichten greifen, können auch aus der vertraglichen Beziehung (als Dienst- oder Geschäftsbesorgungsvertrag)[1189] spezielle Pflichten bezüg-

[1186] *Gola/Schomerus*, § 9 BDSG Rn. 7.
[1187] Quaas/Zuck-*Zuck*, § 2 Rn. 52, 54; *Abel,* in: Roßnagel, Handbuch Datenschrecht , Kap. 7.11 Rn. 38.
[1188] *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.11 Rn. 38.
[1189] Palandt-*Weidenkaff*, § 611 BGB Rn. 20**.**

lich der IT-Sicherheit bestehen. Die Verletzung von Nebenpflichten kann Schadensersatzansprüche aus §§ 280 ff. BGB nach sich ziehen. Dabei werden derartige IT-bezogene Nebenpflichten umso eher anzunehmen und umso weit reichender sein, je mehr die Parteien auf eine vertrauensvolle Zusammenarbeit angewiesen sind, oder sich eine Partei auf die Fachkunde der anderen verlassen muss, einschließlich der IT-bezogenen Sachkunde und Ressourcen.[1190]

617 Selbstverständlich erwartet der Mandant einen **besonders sorgsamen Umgang** mit den offenbarten sensiblen Daten. Daraus ergeben sich eben auch Sorgfaltspflichten hinsichtlich der Daten und der Ergreifung von speziellen Sicherungsmaßnahmen gegen bekannte Gefahren. Wie bereits dargelegt (Rn.434) kann die Verletzung der Pflichten aus § 9 BDSG mittelbar über die Konkretisierung der geschuldeten Sorgfalt vertragliche Ansprüche oder gar eine deliktische Haftung auslösen.[1191] Wer also schon Sicherungsmaßnahmen nach dem BDSG nicht ergreift, unterliegt der Haftung.[1192] Dem Anwalt können also jedenfalls mindestens die Pflichten eines kommerziellen Nutzers auferlegt werden. Die Verpflichtung zur Ergreifung von Sicherungsmaßnahmen endet auch nicht mit der Aufgabe oder Beendigung des Mandats. Soweit auch die Aufbewahrung von Akten über diesen Zeitraum hinaus notwendig ist, wirken die Pflichten als nachwirkende Vertragspflichten fort.[1193]

d) Deliktische Haftung

618 Sanktionen für die Verletzung entsprechender Pflichten können sich neben der vertraglichen Haftung auch aus § 823 Abs. 1 BGB ergeben, bei der vorsätzlichen Preisgabe zusätzlich aus § 823 Abs. 2 BGB i.V.m. § 203 StGB oder § 826 BGB. Schutzgut des § 823 Abs. 1 StGB ist dabei das Recht auf informationelle Selbstbestimmung. Wiederum sind die jeweiligen Verkehrssicherungspflichten des Anwalts maßgeblich, auch im Hinblick auf das geschützte Rechtsgut. Aufgrund der extrem hohen Sensibilität der Daten ist der Anwalt demnach einem besonders hohen Standard in Bezug auf die Sicherungspflichten unterworfen. Die dem kommerziellen Nutzer obliegenden Pflichten sind somit

[1190] Bamberger/Roth-*Grüneberg-Sutschet*, § 241 BGB Rn. 44.

[1191] *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.11 Rn. 28.

[1192] *Horns* in: Abel, Datenschutz in Anwaltschaft, Notariat und Justiz, § 14 Rn. 73.

[1193] Die Pflicht zur Aufbewahrung der Handakten ergibt sich aus § 50 Abs. 2 S. 1 BRAO. Besteht diese Pflicht, so muss die Aufbewahrung natürlicherweise bei Mandatsende genauso ausgestaltet sein, wie bei Fortführung des Mandats.

als absoluter Mindeststandard anzusehen. Auch hier kann der Anhang zu § 9 BDSG als Orientierungshilfe dienen.[1194]

e) Ergebnis

619 Der Anwalt ist verpflichtet, diejenigen Pflichten zu ergreifen, die auch einem kommerziellen Nutzer obliegen würden. Durch das besondere Vertrauensverhältnis zwischen ihm und seinen Klienten besteht diesbezüglich auch eine besondere vertragliche Pflicht, die auch deliktsrechtlich untermauert wird.

4. Steuerberater

620 Das Verhältnis zwischen dem Steuerberater und seinem Klienten ist durch ein ähnliches Vertrauensverhältnis gekennzeichnet. Es ist deshalb für den Steuerberater anerkannt, dass das Vertrauensverhältnis dem zwischen Anwalt und Mandant vergleichbar ist.[1195] Der Steuerberater nimmt ebenfalls eine unabhängige Organstellung ein,[1196] die Steuerberatung ist nur ein Teil der Rechtsberatung.[1197]

621 Für Steuerberater enthält § 9 der Berufsordnung der Steuerberater (BOStB) die Verschwiegenheitspflicht. Sie ist ähnlich § 2 BORA angelegt, aber umfangreicher und deutlicher. So hält § 9 Abs. 6 BOStB ausdrücklich fest, dass der Steuerberater dafür Sorge zu tragen hat, dass Unbefugte keinen Einblick in die Unterlagen erhalten. Demgemäß hat der Steuerberater die Pflicht, die Daten ausreichend gegen den Zugriff von Dritten zu sichern, wobei auch hier die Pflichten denen des Anhangs von § 9 BDSG vergleichbar sein dürften. Da der rechtliche Status dem eines Anwalts ähnlich und auch der Schutz vor staatlichen Eingriffen ebenso zu gestalten ist,[1198] dürfte eine Kontrolle der Einhaltung bezüglich der geschützten Daten ebenfalls nur durch die Bundessteuerberaterkammer erfolgen.

622 Für die **vertraglichen Nebenpflichten und die deliktische Haftung** ergeben sich gegenüber den Ausführungen zum Verhältnis zwischen Anwalt und Mandant **keine Besonderheiten**.

5. Ärzte

[1194] *Abel,* in: Roßnagel, Handbuch Datenschutzrecht*,* Kap. 7.11 Rn. 28.
[1195] BVerfG NJW 2005, 1917 (1919).
[1196] BVerfG NJW 1989, 2611 (2612).
[1197] BVerfG NJW 1989, 2611 (2612).
[1198] BVerfG NJW 2005, 1917 (1919).

623 Wie das Verhältnis von Anwalt zu Mandanten ist erst recht dasjenige zwischen Arzt und Patienten durch ein besonderes gegenseitiges Vertrauen gekennzeichnet.[1199] Die Informationen, die der Patient notwendigerweise für eine Behandlung dem Arzt anvertraut, sind in aller Regel höchstpersönlicher Natur. Die Verschwiegenheit des Arztes dient hier also erneut dem Schutz des Klienten. Sie bildet das Kernstück der ärztlichen Berufsethik.[1200] Zwar gibt es auch im Bereich des Arztrechts berufsrechtliche Regelungen, die Mitteilung von Daten aus dem Verhältnis wird ebenfalls nach § 203 StGB mit Strafe bedroht; allerdings gibt es gesetzliche Regelungen, die ausdrücklich die Aufzeichnung und Übermittlung der Daten verlangen.

a) Berufsrecht[1201]

624 Die Berufsordnung der Ärzte dient der Festlegung von Einzelheiten für die Ausübung des ärztlichen Berufs; die Missachtung kann berufsgerichtlich sanktioniert werden.[1202] Die Berufsordnungen sind unmittelbar rechtsverbindliche autonome Satzungen der Landesärztekammern. Sie werden auf Grundlage der Kammergesetze der Länder erlassen, wobei sich die Landesberufsordnungen regelmäßig an den Vorschlägen bzw. Musterberufsordnungen der Bundesärztekammer und der Ärztetage orientieren.[1203] Die Praxis der Delegation der Regelung der Berufsordnung durch den Gesetzgeber an die autonomen Ärztekammern ist nur in gewissen Grenzen möglich, denn der Gesetzgeber muss weiterhin Einfluss auf die inhaltliche Rechtsetzung haben.[1204]

625 Die Pflicht zur Verschwiegenheit wird durch § 9 BerufsO geregelt; danach hat der Arzt über alles, was ihm in seiner Eigenschaft als Arzt anvertraut wurde, zu schweigen. Zeitlich gilt die Schweigepflicht unbegrenzt, sie endet insbesondere nicht mit der Aufgabe der Praxis[1205] oder dem Tode des Patienten, zumal bestimmte Diagnosen auch Rückschlüsse auf ähnliche Erkrankungen bei Verwandten ermöglichen könnten.[1206] Der Arzt kann jedoch durch die Einwilligung des Patienten von seiner Schweigepflicht entbunden werden oder zum Zwecke des erforderlichen Schutzes eines höherwertigen Rechts-

---

[1199] BGH NJW 1959, 811 (813).

[1200] *Laufs,* in: Laufs/Uhlenbruck*,* § 70 Rn. 1.

[1201] Bezug genommen wird hier jeweils auf die (Muster-)Berufsordnung der Bundesärztekammer, Stand 2004, abrufbar unter: http://www.bundesaerztekammer.de/30/Berufsordnung/Mbopdf.pdf.

[1202] *Laufs,* in: Laufs/Uhlenbruck, § 5 Rn. 4.

[1203] *Laufs,* in: Laufs/Uhlenbruck, § 5 Rn. 5.

[1204] BVerfG NJW 1972, 1504 (1507).

[1205] *Ulsenheimer*, in: Laufs/Uhlenbruck, § 69 Rn. 14.

[1206] *Spickhoff*, NJW 2005, 1983; *Ulsenheimer*, in: Laufs/Uhlenbruck, § 70 Rn. 10.

gutes zur Preisgabe befugt sein.[1207] Mitarbeiter und andere in der Arztpraxis tätige Personen sind über ihre Schweigepflicht zu belehren. Des Weiteren kann der Arzt gesetzlich zur Herausgabe von Daten verpflichtet werden;[1208] § 9 BerufsO schränkt solche Herausgabeverpflichtungen nicht ein. Hierin unterscheidet sich das Berufsrecht der Ärzte grundlegend von dem der Anwälte.

626 Die vorsätzliche (mindestens also bedingter Vorsatz)[1209] und unbefugte Verletzung der Schweigepflicht kann mit Berufsverbot nach § 70 Abs. 1 StGB durch die Berufsgerichte oder Strafgerichte sanktioniert werden.

627 Sowohl § 203 StGB als auch § 9 BerufsO regeln jedoch **nur** den typischen Fall der bewussten - sprich **vorsätzlichen - Weitergabe der anvertrauten Informationen**, auch durch Eröffnung des Zugriffs durch Unterlassen.[1210] Eine explizite Normierung zur Sicherung der Daten bzw. Informationskomponenten besteht hingegen nicht.

b) SGB

628 Die Sozialgesetzbücher enthalten grundsätzliche Regelungen für diejenigen, die Sozialleistungen in Anspruch nehmen. Hierzu gehören nach § 21 ff. SGB I u. a. diejenigen, die als gesetzlich Krankenversicherte ärztliche Hilfe in Anspruch nehmen. Die im Zuge der Behandlung erhobenen, verarbeiteten oder genutzten Daten, also personenbezogene Einzelangaben über persönliche oder sachliche Verhältnisse, sind nach § 67 SGB X Sozialdaten und unterliegen nach § 35 SGB I dem Sozialgeheimnis. Dazu gehören sowohl die behandelnden Ärzte sowie deren Diagnosen.[1211] Die Sozialdaten sollen einem besonderen, dem Steuergeheimnis vergleichbaren Schutz unterliegen.[1212]

629 Der Arzt ist jedoch keine Stelle i.S.d. § 35 SGB I, was sich z.B. aus § 76 SGB X ergibt, nach dem Daten von Ärzten den Sozialstellen nur zu übermitteln sind, sofern § 203 Abs. 1 StGB dies zulässt. Die Daten i.S.d. Sozialgesetzbücher werden folglich vom Arzt erhoben, nicht aber vom Patienten. Die diesbezüglichen Pflichten treffen damit die So-

---

[1207] *Deutsch/Spickhoff*, Medizinrecht, Rn. 478 ff.; *Ulsenheimer*, in: Laufs/Uhlenbruck, § 71 Rn. 1 ff. Eine Entbindung von der Schweigepflicht liegt zum Beispiel beim Bestehen von gesetzlichen Meldepflichten nach den §§ 11 II, 12, 13 GeschlechtskrankheitenG; §§ 7 ff., 11, 12, 49 Infektionsschutzgesetz etc. oder in § 12 GeldwäscheG vor.

[1208] Zum Beispiel bei der Verpflichtung, die bei Versicherungsleistungen notwendigen Daten an die Krankenkassen herauszugeben, dazu: *Krauskopf*, in: Laufs/Uhlenbruck, § 36 Rn. 18.

[1209] Schönke/Schröder-*Lenckner*, § 203 StGB Rn. 20.

[1210] Schönke/Schröder-*Lenckner*, § 203 StGB Rn. 20; unklar bzw. nur auf den objektiven Tatbestand abstellend *Hermeler*, Rechtliche Rahmenbedingungen der Telemedizin, S. 46.

[1211] v. Wulffen-*Bieresborn*, § 67 SGB X, Rn. 7 f.

[1212] BT-Drucks. 8/4022, 80 (96).

zialträger. Die Spezialregelungen bezüglich der Pflichten von Daten erhebenden Stellen in §§ 67 ff. SGB X treffen die Ärzte somit nicht.

630 Allerdings sehen die Sozialgesetzbücher gerade **Übermittlungstatbestände** vor: Nach § 295 SGB V sind z.B. für die Abrechnung die Daten bezüglich der Behandlung inklusive Diagnose der Krankenkasse zu übermitteln.[1213] Diese Daten sind nicht etwa anonymisiert, sondern werden nach § 295 i.V.m. § 291 Abs. 2 SGB V unter Angabe der Patientendaten der Krankenkasse mitgeteilt. Eine absolute Verschwiegenheit wie beim Anwalt ist demnach gerade nicht gewährleistet, sie wird zugunsten der Sozialträger gelockert.

c) BDSG

631 Das BDSG findet auf die durch Ärzte erhobenen und verarbeiteten Daten Anwendung.[1214] Insofern gelten die zum Umfang der Pflichten von Anwälten gemachten Ausführungen, insbesondere zu § 9 BDSG.[1215] Die **Pflichten des Anhangs zu § 9 BDSG** werden allerdings durch eine **Empfehlung der Bundesärztekammer weiter konkretisiert**.[1216] So ist z.B. die Fernwartung ausgeschlossen. Zielrichtung des Anhangs ist jedoch hauptsächlich der Schutz vor dem direkten Zugriff von Unbefugten vor Ort oder durch unsachgemäßen Transport von Datenträgern. Im Rahmen der Benutzerkontrolle wird empfohlen, keine ständige Verbindung ins Internet zu halten und den Zugang von außen nur dann zu gestatten, wenn die Daten geschützt sind – was entsprechende Sicherungsmaßnahmen impliziert. § 39 BDSG enthält darüber hinausgehende Restriktionen hinsichtlich der Zweckbindung von Daten, die durch Stellen erhoben werden, die einem Berufsgeheimnis unterliegen. Hierzu gehören auch medizinische Daten.[1217]

632 Die Offenbarung von medizinischen Daten ist demnach sowohl **strafrechtlich als auch durch** das **BDSG** selbst **sanktioniert**. Problematisch ist erneut die Kontrolle. Die Aufsicht führen grundsätzlich die Aufsichtsbehörden der Länder. Der Arzt kann sich jedoch auf § 38 Abs. 3 Satz 2 BDSG berufen und die Herausgabe der Patientendaten verweigern. Die Kontrolle ist insofern beschränkt, erfolgt aber dennoch durch die Aufsichtsbehörden. Im Verhältnis zwischen Arzt und Patienten greifen nicht die Bedenken, die für

---

[1213] Zu Einzelheiten *Krauskopf,* in: Laufs/Uhlenbruck*,* § 36 Rn. 18 ff.

[1214] *Schlund,* in: Laufs/Uhlenbruck, § 76 Rn. 16; *Hermeler,* Rechtliche Rahmenbedingungen der Telemedizin, S. 55; Quaas/Zuck-*Zuck*, § 2 Rn. 45.

[1215] S.o. Rn. 409 ff.; ebenso *Hermeler*, Rechtliche Rahmenbedingungen der Telemedizin, S. 82.

[1216] Empfehlungen der Bundesärztekammer zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, abrufbar unter: http://www.bundesaerztekammer.de/30/Richtlinien/Empfidx/Schweigepfl/Anhang.html.

[1217] *Gola*, NJW 1993, 3109 (3115 f.).

den Anwalt gelten. Während beim Anwalt keine Datenzugriffsbefugnisse bestehen, werden im Rahmen der Sozialgesetzbücher weitreichend Daten unter strenger Zweckbindung übermittelt. Wenn staatliche Stellen die Abrechnung übernehmen und anhand der übertragenen Daten auch Kontrollen z.B. zur Abrechnung durchführen dürfen, so ist nicht ersichtlich, warum die staatlichen Aufsichtsbehörden von der Kontrolle ausgeschlossen sein sollten, solange der Schutz der höchstpersönlichen Daten durch das Verweigerungsrecht des Arztes gewährleistet ist.

633 Den Arzt treffen somit die in § 9 BDSG und dem zugehörigen Anhang konkretisierten speziellen Pflichten zur Ergreifung von Sicherungsmaßnahmen. Auf den Verhältnismäßigkeitsgrundsatz nach § 9 Satz 2 BDSG kann er sich nicht bzw. nur sehr eingeschränkt berufen.[1218]

d) Vertragliche Nebenpflichten

634 Patient und Arzt schließen regelmäßig einen Behandlungsvertrag. Das Verhältnis geht zwar über ein reines Vertragsverhältnis hinaus, dennoch ist der Behandlungsvertrag grundsätzlich als Dienstvertrag einzustufen.[1219] Insofern können sich auch hier Nebenpflichten zur Ergreifung von Sicherungsmaßnahmen entsprechend § 241 Abs. 2 BGB ergeben.[1220] Die Pflichten sind aufgrund des besonderen Vertrauensverhältnisses ähnlich denen beim Anwalt ausgestaltet.[1221]

e) Deliktische Haftung

635 Die deliktische Haftung ist zwar im Verhältnis zwischen Arzt und Patient besonders ausgeprägt;[1222] doch spielt sie im Rahmen der IT-Sicherheit keine andere Rolle als etwa bei anderen Berufsgruppen, die mit sensiblen Daten umgehen, so daß insofern wird auf die Ausführungen zu den Anwaltspflichten verwiesen werden kann.[1223] Allerdings werden aufgrund der stets vorliegenden Verletzung eines der absolut geschützten Rechtsgüter infolge der Heilbehandlung eher die IT-Sicherheitspflichten Eingang finden können in die Gesamtbeurteilung, ob der Arzt seine Verkehrspflichten verletzt hat.

f) Ergebnis

[1218] *Heibey,* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5. Rn. 26.

[1219] BGHZ 63, 306 (309); 76, 249 (261); 97, 273; BGH NJW 1981, 613.

[1220] Quaas/Zuck-*Zuck*, § 2 Rn. 48; vgl. *Schlund,* in: Laufs/Uhlenbruck, § 77 Rn. 2.

[1221] S.o. Rn. 616 f.

[1222] Zum deliktischen Arzthaftungsrecht Bamberger/Roth-*Spindler*, § 823 BGB Rn. 585 ff. mwN.

[1223] S.o. Rn. 608 ff.b

636 Auch der Arzt ist verpflichtet, den Pflichten eines kommerziellen Nutzers nachzukommen. Das besondere Vertrauensverhältnis und die Sensibilität der Daten begründen eine weiter gehende vertragliche Pflicht. Im Rahmen der deliktischen Haftung besteht ebenfalls eine erhöhte Sicherungspflicht.

6. Zwischenergebnis: besondere Verantwortlichkeit von Experten und beratenden Berufen

637 Obwohl IT-Sicherheit nicht speziell für beratende Berufe und Experten geregelt ist, können die vorhandenen Regelungskomplexe dennoch ohne weiteres auf diese angewandt werden. Grundsätzlich sind die normierten Sicherungspflichten ausgeprägter, orientieren sich aber zumindest als Mindeststandard an dem für andere kommerzielle IT-Nutzer.

638 Unterschiede ergeben sich jedenfalls bei der vertraglichen und deliktischen Haftung. Aufgrund des besonderen Vertrauensverhältnisses lassen sich einerseits erhöhte vertragliche Nebenpflichten in Form von speziellen Sicherungspflichten und andererseits verschärfte Verkehrssicherungspflichten herleiten.

VI. Pflichten kommerzieller Nutzer – Übersicht

639 Die Pflichten der kommerziellen Nutzer werden wie gezeigt durch verschiedene Normen umschrieben bzw. geregelt. Wie dargestellt existieren teilweise sektorspezifische Regelungen, die bestimmte, bereichsspezifische Anforderungen an kommerzielle Nutzer festlegen. Hinzu können sich Ansprüche aus Deliktsrecht ergeben, sofern die festgelegten Pflichten als Schutzgesetz im Rahmen von § 823 II BGB einzuordnen sind. Schließlich können im Rahmen der Haftung nach § 823 I BGB allgemeine Schutzpflichten bestehen, die mit den Selbstschutzpflichten privater Nutzer spiegelbildlich korrelieren. Dadurch ergibt sich zwangsläufig eine gewisse Zersplitterung der Pflichten abhängig davon, welche tatbestandlichen Voraussetzungen ein kommerzieller Nutzer erfüllt. Um kommerziellen Nutzern eine möglichst kompakte und handhabbare Übersicht über die Pflichten zu geben, müssen demnach die insgesamt übereinstimmenden Pflichten, die Unterschiede sowie das Verhältnis der einschlägigen Normen zueinander bestimmt werden.

640 Dabei ist zu beachten, dass nur die wenigsten gesetzlichen Regelungen überhaupt ausdrücklich IT-spezifischen Inhalt besitzen, also die Konkretisierung auf einzelne Pflichten jeweils Ergebnis einer Rechtsfortbildung seitens der Rechtsprechung oder durch die

Anwendung von Auslegungsregeln ist. Zur Folge hat dies aber auch, dass Pflichten selten ganz konkret benannt werden können bzw. Alternativen nur in Ausnahmefällen tatsächlich ausgeschlossen sind. Vielmehr handelt es sich um „weiche“ Normen, deren Zielsetzung in unterschiedlicher Weise erreicht werden kann und erreicht werden darf, wobei die Anforderungen an das IT-Riskmanagement von den individuellen Faktoren des jeweiligen Unternehmens wie Art, Umfang, Komplexität und Risikogehalt[1224] des Geschäftsbetriebs abhängen.

1. Betrachtete Normen

641 Im Folgenden soll deshalb übersichtshalber versucht werden, die bisher dargestellten Ergebnisse kompakt zusammenzufassen. In die Übersicht einbezogen werden § 91 Abs. 2 AktG sowie § 43 GmbHG für Unternehmen einer bestimmten Organisationsform, § 25a KWG für Kredit- und Finanzleistungsinstitute, § 33 Abs. 1 WpHG, dessen Adressaten Kreditinstitute und Wertpapierhandelsunternehmen sind, die einschlägigen Normen des Sarbanes-Oxley-Act für in den USA börsennotierte Unternehmen, das Datenschutzrecht, also insbesondere BDSG und TMG sowie § 109 TKG für Telekommunikationsdiensteanbieter. Etwas außerhalb dieses Systems stehen schließlich die nur mittelbar wirkenden Pflichten, die Basel II impliziert.

2. Gemeinsame Pflichten

642 Am deutlichsten zeigen sich die Gemeinsamkeiten in der Regelungstechnik bei §§ 91 Abs. 2 AktG bzw. 43 GmbHG, 25a KWG sowie 33 Abs. 1 WpHG. Ihnen allen zugrunde liegt eine bestimmte Form des IT-Riskmanagements. Dies beinhaltet jedenfalls eine mindestens rudimentäre **einmalige Risikoanalyse** sowie eine Organisation, die dauerhaft die **Gefahrenerkennung** ermöglicht und **Verantwortlichkeiten** dergestalt festlegt, dass auf Gefahrensituationen angemessen reagiert werden kann. Diese Pflichten lassen sich jedoch auch für das Datenschutzrecht sowie § 109 TKG statuieren.

643 **Kriterien** für die Intensität der Risikoanalyse aber auch die Vorhaltung bzw. den Einsatz von entsprechenden Kapazitäten zur Risikominimierung und –behebung sind insbesondere die Art, der Umfang und die Bedeutung des Einsatzes von EDV für das Unternehmen, eingesetzte Hardware, die Organisation der Datenverarbeitung, Art und Sensitivität der Daten speziell auch im Hinblick auf den Geschäftsbetrieb sowie die Gefahr der Verletzung von Interessen Dritter.

[1224] So konkretisiert in § 25a Abs. 2 Satz 1 KWG-RefE (2006) zur Umsetzung der MiFID.

644 Als **konkrete Maßnahmen** wurden identifiziert:

- Festlegung von Zuständigkeiten,
- Vier-Augen-Prinzip,
- Einmalige Benennung und Bewertung möglicher Risiken (Risikoanalyse),
- Ergreifung von Maßnahmen zur Risikoabwehr bzw. –minimierung, wobei sich die Konkretisierung insbesondere auch durch die allgemeinen Pflichten ergeben kann,
- Einrichtung eines Systems zur Erkennung von Veränderungen des Systems, also Gefahrerkennung,
- (regelmäßige) Prüfung von verwendeter Software,
- **Dokumentation** des Ergebnisses der Risikoanalyse als Ist-Zustand,
- Dokumentation der getroffenen Maßnahmen z.B. durch entsprechende Checklisten **und** ihrer Durchführung,
- Regelmäßige Datensicherungen und bei Bedarf Vorhaltung von Ersatzkapazitäten bzw. technischer Alternativen zur Bewältigung des Geschäftsbetriebs bzw. Teilen davon, z.B. der Buchhaltung, auch bei Ausfall der Primärsysteme,
- **Kontrolle** aller Maßnahmen durch das Management (insb. nach SOX),

3. Unterschiede

645 Unterschiede zwischen den Pflichten ergeben sich insbesondere im Hinblick auf die Zielrichtung. Während die Pflichten nach AktG und GmbHG Störungen des Geschäftsbetriebs verhindern bzw. beheben können sollen, zielen KWG und WpHG auch und besonders auf die störungsfreie Durchführung der Aufträge ab. Auf der einen Seite steht somit der Schutz des Unternehmens, auf der anderen der Schutz Dritter bzw. weiterer Verfahren wie eben des Finanzverkehrs.

646 Das Datenschutzrecht sowie die Pflichten von Telekommunikationsanbietern haben zudem einen stark technischen Charakter. Ziel ist hier der Schutz der Daten, verlangt werden deshalb **angemessene technische Vorkehrungen**. Daraus lassen sich zwar auch Pflichten in Richtung eines IT-Sicherheitsmanagements ableiten, aber im Vordergrund steht die Erreichung eines technischen Schutzes. Zudem kann nach § 4f BDSG die Bestellung eines Datenschutzbeauftragten erforderlich sein.

647 Eine Sonderstellung hat des Weiteren der **Sarbanes-Oxley-Act**. Er soll insbesondere die korrekte Rechnungslegung sichern (im Einzelnen siehe III.3.a)(3)(b)), fordert aber über die Festlegung von entsprechenden Zuständigkeiten hinaus auch sogenannte

Whistleblowing-Verfahren, Audit-Commitees sowie eine interne Revision als Kontrollinstanz der Kontrollverfahren. Insgesamt erweitert der Sarbanes-Oxley-Act durch neue Verfahren den Pflichtenbereich der Unternehmen ohne jedoch bisherige Verfahren und Methoden in Frage zu stellen.

648 Wesentliche **Widersprüche** hinsichtlich der zu ergreifenden Maßnahmen oder der Kriterien haben sich nicht ergeben, so dass sich Konfliktsituationen nur daraus ergeben können, wie unterschiedliche Intensitäten der normierten Pflichten zu behandeln sind.

4. Anwendbarkeit bzw. Verhältnis der Normen zueinander

649 Anknüpfungspunkt einer Pflicht kann nur die Erfüllung des Tatbestandes der die Pflicht statuierenden Norm sein. Die hier untersuchten Normen haben dabei insbesondere einen unterschiedlichen persönlichen Anwendungsbereich. Grundsätzlich gilt, dass der Betroffene die Pflichten **aller** Normen erfüllen muss, die für ihn gelten. Wer also der Organisationsform nach unter den Anwendungsbereich des AktG bzw. des GmbHG fällt, den können durchaus auch jene Pflichten treffen, die z.B. durch das WpHG zusätzlich zu erfüllen sind. Insofern ist grundsätzlich von einer parallelen Anwendung der Normen auszugehen. Unterscheiden sich die Normen in der Intensität der anzuwendenden Maßnahmen, so ist schwerlich einzusehen, warum nicht die schärferen Maßnahmen ergriffen werden sollen.

650 Das Verhältnis der datenschutzrechtlichen Normen ist ähnlich unkompliziert. Das TMG enthält bereichsspezifische Regelungen, die die Betreiber von Telemediendiensten betreffen.[1225] § 109 TKG wiederum konkretisiert die Verpflichtungen aus dem BDSG,[1226] steht also im Spezialitätsverhältnis zu § 9 BDSG, wobei dessen Anforderungen nicht verdrängt werden.[1227] Somit gilt auch hier, dass jeweils ein Basisschutz gewährleistet werden muss, der durch die weiteren Normen im Rahmen ihres Anwendungsbereichs ergänzt wird. Abgrenzungsschwierigkeiten aufgrund der Konvergenz von Diensten könnten mit Einführung des Telemediengesetzes aufgelöst werden.

5. Ergebnis

651 Kommerziellen Nutzern ist nach diesen Ausführungen zu raten, in jedem Fall Erfüllung derjenigen Pflichten anzustreben und auch zu dokumentieren, die im Grunde allen hier

[1225] Spindler/Schmitz/Geis-*Schmitz*, Einf. TDDSG Rn. 1.
[1226] Säcker-*Klesczewski*, § 109 TKG Rn. 8.
[1227] Scheurle/Mayen-*Zerres*, § 87 TKG a.F. Rn. 4.

dargestellten Normen gemein sind. Nicht nur erreichen sie damit bereits einen relativ hohen Grad des technischen Schutzes, zusätzlich wird sichergestellt, dass sie von eventuellen rechtlichen Folgen, die sich für sie ergeben können, profitieren. Wenn also z.B. Haftungserleichterungen oder Erleichterungen für die Beweisführung möglich sind, kann die Erfüllung der generellen Handlungspflichten meist solche Rechtsfolgen bereits herbeiführen. Je nachdem, ob spezielle Funktionen erfüllt werden bzw. die Einordnung anhand der genannten Kriterien erhöhte Pflichten bedingt, muss aber auch über die gemeinsamen grundsätzlichen Maßnahmen hinausgegangen werden.

652 Am Anfang jedes Verfahrens steht also die Analyse des eigenen Unternehmens. Dabei sind insbesondere die folgenden Fragen zu beantworten:

- Welcher Art sind eingesetzte IT-Systeme und welchen Umfang hat ihr Einsatz?
- Wie wichtig ist der Einsatz der IT-Systeme für das Gesamtunternehmen, aber auch für einzelne Geschäftsbereiche bzw. Verfahrensabläufe? Als Kontrollfrage könnte der Ausfall eines oder mehrerer Systeme angenommen werden und die Auswirkungen betrachtet werden.
- Was für Daten werden verwendet? Welche Folge hätte ihr Verlust bzw. ihre Veränderung? Welche Geschäftsabläufe wären davon betroffen? Sind Dritte betroffen und wenn ja, in welchem Umfang?
- Wie verhalten sich die Antworten auf diese Fragen zur Gesamtgröße bzw. zur generellen wirtschaftlichen Leistungsfähigkeit des Unternehmens? Da insbesondere Zumutbarkeitsüberlegungen immer nur für den Einzelfall entschieden werden können, spielen auch solch ganz konkrete Gegebenheiten eine wesentliche Rolle. Allerdings können Exkulpationen nur greifen, wenn sich hierfür Anhaltspunkte in der anzuwendenden Norm ergeben; dies betrifft vor allem die allgemeinen haftungsrechtlichen Pflichten. Die Pflichten des AktG, des KWG, WpHG sowie des SOX sind diesen Überlegungen nur bedingt zugänglich.

653 Im Anschluss daran können die beschriebenen Maßnahmen, angefangen mit einer konkreten Risikoanalyse, ergriffen werden, wobei die Beantwortung der vorgeschlagenen Fragen als Indiz für die Intensität und damit auch den zumutbaren wirtschaftlichen und technischen Aufwand gewertet werden darf.

VII. Endergebnis

654 Die IT-Sicherungspflichten ebenso wie die Selbstschutzpflichten hängen erheblich davon ab, welche Tätigkeiten der IT-Nutzer durchführt, ob diese rein privater oder kommerzieller Natur sind. Ein Sonderwissen des IT-Nutzers, dass dieser im Rahmen seiner gewerblichen Tätigkeit gewonnen hat, muß diesem bei einer privaten Tätigkeit zugerechnet werden, sofern der IT-Nutzer auch außerhalb seiner gewerblichen Tätigkeit die

Möglichkeit hat, auf die entsprechenden Ressourcen zuzugreifen, was bei Arbeitnehmern differenziert zu beurteilen ist. Generell sind kommerzielle IT-Nutzer zu wesentlich höheren Sicherungen verpflichtet als private IT-Nutzer.

655 Für **private Nutzer** bestehen nur eingeschränkte Sicherungspflichten zum jetzigen Zeitpunkt: Mangels ausreichender Bekanntheit von Problem und Lösung sind diese lediglich zum Einsatz von Virenscannern sowie zu entsprechenden Aktualisierungen verpflichtet. Im Bereich der Schadensminderungs- und Selbstschutzpflichten können die Grundsätze des Dialer-Urteils des BGH angewandt werden, indem private IT-Nutzer nicht routinemäßig ihre Systeme auf Dialer ohne besondere Verdachtsmomente überprüfen müssen und ihnen nicht die Überwachung des Aufbaus von Verbindungen ins Internet obliegt.[1228] Übertragen auf IT-Sicherungen entfällt jedenfalls derzeit, und solange Bedrohungspotentiale nicht generell bekannt und einfach zu meistern sind, die Pflicht zu Selbstschutzmaßnahmen zumindest bei privaten Softwarenutzern.

656 Bei **kommerziellen Nutzern** sind zunächst die gesellschaftsrechtlichen Anforderungen an IT-Nutzer im Rahmen des Risikomanagements zu berücksichtigen. Im Zuge der weiteren Ausdifferenzierung der von verschiedenen Seiten vorgegebenen Standards (ISO 27001, BSI-Grundschutzhandbuch, MaRisk etc.) müssen die kommerziellen IT-Nutzer höhere Aufwendungen im Bereich der Datenerfassung und –auswertung tätigen, um für ein robustes und effizientes internes Risikoerkennungssystem zu sorgen. Ferner müssen die kommerziellen Nutzer, abhängig auch von der Größe ihrer IT-Infrastruktur, Maßnahmen zur Sicherung ihrer IT-Systeme ergreifen. Dazu gehören die primäre Abwehr, die sekundäre Überprüfung durch Suchprogramme sowie die notwendige Aktualisierung der Programme. Welche Rolle indes diese IT-Standards im Rahmen dieser Pflichten spielen können, ist bislang weitgehend ungeklärt.

657 Dies gilt auch für die mittelbaren IT-Sicherungspflichten, denen Unternehmen infolge der durch die neuen Fremdkapitalvergabevorschriften nach Basel II unterliegen; auch hier werden zwar die genannten IT-Standards berücksichtigt, doch ohne dass bislang deren rechtlicher Stellenwert völlig geklärt wäre.

658 Besonderen Pflichten unterliegen schließlich einige Wirtschaftssektoren und Berufe, denen entweder eine besondere hohe volkswirtschaftliche Bedeutung zukommt (Banken, Finanzsektor) oder bei denen eine besonders intensive Vertrauensbeziehung zu

[1228] BGH NJW 2004, 1590 (1592) = JZ 2004, 1124 (1127) m. Anm. *Spindler.*

dem Kunden bestehen, wie etwa Anwälte, Steuerberater und Ärzte. Bei letzteren lassen sich insbesondere aufgrund des besonderen Vertrauensverhältnisses erhöhte vertragliche Nebenpflichten in Form von speziellen Sicherungspflichten und andererseits verschärfte Verkehrssicherungspflichten herleiten.

659 Allerdings muss der Nutzer, insbesondere der kommerzielle, bei Programmen mit bekannten Sicherheitslücken dieses Programm sperren und darf es nicht mehr einsetzen. Benutzt er es dennoch sehenden Auges und entstehen hierdurch aufgrund Hackerangriffe Schäden, kann sich, wie soeben erörtert, ein völliger Ausschluss des Schadensersatzanspruchs ergeben.

E. Verantwortlichkeit von IT-Intermediären

I. Überblick

660 Quasi zwischen IT-Hersteller und IT-Nutzer stehen die IT-Intermediäre, die gerade über elektronische Kommunikationsnetze Dienstleistungen erbringen. Die Anwendungsgebiete reichen von der Bereithaltung von elektronischen Plattformen für fremde Inhalte (Host-Provider) über die Zugänglichmachung elektronischer Netze (Access-Provider) bis hin zu verschiedensten Mehrwertdiensten, die über elektronische Netze angeboten werden, etwa sog. Web-Services, die es Unternehmen erlauben, mit Hilfe von Dritten spezifische Funktionen, wie den Einkauf und das electronic invoicing, auszulagern und über elektronische Kommunikationsnetze (wieder mit Hilfe von IT-Intermediären) abzuwickeln. Letzteres überlappt sich stark mit kommerziellen IT-Nutzern, die ihrerseits IT-Dienstleistungen erbringen, so dass diesbezüglich auf das entsprechende Kapitel verwiesen wird.

661 IT-Intermediäre können ebenso wie andere IT-Nutzer zahlreichen Gefahren ausgesetzt sein, die auf ihre IT-Nutzer durchschlagen können. Zahlreiche für kommerzielle IT-Nutzer beschriebene Szenarien (o. Rn. 591 ff.) sind mutatis mutandis auf IT-Intermediäre ohne weiteres anwendbar, da sie häufig die IT-Infrastrukturen gerade für Unternehmen zur Verfügung stellen, die selbst nicht diese Infrastrukturen vorhalten wollen (Outsourcing). Als Beispiel seien etwa die Zurverfügungstellung von Web-Plattformen im elektronischen Handel für andere IT-Unternehmen oder Banken erwähnt, die mit Hilfe der IT-Dienstleistungen der Intermediäre ihre eigentlichen Dienstleistungen (Banking, Handel) etc. anbieten und abwickeln können.

662 Demgemäß greifen für IT-Intermediäre zahlreiche Pflichten in ähnlicher Weise wie für kommerzielle IT-Nutzer ein, allerdings modifiziert durch ihre jeweilige Funktion und durch eingreifende besondere **Haftungsprivilegierungen** zu ihren Gunsten, die ihr Verantwortlichkeitsrisiko sowohl straf- als auch zivilrechtlich teilweise signifikant reduzieren. Dies gilt insbesondere für alle Anbieter von Leistungen, die gleichzeitig als Telekommunikationsdienstleistungen qualifiziert werden können, da hier die Haftungsbegrenzung nach § 44a TKG (eingefügt durch die jüngste **Reform des TKG**[1229] als Nachfolger der TKV a.F.) eingreift, wonach für Vermögensschäden die Haftung insgesamt auf 12.500 Euro beschränkt ist – im Gegensatz zum sonstigen Zivilrecht selbst bei grober Fahrlässigkeit. Begründet wird die Haftungsbegrenzung mit den kaum abschätzbaren wirtschaftlichen Risiken, die sich bei einem Verzicht auf eine Haftungshöchstgrenze ergeben könnten.[1230] Unerheblich für die Haftungsbegrenzung ist die Entstehungsgeschichte und der Rechtsgrund des Schadensersatzanspruchs.[1231] Allerdings gilt sie ausdrücklich nur für (primäre) Vermögensschäden, zu denen nach der Begründung des Verordnungsentwurfs[1232] nicht Folgeschäden aus Sach- oder Personenschäden zählen.[1233] Ferner kann § 44a TKG nicht für Schäden Dritter eingreifen, die keine vertragliche Beziehung zu dem Telekommunikationsunternehmen haben. Der Anwendungsbereich der §§ 43a ff. (Teil 3) beschränkt sich auf „Kunden“. Kunden sind nach der Legaldefition des § 1 I TKV a.F., die nach der ratio aber auch für das neue TKG genutzt werden kann, Personen, die Telekommunikationsdienstleistungen vertraglich in Anspruch nehmen oder begehren. Die Anwendbarkeit der §§ 43a ff. TKG auf Kunden ergibt sich zum einen aus der Teilbereichsüberschrift „Kundenschutz“ des Teil 3 TKG und zum anderen aus der Formulierung Endnutzer in § 44a TKG, womit aber lediglich Kunden gemeint sind.[1234] Diese Annahme entspricht auch der Tatsache, dass § 44a TKG im wesentlichen dem § 7 II TKV a.F. entspricht. Die Telekommunikations-Kundenschutzverordnung, die nach § 1 I TKV a.F. auch nur auf Kunden anwendbar war, wurde jüngst durch das TK-Änderungsgesetz in Teil 3 des TKG integriert. Die meisten Schäden für Unternehmen oder andere IT-Nutzer von Dienstleistungen von IT-

[1229] Siehe Bundesgesetzblatt Teil 1 Nr. 5 vom 23.2.2007, S. 106 ff.

[1230] BR-Drucks. 551/97, S. 28.

[1231] BT-Drucks. 15/5213, S. 21; Beck`scher TKG-Kommentar-*Dahlke*, § 44a TKG-E Rn. 9; Scheurle/Mayen-*Schadow*, § 41 TKG Rn. 51.

[1232] BR-Drucks. 551/97, S. 28 f.

[1233] Zur Abgrenzung des reinen Vermögensschadens von anderen Folgeschäden vgl. nur Palandt-*Heinrichs*, vor § 249 BGB Rn. 8 ff. mwN.

[1234] Beck´scher TKG-Kommentar-*Schütz*, § 3 Nr. 8 TKG Rn. 25.

Intermediären werden jedoch vertragliche Beziehungen zu diesen unterhalten, etwa bei beim Hosting von Daten auf einem Web-Server oder der Zurverfügungstellung von Portalen, so dass oftmals die TKV eingreifen kann.

663 Gegenüber der bislang geltenden TKV enthält § 44a TKG jedoch auch etliche Verbesserungen für den Geschädigten: Anders als in § 7 TKV a.F. entfällt in § 44a TKG die individuelle Haftungsbegrenzung zugunsten einer nur insgesamt wirkenden Haftungsbegrenzung, allerdings wie bisher auch für alle selbst grob fahrlässig herbeigeführten Vermögensschäden. Begründet wird dies von der Bundesregierung damit, daß „das Entfallen der individuellen Haftungsbeschränkung zu einer Besserstellung der Geschädigten in den Fällen (führe), in denen nur wenige von einer Schädigung betroffen sind. Damit wird in vielen Fällen vermieden, dass Ersatzansprüche selbst dann begrenzt werden, wenn ein Anbieter den von ihm verursachten Schaden tatsächlich ohne Not tragen kann, der jedoch für den Geschädigten - z.B. bei Datenverlusten - eine die wirtschaftliche Existenz bedrohende Dimension haben kann.“[1235]

664 Die Pflichtenstellung der IT-Intermediäre leitet über zu der Frage, welche Gemeinsamkeiten und Unterschiede zwischen der deliktischen Haftung und einer Haftung für Dienstleistungen (noch) bestehen. Ohne hier auf Details eingehen zu können, [1236] sind die grundsätzlichen Unterschiede nochmals ins Gedächtnis zu rufen:

- die deliktische Haftung greift gegenüber jedermann, die vertragliche nur gegenüber dem Vertragspartner und die in den Schutzbereich einbezogenen Dritten (deren Kreis von der Rechtsprechung allerdings teilweise erheblich ausgedehnt wird)
- die deliktische Haftung ist weitgehend von der Verletzung von bestimmten Rechtsgütern abhängig, indem insbesondere Vermögensschäden nicht erfasst werden, im Gegensatz zur vertraglichen Haftung
- die deliktische Haftung erfasst nur das Integritätsinteresse, nicht das Äquivalenzinteresse
- Unterschiede bestehen ferner nach wie vor bei der Verjährung, trotz der Harmonisierung in der Schuldrechtsreform durch § 199 BGB, da die vertragliche Haftung hinsichtlich des Verjährungsbeginns nach wie vor von einem objektiven System ausgeht.

665 Tendenziell ist daher das nach wie vor größte Risiko beim IT-Einsatz, der Vermögensschaden und insbesondere der Betriebsausfallschaden, nicht von der deliktischen Haftung erfasst, sondern nur von der vertraglichen Haftung. Aber auch hier zeichnen sich

[1235] Begr RegE BT-Drucks. 16/2581 zu § 44a TKG, S. 24.
[1236] S. dazu *Wendehorst,* AcP 206 (2006), 205 ff.

Konvergenzen ab, indem zum einen vertragliche Haftungseingrenzungen für Vermögensschäden, teilweise sogar gesetzliche Haftungsbeschränkungen wie im TKG, zugelassen werden, zum anderen die Reichweite des Rechtsgüterschutzes in § 823 I BGB ausgedehnt wird auf Funktionalitäten des Eigentums.

666 Für die Anwendung der Verantwortlichkeitsprivilegierungen müssen die verschiedenen Risiken für IT-Intermediäre unterschieden werden:

- Zum einen kann der IT-Intermediär selbst Opfer eines IT-Angriffs werden, etwa durch eine Denial-of-Access-Attacke oder das Hacken in das System mit der Folge der Datenausspähung oder Sabotage etc. Anders ausgedrückt ist die Sicherheit des IT-Systems des Intermediärs selbst betroffen, von ihm selbst geht die Gefahr für Dritte aus. In diesem Fall finden die allgemeinen Verkehrspflichten, je nach Funktion modifiziert, Anwendung.

- Zum anderen können Intermediäre in die Verantwortung genommen werden können, wenn sie als Zwischenstelle für Daten agieren, die anschließend beim Nutzer einen Schaden hervorrufen. Der Intermediär stellt also auch mittelbar nicht selbst diese Daten bereit, sondern leitet diese nur in irgendeiner Form weiter, wobei sich die Frage stellt, ob ihn eine Prüfungspflicht hinsichtlich der Gefährlichkeit der Daten trifft. Typisches Beispiel ist die Weiterleitung von virenbefallenen E-Mails an andere Nutzer (Rn. 295 ff.).

667 Unterschieden wird in diesem Zusammenhang gern zwischen Content-, Host- und Access-Provider – auch wenn diese Unterscheidung eher heuristischen Wert hat, da das Gesetz nicht auf diese Begriffe abstellt. Als Content-Provider wird bezeichnet, wer eigene Informationen zur Nutzung im Netz bereithält.[1237] Host-Provider ist, wer fremde Inhalte zum Abruf bereithält.[1238] Der Host-Provider stellt also seinen Kunden nur Speicherplatz bzw. eine Plattform zur Verfügung, den diese mit eigenen Inhalten füllen können. Access-Provider ist derjenige, der technisch den Zugang zum Netz bzw. die Einwahl ins Internet ermöglicht.[1239]

II. Sicherungspflichten der IT-Intermediäre für ihre eigenen Systeme

668 Grundsätzlich ist der IT-Intermediär ein kommerzieller Nutzer von Informationstechnik. Anknüpfungspunkt für Sicherungspflichten ist auch hier die Beherrschung seiner eigenen Systeme als einer Gefahrenquelle, allerdings auch kombiniert mit Schutzpflichten,

[1237] *Sessinghaus*, WRP 2005, 697.
[1238] *Stadler*, Haftung für Informationen im Internet, Rn. 10; *Sessinghaus*, WRP 2005, 697.
[1239] *Stadler*, Haftung für Informationen im Internet, Rn. 11.

da er in aller Regel direkten Zugriff auf alle Daten, aber auch der einzige ist, der die Daten Dritter (seiner Vertragspartner etc.) schützen kann:

669 Anders als bei den Verantwortlichkeitsprivilegierungen nach §§ 7 ff. TMG, deren Rechtsgrund die Unmöglichkeit einer Kontrolle durch die schiere Datenmenge und entgegenstehende Rechte bildet,[1240] kann dieser Gedanke für die Sicherungen des eigenen Systems nicht verfangen, wie § 7 Abs. 1 TMG schon für eigene Informationen klar stellt. Die Haftungsmodifizierungen der §§ 8 - 10 TMG finden hier nur eingeschränkt Anwendung, da sie nur die Haftung für *Inhalte* betreffen, nicht aber die Haftung für die *Funktionstüchtigkeit* und die *Sicherheit* der vom Service Provider angebotenen Dienste.[1241] Hier muß differenziert werden:

670 Wird die Datei eines Nutzers durch einen Virus infiziert, der sich in einer Datei (bzw. Information) befand, die ein Dritter auf den Rechnern des Providers abgespeichert hat, findet § 10 TMG im Prinzip Anwendung – sofern es sich bei dem Dritten wiederum um einen Nutzer handelt, der berechtigterweise auf den Rechnern des Providers Dateien speichern durfte. Handelt es sich dagegen um einen „Hacker", der sich unberechtigterweise Zugang zu den Rechnern des Providers verschafft hat, kann § 10 TMG nicht eingreifen, da § 10 TMG nicht generell jede Verkehrssicherungsmaßnahme des Providers ausschalten will. Im Falle von Access Providern greift dagegen § 8 TMG ein, wenn der Virus sich in einer weitergeleiteten Datei befand, nicht dagegen, wenn der „Hacker" sich Zugang zu dem System des Providers verschafft hat. Werden die Daten und Informationen daher erst beim Intermediär schadhaft, so kann ihn grundsätzlich eine Haftung aus der Verletzung von Sicherungspflichten treffen.[1242] Es greifen die allgemeinen Haftungsnormen ein, sei es Vertrags- oder Deliktsrecht.[1243] Ungeachtet der Haftungsprivilegierungen werden jedoch aufgrund der oftmals vorhandenen vertraglichen Beziehungen über die deliktisch geschützten Rechtsgüter hinaus auch Vermögensschäden erfasst, da eine Verletzung von Sicherungspflichten gleichzeitig eine Vertragsverletzung impliziert (§ 280 I BGB). Sicherungspflichten der Provider werden in aller Regel zu den frei-

[1240] Erwägungsgrund Nr. 42 ECRL; Spindler/Schmitz/Geis-*Spindler*, vor § 8 TDG Rn. 11.

[1241] Anders offenbar *Schneider/Günther*, CR 1997, 389 (391), die Haftungseinschränkungen nach TDG/MDStV – ohne nähere Begründung – auch bei virenverseuchten Online-Diensten annehmen.

[1242] Spindler/Schmitz/Geis-*Spindler*, vor § 8 TDG Rn. 25; *Koch*, NJW 2004, 801 (805 f.); *Pelz,* in: Bräutigam/Leupold, Kap. B I Rn. 72; *Dustmann*, Die priviligierten Provider, 136 f.; *Podehl*, MMR 2001, 17 (21); *Schwarz/Poll*, JurPC 73/2003, Rn. 72.

[1243] Spindler/Schmitz/Geis-*Spindler*, § 8 TDG Rn. 10; i.E. ebenso *Christiansen*, MMR 2004, 185 (186).

zeichnungsfesten Kardinalpflichten gehören, so daß die §§ 8-10 TMG hier auch keine Leitbildfunktion im Sinne von § 307 I BGB entfalten.

671 Demgegenüber wird offenbar für das österreichische Recht davon ausgegangen, daß die Provider keine Verantwortlichkeit nach der E-Commerce-Richtlinie bzw. den entsprechenden Umsetzungsbestimmungen in Österreich treffe.[1244]

1. Vertragliche Verantwortlichkeit

672 Für Schadensersatzansprüche des Vertragspartners gegen seinen IT-Intermediär sind zunächst die jeweils abgeschlossenen vertraglichen Bestimmungen maßgeblich, sei es der Vertrag über den Internetzugang, über die Nutzung der vom Provider angebotenen Dienste oder das Webhosting. Allgemeine Aussagen über die Verantwortlichkeit lassen sich hier aus Raumgründen kaum treffen, da die Verträge völlig unterschiedliche Leistungsinhalte haben und damit auch unterschiedlichen gesetzlichen Leitbilder folgen können, etwa das Webhosting dem Mietvertrag[1245] oder das Access-Providing dem Dienstvertrag[1246]. Darüberhinaus können Leistungsbeschreibungen in den AGB der IT-Intermediäre ebenso eine Rolle spielen wie die Anwendbarkeit des TKG.[1247]

673 Weitestgehend gemein ist jedoch allen Vertragstypen, dass sie Schutzpflichten für den Vertragspartner als Nebenpflichten vorsehen. Diese können auch nur in sehr eingeschränktem Maße durch Allgemeine Geschäftsbedingungen ausgeschlossen werden, da sie oftmals zwar selbst keine Hauptleistungspflicht darstellen, aber für die Erbringung der Hauptleistung des Vertrages doch so wesentlich sind, dass sie als sog. Kardinalpflichten bezeichnet werden können. Anders formuliert nützt dem Kunden die Erbringung einer Speicherleistung nichts, wenn der entsprechende Server in keinster Weise gegenüber unbefugten Zugriffen Dritter geschützt ist. Derartige Kardinalpflichten sind indes gemäß § 307 II Nr. 2 BGB freizeichnungsfest.[1248] Dieser Pflichtenkanon ist häufig weitgehend ähnlich den deliktischen Sicherungspflichten, wenngleich er auch nicht an bestimmten Rechtsgutsverletzungen allein anknüpft. Hinzu können im Einzelfall Pflich-

---

[1244] *Fallenböck* Annex II – Österreich - Rn. 1173.

[1245] *Schuppert*, in: Spindler, Vertragsrecht der Internet-Provider IV, Rn. 47; *Cichon*. Internetverträge, Rn. 182 f., 184 ff.

[1246] BGH CR 2005, 816 (817) (obiter dictum); ausführlich *Spindler*, in: Spindler, Vertragsrecht der Internet-Provider IV, Rn. 93.

[1247] Näher dazu *Spindler*, in: Spindler, Vertragsrecht der Internet-Provider IV, Rn. 21 ff.

[1248] St.Rspr. BGH NJW 1993, 335; BGH NJW-RR 1993, 560 (561); BGH NJW 2002, 673 (674); zuletzt BGH NJW-RR 2005, 1496 (1505 ff.), wonach der Verwender von AGB sich nicht darauf beschränken dürfe, die Verletzung von Kardinalpflichten von der Haftungsfreizeichnung auszunehmen. Er müsse zwar die Kardinalpflichten nicht abschließend in der Klausel aufzählen, jedoch den Begriff zumindest abstrakt erläutern, um die Unwirksamkeit seiner Freizeichnungsklausel wegen Verstoßes gegen das Transparenzgebot (§ 307 I 2 BGB) zu vermeiden.

ten zur Information über Gefahren oder Abwehr der Gefahren kommen. Des weiteren kann als Nebenpflicht auch die Sicherung der Daten des Kunden bestehen.[1249] Dies befreit natürlich die Nutzer umgekehrt nicht von der Pflicht der eigenen regelmäßigen Datensicherung.[1250] Im Einzelfall kann vom Website-Host auch die Vorhaltung redundanter Hardware verlangt werden,[1251] z.B. eines gespiegelten Servers verlangt werden, etwa wenn bereits nach der vertraglichen Vereinbarung die hohe Sensibilität der Daten deutlich wird. Dies kann z.B. die Information über zuverlässige Abwehrprogramme sowie ihre Einrichtung umfassen.

2. Vertragsähnliche Ansprüche

674 Bislang nicht erörtert ist die Frage, ob der Nutzer vertragsähnliche Ansprüche gegen Betreiber von Rechnern hat, die nicht in das Vertragsverhältnis zwischen Nutzer und Provider eingeschaltet sind. Vor allem Ansprüche aus Vertrag mit Schutzwirkung zugunsten Dritter können hier zugunsten des Nutzers eingreifen, etwa wenn der Host Provider mit einem Content Provider Verträge über die Bereitstellung von Inhalten getroffen hat und durch mangelnde Sicherheitsvorkehrungen des Content Providers (Hacker, Virenbefall etc.) Schäden beim Nutzer eintreten. Aber auch Verträge zwischen Access- und Host Provider – soweit nicht bereits miteinander identisch – über die Bereitstellung von Speicherkapazitäten, der Weiteleitung von Daten etc. können grundsätzlich als Anknüpfungspunkt für Schutzpflichten gegenüber Dritten herangezogen werden. Von praktischer Bedeutung ist die Frage von Ansprüchen aus Verträgen mit Schutzwirkung zugunsten Dritter vor allem wegen der bekannten Unterschiede zum Deliktsrecht, insbesondere der nicht möglichen Entlastung für Erfüllungsgehilfen (§ 278 BGB) und der Erfassung von reinen Vermögensschäden.

675 In der Regel dürften die Voraussetzungen für derartige Ansprüche nicht gegeben sein. Denn Leitbild des Vertrages mit Schutzwirkung zugunsten Dritter ist (bislang), dass der Schuldner bei Vertragsabschluss damit rechnen kann, dass Dritte auf Seiten des Gläubigers in den Bereich des Vertrages einbezogen werden, wie etwa im Mietrecht.[1252] Erforderlich ist daher eine gewisse Überschaubarkeit derjenigen, die in den Genuss der Schutzpflichten des Vertrages kommen, nicht zuletzt damit der Schuldner seine Risiken

[1249] Vgl. *Komarnicki*, in: Hoeren/Sieber, Teil 12 Rn. 73; *Czychowski*, in: Bröcker/Czychowski/Schäfer, § 13 Rn. 107.

[1250] Zur Pflicht, Datensicherungen durchzuführen, s. OLG Karlsruhe CR 1996, 346 f.; OLG Karlsruhe NJW 1996, 200 (201); BGH NJW 1996, 2924 (2926) – Optikprogramm, wonach Datensicherung eine „Selbstverständlichkeit" sei.

[1251] *Schuppert*, in: Spindler, Vertragsrecht der Internet-Provider, Teil V Rn. 66.

[1252] S. nur Palandt-*Grüneberg*, § 328 BGB Rn. 16 ff. mwN; MünchKommBGB-*Gottwald*, § 328 BGB Rn. 117, 154.

kalkulieren kann. Zwar sind Aufweichungstendenzen in der Rechtsprechung feststellbar, etwa bei Überweisungsaufträgen im Mehr-Banken-Verkehr,[1253] doch handelt es sich hier in der Regel um bereichsspezifische Ausnahmen, die Risiken für den Kunden überwinden helfen sollen, die allein aufgrund der arbeitsteiligen Erledigung der Aufträge entstehen.

676 **Auf das Internet sind solche Überlegungen nicht übertragbar:** Denn zum einen ist bei Vertragsabschluss zwischen Providern untereinander in der Regel überhaupt nicht vorhersehbar, wieviele Nutzer auf Seiten eines Providers in den Vertrag einbezogen werden, woher diese stammen und welche Schutzmaßnahmen besonders auf diesen Personenkreis erforderlich wären. Das Risiko für den Provider, selbst für Vermögensschäden zu haften, wäre kaum mehr kalkulierbar. Zum anderen stellt sich die Tätigkeit der Provider im Internet für den Nutzer nicht als einheitlicher Vorgang dar, dessen besondere Risiken aus der Arbeitsteilung nicht auf den Nutzer überwälzt werden dürften. Stattdessen handelt es sich um jeweils spezifische Dienstleistungen im Internet, die miteinander verwoben sind, die aber keine Ähnlichkeit etwa mit einer Überweisungskette im Inter-Banken-Verkehr aufweisen.

677 Darüberhinaus mangelt es im Bereich der Übermittlung von Daten im Internet sogar häufig an jeglichen Vertragsbeziehungen, etwa für das Routing zwischen verschiedenen Rechnern. Hier versagen von vornherein jegliche Konstruktionen über vertragsähnliche Ansprüche.

3. Deliktische Verantwortlichkeit

678 Wendet man sich den deliktischen Pflichten (bzw. den Sicherungspflichten allgemein) der IT-Intermediäre zu, lassen sich drei Bereiche des Schutzes des Nutzers und anderer Internet-Teilnehmer unterscheiden:

- der Schutz des Eigentums, insbesondere an Daten
- der Schutz der Privat- und Intimsphäre
- der Schutz des Rechts am eingerichteten und ausgeübten Gewerbebetrieb.

679 Grundlage der Beurteilung ist auch hier eine Abwägung zwischen dem bestehenden Risiko sowie der wirtschaftlichen Zumutbarkeit der Ergreifung von Sicherungsmaßnahmen. Im Rahmen der wirtschaftlichen Zumutbarkeit ist Raum für eine konkrete Ein-

[1253] OLG Frankfurt WM 1984, 726; für Lastschriften BGH WM 1985, 1391.

zelfallbetrachtung, die auch die Umstände der Leistungserbringung einzubeziehen hat, einschließlich der Frage, welchen Preis ein Nutzer für einen Dienst aufbringt.[1254]

680 Dennoch können Intermediäre keinesfalls von den Privilegierungen für private Nutzer im Rahmen der allgemeinen Haftung profitieren: Denn aufgrund der **Multiplikationswirkung und –funktion der Intermediäre**, und dies betrifft sowohl Host- als auch Access-Provider, besteht ein stark erhöhtes Risiko, etwa durch die schnelle Verbreitung von Gefahren. Andererseits sind Intermediäre für die Bereitstellung der Kommunikationsinfrastruktur essentiell, so dass an ihnen und ihren Diensten ein starkes öffentliches Interesse besteht.[1255] Ingesamt verschiebt sich die Beurteilung der Pflichten von Intermediären fast vollständig hin zur Beurteilung der Zumutbarkeit der Ergreifung von Sicherungsmaßnahmen, da sie die Gefahrenquelle tatsächlich beherrschen können, aber auch unabdingbar für die modernen Kommunikationstechnologien und neuen Dienste sind. Des Weiteren verfügen zumindest die Access-Provider in aller Regel über Expertenkenntnisse bzw. entsprechendes Personal, das auch die Beobachtung und Überwachung neuer Gefahrenpotentiale und –lösungen bewältigen kann.

681 Häufig sind Intermediäre allerdings auch nur Nutzer des Dienstangebots anderer Intermediäre. So verwendet der Host-Provider häufig die Dienste eines anderen Host-Providers, meist teilen sich mehrere eine Computeranlage, die teilweise vermietet wird. Hier treffen den Intermediär nur insoweit Pflichten, als er tatsächlich Zugriff hat, und die Gefahrenquelle damit beherrscht.

a) Vernichtung von Daten des Nutzers

682 Das Eigentum eines Nutzers kann außerhalb des Bereichs der Übertragung von Inhalten, zu denen – wie oben dargelegt (Rn. 108 ff.) – grundsätzlich auch Software zählt, insbesondere dann verletzt sein, wenn sein Datenbestand durch einen „Angriff aus dem Netz“, etwa durch Viren, vernichtet oder jedenfalls teilweise beschädigt wird. Wie bereits dargelegt (Rn. 108 ff.), spricht hierfür, dass das Eigentum in der neueren Rechtsprechung des BGH auch im Hinblick auf seine Funktionsfähigkeit definiert wird,[1256] so dass auch Daten auf Festplatten oder Arbeitsspeichern etc. als möglicher Inhalt des Ei-

[1254] BGH NJW 1990, 906 (907) - Pferdeboxen; BGH NJW 1990, 908 (909) - Weinkorken; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 486; MünchKommBGB-*Wagner*, § 823 BGB Rn. 576; *Foerste,* in: v. Westphalen, ProdHaftHdb, § 24 Rn. 10, 48

[1255] Zu parallelen Überlegungen im Rahmen der Interessenabwägungen bei Sperrverfügungen gegenüber IT-Intermediären/Providern s. OVG Münster MMR 2003, 348 ff.*; Spindler/Volkmann* K&R 2002, 398 ff.; Spindler/Geis/Schmidt-*Spindler*, § 8 TDG Rn. 41, § 9 Rn. 41 ff.

[1256] Leitentscheidung: BGHZ 55, 153 - Fleet-Fall; wesentlich weitergehender *Boecken*, Deliktsrechtlicher Eigentumsschutz gegen reine Nutzungsbeschränkungen, S. 122 ff., 160 ff.

gentums bzw. der Funktionsfähigkeit des Speichermediums angesehen werden können (ausführlich oben Rn. 109).[1257] Auch im Werkvertragsrecht betrachtet der BGH den Verlust des Datenbestandes aufgrund einer fehlerhaften Sicherung als mögliche Verletzung eines „selbständigen, vermögenswerten Gutes".[1258] Der Virenbefall über die Plattform des IT-Intermediärs oder andere Arten von Angriffen, die zur Vernichtung von Daten des Nutzers auf seinem Rechner führen, z.B. während einer offenen Kommunikationsvorgang mit dem IT-Intermediär sind daher grundsätzlich geeignet, einen Anspruch aus § 823 Abs. 1 BGB zu begründen.

683 Sind indes Daten des Nutzers zerstört worden, die **auf dem Server des Providers abgelegt worden** sind, scheidet eine Eigentumsverletzung zu Lasten des Nutzers aus, da die Verkörperung der Daten eben nicht auf Eigentum des Nutzers – seiner Festplatte –, sondern auf dem Eigentum des Providers erfolgt. In Betracht kommen daher nur vertragliche Schadensersatzansprüche gegenüber dem Provider; hier kann indes wieder die Haftungsprivilegierung des § 44a TKG, sofern der Provider als Telekommunikationsanbieter agiert hat, zur Geltung kommen, soweit die Schadensursache in der technischen-organisatorischen Seite der Telekommunikation lag.[1259]

(1) Haftung von Host Providern

684 Entscheidend für die Haftung des IT-Intermediärs, insbesondere Host Providers ist daher, ob und gegebenenfalls wie weit er Verkehrspflichten zum Schutz des Eigentums des Nutzers unterliegt. Abgesehen von den vertraglichen Pflichten des Host Providers gegenüber dem Nutzer[1260] ist er verpflichtet, diejenigen Daten, die in seiner Einflusssphäre liegen, auf Virenbefall zu kontrollieren. In diesem Sinne trifft den Provider jedenfalls die Pflicht, grundlegende Anforderungen an die Sicherheit seiner Rechner und der dort gespeicherten Daten seiner Kunden gegenüber Ausspähversuchen oder Miss-

[1257] Ebenso im Ergebnis OLG Karlsruhe NJW 1996, 200 (201); *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 261 unter Berufung auf BGHZ 76, 216 (220) für Sachgesamtheiten, „die gerade durch ihre Vollständigkeit und Ordnung einen Wert repräsentieren, der nicht nur der Summe der Werte der darin zusammengefassten Einzelsachen entspricht, sondern diese oft übersteigt (bspw. Briefmarkensammlungen, Bibliotheken, Fachmuseen etc.). Wird eine solche Sacheinheit durch eine unerlaubte physische Hanndlung zerstört (...), dann handelt es sich gleichfalls um einen Angriff auf das Eigentum, bei dem der deliktische Eigentumsschutz des § 823 Abs. 1 BGB eingreifen muss (...)"; *Wuermeling*, CR 1994, 585 (590); *Hoeren*, PHI 1989, 138 (141); *Meier/Wehlau*, NJW 1998, 1585 (1587 f.); offen gelassen *Koch*, BB 1996, 2049 (2057); offen *Schneider*/*Günther*, CR 1997, 389 (392 f.); abl. LG Konstanz, CR 1997, 84; ebenso *Ertl*, CR 1998, 179 (182).

[1258] BGH NJW 1996, 2924 (2926) – Optikprogramm.

[1259] Vgl. zur Abgrenzung der Anwendungsbereiche von TKG und TDG bei Access-Providern Spindler/Schmitz/Geis-*Spindler*, § 2 TDG Rn. 26.

[1260] Dazu aus schweizerischer Sicht *Briner*, Hilty, Information Highway, S. 489 (511 f.).

bräuchen seitens Dritter einhalten.[1261] Da der Host Provider eine Gefahrenquelle betreibt, können die Überlegungen zu den Verkehrspflichten hinsichtlich der erforderlichen Abwehr von Viren, wie sie für die Produkthaftung entwickelt wurden (Rn. 150 ff.), und Angriffen aus dem Netz, aber auch hinsichtlich anderer technischer Sicherungspflichten, hier entsprechend herangezogen werden. Geht allerdings die Gefahr von einer Information/Datei aus, die ein Dritter auf den Rechnern des Host-Providers gespeichert hat, greift grundsätzlich die Haftungsprivilegierung nach § 10 TMG ein; demgemäß muß grundsätzlich zwischen von außen kommenden Angriffen (Hacking) und vom Provider zugelassenen Informationsspeicherung unterschieden werden.

685 Unabhängig von der Frage des vertraglichen Haftungsausschlusses kann der Host Provider sich seiner Haftung allerdings weitgehend dadurch entschlagen, dass er dem Nutzer **wirksame Anti-Viren-Programme** zur Verfügung stellt und ihn auffordert, diese regelmäßig zu benutzen; denn in diesem Fall ermöglicht der IT-Intermediär dem Nutzer Schutzmaßnahmen, die den Schutzmechanismen des Host Providers äquivalent sein können.

686 Für **sonstige Angriffe aus dem Netz**, die nicht nutzerseitig mit Hilfe von speziellen Software-Programmen aufgefangen werden können, gilt dies indes nicht. Soweit hier eine Absicherung aus technischen Gründen auf Seiten des IT-Intermdieärs nicht vollständig möglich ist, ist der IT-Intermediär zumindest gehalten, den Nutzer zu warnen und ausführlich über Möglichkeiten des Selbstschutzes, wie etwa der Installation von Firewalls, zu instruieren. Die **Warn- und Instruktionshinweise** müssen so deutlich erfolgen, dass dem Nutzer die Tragweite der darin beschriebenen Sicherheitsrisiken klar vor Augen geführt wird.[1262] Unterlässt der Nutzer trotzdem entsprechende Sicherheitsmaßnahmen, so hat der Host seine Verkehrspflichten erfüllt.

(2) Haftung von Access-Providern

687 Aber auch der Access-Provider kann nicht von jeglicher Sicherungspflicht frei sein, insbesondere wenn er sowohl das Herunter- als auch das freie Heraufladen von Daten auf seine Server ermöglicht. Nicht empfehlenswert ist es entgegen vereinzelten Stellungnahmen im Schrifttum, im Vertrag mit dem Endnutzer festzulegen, dass die Dienste

[1261] *Schmitz/v.Netzer*, in: Schuster, Vertragshandbuch Telemedia, Kap. 12 Rz. 21 f.; zurückhaltender wohl *Komarnicki*, in: Hoeren/Sieber, 12 Rz. 72: in der Regel nur gegen zusätzliche Vergütung.

[1262] Zu den Anforderungen an Warnpflichten und Instruktionspflichten s. Bamberger/Roth-*Spindler*, § 823 Rn. 484 ff.;S. auch oben Rn. 128 f.

mit einem Risiko im Hinblick auf die Schädigung durch Dritte (z.B. Hacking oder Virenverseuchung) behaftet seien und der Nutzer die Dienste auf eigene Gefahr in Anspruch nehme.[1263] Eine entsprechende Klausel wäre als vollständiger Haftungsausschluss auch für Gefahren aus dem eigenen Verantwortungsbereich zu qualifizieren, der insbesondere in AGB nach §§ 307, 309 Nr. 7b BGB unwirksam ist. Im Rahmen des Zumutbaren obliegen auch dem Access-Provider grundlegende Verkehrspflichten, die dem Schutz seines Systems vor Angriffen Unbefugter beziehen.[1264] Zu berücksichtigen ist in diesem Zusammenhang, dass der Provider Gefahren, die aus seinem System stammen oder sich darüber verbreiten aufgrund seiner personellen und technischen Ausstattung regelmäßig leichter und effektiver bekämpfen kann, als der private Nutzer.[1265]

688 Vollständige Sicherheit kann und muss der Access-Provider nicht gewährleisten. Er ist jedoch verpflichtet, sein Medium zu beobachten, Meldungen oder Beschwerden seiner Nutzer nachzugehen, die Nutzer über erkannte Sicherheitsrisiken zu warnen und ggf. Sicherheitsmaßnahmen zu ergreifen.[1266] Der Access Provider hat dafür zu sorgen, dass heraufgeladene Dateien oder Software nicht mit Viren befallen sind. Ebensowenig darf der Access Provider durch sorglosen Umgang mit Sicherungsmaßnahmen, seien sie technischer oder organisatorischer Natur, das Risiko für Eingriffe in die Sphäre des Nutzers erhöhen, beispielsweise durch Hacker. Der Nutzer darf insbesondere bei entgeltlichem Internet-Zugang ein Minimum an Kontrollen erwarten, die seiner eigenen technischen Sicherheit dienen. Wie für den Service Provider gilt auch hier, dass das Anbieten wirksamer Anti-Virus-Programme in der Regel genügt, um den Pflichten des Access Providers zu genügen.

(3) Haftung von Betreibern von Router-Rechnern

689 Davon zu unterscheiden ist die Haftung der Betreiber von im Internet-Verkehr zwischengeschalteten Rechnern. In Betracht können hier höchstens technische Sicherungspflichten kommen, wie sie z.B. auch für einen Spediteur bestünden, der fremde Güter transportiert.[1267] Auszuscheiden ist beispielsweise eine Haftung für die **Weiterleitung**

[1263] So aber *Roth,* in Loewenheim/Koch, Praxis des Online-Rechts, S. 57 (143).

[1264] *Spindler*, in: Spindler, Vertragsrecht der Internet-Provider, Teil IV, Rn. 357; zust. *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 495.

[1265] *Spindler*, in: Spindler, Vertragsrecht der Internet-Provider, Teil IV, Rn. 357; zust. *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 495.

[1266] *Spindler*, in: Spindler, Vertragsrecht der Internet-Provider, Teil IV, Rn. 357.

[1267] Zu diesem Vergleich s. *Koch*, CR 1997, 193 (199 Fußn. 30).

von Viren, da die Router-Rechner die eingegangenen Datenmengen so weiterleiten, wie sie ankommen, und die Daten in der Regel in verschiedenen Pakete unterteilt verschiedene Rechner passieren können.

690 Dagegen müssen auch die Betreiber der zwischengeschalteten Rechner dafür Sorge tragen, dass ihr Transportgut **nicht in ihrer Einflusssphäre mit Viren *befallen*** werden kann und die transportierten Daten „verseucht" werden. Diese Sicherheitsmaßnahmen werden vernünftigerweise vom Verkehr erwartet. Allerdings ist zu berücksichtigen, dass es sich hier stets um nur mittelbare Rechtsgutsverletzungen handelt, da an den verschickten Datenpaketen selbst kein Eigentum besteht. Selbst wenn man Daten – wie hier –[1268] als eigentumsfähiges Recht betrachtet, setzt dies doch in irgendeiner Weise eine Verkörperung, z.B. auf einer Festplatte voraus, deren Substanz oder Funktionsfähigkeit verletzt werden kann. Mit der Zwischenspeicherung auf dem Router-Rechner wird aber gerade nicht fremdes Eigentum durch Verkörperung begründet, sondern werden nur zugeleitete Daten abgelegt. Daher können nur mittelbare Rechtsgutsverletzungen beim Empfänger, die durch die Vernichtung oder Beeinträchtigung des Datenbestandes beim Empfänger infolge der „befallenen" Nachrichten entstanden sind, in Frage kommen.

691 In gleicher Weise müssen die Betreiber für die notwendigen Sicherungsmaßnahmen sorgen, die verhindern, dass ihre **Rechner zu Angriffen auf andere Internet-Teilnehmer** missbraucht werden können.[1269] Die Situation ist hier nicht anders als in den oben diskutierten Fällen zu bewerten, wenn Dritten der Missbrauch einer Gefahrenquelle leichtfertig eröffnet wird.[1270] In beiden Fällen liegt eine fehlende Sicherung einer Gefahrenquelle vor, für deren Missbrauch der Betreiber der Gefahrenquelle einstehen muss.

b) Verletzungen des allgemeinen Persönlichkeitsrechts außerhalb von Äusserungsdelikten

692 Besondere Fragen werfen Verletzungen des allgemeinen Persönlichkeitsrechts auf, die nicht mit Äusserungen Dritter zusammenhängen, die also nicht auf Inhalte bezogen

[1268] S. Nachw. Rn. 110 ff.

[1269] Ebenso *Koch*, BB 1996, 2049 (2057).

[1270] Vgl. BGH NJW 1991, 459 für die Haftung des KfZ-Halters eines ungesichert abgestellten KfZ`s, das von Dritten zu deliktischen Handlungen verwendet wurde; BGH NJW 2004, 1449 (1450) zur Sicherung einer Wasserrutsche bei missbräuchlicher Benutzung durch Kinder und Jugendliche; OLG Koblenz NVwZ 2002, 745 - Fahrbahnbeschmutzung durch Sand.

sind, die Dritte auf Rechnern der IT-Intermediäre gespeichert oder mit deren Hilfe weitergeleitet haben. Mit diesem Bereich ist der Schutz der Kommunikationskanäle von Privaten und Unternehmen angesprochen, der über IT-Intermediäre eröffnet wird. Die essentielle Bedeutung dieses Bereichs erschließt sich unmittelbar, wenn man sich die heutige Bedeutung des electronic commerce und von Web-Portalen von Unternehmen, inzwischen aber auch von Privaten vor Augen hält. Die über IT-Intermediäre eröffneten Kommunikationsmöglichkeiten sind heute selbstverständlicher Bestandteil der „Schnittstelle“ des Unternehmens oder des Individuums mit der Außenwelt.

(1) Schutz der Intim- und Privatsphäre

693 Das Persönlichkeitsrecht umfasst auch den Schutz der Privat- und Intimsphäre, insbesondere auch in zivilrechtlicher Hinsicht das vom BVerfG so bezeichnete Recht auf informationelle Selbstbestimmung als Grundlage des Datenschutzes.[1271] Da die Darstellung des Datenschutzrechts des TMG, des BDSG und der Länderdatenschutzgesetze sowie der EG-Richtlinien zum Datenschutz den gebotenen Umfang sprengen würde, beschränkt sich die nachfolgende Untersuchung auf die haftungsrechtlichen Besonderheiten im Zusammenhang mit den allgemeinen deliktsrechtlichen Ansprüchen.

694 Das Betreiben von Internet-Rechnern stellt auch im Hinblick auf den Schutz der Intim- und Privatsphäre grundsätzlich eine Gefahrenquelle dar, etwa durch das Ausspähen von persönlichen Daten. Daher sind auch die IT-Intermediäre gehalten, entsprechende Schutzvorkehrungen zu treffen – und zwar sowohl vertraglich als auch deliktisch. Die Sicherungspflichten gegenüber Ausspähversuchen der Daten der Kunden sind ohne weiteres als Nebenpflicht einzustufen.[1272]

695 Zur Konkretisierung der Schutzpflichten können die datenschutzrechtlichen Bestimmungen herangezogen werden. So schützt die EG-Richtlinie zum Datenschutzrecht[1273] auch die Übertragung von Dateien mit persönlichen Daten, Art. 2 b) („Übermittlung“), mithin auch den Datentransport über das Internet, z.B. auch E-Mails. Sie verlangt nach Art. 17 vom Verantwortlichen technische und organisatorische Maßnahmen zum Schutz der Daten mit persönlichem Charakter, insbesondere gegen Veränderung oder unerlaub-

[1271] BVerfGE 65, 2 (42 ff.); BVerfGE 80, 367 (373); BVerfG MMR 2007, 93; BVerfG Urt. v. 23.2.2007 - 1 BvR 2368/06, Rz. 37.

[1272] *Spindler*, in: Spindler: Vertragsrecht der Internet-Provider, Teil IV, Rn. 147.

[1273] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ABl. EG Nr. L 281 vom 23. November 1995, S. 31.

ten Zugriff. Einen Hinweis auf die Abgrenzung der Verantwortlichkeiten bietet auch Art. 2 d) der Richtlinie, wonach nur derjenige, der über die Zwecke und Mittel der Verarbeitung der Daten entscheidet, als Verantwortlicher zu betrachten ist und nicht derjenige, der die Dienstleistung anbietet.[1274] Auch das TMG enthält spezifische datenschutzrechtliche Bestimmungen, die fruchtbar gemacht werden können. So muss der Diensteanbieter gem. § 13 Abs. 4 TMG durch technische und organisatorische Vorkehrungen sicherstellen, dass der Nutzer Teledienste geschützt gegen die Kenntnisnahme Dritter in Anspruch nehmen kann.[1275]

696 Die von der EG-Richtlinie zum Datenschutz und vom T verlangten Sicherheitsvorkehrungen sind aber auch nach allgemeinem Deliktsrecht als grundlegende Sicherheitsstandards im Sinne von Verkehrspflichten von den Betreibern von Rechnern im Netz zu beachten. Das TMG schließt weitergehende zivilrechtliche Ansprüche nicht aus; vielmehr können die datenschutzrechtliche Vorgaben des TMG gegebenenfalls sogar als Schutzgesetze nach § 823 II BGB vom Betroffenen zur Stützung von Schadensersatzansprüchen herangezogen werden.[1276]

697 Demnach haben alle in die Übermittlungskette eingeschalteten Betreiber je nach ihrer Einflusssphäre dafür Sorge zu tragen, dass die Privatsphäre von abgesandten Nachrichten gewahrt bleibt. Insbesondere von Providern, die einen E-Mail-Dienst in ihr Angebot integriert haben, muss verlangt werden, dass die Nachrichten vor dem unbefugten Abhören und gegen den unbefugten Zugriff Dritter gesichert wird.

698 Allerdings ist auch hier wiederum zu berücksichtigen, welchen **Grad an Sicherheit der Verkehr erwartet**: Warnt der Provider den Absender einer E-Mail ausdrücklich vor möglichen Abhörmaßnahmen Dritter und bietet er beispielsweise Verschlüsselungen an, so kann sich der geschädigte Nutzer, der trotzdem eine ungesicherte E-Mail absendet, nicht auf ein Vertrauen in die Einhaltung von Sicherheitsstandards berufen. Häufig werden hier zudem bereits vertragliche Haftungsausschlüsse eingreifen. Macht der Nutzer von bereitgestellter Verschlüsselungssoftware keinen Gebrauch, muss er sich dies zumindest als Mitverschulden gem. § 254 BGB auf seinen Anspruch anrechnen lassen.

[1274] Nach Art. 2 I der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) gelten die Begriffsbestimmungen des Art. 2 der Richtlinie 95/46/EG auch für diese Richtlinie.

[1275] Ausführlich Spindler/Schmitz/Geis-*Schmitz*, § 4 TDDSG Rn. 23 ff.

[1276] Vgl. für das BDSG als Schutzgesetz: zuletzt OLG Frankfurt aM ZIP 2005, 654; OLG Hamm NJW 1996, 131; OLG Hamm ZIP 1983, 552.

Der geforderte Sicherheitsstandard kann wiederum bei kostenlosen Angeboten, insbesondere bei E-Mail-Accounts, abgesenkt werden, da hier zum einen der Grundgedanke des Schenkungsrechts durchschlägt, zum anderen auch eine analoge Anwendung der Maßstäbe des Schenkungsrechts nahe liegt, da der Nutzer oftmals – wenn auch unentgeltliche – vertragliche Beziehung zu dem IT-Intermediär unterhalten wird.

699 Trotz entsprechender Warnungen muss jedenfalls ein Mindeststandard an Sicherungsmaßnahmen seitens der Provider ergriffen werden, der verhindert, dass E-Mail-Nachrichten von jedermann gelesen werden können. Hierzu dürfte die Vergabe von Passwörtern zählen und die stichprobenartige Überwachung der Mail-Server auf unerlaubte Zugriffsversuche Dritter.

700 Ferner kann eine Haftung der Betreiber von Router-Rechnern wegen unterlassener technischer Sicherungsmaßnahmen im Bereich des Zugriffs unautorisierter Dritter auf die Datenpakete in Betracht kommen, z.B. „Abhören" von Kreditkarteninformationen oder Zahlungsvorgängen. Aber auch hier ist zu bedenken, dass die Betreiber von Router-Rechnern in der Regel keinerlei Kenntnis von den Datenpaketen haben werden, für deren Transport ihr Rechner verwendet wird, so dass entsprechende Sicherungsmaßnahmen nicht zumutbar erscheinen. Zudem dürfte es in der Regel an jedem entgeltlichen Geschäftskontakt mit den Absendern der sensiblen Informationen fehlen, so dass im Sinne der Zuordnung der Verantwortung für Risiken dort, wo sie am besten beherrscht und versichert werden können, eine Verantwortlichkeit der Betreiber von Router-Rechnern auch unter diesem Gesichtspunkt ausscheidet. Sofern die **Kreditwirtschaft oder Unternehmen** das Internet durch vollautomatisierte Sofwarekomponenten zur Abwicklung ihrer Geschäftsvorfälle verwenden (**Web-Services**), müssen sie selbst sicherstellen, dass der Missbrauch der Daten verhindert wird, etwa durch die Wahl geeigneter Verschlüsselungsstandards.[1277]

(2) Unerbetene elektronische Post und Störerhaftung

701 Eine andere, eng mit Persönlichkeitsrechten verknüpfte Frage betrifft die deliktsrechtliche Verantwortlichkeit der IT-Intermediäre für die Zusendung unerbetener elektronischer Post. Diese Frage kann hier indes nur angedeutet werden, da sie eine eigene Untersuchung rechtfertigen würde (Spam-Versand und rechtspolitisch sinnvolle Gegenmaßnahmen). Im weitesten Sinne kann auch die Vorkehr vor unerwünschten Mail-

[1277] Näher *Spindler*, DuD 2005, 139 ff.

Sendungen zu Sicherungspflichten eines IT-Intermediärs gehören, etwa durch die Einrichtung von Spam-Filtern, die aber durch den IT-Nutzer beherrschbar bleiben müssen.[1278]

c) Störung der Außenbeziehung des im Internet präsenten Unternehmens

702 Neben den zahlreichen Fällen, in denen ein Anspruch wegen Verletzung der Unternehmenskennzeichen neben namens-, wettbewerbs-, marken- oder sonstigen zeichenrechtlichen Ansprüchen gegeben sein kann und der daher in deren Zusammenhang zu behandeln ist, kann das Recht am eingerichteten und ausgeübten Gewerbebetrieb durch die Sperrung eines Internet-Zugangs verletzt sein. Eine solche Zugangsbehinderung kann beispielsweise durch die Verstopfung der E-Mail-Adresse oder durch den Zusammenbruch der Web-Seite des Unternehmens infolge technischer Probleme des Providers sowie von Denial-of-Service-Attacken erfolgen. Die daraus dem Unternehmen entstehenden Schäden können beträchtlich sein, z.B. wenn wichtige Nachrichten nicht empfangen werden konnten oder gar verloren gingen.

703 Neben etwaigen vertraglichen Schadensersatzansprüchen gegen den IT-Intermediär, kann fraglich sein, ob das Unternehmen auch **deliktische Schadensersatzansprüche** geltend machen kann. Solche Ansprüche können dann von Interesse sein, wenn die Ursache für den Schaden außerhalb der Vertragsbeziehung entstanden ist – andernfalls greift die Haftungsprivilegierung nach § 44a TKG ein – oder Verjährungsfristen anders geregelt sind. Im allgemeinen Deliktsrecht kommen hier nur Ansprüche aus Recht am eingerichteten und ausgeübten Gewerbebetrieb in Betracht, da sowohl der Informationszugang als auch der Informationsabgang kein anderes von § 823 Abs. 1 BGB geschütztes Rechtsgut verletzt. In entsprechender Anwendung der Energiezufuhr-Fälle[1279] könnte hier in der Tat an einen deliktsrechtlichen Schutz des Nutzers gedacht werden, indem der freie Zugang zum Unternehmen gewahrt wird. Bedenkt man, dass die Telekommunikationswege des Unternehmens heute mindestens genauso wichtig sind wie die Energieversorgung, so muss auch die Freihaltung dieser Schnittstellen des Unternehmens zur Außenwelt grundsätzlich dem Recht am eingerichteten und ausgeübten Gewerbebetrieb unterfallen. Daher gehört zum geschützten Bereich des Unternehmens

[1278] Ausführlich und näher dazu *Spindler/Ernst*, CR 2004, 437 ff.; *Hoeren*, NJW 2004, 3513 ff.

[1279] BGHZ 29, 65 ff.; BGHZ 41, 123 (125 f.), der allerdings im konnkreten Fall eine Eigentumsverletzung annimmt; anders BGH NJW 1992, 41 f.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 212; *Foerste,* in: v. Westphalen, ProdHaftHdb, § 21 Rn. 122 f.

auch der freie Zugang, hier per E-Mail und Web-Seite.[1280] Zwar hat der BGH es bisher abgelehnt, die Unterbrechung der Energiezufuhr als einen Eingriff in das Recht am eingerichteten und ausgeübten Gewerbebetrieb anzusehen.[1281] Auch für unterbrochene Telefon- und Telefaxkabel hat die Rechtsprechung einen deliktsrechtlichen Schutz ebensowenig gewährt[1282] wie für unterbrochene Zugangswege.[1283] Eine Verletzung des deliktisch geschützten Rechtsguts des eingerichteten und ausgeübten Gewerbebetriebs soll nur dann vorliegen, wenn der Betrieb in seinen Grundlagen bedroht sei oder gerade der Funktionszusammenhang der Betriebsmittel auf längere Zeit aufgehoben sei.[1284]

704 Gerade wenn man aber akzeptiert, dass das Eigentum in seinem Wert ganz wesentlich von den ausübbaren Funktionen abhängt, kann nicht daran vorbeigegangen werden, dass die Beziehungen einer Sache, insbesondere eines **Unternehmens, zu seiner Außenwelt** erheblich dessen Wert beeinflussen.[1285] Auch wenn die Eigentumsverletzung von einer spürbaren Beeinträchtigung des Marktwertes abhängig gemacht wird,[1286] muss doch berücksichtigt werden, dass vor allem der fehlende Zugang zum Unternehmen dessen Marktwert für einen potentiellen Käufer mindert, sofern die Behinderung über einen nicht unerheblichen Zeitraum andauert.

705 Darüber hinaus können Ansprüche aus §§ 823 I, 826 BGB vorliegen, wenn der E-Mail-Posteingang eines Unternehmens durch massenhaft versandte E-Mail – dem sog. Mail-Bombing –[1287] verstopft wird, z.B. im Rahmen von Boykott- oder anderen Kampagnen[1288] gegen ein Unternehmen.[1289] Derartige Ansprüche richten sich dann allerdings nicht gegen den IT-Intermediär, da dieser nur den vertraglich geschuldeten Posteingang

---

[1280] Ebenso für das schweizerische Recht *Alder*, in: Hilty, Information Highway, S. 331 (344 ff.), allerdings unter dem Gesichtspunkt des Persönlichkeitsrechts.

[1281] S. Fn. 1279.

[1282] BGH VersR 1977, 616 (617); s. auch OLG Düsseldorf VersR 1997, 589: kein betriebsbezogener Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb bei unterlassener Eintragung einer Telefonnummer in die „Gelben Seiten".

[1283] Vgl. BGHZ 86, 152: Im entschiedenen Fall ging es um einen infolge verschuldeten Dammbruchs trockengelaufenen Kanal, der zu einem Umschlagbetrieb führte. Der BGH lehnte einen Anspruch ab, weil der Dammbruch nicht zu einem Eingriff in die Sachsubstanz der Lagerei- und Umschlaganlagen geführt habe (155).

[1284] BGH NJW 1983, 812 (813) - Hebebühne; zust. *Foerste,* in: v. Westphalen, ProdHaftHdb, § 21 Rn. 122.

[1285] S. bereits *Buchner*, Die Bedeutung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb für den deliktsrechtlichen Unternehmensschutz, S. 109, 163 f.; *Taupitz*, Haftung für Energieleiterstörungen durch Dritte, S. 120.

[1286] So MünchKommBGB-*Mertens*, 3. Aufl. 1997, § 823 BGB Rn. 113 f., 491; *Zeuner*, FS Flume, Bd. I, S. 775 (778 f.); krit. dagegen MünchKommBGB-*Wagner*, § 823 BGB Rn. 116.

[1287] Vgl. *Strömer*, Online Recht, S. 108 f.; *Ernst*, JuS 1997, 776 (778); dazu auch *Roggenkamp*, jurisPR-ITR 8/2006 Anm. 4.

[1288] Zur Problematik von „Online-Demonstrationen" AG Frankfurt/M, MMR 2005, 863 ff. (Strafrechtliche Verantwortlichkeit für die Aktion „Lufthansa goes offline"); *Kraft/Meister*, MMR 2003, 366 ff.; *Klutzny*, RDV 2006, 50 ff.

[1289] Ebenso für das schweizerische Recht *Alder*, in: Hilty, Information Highway, S. 331 (344 ff.); *R.H.Weber*, in: Hilty, Information Highway, S. 531 (554); viel zu kurz gegriffen daher *Strömer*, Online Recht, S. 109, der mangels vertraglicher Beziehungen und wegen reinen Vermögensschadens kategorisch Ansprüche aus § 823 Abs. 1 BGB verneint.

sicherzustellen hat[1290] und keine darüber hinausgehenden deliktsrechtlich relevanten Sicherheitserwartungen beim Nutzer geweckt hat, zudem § 44a TKG eingreifen würde. Besonderheiten gegenüber den bekannten Ansprüchen bei Kampagnen gegen ein Unternehmen[1291] ergeben sich dadurch nicht.

706 Ebenso kann der „**Einbruch" von Hackern** in eine (auf einem Rechner des IT-Intermediärs gehostete) Web-Seite eines Unternehmens und deren Unbrauchbarmachung dazu führen, dass gegen die Hacker ein Anspruch aus §§ 823 I, 823 II, 826 BGB besteht – abgesehen von möglichen urheberrechtlichen Ansprüchen. Hat der Provider keine genügenden Sicherungsvorkehrungen gegen das Eindringen von Hackern in das System getroffen, ist auch er gem. § 823 I BGB haftpflichtig für etwaig eingetretene Schäden. Allerdings wird es hier in der Regel kaum möglich sein, einen konkreten Schaden nachzuweisen, der darauf beruhen müsste, daß die Web-Seite nicht zugänglich gewesen ist.

707 Aber auch hinsichtlich des ***Versands* von E-Mail-Nachrichten** können grundsätzlich Ansprüche des Unternehmens gegen einen eingeschalteten Provider oder andere Betreiber von Rechnern geltend gemacht werden, wenn in deren Einflusssphäre die E-Mail infolge mangelnder Sicherungsvorkehrungen geöffnet bzw. abgehört wurde und das Unternehmen im Rahmen seines Rechts am eingerichteten und ausgeübten Gewerbebetrieb dadurch einen Schaden erlitten hat. Hier ergeben sich keine Unterschiede zu den oben behandelten Sicherungspflichten der Provider im Hinblick auf die Wahrung des allgemeinen Persönlichkeitsrechts.[1292] Für die wohl häufigsten Fälle von Schädigungen, dem Ausspähen von Kreditkartenangaben oder anderen finanziell sensiblen Daten, bietet das Deliktsrecht aber keinen Schutz, da diese Daten nicht dem Recht am eingerichteten und ausgeübten Gewerbebetrieb unterfallen, sondern reine Vermögensschäden darstellen.[1293]

4. Einzelne Sicherungspflichten

a) Virenscanner

[1290] Vgl. aus schweizerischer Sicht *Hilty*, in: Hilty, Information Highway, S. 437 (481) sowie *Briner*, in: Hilty, Information Highway, S. 489 (508 ff.).

[1291] S. nur BGHZ 24, 200 ff. - Boykottaufruf; BGHZ 90, 113 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 201 ff. mwN.

[1292] S. oben Rn. 692 ff.

[1293] Zum fehlenden deliktsrechtlichen Schutz des Vermögens MünchKommBGB-*Wagner*, § 823 BGB Rn. 176 ff.

708 Wie die kommerziellen Nutzer trifft den Intermediär in jedem Fall die Pflicht zur Sicherung des eigenen Systems mit Hilfe von Virenscannern. Etwaige Privilegierungen privater Nutzer kann er aufgrund des hohen Gefährdungspotentials nicht geltend machen.[1294]

b) Firewall

709 Sofern der Provider selbst Netzwerktechnik einsetzt, muss er diese auch besonders sichern. Hierzu gehört auch die Einrichtung und Wartung einer Firewall.[1295] Dafür sprechen auch § 104 TKG, der die Gewährleistung der ausreichenden Datensicherheit vom Telekommunikationsanbieter verlangt, sowie aus datenschutzrechtlicher Sicht § 13 Abs. 4 TMG.[1296]

c) System- und Programmupdates

710 Die Programme, die der Intermediär nutzt, befinden sich in der Regel auf einem Computersystem, das für jeden zugängliche Dienste bereitstellt. Während der private Nutzer meist anonym agiert, ist der Provider bekannt und kann daher jederzeit Opfer auch gezielter Angriffe werden. Lücken im verwendeten System oder den Programmen stellen hierbei eine große Gefahr dar. Sofern der Intermediär wirtschaftlich tätig ist, ist ihm somit eine regelmäßige Beobachtung der Entwicklungen bei der von ihm eingesetzten Software zuzumuten. Diese kann z.B. über die Teilnahme an den jeweiligen sog. Mailing-Listen erfolgen. Sollten Sicherheitslücken bekannt werden, so muss er unverzüglich versuchen, diese Lücken zu schließen. Ist dies nicht sofort möglich, kann auch von ihm verlangt werden, die gefährdeten Funktionen nicht weiter anzubieten. Fraglich ist, ob ihm auch die vollständige Einstellung des Betriebs aufgebürdet werden kann. In dieser Situation kann sich aus Art. 12 GG eine Beeinflussung des Haftungsmaßstabs zugunsten des Providers ergeben. Allerdings ist dabei auf die Art der Gefahr abzustellen. Ist das Risiko gering und die erwarteten Schäden ebenso, so müsste der Betrieb so lange aufrechterhalten werden können, bis eine Lösung zur Verfügung steht. Bei einer höheren Gefährdung[1297] müsste der Betrieb jedoch eingestellt werden. Insgesamt obliegt dem Intermediär somit eine Beobachtungs- und Abhilfepflicht in Hinsicht auf System- und Programmupdates.

[1294] Vgl. zusätzlich *Spindler*, in Spindler: Vertragsrecht der Internet-Provider, Teil IV, Rn. 356 f.; insofern keine Nutzung auf eigene Gefahr; aA noch zu § 5 TDG a.F. *Sieber*, in: Hoeren/Sieber, Teil 19 Rn. 248.

[1295] Zutr. *Czychowski*, in: Bröcker/Czychowski/Schäfer, § 13 Rn. 106.

[1296] Darauf weist zu Recht *Schmitz/v.Netzer*, in: Schuster, Vertragshandbuch Telemedia, Kap. 12 Rz. 21 hin.

[1297] Häufig kategorisieren die Hersteller die Sicherheitslücken. Kritische Sicherheitslücken führen jedenfalls zu einer nicht abwälzbaren Pflicht.

711 Den **nicht-kommerziellen Intermediär** kann die Beobachtungspflicht nur in abgeschwächter Form treffen. Er sollte sich dennoch regelmäßig informieren und schnellstmöglich Gegenmaßnahmen ergreifen.

d) Nutzung von Nutzerkonten mit eingeschränkten Rechten

712 Die Nutzung von speziellen Nutzerkonten ist dem Intermediär in jeder Hinsicht zuzumuten, sofern ihm dies möglich ist.

e) Intrusion Detection-Systeme

713 Beim Einsatz von Netzwerken kann hier eher auch der Einsatz von Intrusion Detection-Systemen verlangt werden.

f) Malware-Entfernungsprogramme

714 Auch eine ständige Nachsorge ist dem Provider zuzumuten. Sollten Hinweise auf eine Gefährdung bestehen, so ist jedenfalls nach Schadprogrammen zu suchen, und diese sind zu entfernen. Hierzu besteht eine regelmäßige Verpflichtung, z.B. einmal in der Woche.

g) Ergebnis

715 Grundsätzlich tritt die Pflicht zum Einsatz von Sicherungsmaßnahmen beim Intermediär eher ein und ist auch schärfer anzusetzen. So kann eine ständige Beobachtung auch neuer Gefahrenpotentiale viel eher verlangt werden, notwendige Aktualisierungen sind so oft vorzunehmen, wie dies nötig ist.

5. Zusammenfassung

716 Deliktische und vertragliche Ansprüche gegen den IT-Intermediär wegen Verletzung seiner Sicherungspflichten können sich vor allem auf die Zerstörung von Daten oder die Beschädigung von Hardware infolge von Virenbefall oder anderen Arten von Angriffen aus dem Netz ergeben. Nur vertragliche Ansprüche sind dagegen für Daten des Nutzers auf einem Server des Providers einschlägig.

717 Der IT-Intermediär hat den Nutzer vor Angriffen aus dem Netz durch entsprechende Sicherungsmaßnahmen für seine Rechner zu bewahren. Bei Virenbefall genügt es allerdings, dass der Provider den Nutzer entsprechende Anti-Viren-Programme anbietet und bereithält. Ist dem Provider eine technische Sicherung gegen Angriffe nach dem Stand der Technik nicht möglich, so hat er den Nutzer intensiv auf entsprechende Gefahren hinzuweisen und Schutzmaßnahmen zu empfehlen. Dies gilt auch für den reinen Access

Provider, dem Systemsicherungspflichten obliegen. Auch Betreiber von Router-Rechnern müssen dafür sorgen, dass Daten im Bereich ihres Einflusses nicht von außen beschädigt werden können; allerdings wird es hier oftmals an einer Rechtsgutsverletzung mangels Eigentums an den Daten fehlen. Allerdings werden entsprechende Ansprüche durch § 44a TKG begrenzt, sofern es sich um Vermögensschäden und entsprechende Telekommunikationsdienste handelt.

718 Ansprüche aus Vertrag mit Schutzwirkung zugunsten Dritter zwischen verschiedenen Providern scheitern an der erforderlichen Überschaubarkeit der beteiligten Nutzer. Für Provider wäre das Risiko eines Vermögenschadens von Nutzern, die ihrerseits in Beziehung mit einem Provider stehen, nicht mehr zu kalkulieren.

719 Provider haben Nutzer aber auch vor Angriffen auf die Privat- und Intimsphäre zu schützen, insbesondere dem Ausspähen von E-Mails. Auch wenn Nutzer weitgehend darauf verwiesen werden können, ihre E-Mail zu verschlüsseln, muss der Provider zumindest Passwörter für den Zugang zu E-Mail-Konten vergeben und für gelegentliche Stichproben auf unbefugten Zugang sorgen.

720 Entgegen der Rechtsprechung ist ein deliktsrechtlicher Schutz der Außenbeziehungen des Unternehmens anzuerkennen, der auch den Zugang mittels E-Mail und Web-Seite umfasst. Darüberhinaus bestehen selbstverständlich Ansprüche aus §§ 823 Abs. 1, 826 BGB gegen Versender sog. E-Mail-Bomben, die den Zugang des Unternehmens verstopfen, oder gegen Hacker, die Informationen des Unternehmens ausspähen.

III. Intermediär als reiner Mittler von Informationen

721 Geht der Angriff dagegen nicht direkt vom Intermediär aus, leistet der IT-Intermediär aber einen wesentlichen Beitrag zur Verletzung Dritter, indem er die schädigende Information weitergeleitet, gespeichert oder bereitgestellt hat, stellt sich parallel zu den Sicherungspflichten für eigene Systeme die Frage, ob der Intermediär gehalten ist, den Datenverkehr auf seinen Systemen im Hinblick auf Rechtsverletzungen Dritter zu kontrollieren. So könnte etwa ein Host-Provider verpflichtet sein, das Angebot seiner Kunden auf Viren zu untersuchen, um die Schädigung Dritter zu verhindern.

722 Auf diesen Problemkreis haben sowohl der deutsche als auch der europäische Gesetz- bzw. Richtliniengeber reagiert, indem die Verantwortlichkeitsprivilegierungen der §§ 7 - 10 TMG bzw. die entsprechenden Regelungen der E-Commerce-Richtlinie Art. 12 –

15 ECRL[1298] eingeführt wurden.[1299] Greifen diese Privilegierungen, so ist die Haftung bzw. Verantwortlichkeit ausgeschlossen, allerdings mit der für die Praxis gewichtigen Ausnahme der Störerhaftung bzw. des Unterlassungsanspruchs nach § 1004 BGB.[1300]

723 Grundsätzlich treffen den IT-Intermediär nach § 7 Abs. 2 TMG keine allgemeinen (!) Pflichten, übermittelte oder gespeicherte Informationen, die nicht eigene Informationen nach § 7 Abs. 1 TMG sind, zu überwachen. Grundsätzlich fallen damit auch Viren sowie spezielle Datenpakete unter den Informationsbegriff des § 7 TMG,[1301] so dass Viren, Trojaner, aber auch manipulierte Pakete eines Denial-of-Service-Angriffs erfasst sind. Die Voraussetzungen dieser Privilegierungen hängen von der jeweiligen Funktion des Intermediärs ab:

1. Content-Provider

724 Content-Provider sind nach § 7 Abs. 1 TMG diejenigen, die eigene Informationen speichern und bereitstellen.[1302] Für sie gilt keine Privilegierung. Auf die strittige Frage, wann es sich um eigene, wann um fremde Informationen handelt,[1303] kommt es nicht an, da es sich bei der hier behandelten Information jedenfalls nicht um eine handelt, die sich der Intermediär zu eigen macht und von der er regelmäßig auch keine Kenntnis hat.[1304]

2. Host-Provider

725 Anders ist dies beim Host-Provider. Er vermittelt gerade fremde Informationen. Die Haftung ist nach § 10 TMG ausgeschlossen, wenn er keine Kenntnis von der Information oder den einen Schadensersatzanspruch begründenden Tatsachen hat und die Information entfernt oder den Zugang sperrt, sobald er Kenntnis erlangt.

726 Auf den Fall eines **Angriffs mittels Informationstechnik** übertragen bedeutet dies, dass der Inhaber eines Rechnersystems bzw. IT-Intermediär, von dem ein Angriff ausgeht, den Angriff sofort unterbinden muss, sowie er davon Kenntnis erlangt. Es handelt sich hierbei um Informationen, die der Diensteanbieter im Auftrage des Nutzers speichert, was auch unbewusst geschehen kann. Möglich ist dies z.B. dadurch, dass der

---

[1298] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) .

[1299] Dazu Spindler/Schmitz/Geis-*Spindler*, vor § 8 TDG Rn. 10.

[1300] BGH NJW 2004, 3102; *Spindler*, JZ 2005, 37; *Leible/Sosnitza,* NJW 2004, 3225 (3226).

[1301] *Koch*, NJW 2004, 801 (806); *Spindler*, NJW 2002, 921 (922); *Hoffmann*, MMR 2002, 284 (288).

[1302] *Schwarz/Poll*, JurPC 73/2003, Rn. 61.

[1303] S. nur Spindler/Schmitz/Geis-*Spindler*, § 8 TDG Rn. 4 ff. mwN.

[1304] Zu Schutzpflichten bei eigenen Angeboten s. z.B. OLG Nürnberg NJW-RR 2003, 628 (629).

Nutzer mit Viren verseuchte Dateien ablegt oder selbst Programme installiert, von denen Angriffe auf Dritte ausgehen. Eine Beendigung der Schädigung durch den Provider wäre durch Abschaltung der Anlage oder durch die Entfernung des den Angriff verursachenden Programms, z.B. des Virus. Für die Kenntnis der Umstände zur Begründung eines Schadensersatzanspruchs (nicht für die strafrechtliche Verantwortlichkeit) kann es nach § 10 S. 1 Nr. 2 TMG genügen, wenn auffällige Netzwerkaktivitäten erkannt und gemeldet werden, z.B. durch ein Intrusion Detection-System, sofern ein solches installiert ist.[1305]

3. Access-Provider

727 Der Access-Provider speichert zunächst keine Informationen. Seine Funktion ist nach § 8 TMG vielmehr die Durchleitung von Informationen durch Kommunikationsnetze oder die Vermittlung des Zugangs zu fremden Informationen. Die Verantwortlichkeit ist danach ausgeschlossen, wenn der Provider die Übermittlung der Information nicht veranlasst, und weder Adressat noch Information ausgewählt, sowie die Information nicht verändert hat. Die bloße Bereitstellung von Einwahlknoten kennzeichnet gerade den sog. Access-Provider und ist deshalb als Zugangsvermittlung i.S.v. § 8 TMG anzusehen.[1306] Das TMG hat in diesem Zusammenhang den alten Streit beigelegt, ob Access-Provider überhaupt unter die Haftungsprivilegierungen fallen.[1307]

728 Die Übertragung von **Schadprogrammen** (**Malware**) oder manipulierten Paketen durch ein Kommunikationsnetz fällt demnach auch in den Anwendungsbereich des § 8 TMG. Nach § 8 Abs. 2 TMG ist auch die kurzfristige Speicherung der übermittelten Information gestattet, sofern sie nur zur Übermittlung und nicht länger als für die Übermittlung üblicherweise erforderlich erfolgt. Im Gegensatz zu § 9 TMG ist nur die sehr kurzfristige, technisch notwendige Speicherung, nicht das sog. Caching von der Haftung freigestellt.[1308] Es handelt sich bei den gespeicherten Informationen zudem um solche, auf die der Nutzer keinen Zugriff hat.[1309]

[1305] Dazu Rn 65.

[1306] LG München I CR 2000, 117; OVG Münster MMR 2003, 348 (350); *Kühne*, NJW 1999, 188; Spindler/Schmitz/Geis-*Spindler*, § 9 TDG Rn. 14..

[1307] *Spindler*, CR 2007, 242.

[1308] *Hoffmann*, MMR 2002, 284 (287); Spindler/Schmitz/Geis-*Spindler*, § 9 TDG Rn. 8.

[1309] Begr. RegE BT-Drucks. 14/6098, 24.

729 Entsprechend § 9 TMG ist auch die zeitlich begrenzte, automatische Zwischenspeicherung von der Haftung freigestellt. Hierunter fällt insbesondere das **Caching** zur effizienteren Gestaltung der Übertragung.

IV. Öffentlich-rechtliche Anforderungen

1. Anwendbarkeit des TKG auf IT-Intermediäre

730 Das TKG regelt anders als das TMG nicht Fragen des Inhalts von Tele- oder Mediendiensten, sondern den technischen Vorgang der Telekommunikation und damit des Aussendens, der Übermittlung und des Empfangens von Signalen mittels Telekommunikationsanlagen (vgl. § 3 Nr. 22 TKG). Es handelt sich hierbei im Wesentlichen um öffentliches Marktregulierungsrecht.[1310] Zweck des Gesetzes ist nach § 1 TKG, durch eine technologieneutrale Regulierung den Wettbewerb im Bereich der Telekommunikation und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten. Auch nach der Neufassung des TKG bleibt die Abgrenzung der Telekommunikationsdienste (§ 3 Nr. 24 TKG) zu den Telemediendiensten eines der umstrittensten Probleme. Internet-Provider unterfallen nach h.M. den Regelungen des TKG, soweit sie Telekommunikationsdienste erbringen, wobei eine **funktionale Abgrenzung** zugrunde zu legen ist.[1311] Entscheidend ist demnach die Art der erbrachten Dienste: Bestehen diese lediglich in der Bereitstellung von Übertragungskapazitäten (Network-Provider) oder handelt es sich ausschließlich um die Bereitstellung des Internetzugangs (Internet-by-Call-Anbieter), werden nur Telekommunikationsdienste erbracht. Content-Provider, welche allein Inhalte auf mit dem Internet verbundenen Servern zur Verfügung stellen, erbringen dagegen allein Telemediendienste. Handelt es sich um einen kombinierten Dienst, welcher Telekommunikationsdienste und Telemediendienste miteinander verbindet (z.B. t-online), ist nicht der Schwerpunkt des Dienstes maßgeblich, sondern das jeweils einschlägige Gesetz auf die einzelnen Bestandteile anzuwenden, d.h. der Dienst ist in seine Bestandteile aufzuteilen,[1312] was auch § 1 Abs. 3 TMG zeigt, der davon spricht, dass das TMG das Telekommunikationsrecht unberührt lässt.

2. Anforderungen des TKG an die IT-Sicherheit

[1310] Säcker-*Säcker*, Einl. I Rn. 2 f.

[1311] Beck'scher TKG-Kommentar-Gersdorf, Einleitung, Teil C, Rn 18, 20; Säcker-*Säcker*, § 3 TKG Rn. 38; Spindler/Schmitz/Geis-*Spindler*, § 2 TDG Rn. 22.

[1312] Beck'scher TKG-Kommentar-Gersdorf, Einleitung, Teil C, Rn. 22 f.; Säcker-*Säcker*, § 3 TKG Rn. 40; Spindler/Schmitz/Geis-*Spindler*, § 2 TDG Rn. 22; *Spindler*, CR 2007, 239 (242).

731 Das TKG enthält in den §§ 108 ff. besondere Regelungen im Interesse der öffentlichen Sicherheit, zu denen gemäß § 109 TKG auch technische Schutzmaßnahmen gehören – wobei § 109 TKG nicht durch die im November 2006 verabschiedete Reform berührt wird. § 109 TKG findet, wie auch schon die Vorgängervoschrift des § 87 TKG,[1313] europarechtlich seine Vorgabe in Art. 4 der Datenschutzrichtlinie.[1314] Dabei entspricht § 109 II TKG sinngemäß Art. 4 I DSRL. Durch § 109 I TKG geht er aber über die Vorgabe der Datenschutzrichtlinie noch hinaus, indem er auch jeden Diensteanbieter (anstatt lediglich den Betrieber von Telekommunikation) zum Treffen von technischen Schutzmaßnahmen verpflichtet.[1315] Nicht erwähnt wird dagegen die Unterrichtungspflicht des Art. 4 II der Datenschutzrichtlinie in § 109 TKG. Nach Art. II der Datenschutzrichtlinie muss der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes, wenn ein besonderes Risiko der Verletzung der Netzsicherheit besteht, die Teilnehmer über dieses Risiko und – wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahmen liegt – über mögliche Abhilfen, einschließlich der voraussichtlich entstehenden Kosten, unterrichten. Da diese Umsetzung fehlt wird vorgeschlagen, in richtlinienkonformer Auslegung, die Unterrichtungspflicht als sonstige Maßnahme im Sinne des § 109 TKG zu qualifizieren.[1316]

732 Im Unterschied zur Vorgängerregelung des § 87 TKG 1996 richtet sich die Vorschrift nicht nur an die Betreiber von Telekommunikationsanlagen, sondern an jeden Diensteanbieter. **Diensteanbieter** ist nach § 3 Nr. 6 TKG jeder, der Telekommunikationsdienste (§ 3 Nr. 24 TKG) ganz oder teilweise geschäftsmäßig erbringt oder an der Erbringung solcher Dienste mitwirkt; Internet-Provider können danach den Anforderungen des § 109 TKG unterliegen, wenn sie nach obigen Grundsätzen Telekommunikationsdienste erbringen.

733 Nach **§ 109 I TKG** haben Diensteanbieter angemessene (vgl. § 109 II 4 TKG) technische Vorkehrungen oder sonstige Maßnahmen zum Schutze des Fernmeldegeheimnisses und personenbezogener Daten und der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen. Geschützt werden soll dadurch vor

[1313] Siehe dazu Trute/Spoerr/Bosch-*Trute*, § 87 Rn. 6.
[1314] Richtlinie 2002/48/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) vom 12. Juli 2002.
[1315] S. dazu auch Säcker-*Klesczewski*, § 109 TKG Rn. 4.
[1316] So Säcker-*Klesczewski*, § 109 TKG Rn. 5.

allem die Vertraulichkeit der Telekommunikation (gegen den Eingriff von Dritten)[1317] und der störungsfreie Betrieb. Darüber hinausgehend sind die Betreiber von Telekommunikationsanlagen, die als solche den unmittelbaren technischen Zugriff auf die Systeme haben,[1318] die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, nach § 109 II TKG verpflichtet, angemessene technische Vorkehrungen und sonstige Maßnahmen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen und gegen äußere Angriffe (z. B. durch Hacker) und Einwirkungen von Katastrophen zu treffen. Darunter fällt insbesondere die Pflicht zur **Datensicherung**, wodurch Daten vor Verlust, Zerstörung infolge von Beschädigung der datenverarbeitenden Systeme, vor unbefugter Veränderung und vor Missbrauch geschützt werden sollen.[1319] Mit Missbrauch sind Angriffe von Außenstehenden (Hackern) und die unbefugte Datenverwendung durch Mitarbeiter gemeint.[1320] Welche Schutzmaßnahmen angemessen sind, muss anhand des Einzelfalles entschieden werden.[1321] Hierzu haben sie einen Sicherheitsbeauftragten zu benennen und ein Sicherheitskonzept zu erstellen (§ 109 III TKG). Technische Anforderungen im Sinne von § 109 TKG sind Maßnahmen mit Bezug auf die Funktionsweise der Telekommunikationsanlagen.[1322] Hierunter sind für den Bereich der Störungsabwehr (§ 109 I Nr. 2, II TKG) beispielsweise die Vorhaltung redundanter Systeme oder von Überbrückungsaggregaten zu verstehen.[1323] Bietet ein Diensteanbieter beispielsweise Voice over IP an, so werden Sprachpakete über das Internet versendet. Um zu verhindern, dass dadurch ein offenes Netz entsteht, ist der Diensteanbieter gem. § 109 I TKG gehalten, durch entsprechende Verschlüsselung der Datenpakete für sichere Verbindungen zu sorgen und unerbetene Lauschangriffe auf die Internet-Telefonie wirksam zu verhindern.[1324] Die sonstigen Maßnahmen betreffen vor allem Kontroll- und Organisationsmaßnahmen (z. B. Zugangskontrollen, Zugriffsbeschränkungen bzgl. Daten, Mitarbei-

[1317] *Koenig/Loetz/Neumann*, Telekommunikationsrecht, S. 209.

[1318] *Koenig/Loetz/Neumann*, Telekommunikationsrecht, S. 209.

[1319] *Elbel*, Die datenschutzrechtlichen Vorschriften für Diensteanbieter im neuen Telekommunikationsgesetz auf dem Prüfstand des europäischen und deutschen Rechts, S. 104.

[1320] *Geppert/Ruhle/Schuster*, Handbuch Recht und Praxis der Telekommunikation, Rn. 785; *Elbel*, Die datenschutzrechtlichen Vorschriften für Diensteanbieter im neuen Telekommunikationsgesetz auf dem Prüfstand des europäischen und deutschen Rechts, S. 104; Beck`scher TKG-Kommentar-*Bock*, § 109 TKG Rn. 29.

[1321] *Koenig/Loetz/Neumann*, Telekommunikationsrecht, S. 209.

[1322] Scheurle/Mayen-*Zerres*, § 87 TKG Rn. 16; Säcker-*Klesczewski*, § 109 TKG Rn. 10.

[1323] Säcker-*Klesczewski*, § 109 TKG Rn. 18.

[1324] *Katko*, CR 2005, 189 (192).

terschulung) sowie vertragliche Absicherungen.[1325] Ergreift ein Provider also Maßnahmen zur Abwehr eines Angriffes mit Computerviren, so wird er sich auf § 109 TKG berufen können.[1326] Ähnliches gilt für das Unternehmen, dass ihren Arbeitgebern die private Internetnutzung gestattet. In diesem Fall ist das Unternehmen Diensteanbieter iSd § 109 I TKG und muss danach angemessene Vorkehrungen und Maßnahmen zu Schutz des Fernmeldegeheimnisses, personenbezogener Daten sowie der Telekommunikations- und Datenverarbeitungssysteme treffen, was auch den Schutz gegen Spam und Viren umfasst.[1327]

734 Zur Durchsetzung der die Diensteanbieter und Betreiber von Telekommunikationsanlagen nach dem TKG treffenden Verpflichtungen kann die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen als zuständige Regulierungsbehörde (§ 116 TKG) nach §§ 115, 126 TKG Anordnungen Verwaltungsakte) und andere Maßnahmen treffen.[1328]

735 Das Problem an der Regelung des § 109 TKG ist, dass er dem Betreiber und Diensteanbietern zwar gewisse Sicherheitspflichten aufgibt, ein Mindestniveau für die Sicherheit aber durch die zum Teil wenig konkreten Anforderungen kaum ersichtlich ist.[1329] Noch im alten § 87 TKG war eine Verordnungsermächtigung enthalten, nach der die Bundesregierung die Möglichkeit gehabt hätte, die Maßnahmen zur Gewährleistung der technischen Sicherheit verbindlich festzulegen. Diese Verordnungsermächtigung wurde aber im neuen § 109 TKG gestrichen, da davon nach aktueller Einschätzung kein Gebrauch gemacht werden solle,[1330] weil aufgrund aktueller Studien belegt sei, dass eine hohe Sicherheit und Leistungsfähigkeit in der deutschen Telekommunikationsinfrastruktur bestünde.[1331] Empfehlungen zur Verbesserung des Sicherheitsniveaus wurden zwar bereits vom Bundesamt für Sicherheit in der Informationstechnik abgegeben,[1332] so dass ein Schritt in Richtung Mindeststandard vollzogen wurde. Allerdings handelt es sich dabei um einen Maßnahmenkatalog aus dem Jahr 1998, der aufgrund der schnellen Entwick-

[1325] Säcker-*Klesczewski*, § 109 TKG Rn. 10.

[1326] So *Cornelius/Tschoepe*, K&R 2005, 269 (271).

[1327] *Dendorfer/Niedderer*, AuR 2006, 214 (217).

[1328] Zum Verhältnis der Anordnungsbefugnisse nach § 115 und § 126 TKG Säcker-*Klesczewski*, § 115 TKG Rn. 5; Säcker-*Ruffert*, § 126 TKG Rn. 4.

[1329] IdS auch *Geppert/Ruhle/Schuster*, Handbuch Recht und Praxis der Telekommunikation, Rn. 777.

[1330] So ausdrücklich die Gesetzesbegründung zu § 107 TKG-E BT-Drucks. 15/2316, S. 91.

[1331] Siehe dazu Beck`scher TKG-Kommentar-*Bock*, § 109 TKG Rn. 3.

[1332] BSI, Sicherer Einsatz von digitalen Telekommunikationsanlagen, abrufbar unter: http://www.bsi.bund.de/literat/tkanlage/6001.pdf.

lung im Telekommunikationsbereich heute als veraltet angesehen werden kann. Auch existieren neben § 109 TKG zahlreiche weitere Vorschriften im Post und Telekommunikationssicherstellungsgesetz (PTSG), sowie den daraus erlassenen Verordnungen (Richtlinie für den betrieblichen Katastrophenschutz (RichtlBKO) und Post- und Telekommunikations-Zivilschutzverordnung (PTZSV)), in der Telekommunikations-Sicherstellungsverordnung (TKSIV) sowie dem § 9 BDSG samt Anlage zu Satz 1, die sich teilweise mit dem Anwendungsbereich von § 109 TKG überschneiden. Dabei sind das PTSG und seine Rechtsverordnungen gegenüber § 109 TKG spezieller und § 109 TKG ist gegenüber § 9 BDSG die Spezialvorschrift.[1333] Daher wird § 109 TKG zum Teil sogar als überflüssig angesehen.[1334] Daraus resultiert die weitere Problematik, dass die technische Sicherheit in zahlreichen Normen verstreut zum Teil ohne konkrete Anforderungen geregelt wird, was wiederum zu Rechtsunsicherheiten führt.[1335]

V. Ergebnis

736 Im Bereich der IT-Sicherheit trifft die IT-Intermediäre grundsätzlich eine volle zivilrechtliche Verantwortlichkeit für die Sicherheit ihrer eigenen Systeme, wobei im Einzelfall Haftungsbeschränkungen aufgrund von § 7 TKV a.F. bzw. § 44a TKG 2006 und durch Regelungen in AGB in Betracht kommen. Soweit der Provider als bloßer Mittler für Dritte agiert, kommen ihm dagegen – abhängig von der jeweils ausgeübten Funktion – die Haftungsprivilegierungen der §§ 7 - 10 TMG zugute. Die Rechtslage ist jedoch geprägt durch ein kompliziertes Ineinandergreifen verschiedener Regelungsmaterien, welche die rechtliche Einordnung des Providers im Einzelfall erschweren und zu nicht unerheblicher Rechtsunsicherheit in diesem Bereich beitragen. Dies zeigt sich insbesondere am Beispiel der Anwendbarkeit des TKG auf Internet-Provider, welche wegen der Haftungsregelung des § 7 TKV a.F. bzw. § 44a TKG praktisch bedeutsam werden kann.

F. Endergebnis Teil I: Verantwortungsverteilung und Anreizdefizite im nationalen Recht

[1333] Beck`scher TKG-Kommentar-*Bock*, § 109 TKG Rn. 12 ff.

[1334] So z.B. der BITKOM, Stellungnahme zu BT-Drucks. 15/2316, vom 3.02.2004, abrufbar unter: http://www.bitkom.org/files/documents/StN_BITKOM_TKG_Wirtschaftsausschuss_03.02.04.pdf; Beck`scher TKG-Kommentar-*Bock*, § 109 TKG Rn. 2.

[1335] *Geppert/Ruhle/Schuster*, Handbuch Recht und Praxis der Telekommunikation, Rn. 777; kritisch wegen der unpräzisen Anforderungen in der TKSiV auch Beck`scher TKG-Kommentar-*Bock*, § 109 TKG Rn. 14.

737 Die Verantwortungsverteilung im nationalen Recht für die IT-Sicherheit kann anhand der IT-Wertschöpfungskette (IT-Hersteller – IT-Intermediär – IT-Nutzer bzw. Ersteller weiterer IT-Dienstleistungen) analysiert und differenziert werden.[1336] Einheitliche Regelungen oder ein übergreifender Ansatz zur Gewährleistung einer grundlegenden IT-Sicherheit – unabhängig von vertraglichen Regelungen – fehlen indes; die Strukturen stellen sich als inhomogen dar. Lediglich die Regelungen im Datenschutzrecht bezüglich einer datenschutzsichernden Organisation, die Elemente eines IT-Riskmanagements umfassen, erstrecken sich als spezifische IT-bezogene Normen breitflächig auf zahlreiche Nutzer und IT-Anbieter. Im geltenden Recht muß daher im Wesentlichen auf die allgemeinen Regelungen im bürgerlichen sowie im öffentlichen Recht rekurriert werden. Dabei kann grob zwischen produkt-, dienstleistungs- und organisationsbezogene Regelungen unterschieden werden:

738 Für **IT-Hersteller** sind vor allem die produktbezogenen Sicherungspflichten des Produkthaftungs- und des Produktsicherheitsrecht einschlägig. Allerdings offenbaren sich hier erhebliche Defizite:

- Im öffentlich-rechtlichen Produktsicherheitsrecht finden sich bislang kaum relevante technische Regeln für IT-Produkte, wenn, dann nur als „Abfallprodukt“ anderer Normungen. Ausnahmen wie das Medizinproduktegesetz bestätigen hier die Regel. Zudem sind die meisten Produktsicherheitsnormen, erst recht das allgemeine GPSG, auf Körperschäden sowie auf Verbraucherschutz beschränkt; die für IT-Produkte typischen Schäden, wie Vermögens- oder Eigentumsschäden, werden gerade nicht erfaßt.

- Im Produkthaftungsrecht ist im Rahmen der verschuldensunabhängigen Haftung zunächst die Eigenschaft der Software als Produkt nach wie vor nicht vollkommen geklärt. Für die allgemeine deliktische Haftung zeigen sich ähnlich dem Produktsicherheitsrecht die gleichen Probleme, indem Vermögensschäden nur ausnahmsweise erfaßt werden. Zudem bedarf es einer extensiven Interpretation des Eigentumsbegriffs, die bislang nicht höchstrichterlich abgesichert ist, um Schäden an Daten und Datenbeständen zu erfassen. Gleiches gilt für das Recht am eingerichteten und ausgeübten Gewerbebetrieb.

- Der Geschädigte trägt zudem die Beweislast für die Fehlerhaftigkeit der Software sowie für die Kausalität zwischen fehlerhaftem Produkt und Rechtsgutsverletzung sowie Schaden. Trotz der Umkehr der Beweislast für die Frage der Pflichtwidrigkeit sieht sich der Geschädigte daher gerade bei IT-Produkten eine schier unüberwindlichen Beweislast gegenüber, da zum einen IT-Produkte häufig gemeinsam mit anderen IT-Produkten und –dienstleistungen eingesetzt werden, zum anderen Bedienungs- oder Installationsfehler nie auszuschließen sind.

[1336] Oben Rn. 91 ff.

- Das Deliktsrecht kann keine Schäden erfassen, die grundsätzlich vom Äquivalenzinteresse gedeckt sind. Ob Patches bzw. die nachträgliche Schließung von Sicherheitslücken noch vom Deliktsrecht als Pflichten erfaßt werden (etwa als Rückrufpflichten) ist mehr als fraglich.

739 Hingegen können Produktsicherheits- und Produkthaftungsrecht als Modelle auch für andere Regelungen im Hinblick auf die rechtliche Bedeutung von technischen Standards und Regeln herangezogen werden. So wie DIN-Normen oder andere technische Standards Vermutungswirkungen (Produktsicherheitsrecht) oder Beweiserleichterungen auslösen (Produkthaftungsrecht) können auch die für IT-Produkte entwickelten Common Criteria im Zusammenhang mit Protection profiles als allgemein anerkannte Regeln der Technik im Bereich der Software für bestimmte Produkte angesehen werden.

740 Von den produktbezogenen Regeln und Standards sind die **tätigkeitsbezogenen Pflichten** der IT-Intermediäre und IT-Nutzer zu unterscheiden:

741 Hier besteht für **IT-Intermediäre** eine Gemengelage aus Haftungsprivilegierungen durch das TMG bzw. die E-Commerce-Richtlinie einerseits, Pflichten zur Sicherung der eigenen IT-Systeme andererseits. Letztere werden schließlich im Bereich der Telekommunikationsdienste, die die meisten der IT-Intermediäre erfaßt, wenn sie selbst elektronische Kommunikationsnetze betreiben, erheblich durch die Haftungsprivilegierung des § 44a TKG abgeschwächt. Ob und inwieweit diese Haftungsbegrenzungen gegenüber dem IT-Intermediär auch auf Schäden anzuwenden sind, die der Nutzer eines Netzes infolge von Einwirkungen Dritter erleidet (Hacking etc.), ist bislang noch ungeklärt, wohl aber anzunehmen. Allerdings greifen diese Haftungsprivilegierungen nicht gegenüber Dritten, die über die Netze des IT-Intermediärs geschädigt werden, da keine vertragliche Beziehungen zwischen geschädigtem Dritten und dem IT-Intermediär bestehen, die § 44a TKG aber voraussetzt; indes sieht sich hier der geschädigte Dritte sämtlichen Einschränkungen und Beweisproblemen gegenüber, die auch gegenüber IT-Herstellern eingreifen, insbesondere Kausalität, Anspruchsgrundlage (deliktisch bzw. kein Schutz von Vermögensschäden etc.). Aus öffentlich-rechtlicher Sicht trifft die IT-Intermediäre zwar eine grundsätzlich vorgesehene Pflicht zur Sicherung ihrer Netze; aber auch diese ist offenbar nicht spezifisch auf IT-Sicherheitsfragen ausgerichtet und bislang wenig konkretisiert worden, wenngleich im Grundsatz hier Ermächtigungsgrundlagen zur Verfügung stünden. § 109 TKG ist aber schwerpunktmäßig auf die Sicherung des Netzes gegen Kommunikationsstörungen ausgerichtet, nicht aber hinsichtlich des Schutzes auch Dritter gegenüber Angriffen über das Netz. Die anderen Sicherungspflichten entsprechen denjenigen des Datenschutzrechts. Auch ist bislang ungeklärt, in welchem Verhältnis

solche Anforderungen zu denjenigen der IT-Sicherheit von Intermediären stehen. Selbst im Vergleich zu den IT-Herstellern bestehen daher für IT-Intermediäre insgesamt nur geringe Anreize, die IT-Sicherheit zu verbessern.

742 Anders sieht die Situation dagegen für **IT-Nutzer** aus, insbesondere bei kommerziellen IT-Nutzern, die ihrerseits wiederum Dienstleistungen erbringen oder Produkte mit Hilfe der eingesetzten IT erzeugen: Diese unterliegen zahlreichen Selbstschutzpflichten, die ihrerseits auch wiederum Verkehrssicherungspflichten gegenüber Dritten entsprechen – wobei diese Dritthaftung in ähnlicher Weise wie bei den IT-Herstellern auf die Verletzung bestimmter Rechtsgüter beschränkt ist. Hier ist zu unterscheiden zwischen tätigkeits- und organisationsbezogenen Pflichten: So können etwa bei der Erbringung von IT-Dienstleistungen, wozu auch das Online-Banking gehört, bestimmte Mindestsicherheitsstandards vom Kunden (vertraglich) erwartet werden, deren Verletzung sowohl Konsequenzen im prozessualen Bereich als auch im materiell-rechtlichen Bereich für die Bank hat, etwa fehlende Verschlüsselungen etc. All dies sind **auf die jeweilige Tätigkeit bzw. IT-Dienstleistung bezogene Anforderungen**. Defizite bestehen hier im wesentlichen nicht bei den rechtlichen Grundlagen an sich, da die allgemeinen rechtlichen Vorgaben, wie die im Verkehr übliche Sorgfalt nach § 276 BGB in der Lage sind, flexible Antworten auf neue Gefahren zu geben; vielmehr besteht hier in erster Linie das Problem im Fehlen weitgehend konsentierter Standards, die als Mindestsicherheit auf jeden Fall zu beachten sind, und deren Verletzung per se eine Haftung auslöst. Häufig zeigt sich, daß Kunden nicht über die nötigen Informationen verfügen, um gegebenenfalls ihre Ansprüche durchsetzen zu können (Enforcement-Problem). Auch ist häufig unklar, innerhalb welcher Zeit und wann z.B. Banken auf geänderte Sicherheitsanforderungen und Gefährdungslagen reagieren müssen, z.B. durch Übergang von TAN-Verfahren auf neue sicherere Verfahren. Hier können anderweitig gesetzte Standards Abhilfe schaffen.

743 Davon zu trennen sind die **organisationsbezogenen Pflichten**, die sich auf das IT-Riskmanagement eines Unternehmens beziehen. Das deutsche Recht verweist im wesentlichen in zwei Materien auf Riskmanagement im weiteren Sinne, zum einen in § 91 II AktG, der auch auf andere Gesellschaften anwendbar ist, zum anderen in § 9a BDSG. Doch sind auch hier Defizite zu konstatieren: Die gesellschaftsrechtlichen Regelungen weisen einen hohen Abstraktionsgrad auf, bedürfen der Konkretisierung. Zudem wirken sie nur im Innenverhältnis, bei fehlender Durchsetzung gehen die Vorgaben daher ins

Leere. Hinsichtlich §§ 9, 9a BDSG ist der Schutz nur für personenbezogene Daten von natürlichen Personen gegeben, der zwar weit reicht, keineswegs aber alle Fragen eines IT-Riskmanagements erfaßt, etwa des Einkaufs von IT-Produkten, der Sicherheit von unternehmensinternen Netzen gegenüber davon ausgehenden Angriffen gegenüber Dritten. Ebensowenig werden Daten von juristischen Personen oder nicht-personenbezogene Daten vom Schutz erfaßt – wenngleich die meisten Maßnahmen nach §§ 9, 9a BDSG wohl gleichzeitig auch diese Daten schützen werden. Eines der wesentlichen Probleme neben dem eingeschränkten Anwendungsbereich des §§ 9, 9a BDSG ist aber der Vollzug – es ist keineswegs gesichert, daß die teilweise umfangreichen Anforderungen des Datenschutz-Riskmanagements auch tatsächlich durchgeführt werden, zumal §§ 9, 9a BDSG zivilrechtlich nicht durchsetzbar sind. Herangezogen werden können in diesem Rahmen bereits vorhandene Standards, die auf das IT-Riskmanagement bezogen sind, wie die ISO 27001 oder das BSI-IT-Grundschutzhandbuch.[1337] Diese Standards können wie allgemein anerkannte Regeln wirken und Vermutungswirkungen auslösen, sei es bei ihrer Einhaltung oder Verletzung. Inwieweit hier indes Zertifizierung eine entlastende Wirkung auslösen, ist bislang noch weitgehend ungeklärt.

744 Für **private IT-Nutzer** hingegen ergeben sich nur rudimentäre (Selbst-) Schutzpflichten, die sich auf allgemein bekannte und leicht zugängliche Schutzmaßnahmen beschränken. Je weiter verbreitet indes derartige Eigenschutzmaßnahmen sind, desto eher sind sie auch den privaten IT-Nutzern zuzumuten. Darüberhinausgehende Pflichten lassen sich aber dem geltenden Recht nicht entnehmen, weder dem bürgerlichen noch dem öffentlichen Recht. Insbesondere wenn Gefahren von privaten Nutzern ausgehen, z.B. durch Weiterverbreitung von Viren durch ungesicherte Rechner, kommt in den meisten Fällen keine Haftung in Betracht. Hier stellen sich zum einen diesselben Probleme wie im Rahmen der IT-Produkthaftung (keine Erfassung von Vermögensschäden, Beweisprobleme), zum anderen kann lediglich für völlig offensichtliche Gefährdungslagen von einem Verschulden der privaten IT-Nutzer ausgegangen werden.

745 Überlappt werden alle Probleme schließlich durch **Darlegungs- und Beweisprobleme** für Geschädigte – was wiederum zu einer Abschwächung von rechtlichen Anreizen für Verantwortliche führt. Diese Beweisprobleme betreffen sowohl den Nachweis, dass eingesetzte IT-Produkte fehlerhaft sind, als auch den Nachweis, dass genau dieser Feh-

1337 Zum österreichischen Pendant eines IT-Grundschutzhandbuches s. *Fallenböck* Annex II – Österreich - Rn. 1195 ff.

ler zu dem eingetretenen Schaden geführt hat. Ferner sind IT-Nutzer häufig mit der Frage konfrontiert, welche Standards gelten, insbesondere welche Beweiserleichterungen, wenn es um den Nachweis der Identität und der Authentizität geht, etwa im Bereich des Online-Banking. Der bislang angenommene Anscheinsbeweis beruht auf der Annahme, dass die eingesetzten Verfahren sicher sind – was wiederum im Prozeß der Nutzer derzeit zu erschüttern hat, was ihm meist nicht gelingt, schon aufgrund seiner Unterlegenheit bei den einsetzbaren Ressourcen (Kosten für Sachverständigengutachten, Informationsdefizite).

Tabellarische Übersicht

Verantwortlicher	**Zivilrecht**	**Öffentliches Recht**	**Standards**
IT-Hersteller	Vertragsrecht: - Haftungsausschlüsse - Schwierige Einordnung der Software als Sache (Verbrauchsgüterkauf?) - Keine Haftung von Händler für Mangelfolgeschäden - Kein zwingender Regress bei internationalem Softwareüberlassung (Händlerkette) Produkthaftungsrecht: - Anwendung ProdHaftG auf Software umstritten - Eigentumsbegriff unklar (Daten?) - keine Vermögensschäden - schwierige Beweislage (Kausalität)	Produktsicherheitsrecht: - im wesentlichen nur anwendbar auf Körperschäden - nur Verbraucher eingeschlossen	Common Criter Protection Prof insgesamt noch im Fluß

IT-Intermediär	Deliktsrecht: wie bei IT-Hersteller Vertragsrecht: Haftungsbegrenzung durch TKG selbst bei grober Fahrlässigkeit	Telekommunikationsrecht: ähnlich Datenschutzrecht; Sicherungspflichten nur hinsichtlich der ungestörten Kommunikation	Nur wenige Sta (ISO-Norm zur werksicherheit) künftige Norme BSI?
Kommerzielle IT-Nutzer allgemein (IT-Riskmanagement)	Gesellschaftsrecht: prinzipiell Ansatz über Pflicht zum Riskmanagement, aber ausfüllungsbedürftig Vertragsrecht: - Haftungsausschlüsse - umstr. Anscheinsbeweis, Sicherheitsanforderungen Deliktsrecht: Pflicht zur Sicherung der eigenen Systeme, auch gegenüber Dritten	Aufsichtsrecht: - § 9a BDSG: Pflichten zur Organisation zum Datenschutz (allerdings Enforcement-Probleme)	ISO 27.001 ff.; Grundschutzhan BSI
Kommerzielle IT-Nutzer branchenspezifisch: Finanzdienstleistungssektor	Zusammenspiel Sicherheitsanforderungen und Anscheinsbeweis bzw. Pflichtenbestimmung gegenüber Kunden	Aufsichtsrecht: allgemeine Pflicht zum IT-Riskmanagement (§ 25a KWG), Konkretisierung bislang unklar	MaRisk (BaFin aber relativ abs

G. Teil 2

I. Die Zuweisung von Verantwortlichkeiten und Pflichten

1. Kriterien

746 Die Frage, wie Verantwortlichkeiten sinnvoll zuzuordnen sind, durchzieht nicht nur de lege lata, sondern natürlich auch de lege ferenda das gesamte Sicherheits- und Haftungsrecht wie ein roter Faden. Daher ist es nicht erstaunlich, dass die gleichen Kriterien, wie sie etwa im geltenden Deliktsrecht für die Zuordnung der Verantwortlichkeit

für Gefahrenquellen oder für die Bestimmung der Pflichten, auch des Mitverschuldens, gelten, auch fruchtbar gemacht werden können für die mögliche Reformen oder neue Haftungsmaßstäbe. Zu fragen ist daher stets nach dem „cheapest cost avoider", nach der möglichen Internalisierung von sonst externalisierten Risiken und Schäden sowie nach dem gewünschten Aktivitätsniveau aus gesamtgesellschaftlicher und –wirtschaftlicher Perspektive – entsprechend dem im Teil 1 dargestellten methodischen Grundverständnis der Ökonomischen Analyse des Rechts.[1338] Dabei können sowohl zivil- als auch öffentlich-rechtliche Regulierungen als mögliche „Werkzeuge" in Betracht kommen, je nachdem welche Probleme der Durchsetzung und des Vollzugs (Enforcement) bestehen, welche Defizite die jeweiligen Rechtsgebiete aufweisen. Zivilrecht und öffentliches Recht stellen aus dieser Sicht ein System kommunizierender Röhren dar, das sich gegenseitig beeinflussen und ergänzen kann.

747 Ins Gedächtnis zu rufen ist in diesem Zusammenhang, dass auch bei grundsätzlich möglicher Beherrschung von Gefahrenquellen gesamtwirtschaftlich gesehen bestimmte Risiken und Schäden bei Nutzern durchaus akzeptiert werden, um insgesamt als wünschenswert eingestufte Tätigkeiten nicht zu unterbinden. Beispiele hierfür sind aus heutigem Verständnis die zuvor behandelten Haftungsprivilegien für Access-Provider,[1339] in gewisser Hinsicht auch für Host-Provider – wobei allerdings von vornherein anzumerken ist, daß eine profunde ökonomische Begründung für derartige Haftungsprivilegien nach wie vor fehlt.

748 Für mögliche Reformen gibt es – vergleichbar der Einteilung de lege lata – verschiedene Ansatzmöglichkeiten und „Stellschrauben":

- produkt- bzw. tätigkeitsbezogene Anforderungen
- nutzer- bzw. organisations- und sicherheitsbezogene Anforderungen

749 Beide Bereiche können matrixförmig in öffentlich-rechtliche und zivilrechtliche Regelungen unterteilt werden:

	Öffentliches-Recht	Zivilrecht
Produkt- und tätigkeitsbezogene	Produktsicherheitsrecht; Gewerberecht im weite-	Haftungsrecht

1338 Ausführlicher zu diesen Kriterien s. oben Teil I Rn. 21 ff.

1339 Teil I Rn. 662, 667, 688.

Anforderungen	ren Sinne (Tätigkeits-bezogen)	
Organisationsbezogene Anforderungen	Datenschutzrecht, KWG/VAG, WpHG, sonstige Segmente	Kaufmännische bzw. gesellschaftsrechtliche Anforderungen, § 254 BGB

750 Die Vor- und Nachteile der jeweiligen Regulierungen sind dabei vor dem Hintergrund der Möglichkeiten zur Bewältigung der oben dargestellten Defizite im deutschen Recht näher zu beleuchten (zusammenfassend Teil 1 Rn 738 ff.).

2. Mögliche Akteure und ihre Pflichten

a) Hersteller – Produkthaftungs- und Produktsicherheitsrecht

(1) Verantwortungszuweisung

751 Wendet man das Kriterium des cheapest cost avoider[1340] auf produktbezogene Sicherheitsvorkehrungen an, so liegt es auf der Hand, dass der Hersteller aus Effizienzgesichtspunkten in die Pflicht genommen werden sollte – was im deutschen Deliktsrecht auch durch § 823 I BGB sowie das ProdHaftG umgesetzt wird. Nach *Landes*/*Posner*[1341] und *Adams*[1342] ist das Haftungsregime für eine optimale Produktsicherheit dann irrelevant, wenn Produzent und Nutzer vollständig über Produktrisiken und alternative Produkte informiert sind.[1343] Bei fehlender oder unzureichender Information des Nutzers - wegen der Komplexität der Systeme, unzugänglichem Quellcode und aus anderern Gründen[1344] - verringert sich ohne eine Produkhaftung hingegen die Produksicherheit in einem „race to the bottom".[1345] Nutzer können die Qualität der Produkte nicht vergleichen, einziges Differenzierungskriterium wird der Preis, und hier unterbieten sich die Hersteller.

[1340] Vgl. dazu Teil I, Rn. 32.

[1341] *Landes, W. / Posner, R.*, A postive economic analysis of products liability, 14 Journal of legal studies, 1985, 535.

[1342] *Adams, M*, Produkthaftung – eine ökonomische Analyse, BB 1987, Beil. 20 zu Heft 31.

[1343] Diese Aussage setzt weiter voraus, dass die Schäden nur die Vertragspartner treffen, was hier ebenfalls nicht der Fall ist, vgl. Rn. 315.

[1344] Vgl. auch unter bei Rn. 296 ff.

[1345] Grundlegend für viele Rechtsgebiete *Akerlof, G.*, The Market for Lemons, Qualitive Uncertainty and the Market Mechanism, 84 Quaterly Journal of Economics, 1970, 488.

752 Um diese Entwicklung zu vermeiden kann über Haftungsrecht der Anreiz gesetzt werden, die Verbraucher über Produktgefahren richtig aufzuklären.[1346] Nimmt man einen Konstruktionsfehler eines Produktes dann an, wenn sich bei der Benutzung Gefahren ergeben, über die der Nutzer nicht aufgeklärt wurde oder aufgeklärt werden kann (Consumer Awareness Test)[1347], so ist für Nutzer eine an Qualitätskriterien ausgerichtete Kaufentscheidung möglich, ein „race to the bottom" findet nicht statt.

753 Die Verantwortungszuweisung könnte zwar auch im Rahmen der vertraglichen Leistungsbeziehungen vom Kunden zum Händler zum Hersteller im Wege des Regresses erfolgen; doch wie in Teil 1 Rn. 15 bereits dargelegt, tauchen hier verschiedene Probleme auf, die eine einfache Risiko- und Verantwortungszuweisung für die Einhaltung von Mindestsicherheitsstandards gefährden, wie etwa Haftungsausschlüsse in der vertraglichen Leistungskette. Demgemäß mag das Vertragsrecht zwar in vielen Bereichen eine sinnvolle Risikozuweisung erreichen. Eine effiziente Risikozuweisung durch Marktmechanismen setzt jedoch nach dem Coase-Theorem geringe Transaktionskosten[1348] voraus.[1349] Gerade in Bereichen mit großem Informationsgefälle wie bei IT-Produkten sind die Transaktionskosten aber hoch. Des Weiteren wird durch vertragliche Risikozuweisung nicht garantiert, dass eine Mindestsicherheit für *jedermann* erreicht wird, insbesondere außerhalb der entsprechenden Vertragsbeziehungen.[1350] Eine solche Sicherheit ist aber gerade für Schäden, die Dritte erleiden, etwa durch Viren, die über unsichere Systeme weiterverbreitet werden, unerlässlich.

754 Allerdings unterliegt – wie in Teil 1 Rn. 203 dargelegt - auch das **Produkthaftungsrecht einigen Defiziten**, die insbesondere für IT-Schäden relevant sind, nämlich in Gestalt der Ausgrenzung von Vermögensschäden, was nur teilweise durch eine erweiternde Auslegung der Eigentumsschäden kompensiert werden kann.[1351] Gleiches gilt für das

[1346] Vgl. *Schäfer/Ott,* Ökonomische Analyse des Zivilrechts, S. 345.

[1347] Vgl. *Finsinger, J. / Simon, J.*, Eine ökonomische Bewertung der EG-Produkthaftungsrichtlinie und das Produkthaftungsgesetzes der Bundesrepublik Deutschland, Lüneburg, 1989.

[1348] *R. Coase*, The Problem of Social Cost, Journal of Law and Economics 3 (1960), S. 15.

[1349] Im theoretischen Modell keinerlei Transaktionskosten, näheres *Thomas J. Miceli*, Economics of the Law (1997), S. 9; *R. Coase*, The Problem of Social Cost, Journal of Law and Economics 3 (1960); *ders.*, in: Assmann/Kirchner/Schanze, Ökonomische Analyse des Rechts, 1993, S. 129, 148 ff.

[1350] Vgl. *Schäfer /Ott*, Ökonomische Analyse des Zivilrechts, S. 335.

[1351] S. oben Teil I Rn. 108.

Öffentliche Recht, das abgesehen von wenigen sektorspezifischen Regelungen in der Regel auf Verletzungen von Leib und Leben bzw. Gesundheit abstellt.[1352]

755 **Anreize für Hersteller**, sichere IT-Software herzustellen, bestehen daher aus rechtlicher Sicht im Rahmen der Produkthaftung ebenfalls **nur sehr eingeschränkt**. Risiken, die aus unsicheren Produkten entstehen, werden somit weitgehend nicht internalisiert, sondern verbleiben bei den Anwendern; lediglich Risiken, die bei besonders hochrangigen Rechtsgütern entstehen, wie Leib und Leben, werden derzeit von der Rechtsordnung erfasst. Selbst in diesen Bereichen ist die produkthaftungsrechtliche Internalisierung von Risiken indes bislang eher graue Theorie, da einer entsprechenden Geltendmachung von Ansprüchen erhebliche Hürden entgegenstehen: So muss der Anwender nach wie vor die Kausalität einer fehlerhaften Software für seinen entstandene Rechtsgutsverletzung nachweisen – was gerade bei komplexen, interaktiven Systemen (die mit anderen Systemen vernetzt sind, z.B. Zusammenwirken von Applikationssoftware mit Betriebssystemsoftware) wesentlich erschwert ist.[1353] Hinzu kommt der in der Praxis ebenfalls schwer zu entkräftende Einwand des Herstellers, dass der Benutzer selbst einen Bedienungsfehler begangen hat.[1354]

756 Ferner bleibt es dabei, dass der Anwender den eigentlichen Softwarefehler nachweisen muss – was ihm, ganz abgesehen von dem Informationsungleichgewicht gegenüber dem Hersteller, angesichts der Unzugänglichkeit des Softwarequellcodes kaum möglich ist. Ähnlich dem Arzthaftungsprozess[1355] ist der Anwender hier auf Evidenzbeweise und Darlegungen beschränkt – die aber auch ausreichen können, sofern die Rechtsprechung ihre Regelungen der sekundären Behauptungs- und Beweislast entsprechend ausdehnen würde.

(2) Vorteile und Grenzen einer Ausdehnung des Anwendungsbereichs der deliktischen Haftung

[1352] S. oben Teil I Rn. 222.

[1353] Dieser Kausalitätsnachweis ist nur dort einfacher zu führen, wo der Softwarefehler praktisch untrennbarer Teil des Gesamtproduktes ist, etwa bei embedded systems – hier ist die gesamte Funktionalität des Produktes maßgeblich. Bei einer softwareneutralen Hardware jedoch (PCs, Mainframes etc.) mit u.U. mehreren Softwareapplikationen wird es für den Anwender schwierig, den einzelnen Softwarefehler als kausales Ereignis einer Rechtsgutsverletzung zuzuordnen.

[1354] Diese Frage ist indes bislang kaum behandelt. Denkbar wäre, dass die Beweislast, dass der Nutzer einen Bedienungsfehler begangen hat, beim Hersteller liegt, was auch in etwa auf der Linie der Rechtsprechung zu Instruktionspflichten läge. Gelänge es jedoch dem Hersteller nachzuweisen, dass seine Installatonsanleitungen und –routinen den üblichen Standards entsprechen, obläge es dem Nutzer, seinerseits den – praktisch kaum zu führenden – Nachweis zu erbringen, dass er alle Pflichten seinerseits beachtet hat.

[1355] Ausführlich dazu Bamberger/Roth/*Spindler*, § 823 BGB Rn. 784 ff. mwNachw.

757 Die Ausdehnung einer deliktischen Haftung de lege ferenda für Software, etwa durch Erweiterung bestehender (öffentlich-rechtlicher) Produktsicherheitsregeln auf (schwerwiegende) Vermögensschäden, könnte die Grauzone zwischen Eigentums- und Vermögensschäden sicherer erfassen, insbesondere Betriebsausfallschäden. Hierfür wäre es nicht erforderlich, den Tatbestand des § 823 I BGB auszudehnen oder gar das ProdHaftG zu erweitern; vielmehr könnte es genügen, ein entsprechendes IT-Sicherheitsgesetz zu schaffen, das auch dem Individualschutz dient, oder die bestehenden Regelungen um derartige Tatbestände zu erweitern. Denn hierdurch wäre aufgrund des generell anerkannten Schutzgesetzcharakters der Produktsicherheitsgesetze (sowie Verordnungen)[1356] weitgehend über § 823 II BGB der Bereich der Vermögensschäden abgedeckt. Andererseits darf der Bereich der Erfassung von Vermögensschäden auch nicht über Gebühr ausgedehnt werden, um zum einen zu verhindern, dass deliktsrechtlich das Äquivalenzinteresse geschützt würde, zum anderen eine Ausuferung der Haftungsrisiken, insbesondere in Richtung von „pure economic losses“ zu vermeiden – wie auch das britische Recht in anderem Zusammenhang zeigt.[1357]

758 Ohne bereits an dieser Stelle auf weitere Ausformungen dieses Ansatzes einzugehen, sind einige Vorbehalte zu formulieren und zu diskutieren:

759 Wie bereits oben angesprochen (Rn. 755) bleibt die Frage der **Kausalität** – und der entsprechenden Einwände – auch bei einer entsprechenden Ausdehnung des Kreises der geschützten Rechtsgüter ungelöst. Die Schwierigkeit, die kausale Verursachung des Schadens durch einen Softwarefehler nachzuweisen, ließe sich nur durch eine Verlagerung der Beweislast auf den Hersteller beseitigen – allerdings ist fraglich, ob eine derartige generelle Beweislastumkehr nicht über das Ziel der Internalisierung hinausschösse, da auch der Hersteller einer tauglichen Software mit dem Nachweis belastet wäre, dass andere Software oder Fehler den Schaden verursacht haben. Diesem Problem ließe sich wiederum dadurch begegnen, dass die Beweislastumkehr nicht eingreift, wenn der Hersteller seinerseits nachweist, dass er den allgemeinen Sicherheitsstandards genügt hat.

760 In ähnlicher Weise kann mit dem Einwand umgegangen werden, der sich auf die **mangelnde Vorhersehbarkeit** eines durch Softwarefehler verursachten Schadens bezieht: Denn gerade die zivilrechtliche Haftung erlaubt es, in einer Art Fine-Tuning im Einzel-

[1356] Siehe dazu Teil 1 Rn. 188.

[1357] S. dazu *Reed* – Annex II – Rn. 1293 ff., wobei die dort geführte Diskussion im deutschen Recht sich eher im Bereich des Vertrages mit Schutzwirkung zugunsten Dritter bewegt.

fall diesem Einwand gerecht zu werden, sei es auf der Ebene der objektiven Pflichtwidrigkeit, sei es auf der Ebene der Definition des Produktfehlers (ProdHaftG), der wiederum von den berechtigten (verallgemeinerten) Erwartungen des Verkehrs abhängig ist. Nicht vorhersehbare Schäden sind dabei in der Regel auf nicht vorhersehbare Fehler zurückzuführen, so dass eine entsprechende Haftung entfallen würde. Dass der Hersteller jedenfalls bei standardisierter Software und fehlenden unmittelbaren Kontakt mit dem Nutzer nicht in der Lage ist, die Risiken zu kalkulieren und sein Verhalten darauf einzustellen, kann in diesem Rahmen berücksichtigt werden – führt aber nicht dazu, jegliche Haftung von vornherein abzulehnen.[1358] Darüber hinaus wäre die öffentlich-rechtliche Seite (Produktsicherheit) hiervon unberührt, da Anpassungen der Produkte für die Zukunft verlangt werden könnten, um die – nunmehr bekannten – Schäden zu vermeiden.

761 Abgesehen von der Stellschraube „Pflichtwidrigkeit“ bzw. „Vorhersehbarkeit“ lässt sich ein ähnliches Ergebnis auch mit einer **Haftungsbegrenzung** bei nur schwer vorhersehbaren Schäden erreichen: Damit würde zwar eine gewisse Internalisierung der hervorgerufenen Risiken erreicht – und damit auch Anreize zur sicheren Konstruktion von Software geschaffen – jedoch andererseits keine überzogenen Risiken für den Hersteller hervorgerufen.

762 Durch beide Instrumente kann daher dem Phänomen Rechnung getragen werden, dass der Hersteller durch minimale Sicherheitslücken in seinem komplexen Produkt Software Einbrüche Dritter in das System des Nutzers ermöglichen könnte – und damit unkalkulierbare Risiken für ihn entstünden.

(3) Produktsicherheit after sale

763 Eine der weiteren Charakteristika von IT-Produkten ist ebenfalls durch ihre Komplexität und Interaktion mit anderen Produkten bedingt: die Notwendigkeit stetiger, nachträglicher Anpassungen. In der Praxis von Softwareüberlassungsverträgen wird daher häufig gleichzeitig ein Softwarepflegevertrag abgeschlossen, der selbständig neben die üblichen Gewährleistungsrechte tritt.[1359]

764 Wie oben dargelegt (Rn. 104 ff.), ist dagegen die vollständige Internalisierung dieser Risiken und Kosten deliktsrechtlich im geltenden System kaum möglich: Zwar kennt das deutsche Recht inzwischen eine Rückrufpflicht von Produkten, insbesondere auch

[1358] S. dazu oben Teil 1 Rn. 102.

[1359] Ausführlich zu Softwarepflegeverträgen *Peter*, in: Schneider/v.Westphalen, Softwareerstellungsverträge, 2006. Teil G.

in Verbindung mit öffentlich-rechtlichen Produktsicherheitsrechtsvorschriften[1360] – doch beschränkt sich dieser Rückruf im Prinzip aufgrund der nötigen Abgrenzung zu den Gewährleistungsrechten nach wie vor auf die Warnung des Kunden vor dem weiteren Einsatz des Produktes, ohne dass die Kosten der Reparatur des Produktes erfasst wären, geschweige denn dessen Verbesserung.[1361] Öffentlich-rechtliche Anordnungsbefugnisse (vgl. § 8 Abs. 4 Nr. 7 GPSG) bestehen zudem nur bei Gefahren für Sicherheit und Gesundheit der Produktverwender und Dritter.[1362]

765 Haftungsrechtlich könnte eine solche Pflicht zur stetigen Nachbesserung nur durch die Ausweitung der bereits erwähnten öffentlich-rechtlichen Produktsicherheitsrechtspflichten erreicht werden. Schwierig bleibt indes die Abgrenzung zu den von der Gewährleistung erfassten Risiken und den Fehlern; denn eine Ausweitung von Rückrufpflichten darf nicht de facto zu einer stetigen Nachbesserungs- und Nachlieferungspflicht der Softwarehersteller führen, da hiermit das grundlegende Modell der Softwareüberlassung zu einem solchen der zeitweisen Softwareüberlassung verändert würde. Mit anderen Worten würde eine solche produkthaftungsrechtliche Pflicht sich de facto wie ein Mietvertrag über Software auswirken, ohne dass dem ein Äquivalent eines Mietzinses (oder Softwarepflegevertrages) entgegenstünde. Von einer solchen Ausdehnung ist daher abzuraten, da sie über das Ziel einer effizienten Zuweisung von Risiken in erheblichem Maße hinausschießen würde.

766 Dem Problem der nachträglichen auftretenden Fehler ist daher nach wie vor nur im System der vertragsrechtlichen Haftung und eingeschränkt im Deliktsrecht durch die aufgrund der Produktbeobachtung erforderliche Warnung vor weiteren Gebrauch des fehlerhaften Produktes Rechnung zu tragen. Darüber hinaus kann durch öffentlich-rechtliche Anordnungsbefugnisse bei besonderen Gefährdungen ein Ausgleich für die zivilrechtlich fehlenden Anreize zu nachträglichen Patches geschaffen werden (z.B. Produkte, die anfällig sind für Straftaten, die über die Software bzw. deren Sicherheitslücken ausgeübt werden können).

b) Intermediäre

[1360] Teil 1 Rn. 208.
[1361] S. dazu Teil 1 Rn. 240.
[1362] Teil 1 Rn. 252.

767 Für die Intermediäre wurden oben[1363] dargelegt, dass für sie im weiten Umfang Haftungsprivilegierungen eingreifen, sei es generell im Rahmen des Bereithaltens fremder Inhalte aufgrund der Art. 12-15 E-Commerce-Richtlinie (bzw. §§ 8 – 10 TMG), sei es halb gesetzlich, halb vertraglich aufgrund der Haftungsdeckelungen in § 7 TKV bzw. im neuen § 44a TKG, soweit die Intermediäre Teile eines elektronischen Kommunikationsnetzes sind – was oftmals der Fall ist.

768 Derartige Haftungsprivilegierungen, die ohne Rücksicht auf die Verletzung oder Erfüllung von Pflichten eingreifen, werfen generell die Frage auf, ob sie nicht zu einer ineffizienten Absenkung der aus volkswirtschaftlicher Sicht gewünschten Aktivitäten zur Sicherung der Intermediäre führen. Anders gewendet wird im Prinzip durch Haftungsprivilegien, die wie ein Rasenmäher wirken, auch derjenige begünstigt, der keinerlei Anstrengungen an den Tag legt, um seine Systeme gegenüber Angriffen von außen zu sichern. Für die Haftungsprivilegierungen der Art. 12 – 15 ECRL wird dies in zunehmenden Maße diskutiert, etwa wenn Firmen wie eBay eigene Prüfprogramme einsetzen, andere Firmen hingegen jedoch gleich behandelt werden, ohne dass diese äquivalente Sicherungsmechanismen einsetzten.

769 Ohne dass im Rahmen der vorliegenden Untersuchung diesen Fragen rund um die Art. 12 – 15 ECRL weiter nachgegangen werden könnte,[1364] ist festzuhalten, dass ähnliche Zweifel hinsichtlich der Rechtfertigung der weitgehenden Haftungsprivilegierungen für die Betreiber von elektronischen Kommunikationsnetzen auftreten – wozu, wie oben dargelegt,[1365] fast alle Provider mit einer Schnittstelle zum Internet zählen.

770 Ausgangspunkt der Überlegungen sollte auch hier die **Schaffung von allgemeinen Sicherheitsstandards**[1366] anstelle gleichförmiger Haftungsprivilegierungen sein, die öffentlich-rechtlicher Natur sein können, die zudem zivilrechtlich durch in besonderen Konstellationen hinzutretende Pflichten flankiert werden können. Derartige pflichtenbezogene Konzepte haben den Vorteil, dass Intermediäre gehalten sind, einen Mindest-

[1363] Teil 1 Rn. 662.

[1364] Im Grundsatz ist eine Haftungsfreistellung angebracht, in Abhängigkeit von den Kontrollmöglichkeiten der Provider und dem Ausmaß der sozialen Nützlichkeit ihrer Tätigkeit. Anders gewendet können externe Effekte, die von Providern hervorgerufen werden, gesamtwirtschaftlich toleriert werden, solange ihre positiven Effekte der verbesserten Kommunikationsmöglichkeiten diese Effekte überwiegen. Ein gutes Beispiel dafür, dass das Gleichgewicht wohl erreicht worden ist oder gar die negativen externen Effekte drohen zu überwiegen, ist die Verbreitung von Spam. Diese Fragestellungen sind Gegenstand einer von der EU-Kommission in Auftrag gegebenen Studie, die im Herbst 2007 erscheinen wird.

[1365] Teil 1 Rn. 660.

[1366] In welchem Rechtsgebiet derartige Standards verankert werden könnten, bleibt noch zu diskutieren (s. Rn. 150 ff.) – sowohl im Telekommunikationsrecht, vergleichbar der TKV, als auch in einem IT-Anlagensicherheitsgesetz wären entsprechende Normierungen denkbar.

standard einzuhalten, um überhaupt in den Genuss einer Haftungsfreistellung zu kommen – eine solche „Freistellung“ ist jedem pflichtenbasierten Konzept immanent, da die Pflichtenerfüllung als eine solche Freistellung etwa gegenüber einer reinen Gefährdungshaftung begriffen werden kann.

771 Allerdings ist auch hier dem Problem der **Vorhersehbarkeit der Schäden** Rechnung zu tragen, dass in ähnlicher Weise wie bei Software auch bei Intermediären auftritt; denn deren Dienste können oftmals von jedermann zu den unterschiedlichsten Zwecken benutzt werden, ohne dass für den Provider konkret vorhersehbar wäre, welche Haftungsrisiken mit der Verwendung seiner Dienste beim Nutzer verbunden sind. Das beste Beispiel hierfür ist der Access Provider, der nur die Durchleitungen von Daten – gleich welcher Natur – gewährleistet. Dem Problem der Vorhersehbarkeit der Schäden kann wiederum durch die Konzentration auf Pflichten, denen dieses Element immanent ist, sowie durch eine Haftungsbegrenzung Genüge getan werden.

772 Schließlich wären die entsprechenden **Haftungsprivilegierungen des TKG** aus dem TK-Recht herauszulösen und dem allgemeinen AGB-Recht nach §§ 305 ff. BGB zu unterstellen – damit wäre entsprechend dem soeben dargelegten Konzept möglich, dass der zur Inhaltskontrolle berufene Richter sowohl im Einzelfall als auch in einer abstrakten Inhaltskontrolle nötige Feinjustierungen je nach Vorhersehbarkeit und Versicherbarkeit von Risiken bei den Providern vornehmen könnte. Zwar wird mit dem neuen § 44a TKG 2006 bereits eine erhebliche Verbesserung erreicht, indem die Haftungsbegrenzung nicht mehr für jeden einzelnen Geschädigten wirkt, sondern nur noch global; doch ist dies – abgesehen von Fragen, wie diese Haftungsbegrenzungen zivilrechtlich überhaupt anwendbar sind – nicht hinreichend, um entsprechende Anreize und einen Gleichlauf mit sonstigen Haftungsklauseln zu erzielen. Last but not least wären nicht nur materiell-rechtlich entsprechende Anreize gesichert, sondern auch im Hinblick auf ihr „Enforcement“, da sich zum einen in Individualstreitigkeiten der Nutzer auf die Anwendung der AGB-Inhaltskontrolle berufen kann als auch die Möglichkeit der Verbandsklage eröffnet wäre. Die Verankerung im Vertragsrecht entlastet den Nutzer zudem jedenfalls teilweise von seiner Behauptungs- und Beweislast im Bereich des Verschuldens (§ 276 BGB) – die oben für Softwareprodukte geschilderten Probleme des Nachweises der Kausalität und der Fehlerhaftigkeit des Services bleiben indes tendenziell auch hier bestehen.

773 Deliktsrechtlich hingegen bietet das geltende Recht nur wenige Anreize für Intermediäre, auch gegenüber Dritten die nötige Sicherheit ihrer Netze zu gewährleisten. Wie in Teil I Rn. 106 ff. dargelegt, ist auch hier ähnlich wie bei den IT-Herstellern fraglich, ob eine relevante Rechtsgutsverletzung vorliegt (Vermögensschäden), abgesehen von den wiederum auftretenden Problemen des Nachweises von Kausalität und Pflichtwidrigkeit. Anders gewendet braucht der IT-Intermediär, von dessen Netzen oder Servern Angriffe auf Dritte ausgehen nur in den seltensten Fällen einen Regress zu befürchten.[1367]

774 Letztlich würde auch hier wieder nur ein **öffentlich-rechtlicher Standard** Abhilfe schaffen, der als Schutzgesetz Individualschutz vermitteln könnte, etwa durch ein IT-AnlagensicherheitsG, so dass bei Verletzung der hier festgelegten IT-Sicherheitsstandards über § 823 II BGB ein unmittelbarer Schadensersatzanspruch auch bei Fahrlässigkeit gegeben wäre. Problemen der Vorhersehbarkeit und der Kausalität kann man in der vorstehend beschriebenen Weise gerecht werden.

c) Nutzer und IT-Dienstleister

775 Für Nutzer resultieren je nach dem Charakter ihrer Anwendung von IT-Produkten unterschiedliche Anforderungen: Sofern sie als gewerbliche Anwender von IT-Produkten als Nutzer auftreten, treffen sie eine Reihe von Pflichten im technischen und organisatorischen Bereich, die allerdings nur wenig miteinander harmonisiert sind.[1368] Private Nutzer dagegen sehen sich nach geltendem Recht nur rudimentären Pflichten gegenüber, etwa dem Einsatz von verfügbaren Viren-Scannern.[1369]

(1) Unterscheidung private und gewerbliche Nutzer

776 Dass auch in Zukunft eine Trennung von privaten und gewerblichen Nutzern sinnvoll und erforderlich ist, liegt auf der Hand: Schon allein ihr unterschiedliches Potential, Gefahrenquellen zu erkennen und zu beherrschen, zwingt dazu, verschiedene Maßstäbe anzulegen. Sonderkenntnisse und –wissen privater Nutzer im Einzelfall können zudem über flexible Sorgfaltsmaßstäbe berücksichtigt werden.[1370]

(2) Gewerbliche Nutzer

777 Betrachtet man zunächst gewerbliche IT-Nutzer, fällt die große Bandbreite an Anforderungen und unterschiedlichster Rechtsgrundlagen auf, die von segment- bzw. tätigkeits-

---

1367 S. oben Teil 1 Rn. 682 f.

1368 S. oben Teil 1 Rn. 403.

1369 S. oben Teil 1 Rn. 297, 385.

1370 S. dazu oben Teil 1 Rn. 654.

spezifischen Anforderungen, etwa im Kreditgewerbe, bis hin zu querschnittsartigen, für alle Branchen geltenden Maßstäben, etwa nach Datenschutzrecht[1371] reichen. Daher liegt die Frage auf der Hand, ob nicht eine einheitliche Behandlung aller von einem gewerblichen Nutzer zu treffenden Maßnahmen sinnvoller wäre. Indes ist auch hier zu differenzieren: Die Bedeutung bestimmter Branchen für die gesamte Wirtschaft ebenso wie der Rang bestimmter Rechtsgüter kann eine andere Behandlung, insbesondere höhere Anforderungen, als in anderen Branchen rechtfertigen, ökonomisch auch effizient sein. Die hohe Sensibilität etwa des Finanzdienstleistungssektor erfordert einen wesentlich höheren Grad an Regulierung als etwa im gewöhnlichen Handel;[1372] zahlreiche Branchen können als „kritische Infrastrukturen" bezeichnet werden, bei denen sich entsprechende IT-Fehler oder IT-Sicherheitslücken besonders gravierend auswirken können.[1373] Zu unterscheiden sind zudem tätigkeits- bzw. dienstleistungsbezogene Anforderungen einerseits und organisationsbezogene Anforderungen andererseits.

(a) Die Gewährleistung einer Basissicherheit (IT-Riskmanagement)

778 Kann man daher zwischen einer Art **Basissicherheit** und **weitergehenden, segment- oder tätigkeitsspezifischen Anforderungen** unterscheiden, stellt sich die Frage, ob die existierenden, für alle Branchen geltenden Anforderungen ausreichend Anreize für die Gewährleistung der IT-Sicherheit bieten. Wie oben (Teil I Rn. 333 ff.) dargelegt, finden sich im wesentlichen in zwei Rechtsgebieten übergreifende Anforderungen an die IT-Sicherheit: zum einen gesellschaftsrechtlich durch die Pflicht zum IT-Riskmanagement, über § 91 II AktG, die als generelles Element der Geschäftsführungs- und Organisationspflichten rechtsformunabhängig bezeichnet werden kann, mithin auch über die AG für die GmbH, OHG, KG etc. bis hin zu der für jeden Kaufmann geltenden Sorgfaltspflicht gelten kann. Zum anderen greifen die in § 9 BDSG normierten Organisationspflichten für alle Unternehmen ein (Teil I Rn. 409 ff.), die in irgendeiner Weise personenbezogene Dateien natürlicher Personen verarbeiten, so dass sich de facto auch hier ein fast alle Branchen überspannendes Pflichtenprogramm zur IT-Sicherheit ergäbe.

[1371] S. dazu oben Teil 1 Rn. 404 ff.

[1372] Wobei natürlich auch hier etwa Lebensmittel- oder Pharmaprodukte ein anderes Gefahrenpotential als sonstige Produkte aufweisen – was sich wiederum in besonderen Regulierungen niederschlägt, sei es im LebensmittelG oder im ApothekenG.

[1373] S. dazu *Holznagel/Koenig*, Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, 2002, abrufbar unter http://www.bsi.bund.de/fachthem/kritis/Regelungsumfang_ITSich_KRITIS.pdf.

779 Die bereits in Teil 1 Rn. 742 aufgeführten **gravierende Defizite** seien hier noch einmal ins Gedächtnis gerufen:

780 Für den **gesellschaftsrechtlichen Bereich** beschränken sich die Anforderungen auf rein interne, also im Verhältnis von Geschäftsführer zur Gesellschaft, wirkende Pflichten – eine Außenwirkung gegenüber Dritten kommt ihnen in der Regel gerade nicht zu. Damit hängt die Effektivität derartiger Pflichten entscheidend von der Wirkungsweise der Corporate Governance ab; ohne dies hier vertiefen zu können, mag der Hinweis genügen, dass gerade die Effektuierung der intern wirkenden Geschäftsführungspflichten eines der zentralen Probleme des Gesellschaftsrechts darstellt[1374] und keineswegs gesichert ist, dass über Klagemöglichkeiten von Aktionären, Insolvenzverwaltern etc. genügend Anreize bestehen, dass etwa IT-Sicherheitspflichten stets erfüllt werden. Hinzu kommt, dass diese Pflichten rechtsformspezifisch sind, mithin aufgrund des gesellschaftsrechtlichen Ansatzes kaum für ausländische Rechtsformen mit Sitz in Deutschland, etwa die englische Limited greifen können.[1375]

781 Andere Defizite weist schließlich der Ansatz über **§ 9 BDSG** auf: Denn die Pflichten des § 9 BDSG beziehen sich nur auf den vom BDSG intendierten Schutz der personenbezogenen Daten natürlicher Personen, mithin nicht auf andere Daten, etwa von juristischen Personen, ebenso wenig auf den Schutz von Daten und Rechtsgütern Dritter, wie anderer Internetteilnehmer, da deren Daten nicht von dem Unternehmen verarbeitet werden[1376]. Ob zudem die von § 9 BDSG normierten Pflichten überhaupt im zivilrechtlichen Sinne (§ 823 II BGB) dem Individualschutz dienen, ist zudem höchst strittig.[1377] Mithin ergeben sich bildlich gesprochen zwar erhebliche Schnittmengen zwischen IT-Sicherheitsanforderungen und den Organisationspflichten und technischen Schutzmaßnahmen nach § 9 BDSG – sie sind jedoch keineswegs kongruent.

782 **Drittbezogene Pflichten** ergeben sich zwar aus den allgemeinen deliktsrechtlichen Grundsätzen, wie sie oben dargelegt wurden.[1378] Allerdings liegen dann auch wiederum – vergleichbar der Rechtslage bei Herstellern – alle entsprechenden Einschränkungen

[1374] S. etwa für die parallele Frage des Gläubigerschutzes und der rechtzeitigen Stellung eines Insolvenzantrages *Spindler*, JZ 2006, 839 ff. mwNachw.

[1375] Im Gefolge der Rechtsprechung des EuGH müssen Rechtsformen anderer Mitgliedstaaten im Inland anerkannt werden, ihr Organisations- und Gesellschaftsrecht richtet sich nach dem Recht am Gründungsort, EuGH, NJW 2003, 3331 – Inspire Art; EuGH, NJW 2002, 3614 ff. - Überseering. Näher dazu *Spindler/Berner*, RIW 2003, 949 ff.; *Spindler/Berner*, RIW 2004, 7 ff.; *Ebke*, EBLR 2005, 9 ff.

[1376] S. oben Teil 1 Rn. 412.

[1377] S. oben Teil 1 Rn. 434.

[1378] Teil 1 Rn. 417.

auf der Hand, allen voran die Einschränkung des Schutzes auf bestimmte Rechtsgüter, die gerade volkswirtschaftlich besonders relevante Schäden, wie Betriebsausfallschäden, nicht unbedingt erfassen.[1379] Selbst für besonders sensible Branchen wie das Kreditgewerbe wirken entsprechende IT-Sicherheitspflichten, die z.B. in § 25a KWG niedergelegt sind, keineswegs gegenüber Dritten, da sie oftmals nicht als Schutzgesetz qualifiziert werden.[1380] Auch hier wirken damit die Anreize aus dem geltenden Recht gegenüber Dritten zur Einhaltung von bestimmten IT-Sicherheitspflichten nur sehr bedingt – ganz abgesehen von den Durchsetzungsproblemen entsprechender Ansprüche.[1381]

783 Fasst man diese Überlegungen zusammen, spricht viel dafür, **einen generell für gewerbliche Nutzer wirkenden Rechtsrahmen** zu schaffen, der diese zur Einführung und Unterhaltung einer sicheren IT-Organisation und IT-Struktur verpflichtet – mit gleichzeitiger Wirkung gegenüber Dritten und unter Umfassung der IT-relevanten Schäden. Als ein solcher Ansatz bietet sich die Schaffung eines IT-Anlagensicherheitsgesetzes oder die Aufnahme einer entsprechenden Norm in der für alle Gewerbetreibenden Gewerbeordnung (GewO) an. Ein solcher Ansatz hätte den Vorteil, dass grundlegende Anforderungen an die IT-Sicherheit festgelegt werden könnten, die als öffentlich-rechtliche Pflichten durchgesetzt werden können; gleichzeitig können derartige Pflichten als Schutzgesetz über § 823 II BGB auch Ansprüche Dritter begründen, so dass auch deren IT-spezifische Schäden – anders als bei § 823 I BGB – erfasst werden könnten. Die verfahrensrechtliche Probleme des Kausalitätsnachweises ebenso wie der sicheren IT-Struktur könnten ähnlich den Regelungen in § 6 UmweltHG bewältigt werden: Für Anlagen, die nicht einem Gütesiegel entsprechen bzw. nicht den Anforderungen der Basissicherheit entsprechen, greift eine widerlegliche Vermutung ein, dass die Gefahr und damit auch die Schadensverursachung von ihr ausging. Umgekehrt könnte dem Geschädigten der Nachweis der Kausalität ebenso wie der unsicheren IT-Struktur aufgebürdet werden, wenn die Anlage entsprechenden Basisanforderungen an die IT-Sicherheit, formuliert durch Standards nach dem IT-AnlagensicherheitsG, entspricht (s. auch oben Rn. 759).

[1379] Teil 1 Rn. 412.

[1380] Teil 1 Rn. 446.

[1381] Schon allein der Nachweis der Kausalität eines Angriffs, ausgehend von einem unsicheren IT-Netz bzw. IT-Anlagen eines Unternehmens, und die Information über dessen IT-Sicherheitsorganisationsstrukturen und Defizite erscheint außerordentlich problematisch; hier müsste wiederum mit Regeln über die Darlegungs- und Beweislastverteilung gearbeitet werden.

784 Dies schließt nicht aus, für bestimmte Branchen **weitergehende Anforderungen** zu formulieren, etwa im KWG. Sicherzustellen wäre indes auch hier die Verzahnung der weitergehenden Pflichten mit den in einem breitflächigen IT-SicherheitsG zu formulierenden Sicherungspflichten, etwa in Gestalt von Verfahrensregelungen, die die Beachtung eines IT-SicherheitsG auch im Rahmen der spezifischen Vorgaben eines Sektors sicherstellen (z.B. im KWG durch das Erfordernis der Einhaltung aller öffentlich-rechtlichen Regelungen).

(b) Tätigkeitsbezogene Anforderungen

785 Wie im Teil 1 Rn. 280 ff., 742 bereits festgestellt, sind zwar im Grunde zivilrechtliche Regelungen in der Lage, im Rahmen der allgemeinen Tatbestände wie der im Verkehr erforderlichen und üblichen Sorgfalt den **IT-Dienstleistern**/Nutzern Pflichten zur Einhaltung einer Mindestsicherheit aufzuerlegen, etwa im **Online-Banking**. Doch fehlt es in der Praxis häufig an entsprechenden allgemeinen Standards sowie an deren Durchsetzung. Allein den Zivilgerichten die Entwicklung und Durchsetzung allgemeiner Standards zu überlassen, würde daher zu Ineffizienzen führen, da allenfalls mit punktuellen und tendenziell zu spät kommenden Reaktionen durch die Justiz zu rechnen ist; die Anreize für Kunden von IT-Dienstleistern und ihre Ressourcen sind zu gering, um die bestehenden Informationsungleichgewichte zu überwinden.

786 Erforderlich sind daher auch hier **öffentlich-rechtliche Flankierungen** durch die Entwicklung von allgemeinen Standards für bestimmte IT-Dienstleistungen, wie dem **Online-Banking**. Derartige Standards, wie etwa Verschlüsselungsnormen, würden nicht nur öffentlich-rechtlich über Produktsicherheits- oder spezielle segmentspezifische Ermächtigungsgrundlagen (z.B. KWG) durchgesetzt werden können, sondern würden sich – vergleichbar z.B. den Regelungen im WpHG – auch im Vertragsrecht auswirken, indem sie einen wesentlichen Hinweis auf die Pflichten der IT-Dienstleister im Rahmen der Konkretisierung der Nebenpflichten und der im Verkehr erforderlichen Sorgfalt nach § 276 BGB gäben.

787 Neben den öffentlich-rechtlichen, aber auch zivilrechtlich sich auswirkenden Regulierungen einer Basis-IT-Sicherheit können weitere Anreize durch **flankierende Maßnahmen durch Vermutungswirkungen bei Einhaltung von Standards** in Betracht. Wie oben bereits im Rahmen des Online-Banking dargelegt, hängt die Zuerkennung eines Anscheinsbeweises von der Annahme eines Erfahrungssatzes ab, der wiederum auf

technische Sicherheitsvorkehrungen rekurriert.[1382] Daher würde es einen zusätzlichen Anreiz für Unternehmen bedeuten, die auf den Austausch von Erklärungen, Dokumenten etc. im Rahmen ihrer Kommunikation aufbauen, wenn sie bei Einhaltung eines bestimmten IT-Standards, was gegebenenfalls auch zertifiziert sein könnte, in den Genuss eines Anscheinsbeweises kämen (dazu Rn. 891 ff.).

(3) Private Nutzer

788 In ähnlicher Weise erhebt sich für private Nutzer die Frage, ob und in welcher Weise die Anreize für sie verstärkt werden könnten, IT-Sicherungsmaßnahmen zu ergreifen. Derzeit sind diese für private IT-Nutzer eher schwach ausgeprägt, da sie kaum Sanktionen befürchten müssen, wenn ihre Rechner selbst zur Verbreitung von schadhafter Software beitragen – zumindest wenn sie nicht über besonderes Wissen im Umgang mit IT-Risiken verfügen.[1383] Da zudem die bereits oben angesprochenen Hemmnisse einer Geltendmachung von Ersatzansprüchen (Teil 1 Rn. 108 ff. sowie Rn. 172) auch hier eingreifen (grundsätzlich keine Vermögensschäden, Probleme des Kausalitätsnachweises etc.) ist die von Haftungsmechanismen ausgehende Anreizwirkung gering.

789 Daher spräche auf den ersten Blick einiges für die Verstärkung der Anreize für private Nutzer, die durch mehrere Maßnahmen erreicht werden könnte, sei es durch eine Verschärfung der Haftung, analog zu den oben für die gewerblichen Nutzer beschriebenen Haftungstatbestände, sei es durch andere öffentlich-rechtliche Maßnahmen, etwa durch einen Zwang zur Ablegung von Prüfungen bevor ein Internet-Anschluss benutzt werden darf („Internet-Führerschein“).

790 Hier sind allerdings gegenläufige Faktoren zu berücksichtigen: Eine größere Haftung für Private (ebenso wie andere Schranken, z.B. vorherige Schulungen oder Genehmigungen) verringert grundsätzlich ihre Bereitschaft (ihr Aktivitätsniveau), sich am Internet zu beteiligen und hemmt somit tendenziell die Kommunikation und den Durchfluss von Informationen – die Durchdringung der Gesellschaft mit den Neuen Medien wird aber allseits für ein gesellschafts- und wirtschaftspolitisches erstrebenswertes Ziel erachtet. Gegen entsprechende „Führerscheine“ spricht auch die Überlegung, dass im Gegensatz etwa zum Straßenverkehr die Sicherheitsanforderungen und die Gefahrenszenarien sich im IT-Bereich ständig ändern, so dass entweder eine ständige Nachschulung erforderlich wäre oder man sehenden Auges die schnelle Überholung einer solchen IT-

1382 Teil 1 Rn. 573.

1383 S. oben Teil 1 Rn. 283.

Grundausbildung in Kauf nehmen müsste. Ob daher die (gesellschaftlichen) Kosten den Nutzen eines solchen Führerscheins ausgleichen oder übersteigen würden, kann hier nicht abschließend beurteilt werden.

d) Zusammenfassung

791 Fasst man die obigen Überlegungen schlagwortartig zusammen, ergibt sich folgendes Bild:

- Für Hersteller sollten die Produktsicherheitsregulierung auf gravierende Vermögensschäden ausgedehnt werden, verbunden mit der Möglichkeit, Produktsicherheitsstandards für IT-Produkte zu schaffen
- Für IT-Intermediäre sollte das Recht der Haftungsprivilegierungen für die Sicherungspflichten aus dem Telekommunikationsrecht herausgelöst und in das Recht der allgemeinen AGB-Inhaltskontrolle überführt werden
- Für gewerbliche Nutzer sollten Regelungen für eine IT-Basissicherheit in einem besonderen IT-SicherheitsG, hilfsweise in der GewO, geschaffen werden, wiederum mit der Möglichkeit, bestimmte Standards zu entwickeln; flankierend können an die Einhaltung bestimmter Standards prozessuale Vermutungswirkungen geknüpft werden. Darüber hinaus sollten diejenigen kommerziellen IT-Nutzer, die ihrerseits IT-Dienstleistungen erbringen, ebenfalls bestimmten allgemeinen technischen Sicherheitsstandards unterworfen werden.
- Für private IT-Nutzer empfehlen sich dagegen keine besonderen Regelungen, da nicht anzunehmen ist, dass sie die entsprechenden Gefahrenquellen beherrschen können.

II. Die Standardsetzung

792 Die oben im Ansatz beschriebenen rechtlichen Regulierungen hängen in ihrer Wirksamkeit maßgeblich davon ab, dass entsprechende Standards formuliert und mit rechtlicher Wirkung versehen werden. Andernfalls wären die abstrakten Pflichten mangels entsprechender Konkretisierung ohne ständige Hinzuziehung externer Sachverständiger kaum durchsetzbar. Das technische Sicherheitsrecht kommt oftmals nicht umhin, die geforderte Sicherheit mit unbestimmten Rechtsbegriffen wie beispielsweise „anerkannte Regeln der Technik“ usw., „Stand der Technik“ und „Stand von Wissenschaft und Technik“ zu umschreiben.[1384] In diesem Zusammenhang können technische Standards zur Konkretisierung dieser abstrakten Begriffe beitragen und damit insbesondere für die unternehmerische Praxis handhabbar machen. Wegen der Dauer der entsprechenden förmlichen Normsetzungs- und –änderungsverfahren können Standards von vornherein nicht auf **gesetzlicher Ebene** – und nur unter erheblichen Schwierigkeiten durch **Rechtsverordnungen** – festgesetzt werden.

[1384] Ausführlich zur Abgrenzung *Marburger*, Die Regeln der Technik im Recht, 1979, S. 145 ff., 158 ff., 164 ff..

793 Im Technikrecht haben sich zur Erarbeitung von technischen Standards daher die im folgenden näher zu erörternden **Verfahren kooperativer Regelsetzung** herausgebildet.[1385] Die Verfahren sind durch eine Zusammenarbeit staatlicher Stellen und privater sachverständiger Gremien gekennzeichnet. Im Einzelnen ergeben sich Unterschiede vor allem im Hinblick auf die Intensität der staatlichen Beteiligung und Einflussnahme sowie im Umfang der Wirkung der Standards. Zu unterscheiden sind danach:

- Normkonkretisierende (standardisierende) Verwaltungsvorschriften (unten 2.a))
- Halbstaatliche Standardsetzungen durch Normenausschüsse (unten 2.b))
- Private Standardsetzung durch Normungsorganisationen – sei es auf nationaler[1386], sei es auf internationaler Ebene[1387] –, wobei zwischen Standards mit und solchen ohne amtliche Einführung zu unterscheiden ist (unten 2.c))

794 Gegen jede der genannten Formen kooperativer Regelsetzung werden **rechtliche Bedenken** im Hinblick auf eine Überrepräsentation wirtschaftlicher Interessen, unzureichende Beteiligung der Öffentlichkeit, Intransparenz des Normungsverfahrens sowie unzulässiger Delegation von Normsetzungsbefugnissen auf demokratisch nicht legitimierte Gremien vorgebracht. Hierbei handelt es sich indes um ein seit langem bekanntes Problem, welches hier nur angedeutet, nicht aber vertieft oder gar geklärt werden kann.[1388]

795 Bevor auf die verschiedenen Muster kooperativer Standardsetzung und ihre rechtlichen Wirkungen näher eingegangen wird, gilt es sich Klarheit über die Ziele und Anforderungen an untergesetzliche Standardisierungen zu verschaffen:

1. Anforderungen an eine Standardsetzung

796 Da IT-Produkte, Dienstleistungen ebenso wie Standards grundsätzlich grenzüberschreitenden Charakter tragen, ist eine möglichst hohe Akzeptanz auf europäischer und internationaler Ebene wünschenswert. Nationale Insellösungen sind kaum erfolgversprechend.

- Standards sollten im Idealfall schnell entwickelt, aber doch breit konsentiert werden, um auch außerhalb des eigentlich rechtlichen Vollzugs durchsetzbar zu sein. Anders formuliert können Standards, die sich gegen eine breite Überzeugung in Anwenderkreisen richten, nur mit Mühe und unter hohen Enforcement-Kosten durchgesetzt werden.

[1385] Ausführlich *Lamb*, Kooperative Gesetzeskonkretisierung, 1995.

[1386] Z.B. DIN.

[1387] Z.B. CEN, CENELEC, ETSI, ISO.

[1388] Eingehend *Kloepfer*, in: Schulte, Handbuch des Technikrechts, 2002, S. 143 ff.; *Röthel*, Technische Regeln im Umwelt- und Technikrecht, UTR Band 86, 2006, S. 33 (50 ff.).

- Standards und die Verfahren zu ihrer Setzung müssen in der Lage sein, weitere Konkretisierungen und Anpassungen zu erlauben. Eine gewisse Offenheit und Fähigkeit der Weiterentwicklung, z.B. durch zusätzliche, segmentspezifische Standards muß gewährleistet sein.
- Standards sollten ferner in ihrer rechtlichen Wirkung zwar Rechtssicherheit für Anwender erzeugen, nicht aber die Entwicklung neuer und gegebenenfalls besserer Konzeptionen verhindern bzw. ausschließen. Die Anreizwirkung solcher Standards darf nicht zur Verringerung von Innovationsbemühungen führen. Die Anwendung von Standards muss daher freiwillig bleiben.
- Standards sollten möglichst nicht rechtsgebietsspezifisch formuliert sein, sondern vielmehr rechtsgebietsübergreifend wirken können. Anders gewendet sollten Standards nicht nur im öffentlichen Recht Wirkung entfalten, sondern auch zivilrechtlich fruchtbar gemacht werden können. Andererseits können und sollten in bestimmten Fällen Standards branchen- bzw. segmentspezifisch ausgestaltet sein, um den Besonderheiten bestimmter IT-Sicherheitsrisiken gerecht zu werden.
- Die Verfahren zur Standardsetzung sollten transparent und offen für die Beteiligung interessierter Gruppen sein, einschließlich der Beteiligung des Staates – zusätzliche staatliche Akzeptanz- bzw. Rezeptionsakte können ratsam sein, um verfassungsrechtlichen Anforderungen zu genügen.

2. Regelungsmodelle für die Standardsetzung

a) Normkonkretisierende (standardisierende) Verwaltungsvorschriften

797 Die wohl weitestgehende Bindung von Standards, welche nicht auf gesetzlicher oder auf Verordnungsebene formuliert werden, entfalten derzeit die sog. **Technischen Anleitungen** (TA)[1389], deren Aufstellung in den staatlichen Aufgabenbereich fällt. Auf der Grundlage des § 48 BImSchG werden sie im Rahmen eines konkret vorgegebenen Verfahrens nach Anhörung der beteiligten Kreise (§ 51 BImSchG)[1390] von der Bundesregierung mit Zustimmung des Bundesrates als **Verwaltungsvorschriften** erlassen. Während TAs zunächst antizipierte Sachverständigengutachten gewertet wurden,[1391] spricht man heute überwiegend davon, die Verwaltung habe einen Standardisierungsspielraum.[1392] Da die technischen Anleitungen in einem geordneten Verfahren unter Beteiligung der Betroffenen und sachverständiger Kreise aufgestellt werden, wird ihnen von der Rechtsprechung eine **normkonkretisierende Wirkung** beigemessen, etwa für die Bestimmung von zulässigen Grenzwerten für Emissionen oder Lärm.[1393] Die normkonkretisi-

[1389] Sechste Allgemeine Verwaltungsvorschrift zum Bundes-Immissionsschutzgesetz, Technische Anleitung zum Schutz gegen Lärm (TA Lärm) vom 26.8.1998, GMBl. S. 503; Erste Allgemeine Verwaltungsvorschrift zum Bundes-Immissionsschutzgesetz, Technische Anleitung zur Reinhaltung der Luft (TA Luft) vom 24.7.2002, GMBl. S. 511

[1390] Es handelt sich um einen auszuwählenden Kreis von Vertretern der Wissenschaft, der Betroffenen, der beteiligten Wirtschaft, des beteiligten Verkehrswesens und der für den Immissionsschutz zuständigen obersten Landesbehörden.

[1391] BVerwG, NJW 1978, 1450; OVG Berlin, NVwZ 1985, 759; OVG Nordrhein-Westphalen, NVwZ-RR 1989, 640.

[1392] OVG Nordrhein-Westphalen, NVwZ 1988, 173; *Breuer*, NVwZ 1988, 104 (110 ff.); *Jarass*, § 48 BImSchG Rn. 2, 45; *Hatje/Hansmersmann*, in: Kotulla, Bundes-Immissionsschutzgesezt, § 48 BImSchG Rn. 50.

[1393] BVerwG, NVwZ 2000, 440; BVerwG, NVwZ 2001, 1165; BVerwG, NVwZ-RR 1996, 499; BVerwGE 72, 300 (320); dazu ausführlich *Jarass*, § 48 BImSchG Rn. 43 ff.; *Hatje/Hansmersmann*, in: Kotulla, Bundes-Immissionsschutzgesezt, § 48 BImSchG Rn. 49 f.; *Spindler*, Unternehmensorganisationspflichten, 2001, S. 516 ff..

ernden Verwaltungsvorschriften sind daher – innerhalb bestimmter Grenzen[1394] – für Verwaltung und Gerichte bindend.[1395]

798 Zivilrechtlich haben derartig verabschiedete Standards gesetzliche Anerkennung in **§ 906 Abs. 1 Satz 3 BGB** gefunden, der für die Frage der Erheblichkeit von Immissionen die entsprechenden TAs für anwendbar erklärt. Durch den Verweis auf Verwaltungsvorschriften im Sinne des § 48 BImSchG wollte der Gesetzgeber die in ihrer Beurteilung unabhängigen Zivilgerichte an die Grenzwerte – insbesondere auch im Hinblick auf den Schutz öffentlicher Planungsvorhaben – binden und zugleich die Angleichung der öffentlich-rechtlichen und privatrechtlichen Standards im Immissionsschutz festschreiben, wie sie durch die Rechtsprechung des BGH und des BVerwG bereits vorgezeichnet war.[1396]

b) Halb-staatliche Standardsetzung: öffentlich-rechtliche technische Ausschüsse

799 Das Technikrecht kennt Mischformen halb-staatlich aufgestellter technischer Normen, welche von Sachverständigenausschüssen erarbeitet werden.[1397] Beispiele halbstaatlicher Standardsetzung bilden etwa die sog. KTA-Regeln des Kerntechnischen Ausschusses (KTA)[1398], die vom Ausschuss für Betriebssicherheit (ABS)[1399] ermittelten Technischen Regeln für Betriebssicherheit (TRBS).[1400]

800 Die Ausschüsse sind nicht in die Verwaltungshierarchie eingegliedert, doch verfügt die Verwaltung durch die Ernennung der Ausschussmitglieder, die Bestätigung der Geschäftsordnung des Ausschusses und ein Anwesenheits- und Anhörungsrecht über weit

---

[1394] *Jarass*, § 48 BImSchG Rn. 45, 49 ff.; *Hatje/Hansmersmann*, in: Kotulla, Bundes-Immissionsschutzgesezt, § 48 BImSchG Rn. 51 ff..

[1395] BVerwG, NVwZ 2000, 440; BVerwG, NVwZ 1995, 994; *Jarass*, § 48 BImSchG Rn. 45; *Hatje/Hansmersmann*, in: Kotulla, Bundes-Immissionsschutzgesezt, § 48 BImSchG Rn. 50..

[1396] Bamberger/Roth-*Fritzsche*, § 906 BGB Rn. 41.

[1397] *Kloepfer*, in: Schulte, Handbuch des Technikrechts, 2002, S. 138; *Lamb*, Kooperative Gestzeskonkretisierung, 1995, S. 97 ff.; *Spindler*, Unternehmensorganisationspflichten, 2001, S. 530 ff..

[1398] Bekanntmachung über Neufassung der Bekanntmachung über die Bildung eines Kerntechnischen Ausschusses vom 20.7.1990, abrufbar unter http://www.kta-gs.de/.

[1399] § 24 Verordnung über Sicherheit und Gesundheitsschutz bei der Bereitstellung von Arbeitsmitteln und deren Benutzung bei der Arbeit, über Sicherheit beim Betrieb überwachungsbedürftiger Anlagen und über die Organisation des betrieblichen Arbeitsschutzes (Betriebssicherheitsverordnung - BetrSichV) vom 27.9.2002, zuletzt geändert durch Art. 439 Neunte ZuständigkeitsanpassungsVO vom 31. 10. 2006 (BGBl. I S. 2407), BGBl. I S. 3777. Die BetrSichV löst die bisherigen Verordnungen zum Betrieb überwachungsbedürftiger Anlagen wie z.B. Aufzugsverordnung, Dampfkesselverordnung usw. ab, s. zur alten Rechtslage *Peine*, § 11 GSG Rn. 9 ff..

[1400] Abrufbar unter http://www.baua.de/de/Themen-von-A-Z/Anlagen-und-Betriebssicherheit/TRBS/TRBS.html__nnn=true.

reichende Einflussmöglichkeiten.[1401] Im Unterschied zur Normsetzung durch die Exekutive liegt die Initiative zur Einleitung eines Normsetzungsverfahrens im Rahmen der halbstaatlichen Standardsetzung bei den betreffenden Sachverständigengremien. Anders als bei der noch zu erörternden privaten Standardsetzung ist die Normung im halbstaatlichen Bereich von vornherein auf eine staatliche Übernahme hin ausgerichtet. Die Ausschüsse erarbeiten Normen gerade im Hinblick auf die Konkretisierung der gesetzlichen Sicherheitsanforderungen.[1402] Mit Veröffentlichung der Standards in den einschlägigen Amtsblättern gelten die aufgestellten Standards als „amtlich eingeführt".[1403]

801 Der KTA hat die Aufgabe, auf Gebieten der Kerntechnik für die Aufstellung sicherheitstechnischer Regeln zu sorgen und deren Anwendung zu fördern.[1404] Mitglieder sind Vertreter der Hersteller und Betreiber von Atomanlagen, für den Vollzug des AtG zuständige Behörden des Bundes und der Länder, sowie Gutachter und Beratungsorganisationen. Der ABS wird aus sachverständigen Mitgliedern der öffentlichen und privaten Arbeitgeber, der Länderbehörden, der Gewerkschaften, der Träger der gesetzlichen Unfallversicherung, der Wissenschaft und der zugelassenen Stellen gebildet (§ 24 Abs. 1 BetrSichV).[1405]

802 Ebenso wie privaten Standards kommt den Regelwerken technischer Ausschüsse keine Rechtsnormqualität und damit trotz amtlicher Einführung keine rechtliche Verbindlichkeit zu.[1406] Im Gegensatz zu den technischen Anleitungen im Immissionsschutzrecht ist den halbstaatlichen Regelwerken auch die Qualität von normkonkretisierenden Verwaltungsvorschriften bislang versagt geblieben;[1407] grundsätzlich wird nur eine **Indizwirkung** angenommen.[1408] Jedoch kommt beispielsweise den vom Ausschuss für Betriebs-

[1401] *Lamb*, Kooperative Gesetzeskonkretisierung, 1995, S. 97. Siehe beispielsweise für den Ausschluss für technische Arbeitmittel und Verbraucherprodukte (AtAV) § 13 Abs. 3, 4 GPSG, für den Ausschuss für Betriebssicherheit § 24 Abs. 3, 6 BetrSichV.

[1402] *Lamb*, Kooperative Gesetzeskonkretisierung, 1995, S. 106.

[1403] *Kloepfer*, in: Schulte, Handbuch des Technikrechts, 2002, S. 138; *Lamb*, Kooperative Gesetzeskonkretisierung, 1995, S. 97.

[1404] § 2 der Bekanntmachung über Neufassung der Bekanntmachung über die Bildung eines Kerntechnischen Ausschusses vom 20.7.1990.

[1405] Ein Mitgliederverzeichnis ist abrufbar unter http://www.baua.de/nn_12052/de/Themen-von-A-Z/Anlagen-und-Betriebssicherheit/ABS/Ueber-den-ABS/Mitgliederverzeichnis-ABS.pdf.

[1406] Siehe dazu BMU, Umweltgesetzbuch (UGB-KomE), 1998, S. 493; für Normen des Ausschusses für Betriebssicherheit *Kohte*, Technische Regeln im Umwelt- und Technikrecht, UTR Band 86, 2006, S. 142.

[1407] *Spindler*, Unternehmensorganisationspflichten, S. 50 f., 531; *Jarass*, in: Lukes (Hrsg.), Reformüberlegungen zum Atomrecht, 1991, S. 367 (428 ff.); *Vieweg*, Atomrecht und technische Normung, 1982, S. 150 ff., 159 f..

[1408] BVerwG, NVwZ 1989, 1145 (1146) (zu Empfehlungen der Reaktorsicherheitskommission); *Jarass*, in: Lukes (Hrsg.), Reformüberlegungen zum Atomrecht, 1991, S. 367 (403); BMU, Umweltgesetzbuch (UGB-KomE), 1998, S. 493; *Spindler*, Unternehmensorganisationspflichten, 2001, S. 532. Nach BVerwG, DVBl. 1993, 1149 (1150 f.) soll bei Regeln der

sicherheit ermittelten und bekannt gemachten[1409] Regeln aufgrund § 24 Abs. 5 Satz 2 BetrSichV eine **Vermutungswirkung** dahingehend zu, dass bei Einhaltung dieser Regeln die normierten Sicherheitsanforderungen erfüllt sind, wodurch die Bedeutung der Normung erheblich gesteigert wird.

803 Eine etwas andere Funktion nimmt der **Ausschuss für technische Arbeitsmittel und Verbraucherprodukte (AtAV)** ein, dem durch das GPSG eine „Regelungsermittlungsfunktion" zugewiesen wurde.[1410] Der AtAV erarbeitet keine eigenen Regelwerke, sondern sichtet nur vorhandene Regelwerke und trifft eine Auswahl.[1411]

c) Private Standardsetzung: privatrechtliche Normungsorganisationen

804 Neben den Verwaltungsvorschriften und den Regelwerken halbstaatlicher Sachverständigengremien spielen vor allem private Normungsorganisationen eine herausragende Rolle bei der Erarbeitung von technischen Standards.[1412] Auf nationaler Ebene sind dies beispielsweise DIN, VDI und VDE, auf europäischer und internationaler Ebene CEN, CENELEC, ETSI oder ISO. Die Normsetzung ist im Unterschied zur halbstaatlichen Verfahren der Standardsetzung nicht von vornherein auf staatliche Anerkennung gerichtet,[1413] doch erfahren die technischen Regelwerke privater Normungsorganisationen in der Praxis eine überaus große Bedeutung bei der Konkretisierung unbestimmter Rechtsbegriffe die „anerkannte Regeln der Technik" usw.[1414] Zur zivilrechtlichen Bedeutung bereits ausführlich Teil 1 Rn. 143 f.

(1) Standards ohne amtliche Einführung, insbesondere DIN-Normen

805 Das Verfahren der Normsetzung durch private Normungsorganisationen ist gesetzlich nicht geregelt. Die Beziehung zwischen dem DIN – als der bedeutendsten deutschen Normungsorganisation – und der Bundesrepublik Deutschland wurde 1975 auf eine ver-

kerntechnischen Gremien zumindest eine Vermutung für die Wiedergabe des Standes von Wissenschaft und Technik bestehen. Ohne jeden Anhaltspunkt für abweichende Auffassungen in Wissenschaft und Technik bestehe für die Behörden keine Veranlassung die sicherheitstechnischen Ermittlungen durch Beauftragung von Sachverständigen von vorn zu beginnen.

[1409] Normen des Ausschusses für Betriebssicherheit können vom Bundesministerium für Arbeit und Soziales (BMAS) im Bundesarbeitsblatt (§ 24 Abs. 5 Satz 1 BetrSichV) bekannt gemacht werden.

[1410] Siehe dazu Teil 1 Rn. 246.

[1411] *Klindt*, § 13 GPSG Rn. 5.

[1412] Dazu *Lamb*, Kooperative Gesetzeskonkretisierung, 1995, S. 72 ff.; *Kloepfer*, in: Schulte, Handbuch des Technikrechts, 2002, S. 138 ff.; *Spindler*, Unternehmensorganisationspflichten, 2001, S. 533 ff..

[1413] *Kloepfer*, in: Schulte, Handbuch des Technikrechts, 2002, S. 138.

[1414] *Lamb*, Kooperative Gesetzeskonkretisierung, 1995, S. 72; *Kloepfer*, in: Schulte, Handbuch des Technikrechts, 2002, S. 138.

tragliche Grundlage gestellt.[1415] Darin werden unter anderem allgemein die Berücksichtigung öffentlicher Interessen bei der Normung (§ 1 Abs. 2)[1416], die Beteiligung staatlicher Stellen (§ 2), die Verpflichtung des DIN zur Einhaltung eines bestimmten Verfahrens (Einhaltung der DIN 820 und der „Richtlinie für Normungsausschüsse", § 3), die bevorzugte Bearbeitung staatlicher Normungsaufträge (§ 4), sowie die Vertretung deutscher Interessen in den europäischen und internationalen Normungsorganisationen (§ 6) durch das DIN geregelt. Andere Normungsorganisationen werden durch diesen Vertrag nicht gebunden.

806 Eine DIN Normung kann von jedermann beantragt werden. Im betreffenden Normenausschuss erarbeiten fachkundige Vertreter der interessierten Kreise einen Norm-Entwurf, welcher anschließend veröffentlicht wird. Externe Experten und die Öffentlichkeit können innerhalb von vier Monaten zu dem Entwurf Stellung nehmen. In Streitfällen steht ein Schlichtungsverfahren zur Verfügung. Die endgültige Fassung wird vom DIN als DIN-Norm veröffentlicht. Spätestens alle fünf Jahre werden die Normen einer Überprüfung unterzogen.

807 Technische Regeln privater Normungsorgane sind rein private Festlegungen, welchen **keine Rechtsnormqualität** zukommt;[1417] auch der Vertrag zwischen dem DIN und der Bundesrepublik hat daran nichts geändert. Sie bleiben auf freiwillige Einhaltung angelegte bloße Empfehlungen der Normungsverbände. Anders als die Normen technischer Ausschüsse sind die Normen privater Normungsorganisationen nicht von vornherein auf eine amtliche Einführung gerichtet. Ebenso wenig sind sie daraufhin ausgelegt, gesetzliche Bestimmungen zu konkretisieren; auch wenn nach DIN 820 gesetzliche Vorgaben beachtet werden sollen, ist nicht davon auszugehen, dass DIN-Normen das gesetzlich geforderte Sicherheitsniveau in jedem Fall erfüllen.[1418] Im Unterschied zu normkonkretisierenden Verwaltungsvorschriften[1419] sind die technischen Regelwerke folglich **we-**

[1415] Vertrag zwischen der Bundesrepublik Deutschland, vertreten durch den Bundesminister für Wirtschaft und dem DIN Deutsches Institut für Normung e. V., vertreten durch dessen Präsidenten, vom 5.6.1975, Beilage zum BAnz. Nr. 114 vom 27.6.1975.

[1416] Beispiele: Sicherheitstechnik, Gesundheits-, Umwelt- und Verbraucherschutz, gesamtwirtschaftliche und arbeitswirtschaftliche Interessen, Bedeutung der Norm für die Verwaltung und das öffentliche Beschaffungswesen, Erläuterungen Vertrag zwischen der Bundesrepublik Deutschland und dem DIN Deutsches Institut für Normung e.V., Beilage zum BAnz. Nr. 114 vom 27.6.1975, S. 25.

[1417] *Jarass*, NJW 1987, 721 (726); *Roßnagel*, in: Koch/Scheuing, § 22 BImSchG Rn. 86.

[1418] *Lamb*, Kooperative Gesetzskonkretisierung, 1995, S. 86 f..

[1419] Dazu oben Rn. 797.

der für Verwaltung und Gerichte, noch für Private rechtlich bindend,[1420] auch wenn ihnen aufgrund des Sachverstands der erarbeitenden Institutionen eine Indizwirkung zukommen kann.[1421] Für Unternehmen bestehen in jedem Fall große Anreize, entsprechende Standards einzuhalten, aber auch sich an deren Erstellung zu beteiligen – was aus ökonomischer Sicht die von der public-choice-Theorie[1422] oftmals beschriebenen Probleme des „Interest-capture“ [1423] von Regulierungsstellen hervorruft.

(2) Standards mit amtlicher Einführung

808 Die ohnehin große praktische Bedeutung privater Standards wird nochmals erhöht durch die amtliche Einführung im Wege der **öffentlichen Bekanntmachung** der Standards, wie sie vor allem im Rahmen des „New Approach“[1424] auf europäischer Ebene praktiziert wird. Die Normungsarbeit der europäischen Normungsorganisationen CEN, CENELEC und ETSI erfolgt seit 1985 auf Grundlage der „Allgemeinen Leitlinien für die Zusammenarbeit“.[1425] Die Kommission erteilt nach Anhörung der zuständigen Stellen in den Mitgliedsstaaten Normungsaufträge an die europäischen Normungsorganisationen, welche ein Normungsverfahren durchführen.[1426] Die Fundstellen der harmonisierten Normen werden nach Übermittlung durch die Normungsorganisationen von der Kommission im Amtsblatt veröffentlicht. Bevor die Kommission die Fundstelle veröffentlicht, kann sie überprüfen, ob die Anforderungen des Normungsauftrags erfüllt sind,[1427] was jedoch nur im Ausnahmefall geschieht.[1428] Die nationalen Normungsorga-

---

[1420] *Reiff*, Technische Regeln im Umwelt- und Technikrecht, UTR Band 86, 2006, S. 159; *Jarass*, § 48 BimSchG Rn. 62.

[1421] BVerwG, NJW 1988, 2396 (2397); *Hagen*, NVwZ 1991, 817 (819 f.); *Jarass*, NJW 1987, 721 (726) (Richtwert); *Roßnagel*, in: Koch/Scheuing, § 22 BImSchG Rn. 87; *Jarass*, § 48 BImSchG Rn. 63. Zur zivilrechtlichen Bedeutung ausführlich Teil 1 Rn. 146 (Konkretisierung von Verkehrspflichten) und 174 (Beweis).

[1422] Begründet in *Buchanan, James M. / Tullock, Gordon*, The Calculus of Consent, Ann Arbor, 1962; vgl. auch *Gwartney, James D. / Stroup, Richard L.*, Economics: Private and Public Choice, 6. Aufl. 1992, Kapitel 4, 30; Posner, R., Theories of Economic Regulation, Bell Journal of Economics and Management Science, 5(2),1974, 335–358.

[1423] Vgl. *Stigler, George J.*, Theory of Economic Regulation, Bell Journal of Economics and Management Science 2 (Spring), 1971, 3-21. *Peltzman, S.*, Toward a More General Theory of Regulation, Journal of Law and Economics 19 (August), 1976, 211-40. *Becker, G.S.*, A Theory of Competition Among Pressure Groups for Political Influence, Quarterly Journal of Economics 98 (August), 1983, 371-400. *Levine, Michael E. / Forrence Jennifer L.*, Regulatory Capture, Public Interest, and the Public Agenda: Toward a Synthesis, Journal of Law, Economics, & Organization, Vol. 6, 1990, 167-198.

[1424] Dazu ausführlich unten Rn. 841 ff.

[1425] Allgemeine Leistlinien für die Zusammenarbeit zwischen CEN, CENELEC und ETSI sowie der Europäischen Kommission und der Europäischen Freihandelsgemeinschaft vom 28.3.2003, ABl. EG C 91, S. 7.

[1426] Zum Normungsverfahren ausführlich *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfaßten Richtlinien, 2000, S. 30 f.. abrufbar unter http://ec.europa.eu/enterprise/newapproach/legislation/guide/document/guidepublicde.pdf.

[1427] *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfaßten Richtlinien, 2000, S. 31.

[1428] Die Mitgliedsstaaten können gegen harmonisierte Normen nur im Schutzklauselverfahren der Richtlinien vorgehen, siehe dazu *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfaßten Richtlinien, 2000, S. 59 ff.

nisationen setzen die europäischen Normen in nationale Normen (DIN EN-Normen) um, deren Fundstellen von den Behörden der Mitgliedsstaaten veröffentlich werden.

809 Die besondere rechtliche Bedeutung der amtlich eingeführten harmonisierten Normen (s. § 2 Abs. 16 GPSG) zeigt sich in der **Vermutungswirkung**, welche in den Harmonisierungsrichtlinien bzw. § 4 Abs. 1 Satz 2 GPSG an ihre Einhaltung geknüpft wird (dazu ausführlich unten Rn. 883).[1429] Grundlage für die Annahme dass harmonisierte Normen die Sicherheitsanforderungen der Richtlinien wiedergeben bilden die Normungsaufträge der Kommission in Verbindung mit der Normaufstellung anhand der allgemeinen Leitlinien.[1430] Auch die harmonisierten Normen bleiben jedoch rechtlich unverbindlich.[1431] Die Normungsorganisationen tragen die Verantwortung dafür, dass die harmonisierten Normen den wesentlichen Sicherheitsanforderungen[1432] der europäischen Richtlinien entsprechen.[1433]

810 Außerhalb des Produktsicherheitsrechts ist diese Konzeption– auch auf europäischer Ebene – noch nicht fruchtbar gemacht worden, weder im Umweltrecht noch im sonstigen Anlagensicherheitsrecht.[1434] Doch sieht der **Entwurfs eines Umweltgesetzbuchs** der unabhängigen Sachverständigenkommission zum Umweltgesetzbuch beim Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit in §§ 32, 33 UGB-KomE eine Regelung zur amtlichen Einführung technischer Regelwerke durch öffentliche Bekanntmachung vor. Voraussetzung der Bekanntmachung ist danach die Einhaltung bestimmter Anforderungen im Hinblick auf Einhaltung der umweltrechtlichen Vorschriften, ausgewogene Zusammensetzung der erlassenden Stellen, Begründung, Fachöffentlichkeit des Verfahrens, Beteiligung der zuständigen obersten Bundesbehörden, Veröffentlichung und Zugänglichkeit (§ 32 Abs. 1 Satz 1 UGB-KomE). Es handelt

---

[1429] Zur Konformitätsvermutung siehe *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfaßten Richtlinien, 2000, S. 31 f.; Wilrich, § 4 GPSG Rn. 23 ff..

[1430] Siehe Anhang II zur Entschließung des Rates vom 7. Mai 1985 über eine neue Konzeption auf dem Gebiet der technischen Harmonisierung und der Normung, ABl. C 136 vom 4.6.1985, S. 1: „Damit dieses System funktioniert, müssen [...] die Normen Qualitätsgarantien hinsichtlich der in den Richtlinien aufgestellten " grundlegenden Anforderungen " bieten [...]. Die Güte der harmonisierten Normen muß durch Normungsaufträge sichergestellt werden, die von der Kommission vergeben werden und deren Ausführung den allgemeinen Leitlinien, die zwischen der Kommission und den europäischen Normeninstitutionen vereinbart worden sind, entsprechen muß."

[1431] *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfaßten Richtlinien, 2000, S. 30 f..

[1432] Dazu näher unten Rn. 843.

[1433] *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfaßten Richtlinien, 2000, S. 30; *Röthel*, Technische Regeln im Umwelt- und Technikrecht, UTR Band 86, 2006, S. 33 (43).

[1434] So enthalten weder die IPPC-Richtlinie (Integrated Prevention and Pollution Control) noch die Seveso II-Richtlinie einen Verweis auf private Sicherheitsstandards – obwohl dies angesichts der entsprechenden Normierungen im Umweltmanagementbereich der ISO 14.000 ff. nahe gelegen hätte.

sich um Kriterien, welche typischerweise auf eine Konformität der technischen Regelwerke mit dem normativen Standard des UBG-KomE schließen lassen, und die an amtlich eingeführte Regelwerke anknüpfende Vermutungswirkung des § 33 UGB-KomE rechtfertigen.[1435] Danach wird bei amtlich eingeführten Regelwerken vermutet, dass sie den Stand der Technik oder den Stand von Wissenschaft und Technik zutreffend wiedergeben. Im Falle des Entwurfs zu Umweltgesetzbuch sollte amtlich eingeführten Regelwerken gemäß § 32 Abs. 1 Satz 2 UGB-KomE zudem die Wirkung von allgemeinen Verwaltungsvorschriften zukommen.

811 Eine ähnliche Tendenz lässt sich im **Rechnungslegungsrecht** beobachten: Hier rezipieren sowohl die EU als auch Deutschland explizit Normen, die in einem rein privatrechtlichen Verfahren entwickelt und verabschiedet wurden, die International Finance Reporting Standards (IFRS), vormals IAS (International Accounting Standards).[1436] Abgeschwächter gegenüber dem Beispiel der Produktsicherheit werden auch hier die Normen einer Art staatlicher Akzeptanzprüfung unterworfen. Über die Anwendbarkeit internationaler Rechnungslegungsstandards in der EU beschließt gemäß Art. 3 Abs. 1 der Verordnung betreffend die Anwendung internationaler Rechnungslegungsstandards[1437] die EU-Kommission anhand der Vorgaben des Art. 3 Abs. 2[1438]; übernommene Rechnungslegungsstandards werden im Amtsblatt der EG veröffentlicht (Art. 3 Abs. 4). Umgekehrt entfalten diese Normen aber einen (noch) höheren Konkretisierungs- und Bindungsgrad als die harmonisierten Normen im Produktsicherheitsrecht: Während letzteren eine Vermutungswirkung beigemessen wird, sind die IFRS sogar rechtlich verbindlich für die Aufstellung entsprechender Abschlüsse – was indes verfassungsrechtlich höchst zweifelhaft ist.[1439]

3. Rechtsschutz und Haftung bei Standardsetzung

[1435] BMU, Umweltgesetzbuch (UGB-KomE), 1998, S. 495, 498 f..

[1436] Art. 3 der Verordnung (EG) Nr. 1606/2002 des Europäischen Parlaments und des Rates vom 19. 7.2002 betreffend die Anwendung internationaler Rechnungslegungsstandards, ABl. Nr. L 243, S. 1 und § 315a HGB.

[1437] Verordnung (EG) Nr. 1606/2002 des Europäischen Parlaments und des Rates vom 19. 7.2002 betreffend die Anwendung internationaler Rechnungslegungsstandards, ABl. Nr. L 243, S. 1.

[1438] Siehe dazu Art. 3, 6 Abs. 2 VO 1606/2002/EG sowie den Beschluss 1999/468/EG des Rates vom 28. Juni 1999 zur Festlegung der Modalitäten für die Ausübung der der Kommission übertragenen Durchführungsbefugnisse, ABl. Nr. L 184 vom 17.7.1999, S. 23.

[1439] Die verfassungsrechtliche Legitimation auch der Rechnungslegungsstandards verneinend *Hommelhoff/Schwab* in Großkomm. HGB, § 342 HGB Rn. 89; *Budde/Steuber* in FS Peltzer, 2001, S. 39 (49 ff.).

812 Kaum behandelt wird die Frage, wie sich Betroffene gegenüber fehlerhaften Standards zur Wehr setzen können; eng damit zusammen hängt ferner die – ebenfalls kaum diskutierte – Haftung der Standardsetzer für entsprechende Fehler:

a) Gegenüber staatlich gesetzten Standards

813 Handelt es sich um eine rein staatliche Norm, stellt sich zunächst die Frage, wie sich die Norm im Rahmen der Nomenklatur des Öffentlichen Rechts qualifizieren lässt. Da es sich mangels entsprechender Befugnisnormen und demokratischer Legitimationen offensichtlich weder um ein Gesetz noch eine Rechtsverordnung noch eine Satzung handelt, scheiden entsprechende Normenkontrollklagen aus. Umgekehrt sind staatlich gesetzte Standards keine unmittelbar nach außen wirkende Einzelfallregelungen, so dass sie ebenso wenig als Verwaltungsakt oder Allgemeinverfügungen zu charakterisieren wären. Lediglich intern wirkende Vorschriften, wie normale Verwaltungsvorschriften, lassen sich nicht separat angreifen, allenfalls inzidenter über den Rechtsschutz gegenüber konkretisierenden Verwaltungsakten. Entfalten sie jedoch auch gegenüber Dritten unmittelbare Wirkung, wie bei normkonkretisierenden Verwaltungsvorschriften, würde eine nur inzident wirkende Normenkontrolle zu kurz greifen – hier könnte (auch wenn bislang kaum erörtert) doch eine Analogie zur Normenkontrollklage nach § 47 VwGO in Betracht kommen.

814 Die Haftung der Standardsetzer hängt wiederum von der Normenqualität der Standards ab: bei unmittelbarer Außenwirkung (normkonkretisierende Verwaltungsvorschriften) kommen entsprechende Analogien zur (fehlenden) Haftung der gesetzgebenden Organe für fehlerhafte Gesetze bzw. Normen in Betracht.[1440] Fehlt es an einer unmittelbaren Außenwirkung, kommt dagegen die allgemeine Staatshaftung nach §§ 839 BGB, Art. 34 GG in Betracht.

b) Gegenüber privaten Standards

815 Das Gegenstück zu den öffentlich-rechtlichen Standardsetzungen stellen rein privatrechtlich erfolgende Normierungen dar. Hier greifen die allgemeinen Haftungsgrundlagen ein, insbesondere die deliktsrechtlichen Normen nach §§ 823 ff. BGB. Mangels besonderer Schutzgesetze kann daher eine Haftung nur im Bereich der Schädigung der von § 823 I BGB aufgezählten Rechtsgüter in Betracht kommen – abgesehen von sit-

[1440] BGH, NJW 1988, 478 (482); MünchKommBGB-*Papier*, § 839 BGB Rn. 260 f.

tenwidrig aufgestellten Standards, z.B. bei Monopolen. Praktisch relevant geworden ist die Haftung von Normungsorganisationen – soweit ersichtlich – bislang nicht.

c) Gegenüber privaten Standards mit staatlicher Rezeption

816 Kaum behandelt sind schließlich die Mischformen der privaten Standardsetzung mit staatlicher Rezeption, wie sie insbesondere dem europäischen Ansatz in der Produktsicherheit zugrunde liegen, aber auch der Rezeption der IFRS im Bilanzrecht. Hier wird zwischen den jeweiligen Tätigkeitsbereichen zu trennen sein: Da die Normungsorganisationen trotz ihrer Mandatierung nicht als Beliehene angesehen werden können, da sie keine öffentlich-rechtlichen Funktionen gegenüber Dritten ausüben, kann ihre Normungstätigkeit ebenso wie bei den rein privaten Standardsetzungen nur nach deliktischen Grundsätzen beurteilt werden.

817 Demgegenüber kann für die staatlichen Stellen, die die von den privaten Normungsorganisationen erstellten Standards durch einen Rechtsakt rezipieren, eine Staatshaftung eingreifen. Die Klärung dieser Frage(n) liegt allerdings noch weitgehend im Dunkeln, da schon strittig ist, ob die privaten Standards durch den staatlichen Rezeptionsakt eine andere Qualität erlangen, insbesondere ob sie als staatliche Normen dadurch zu betrachten sind, so dass die staatliche Behörde praktisch einen Normsetzungsakt vollzöge – wozu sie in den seltensten Fällen wirklich ermächtigt wäre. Näher liegt es, die Haftung der Behörde auf den reinen Rezeptionsakt als schlichtes staatliches Handeln zu qualifizieren, da die Normen keine unmittelbar bindende Wirkung entfalten, ihnen vielmehr nur eine Vermutungswirkung zukommt. Folge hiervon wäre, dass allein die Staatshaftung nach §§ 839 BGB, Art. 34 GG in Betracht käme, der Rechtsschutz sich nur in Form von Feststellungsklagen realisieren ließe – was indes einen schalen Nachgeschmack enthält, da die staatliche Rezeption de facto zu einer normativen Wirkung führt, die weit über ein schlichtes Verwaltungshandeln hinaus reicht.

4. Zusammenfassung

818 Im Hinblick auf die Erarbeitung von Standards für den IT-Bereich zeigt sich, dass die Übertragung der im Immissionsschutzrecht für Technische Anleitungen gefundene Lösungen mit erheblichen Schwierigkeiten behaftet ist, da ein komplexes, austariertes Verfahren eingehalten werden muss, welches eine erhebliche Zeitspanne in Anspruch

nimmt.[1441] Dies hat den TA auch den Vorwurf eingetragen hat, dass sie auch in Gestalt von Verordnungen hätten erlassen werden können, was teilweise für manche der Verordnungen nach dem BImSchG auch zutrifft, etwa der Elektrosmog-VO oder der Sportlärm-VO. Hält man sich das Bedürfnis nach – relativ – raschen Reaktionen auf sich wandelnde Bedrohungen und technischer Entwicklung vor Augen, ist daher Vorsicht vor der Übernahme derartiger Standardsetzung für Zwecke der IT-Sicherheit geboten.

819 Die Technischen Anleitungen sind rein nationales Recht und entbehren anders als die rein privaten ISO-Normen einer europäischen oder internationalen Anerkennung. Für das Immissionsschutzrecht, welches auf schädliche Umwelteinwirkungen auf dem Territorium der Bundesrepublik abstellt, kann dies durchaus sinnvoll sein, nicht jedoch für solche, die wie im IT-Sektor tendenziell mit grenzüberschreitenden Wirkungen[1442] und Produkten konfrontiert sind, so dass von vornherein Fragen des europäischen Binnenmarktes und auch der internationalen Akzeptanz auftreten. Dies gilt natürlich erst recht vor dem Hintergrund europarechtlicher Vorgaben, die grenzüberschreitende Produkte und Dienstleistungen betreffen.[1443]

820 Von den vorgestellten Modellen kooperativer Regelsetzung dürften für den IT-Bereich damit eine halbstaatliche Standardsetzung durch einen technischen Ausschuss bzw. die Normung durch private Normungsorganisationen in Betracht kommen. Hierzu und zur Rolle des BSI im Rahmen der Standardsetzung ausführlich unten Rn. 914 ff..

III. Vollzugsmodelle (Enforcement)

1. Grundlagen

821 Jegliches Sicherheitsrecht, sei es öffentlich-rechtlicher oder zivilrechtlicher Natur, bedarf der effektiven Durchsetzung, soll es seiner Funktion zur Verhaltenssteuerung und Schadensvermeidung gerecht werden. Im gesamten Umwelt- und Technikrecht wird indessen seit langem ein „Vollzugsdefizit“ beklagt.[1444] Es handelt sich hierbei im Kern wiederum um ein Anreizproblem: Im Fall der Schädigung etwa öffentlicher Güter (Luft, Wasser etc.) bestehen aufgrund der mangelnden Zuordnung dieser Rechte keine Anreize

[1441] TA Lärm und TA Luft werden nur in Abständen von ca. zehn Jahren oder länger novelliert, siehe *Hansmann*, NVwZ 2003, 266 (274).

[1442] Auch Umwelteinwirkungen sind natürlich grenzüberschreitender Natur – nicht aber die ihnen zugrundeliegenden Produktionsanlagen etc.

[1443] S. dazu unten Rn. 987 ff.

[1444] Siehe beispielsweise *Seelig/Gründling*, NVwZ 2002, 1033 (1034) (im Zusammenhang mit der Verbandsklage im Umweltrecht); *Lübbe-Wolf*, NuR 1993, 217; *Lorenz*, UPR 1991, 253.

für Private, diese externen Effekte (Schäden) geltend zu machen und damit beim Schädiger zu internalisieren – öffentliche Durchsetzung von Schutzstandards ist daher unausweichlich, allerdings wiederum verbunden mit dem Problem der Anreize für die mit der Vollstreckung Betrauten. Zwar ist eine privatrechtliche strukturierte Durchsetzung in aller Regel effizienter als eine staatliche,[1445] doch besteht hier oft das Problem des Marktversagens,[1446] sei es wegen fehlender Eigentumsrechte,[1447] sei es wegen tatsächlicher Probleme der Kontrolle der Tätigkeit anderer und des Nachweises in einem justizförmigen Verfahren. Gerade letzteres ist – wie oben dargelegt[1448] – eines der typischen Probleme für IT-Schäden, verursacht durch Dritte. Gleiches gilt jedenfalls außerhalb des B2B-Bereiches auch im Vertragsrecht: Hier schlagen Probleme der small-claims-Ansprüche durch,[1449] für die es sich für den Einzelnen nicht lohnt, seine Rechte durchzusetzen, ganz abgesehen von den bestehenden Informationsungleichgewichten zwischen IT-Hersteller und Anwender. Eine reine auf das Privatrecht beschränkte Durchsetzung würde daher auf erhebliche Enforcement-Probleme stoßen und damit tendenziell ineffizient sein;[1450] erforderlich ist ein komplementärer Ansatz.

2. Öffentlich-rechtlicher Vollzug

822 Umgekehrt sieht sich eine rein öffentlich-rechtliche Vollzugslösung den typischen Problemen einer staatlichen Regulierung gegenüber: Die radikalste Lösung einer vor Aufnahme einer Tätigkeit erforderlichen staatlichen Genehmigung (Verbot mit Erlaubnisvorbehalt) lässt sich für querschnittsartige Tätigkeiten praktisch nicht realisieren, sondern kann allenfalls segmentspezifisch durchgeführt werden, wie z.B. im Kreditwesenbereich. Gerade in der IT-Branche würde aber eine solche Genehmigungspflicht dazu führen, daß staatliche Prüfungsbehörden allein schon durch die schiere Zahl der IT-

[1445] *Cooter, Robert / Ulen, Thomas*, Law & Economics, Boston 2004, S. 342; *Becker, Gary / Stigler, George*, Law Enforcement, Malfeasance, and Compensation on Enforcers, 3 J. Leg. Studies 1974, 1; *Stephenson, Matthew*, Public Regulation of Private Enforcement: The Case for Expanding the Role of Administrative Agencies 91 Va. L. Rev., 2005, 93 (108) m.w.N.

[1446] Explizit *Rosenberg, David / Sullivan, James P.*, Coordinating private class action and public agency enforcement of antitrust law, 2 J. Competition L. & Econ. 2006, 159, (170).

[1447] *Landes, William M. / Posner, Richard A.*, The Private Enforcement of Law, NBER Working Paper series, 1974, 17.

[1448] S. oben Rn. 754 ff. sowie Teil 1 Rn. 173.

[1449] Zur Problematik *Landes, William M. / Posner, Richard A.*, The Private Enforcement of Law, NBER Working Paper series, 1974, 32f. *Rosenberg, David / Sullivan, James P.*, Coordinating private class action and public agency enforcement of antitrust law, 2 J. Competition L. & Econ. 2006, 159, (170). Detaillierte ökonomische Analyse bei *Shavell, Steven*, The fundamental divergence between the private and the social motive to use the legal system, 26 J. Legal Stud. 1997, 575, (583f.).

[1450] *Bucy, Pamela H.*, Private Justice, 76 S. Cal. L. Rev. 2002, 1, bei Fn. 166ff. *Shavell, Steven,* The fundamental divergence between the private and the social motive to use the legal system, 26 J. Legal Stud. 1997, 575, (583f.).Kritisch auch bezüglich der Effizienz privaten Enforcements i.e.S.: *Polinsky, Mitchell*, Private versus public enforcement, NBER Working Papers, 1981, 105.

Anwendungen überfordert wären, was zu volkswirtschaftlich höchst unerwünschten Effekten führen würde. Dies schließt nicht aus, daß IT-bezogene Probleme im Rahmen spezifischer Genehmigungen berücksichtigt werden, wie etwa im Kreditgewerbe oder im Anlagensicherheitsrecht.

823 Scheidet damit eine allgemeine, ex ante erforderliche Genehmigung aus, kommen zwei **andere Typen der staatlichen Überwachung** in Betracht: Zum einen die aus dem Produktsicherheitsrecht bekannte Typengenehmigung, die nicht jedes einzelne Produkt einer Genehmigung unterzieht, sondern nur den jeweiligen Typus, zum anderen eine anlassbezogene Aufsicht, die bei Missständen der IT-Sicherheit eingreifen kann. Darüber hinaus kann im Bereich dieser Überwachungstypen noch weiter nach Art und typischen Anwendungsfällen von Produkten differenziert werden; denn selbst eine Typengenehmigung würde im Hinblick auf die Vielfalt von IT-Produkten und entwickelter Software gegebenenfalls zu einer Überlastung der Behörden und damit zu einer ineffizienten Blockierung neuer Produkte führen, ohne dass dies in Korrelation zu den hervorgerufenen Gefahren stünde. Vorzugswürdig erscheint daher eine anlassbezogene Überwachung, die dem Staat das Eingreifen bei Missständen ermöglicht, einschließlich der Setzung von Anreizen zum vorherigen Durchlaufen von Qualitätsprüfungen (etwa nach ISO 9000 ff.).

3. Zivilrechtlicher Vollzug

824 Die oben beschriebene Probleme des zivilrechtlichen Enforcement beziehen sich auf zwei Fragenkreise: die Nachweisführung im Prozess (Kausalität, Schäden, Fehler etc.) sowie zu niedrige Anreize im Verhältnis der IT-Industrie (IT-Hersteller, IT-gewerbliche Nutzer) gegenüber ihren Kunden außerhalb des B2B-Bereichs bzw. bei klein- und mittelständischen Unternehmen (small claims).

825 Das Problem der Informationsasymetrie zwischen IT-Anbietern und Anwendern [1451] lässt sich nur durch die Einführung entsprechender **Beweislastgrundsätze** bewältigen, sei es in Gestalt einer gesetzlich eingreifenden Beweislastumkehr, sei es in Form eines gesetzlich angeordneten oder richterrechtlich wirkenden Anscheinsbeweises. Wie oben dargelegt, können solche Ansätze unter Umständen in Verbindung mit Gefährdungshaftungsregeln, aber auch (gegebenenfalls allein) in Verbindung mit öffentlich-rechtlichen Produkt- und Anlagensicherheitsgesetzen geschaffen werden. Die Vermutungswirkung,

[1451] Zu denen nicht nur die IT-Hersteller sondern auch die IT-Intermediäre und selbst auch die gewerblichen IT-Nutzer gehören, sofern diese wiederum IT-Produkte/Dienstleistungen anbieten, wie z.B. Online-Banking.

die im öffentlichen Recht zugunsten der Konformität einer Anlage mit grundlegenden Sicherheitsstandards eingreift, könnte damit auch auf den Zivilprozess ausgedehnt werden – allerdings ist nach geltendem Recht derartigen Zertifizierungen[1452] im Zivilrecht noch keine entsprechende Wirkung beigemessen worden, weder von der Rechtsprechung noch vom Gesetzgeber.

826 Das Problem fehlender Anreize durch **small claims** dagegen kann nur durch Formen der Verbandsklage angegangen werden, so wie es etwa im Ansatz das neue UWG im Bereich der Gewinnabschöpfung gegenüber unlauter handelnden Wettbewerbern vorsieht.[1453]

827 Eine weitere Abhilfemöglichkeit gegenüber Beweisproblemen wäre die **Einführung von Auskunftsansprüchen gegenüber IT-Intermediären**, wie sie derzeit im Rahmen der Enforcement-Richtlinie befürwortet und wohl auch umgesetzt wird.[1454] Damit könnte ein geschädigter Dritter Identität und gegebenenfalls auch Aktivitäten eines Schädigers ermitteln, um seine Ansprüche durchzusetzen. Indes stoßen derartige Auskunftsansprüche auf zahlreiche Probleme: Zunächst müsste hierfür wohl die einschlägige TK-Datenschutzrichtlinie 2002 der EU geändert werden, da diese keine Preisgabe von Daten der Nutzer an Dritte vorsieht.[1455] Zudem steht eine solche Auskunftspflicht in potentiellem Widerspruch zu dem Verbot der Einführung allgemeiner Überwachungspflichten nach Art. 15 der E-Commerce-Richtlinie. Schließlich ist zweifelhaft, ob ein Auskunftsanspruch alle Probleme des Geschädigten in der Beweisführung beseitigen würde; denn allein die Kenntnis der Identität des Schädigers führt nicht dazu, dass der Geschädigte die Kausalkette schon bewiesen hätte. Vielmehr dürfte es sich bei zahlreichen Schäden über das Internet um Phänomene der Summationsschäden oder zahlreicher Schädiger handeln. Bei einzelnen Angriffen eines Hackers indes wäre die Nachweisführung des Geschädigten erheblich erleichtert. Schließlich würde auch die Kenntnis der Identität eines Schädigers nichts daran ändern, dass die Netze des IT-Intermediärs (oder kommerziellen IT-Nutzers) sich als unsicher erwiesen haben; das eigentliche Problem

[1452] Damit dürfen nicht die Wirkungen der Standards selbst verwechselt werden – die Zertifizierungen beziehen sich allein auf die jeweilige in Verkehr gebrachten Produkte oder Dienstleistungen.

[1453] Diese Regelung hat allerdings zu Recht viel Kritik erfahren, da sie den Verbänden praktisch keine Anreize bietet, derartige Klagen durchzuführen – denn nach § 10 UWG fließt der dann abgeschöpfte Gewinn in die Staatskasse, das Risiko des Prozesses trägt aber der Verband.

[1454] Zur geplanten Umsetzung der Enforcement-RL näher *Spindler/Weber*, ZUM 2007, 257.

[1455] Eingehend dazu *Spindler/Dorschel*, CR 2006, 341 (345) mwNachw.

der IT-Sicherheit – nämlich der Schutz im Vorfeld gegenüber schädigenden Aktivitäten – würde damit nicht behoben.

IV. Rechtssetzungs-Vorschlag: IT-Sicherheitsgesetz

828 Führt man die verschiedenen oben diskutierten Stränge zusammen, kristallisiert sich eine Schnittmenge an produkt-, dienste- und anlagen bzw. organisationsbezogenen Sicherheitspflichten heraus, die nicht nur dem Schutz bestimmter Rechtsgüter dienen sollten, sondern allgemein gravierende Schäden für die Volkswirtschaft ebenso wie für das Vermögen und das Eigentum des Einzelnen vermeiden sollten. Dabei ergeben sich Unterscheidungen je nach Art der angebotenen Dienste und Tätigkeiten, Zuschnitt und Umfang eines IT-Dienstleisters, IT-Intermediärs, gewerblichen Nutzers bzw. IT-Hersteller. Die derzeitigen Regelungen weisen etliche rechtliche, aber auch praxisbezogene Defizite auf, die in ihrem Zusammenwirken offenbar dazu geführt haben, daß insgesamt bislang keine Mindestsicherheitsanforderungen rechtlich umgesetzt wurden (s. Teil 1 Rn. 257 ff. sowie für die einzelnen Akteure oben Rn. 751 ff.).

829 Derartige detaillierte genauso wie abstrakte Regelungen könnten aber in einem allgemeinen IT-Sicherheitsgesetz aufgefangen werden, das im folgenden näher diskutiert wird, zunächst hinsichtlich der umfassten Regelungsmaterien:

1. Anwendungsbereich

a) Sachlicher Schutzbereich

830 Wie oben herausgearbeitet, besteht eines der zentralen Probleme in der Einschränkung des Schutzes auf Körperschäden sowie – teilweise – auf Eigentumsschäden. Da viele Schäden durch fehlerhafte Software oder Software, welche Sicherheitslücken enthält, über die Dritte schädigende Handlungen durchführen können, **Vermögensschäden** sind, stellt sich die Frage, wie ein IT-SicherheitsG derartige Schadensszenarien bewältigen kann. Eine Ausdehnung auf sämtliche Vermögensschäden würde zu exzessiven Haftungsrisiken führen und hätte eine übermäßige Abschreckungswirkung auf Hersteller und IT-Dienstleister zur Folge. Zudem muss berücksichtigt werden, dass das Risiko, ob eine Software die in sie gesetzten Erwartungen erfüllt, dem Vertragsrecht zuzuordnen ist. In Betracht kommt daher nur um die Gewährleistung einer Basissicherheit im Interesse aller Beteiligten, sowie die Regelung segmentspezifischer besonderer Anforderungen an bestimmte besonders gefährdete Bereiche, wie kritische Infrastrukturen, insbesondere den Finanzsektor. Lässt man die Gefahrenszenarien wie Viren, Trojaner,

Phishing etc. (Teil 1 Rn. 58), aber auch den früheren Jahr-2000-Fehler Revue passieren, stehen im Wesentlichen folgende Bereiche in Rede:

- Gefährdung kritischer Infrastrukturen einschließlich des Finanzbereichs
- Erleichterung von Angriffen Dritter durch Sicherheitslücken
- Schäden an Daten und Datenbeständen des IT-Nutzers einschließlich Folgeschäden

831 Ein IT-SicherheitsG, das eine öffentlich-rechtliche Grundlage hat, aber mit zivilrechtlichen Auswirkungen, sollte sich auf diese Tatbestände beschränken, um nicht unnötig in Äquivalenzbeziehungen von Vertragsparteien einzugreifen. Problematisch ist in diesem Rahmen allerdings, wie die Tatbestände näher umrissen werden können:

(1) Gefährdung kritischer Infrastrukturen

832 Für die Gefährdung kritischer Infrastrukturen kann auf die Definitionsversuche aus anderen Forschungsprojekten[1456] sowie der EU[1457] zurückgegriffen werden. Danach können „kritischen Infrastrukturen“ als Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen definiert werden, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.[1458] Beispiele hierfür sind etwa Transport und Verkehr, Energie, Gefahrenstoffe, Informationstechnik und Telekommunikation, das Finanz- und Versicherungswesen, sowie Verwaltung und Justiz.[1459] In ähnlicher Weise beobachtet Österreich die Vorhaben auf EU-Ebene, bereitet allerdings schon jetzt die Klassifikation bestimmter Infrastrukturbereiche je nach deren Gefährdung und ihren Auswirkungen vor.[1460]

(2) Erleichterung von Angriffen Dritter

833 Die zweite Gruppe – Erleichterung von Angriffen Dritter – wäre als ein Vorfeldschutz im Bereich von Straftaten konzipiert, welche unter Ausnutzung fehlerhafter IT-Produkte begangen bzw. die hierdurch ermöglicht werden (Sicherheitslücken). Das IT-Sicherheitsgesetz könnte für diese Fälle **Ermächtigungsgrundlagen** für Anordnungen

---

[1456] *Holznagel/Koenig*, Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, 2002, abrufbar unter http://www.bsi.bund.de/fachthem/kritis/Regelungsumfang_ITSich_KRITIS.pdf.

[1457] Grünbuch über ein Europäisches Programm für den Schutz kritischer Infrastrukturen vom 17.11.2005, KOM(2005) 576 endgültig, abrufbar unter http://europa.eu.int/eur-lex/lex/LexUriServ/site/de/com/2005/com2005_0576de01.pdf. Weitere Informationen zum Europäischen Programm für den Schutz kritischer Infrastrukturen (EPICP) sind abrufbar unter http://ec.europa.eu/justice_home/funding/epcip/wai/funding_epcip_de.htm.

[1458] Ausführlich *Sonntag*,IT-Sicherheit kritischer Infrastrukturen, 2005, S. 19 ff.; http://www.bsi.bund.de/fachthem/kritis/index.htm.

[1459] Siehe dazu http://www.bsi.bund.de/fachthem/kritis/index.htm.

[1460] *Fallenböck* Annex II – Österreich - Rn. 1183 f.

gegenüber IT-Herstellern, IT-Dienstleistern und IT-Betreibern schaffen, um derartige Sicherheitslücken zu schließen.

834 Tatbestandlich könnte ein solcher Vorfeldschutz an das **Computerstrafrecht** anknüpfen, welches derzeit beispielsweise Straftatbestände wie Datenveränderung (§ 303a StGB), Computersabotage (§ 303b StGB) und Ausspähen von Daten (§ 202a StGB) umfasst.[1461] Ende 2006 legte die Bundesregierung ein „Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität“[1462] vorgelegt,[1463] durch das der Straftatbestand des Ausspähens von Daten (§ 202a StGB) auf den unbefugten Zugang zu Daten und somit auch auf „Hacking“ erweitert wurde. Ein neuer § 202b StGB soll das Abfangen von Daten unter Strafe stellen. Der Tatbestand der Computersabotage (§ 303b StGB) soll künftig neben Behörden und Unternehmen auch private Datenverarbeitung von wesentlicher Bedeutung schützen und durch die Ausdehnung auf die Störungshandlungen „Eingeben“ oder „Übermittlung“ von Daten auch „Denial-of-Service-Angriffe“ erfassen. Mit § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten) des Entwurfs soll schließlich ein Vorbereitungsdelikt eingeführt werden.

835 Das IT-Sicherheitsgesetz könnte zudem als **Schutzgesetz** konzipiert werden, was geschädigten Dritten erlauben würde, über § 823 Abs. 2 BGB ihre Vermögensschäden zu liquidieren. Die Haftung von Unternehmen könnte in diesem Zusammenhang an einen fahrlässigen Beitrag zu einem der genannten Straftaten anknüpfen und wäre zivilrechtlich durch eine Schadensersatzpflicht sanktioniert. Eine Haftung für vorsätzliches Fehlverhalten (auch unbekannter) Dritter ist dem deutschen Recht nicht unbekannt, wie Beispiele aus der Rechtsprechung zeigen.[1464] Eine solche Lösung würde auch nicht zu ausufernden Haftungsrisiken und der Erfassung sämtlicher Vermögensschäden führen, da sie akzessorisch zu den Straftatbeständen im Bereich des Computer- bzw. IT-Strafrechts ist. Ergänzend wäre an die Schaffung von Haftungshöchstsummen zu denken, welche insbesondere die Versicherbarkeit der Risiken zu erleichtern würden.

[1461] S. auch die parallelen Bestimmungen im österreichischen Strafrecht, *Fallenböck* Annex II – Österreich - Rn. 1229 ff., für das britische Recht *Reed* – Annex II – Rn. 1260 f.

[1462] Grundlagen sind das Übereinkommen des Europarates über Computerkriminalität vom 23.11.2001 und der Rahmenbeschluss 2005/222/JI des Rates vom 24.2.2005 über Angriffe auf Informationssysteme, ABl. EU Nr. L 69, S.67.

[1463] BR-Drucks. 676/06. Abrufbar unter http://www.bmj.bund.de/media/archive/1317.pdf.

[1464] BGH, NJW 1990, 1236 (1237) (Pflicht des Eigentümers und Vermieters eines Mehrfamilienhauses, Abdeckroste eines Lichtschachtes gegen unbefugtes Abheben zu sichern); BGH, NJW 1980, 223 (Sicherung einer Großveranstaltung gegen Übergriffe der Zuschauer auf Dritte); BGHZ 37, 165 (170) (Entfernung von Hindernissen, die durch mutwillige Aktionen auf die Straße geworfen wurden, durch den Sicherungspflichtigen); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 245; MünchKommBGB-*Wagner*, § 823 BGB Rn. 255. Siehe dazu bereits.Teil 1 Rn. 104 ff. (Produkthaftung).

(3) Schäden an Daten des Nutzers

836 Die dritte Gruppe – Schäden an Daten des Nutzers – beträfe die Fälle, in denen **Integritätsinteressen** des IT-Nutzers betroffen sind, nicht aber Äquivalenzinteressen. Zwar sind jetzt schon im Deliktsrecht Ansätze vorhanden, Daten und Datenbestände als Eigentum im Sinne von § 823 Abs. 1 BGB zu schützen; doch ist diese Entwicklung noch keineswegs gesichert, so dass eine gesetzliche Absicherung sinnvoll erscheint. Zudem hätte eine solche Lösung den Vorzug, dass gleichzeitig die Ermächtigung zur Setzung von Standards geschaffen wäre, die wiederum über § 823 Abs. 2 BGB in Verbindung mit dem IT-Sicherheitsgesetz als **Schutzgesetz** einerseits, über die allgemeinen Fahrlässigkeitsstandards andererseits die Entwicklung steuern könnten – und zwar auch dann, wenn die private Rechtsdurchsetzung scheitern sollte.

b) Normadressaten

837 Erfasst werden sollten entsprechend der IT-Wertschöpfungskette alle relevanten Akteure, mithin IT-Hersteller (bzw. IT-Produkte), IT-Dienstleister, IT-Intermediäre und auch kommerzielle IT-Nutzer als Betreiber von IT-Anlagen.

(1) IT-Produzenten und IT-Dienstleister

838 Während für **IT-Hersteller** ebenso wie für **IT-Dienstleister** das Modell des Produktsicherheitsrechts herangezogen werden kann, sollte für **IT-Intermediäre** die rein auf TK-Anbieter bezogene Sicherheitspflichten (§ 109 TKG) abgelöst und in das allgemeine IT-SicherheitsG überführt werden[1465] – dies rechtfertigt sich schon vor dem Hintergrund, dass häufig nicht genau zwischen der Erbringung von TK-Diensten und anderen, „Mehrwert"-Diensten unterschieden werden kann, vielmehr TK-Dienste oftmals eine Vorbedingung für andere Dienste sind, etwa der Erbringung von Online-Inhaltsdiensten. Dies schließt nicht aus, dass Besonderheiten der Telekommunikationsanbieter in entsprechenden Segmentstandards Berücksichtigung finden können – doch wäre gleichzeitig die Koppelung, Abstimmung und Überlappung mit anderen IT-relevanten Standards gewährleistet, ohne dass gegebenenfalls konfligierende rechtliche Anforderungen zwischen TK-Recht und sonstigem Recht entstünden. Ferner sollte aus privatrechtlicher Sicht das Recht der Haftungsprivilegierungen für die Sicherungspflichten aus dem Telekommunikationsrecht herausgelöst und in das Recht der allgemeinen AGB-Inhaltskontrolle überführt werden. Damit würde eine Stärkung der Anreize für TK-

[1465] Dazu sogleich Rn. 839 ff.

Anbieter erreicht, sichere Netze zu entwickeln; gegebenenfalls könnten Haftungsobergrenzen generell in einem IT-SicherheitsG festgeschrieben werden.[1466]

(2) Gewerbliche IT-Nutzer

839 Für **gewerbliche IT-Nutzer** sollten Regelungen für eine IT-Basissicherheit im IT-SicherheitsG, hilfsweise in der GewO, geschaffen werden, wiederum mit der Möglichkeit, bestimmte Standards zu entwickeln. Ansatzpunkt derartiger Sicherheitsbestimmungen sollte das **Betreiben einer IT-Anlage** sein, gegebenenfalls mit verschiedenen Abstufungen in den Sicherheitsanforderungen in Abhängigkeit davon, inwiefern Dritte bzw. andere Netze mit der IT-Anlage in Berührung kommen. Der Bezug auf eine Anlage empfiehlt sich insbesondere vor dem Hintergrund der oben dargelegten Pflicht zur Anerkennung ausländischer Rechtsformen, die nahe legen, entsprechende Pflichten nicht auf die Rechtsform zu knüpfen, sondern an die Gefahrenquelle, mithin die IT-Anlage. Das schließt nicht aus, dass die Anlage oder der Betrieb selbst entsprechenden IT-Sicherheitspflichten auch organisatorischer Art unterworfen wird – wie dies etwa die Seveso II-Richtlinie zeigt, die dem Betreiber einer Störfall-Anlage nach der 12. BImSchV bzw. der Seveso II-Richtlinie umfangreiche Maßnahmen des Sicherheitsmanagements abverlangt, ohne dass auf die Rechtsform Bezug genommen würde.[1467]

2. Regelungsansatz: „Nationaler New Approach“ im IT-Sicherheitsrecht

840 Das IT-SicherheitsG selbst sollte entsprechend dem von der EU im Rahmen des sog. **New Approach** verfolgten Ansatzes im Produktsicherheitsrecht (dazu a)) generalklauselartig nur die **grundlegenden Sicherheitsanforderungen** vorsehen (dazu b)(1)). Für den Normadressaten besteht ein Anreiz bestimmte **technische Normen** einzuhalten, da er von einer **Konformitätsvermutung** hinsichtlich der Wahrung der im Gesetz vorgegebenen Sicherheitsstandard profitiert (dazu b)(2)).

a) Das Modell des New Approach im Produktsicherheitsrecht

841 Überwiegend vollzieht sich die Rechtsetzung im Bereich der Produktsicherheit heute im europäischen Rahmen. Mit der Entschließung des Rates vom 7.5.1985 über eine Neue

[1466] S. unten Rn 886 ff.

[1467] Krit. dazu *Spindler/Peter*, in: Friedenstab/Jochum/Peter/Spindler, Industriepark und Störfallrecht, 2003, Rn. 142 ff.

Konzeption auf dem Gebiet der technischen Harmonisierung und der Normung[1468] wandte sich die EG vom zunächst verfolgten Konzept der Totalharmonisierung durch Richtlinien ab, welches sich als zu unflexibel und schwerfällig erwiesen hatte.[1469] Grundlage des New Approach ist zum einen das durch die Entscheidung des EuGH Cassis de Dijon[1470] vorgezeichnete **Prinzip der gegenseitigen Anerkennung**, wonach die Regelungen der Mitgliedsstaaten zum Schutz der Sicherheit und Gesundheit der Bürger und die Vorschriften des Verbraucherschutzes grundsätzlich gleichwertig sind,[1471] zum anderen die **Harmonisierung durch EU-Richtlinien**, welche jedoch keine Detailharmonisierung vornehmen, sondern lediglich die **wesentlichen Anforderungen** an die Sicherheit festlegen.

842 Zusammengefasst liegen dem New Approach folgende **Prinzipien** zugrunde[1472]:

- Die Harmonisierung beschränkt sich auf die wesentlichen Anforderungen, die in den Anhängen der Richtlinien näher beschrieben werden[1473].
- Nur Produkte, die den wesentlichen Anforderungen entsprechen, können in den Verkehr gebracht oder in Betrieb genommen werden.
- Bei harmonisierten Normen, deren Fundstellen im Amtsblatt veröffentlicht und die in nationale Normen umgesetzt worden sind, ist eine Übereinstimmung mit den entsprechenden wesentlichen Anforderungen anzunehmen.
- Die Anwendung harmonisierter Normen oder anderer technischer Spezifikationen bleibt freiwillig, und den Herstellern steht die Wahl jeder technischen Lösung frei, solange die Konformität mit den wesentlichen Anforderungen gewährleistet ist.
- Hersteller haben die Wahl zwischen verschiedenen Konformitätsbewertungsverfahren, die in den anwendbaren Richtlinien vorgesehen sind.

843 Den **europäischen Normungsorganisationen** CEN, CENELEC und ETSI[1474] fällt die Aufgabe zu, nach dem Stand der Technik technische Spezifikationen für Produkte in sog. harmonisierten Normen nieder zu legen. Indem Detailregelungen vom Gesetzge-

[1468] ABl. EG Nr. C 136, S. 1, siehe http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31985Y0604(01):DE:HTML.
[1469] *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfaßten Richtlinien, 2000, S. 7.
[1470] EuGH, Rs. 120/78, *Cassis de Dijon,* Slg. 1979, 649.
[1471] *Wilrich*, Geräte- und Produktsicherheitsgesetz (GPSG), Einl. Rn. 38.
[1472] *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfaßten Richtlinien, 2000, S. 7.
[1473] Siehe beispielsweise Siehe beispielsweise Anhang I der Richtlinie 98/37/EG des Europäischen Parlaments und des Rates vom 22.6.1998 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für Maschinen, ABl. EG L 207 vom 23.7.1998, S. 1. Die Maschinenrichtlinie wurde in nationales Recht umgesetzt durch die Neunte Verordnung zum Geräte- und Produktsicherheitsgesetz (Maschinenverordnung 9. GPSGV) vom 12.5.1993, BGBl. I, S. 704, 2436, zuletzt geändert am 6.1.2004 (BGBl. I, S. 2), siehe dort § 2 (Sicherheitsanforderungen). Die neue Maschinenrichtlinie 2006/42/EG vom 17.5.2006 (ABl. EG L 157) muss bis 29.6.2008 umgesetzt werden.
[1474] Teil 1 Rn.148.

bungsverfahren auf die Verbandsarbeit verlagert werden, soll die oben angesprochene Flexibilität im Hinblick auf neue technische Entwicklungen gewährleistet werden.[1475]

844 Die Neukonzeption der technischen Normung auf europäischer Ebene wird ergänzt durch das **Informationsverfahren auf dem Gebiet der technischen Normen und technischen Vorschriften**[1476], welches eine präventive Kontrolle der nationalen technischen Normung zur Vermeidung erneuter technischer Handelshemmnisse sowie ggf. die Ingangsetzung einer europäischen Normung in dem betreffenden Gebiet ermöglichen soll. Hinzu kommt das **„Globale Konzept für Zertifizierung und Prüfwesen"** der Kommission vom 15.6.1989[1477] im Zusammenhang mit dem in den Richtlinien vorgesehenen Konformitätsbewertungsverfahren und dem CE-Kennzeichen (siehe Teil 1 Rn. 248 ff.).

(1) Grundlegende Sicherheitsanforderungen

845 Die Beschränkung der Richtlinien des New Approach auf die bindende Festlegung der grundlegenden Sicherheits- und Gesundheitsanforderungen wird im europäisch harmonisierten Bereich beispielhaft veranschaulicht durch **§ 4 Abs. 1 GPSG** in Verbindung mit der **Maschinenverordnung (9. GPSGV)**[1478], welche die **Maschinenrichtlinie 98/37/EG** vom 22.6 1993 umsetzt[1479], sowie im nicht-harmonisierten Bereich durch **§ 4 Abs. 2 GPSG** („nationaler New Approach") (siehe dazu auch Teil 1 Rn. 234 ff.).

846 § 2 der 9. GPSGV bzw. Art. 3 der Maschinenrichtlinie lauten:

> § 2 Sicherheitsanforderungen
>
> Maschinen und Sicherheitsbauteile dürfen nur in Verkehr gebracht werden, wenn sie den grundlegenden Sicherheits- und Gesundheitsanforderungen des Anhangs I der Richtlinie 89/392/EWG[1480] entsprechen und bei ordnungsgemäßer Aufstellung und Wartung und bestimmungsgemäßem Betrieb die Si-

[1475] *Wilrich*, Geräte- und Produktsicherheitsgesetz (GPSG), Einleitung Rn. 39.

[1476] Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften, ABl. EG L 204, S. 37 und Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20. Juli 1998 zur Änderung der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften.

[1477] ABl. EG 1989, C 267.

[1478] Neunte Verordnung zum Geräte- und Produktsicherheitsgesetz (Maschinenverordnung 9. GPSGV) vom 12.5.1993, BGBl. I, S. 704, 2436, zuletzt geändert am 6.1.2004 (BGBl. I, S. 2). Erlassen auf Grundlage von § 4 GSG aF (jetzt § 3 Abs. 1 GPSG).

[1479] Richtlinie 98/37/EG des Europäischen Parlaments und des Rates vom 22.6.1998 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für Maschinen, ABl. EG L 207 vom 23.7.1998, S. 1. Die neue Maschinenrichtlinie 2006/42/EG vom 17.5.2006 (ABl. EG L 157) muss bis 29.6.2008 umgesetzt werden.

[1480] Richtlinie 89/392/EWG des Rates vom 14. Juni 1989 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten für Maschinen, ABl. EG L 183 vom 29.06. 1989 S. 9.

cherheit und die Gesundheit von Personen und die Sicherheit von Haustieren und Gütern nicht gefährden.

Artikel 3

Die Maschinen und Sicherheitsbauteile im Sinne dieser Richtlinie müssen die in Anhang I aufgeführten grundlegenden Sicherheits- und Gesundheitsanforderungen erfüllen.

847 Der **Anhang I zur Maschinenrichtlinie** stellt detaillierte, aber technikneutrale Sicherheitsanforderungen auf, ohne jedoch technische Lösungen für den Einzelfall bindend vorzuschreiben.[1481] Punkt 1.2.4. des Anhangs I zur Maschinenrichtlinie betreffend grundlegende Sicherheits- und Gesundheitsanforderungen bei Konzipierung und Bau von Maschinen lautet auszugsweise: 1.2.4. Stillsetzen [...]
Stillsetzen im Notfall
Jede Maschine muß mit einer oder mehreren Notbefehlseinrichtungen ausgerüstet sein, durch die unmittelbar drohende oder eintretende gefährliche Situationen vermieden werden können. [...]

848 Die Maschinenrichtlinie unterscheidet innerhalb der grundlegenden Sicherheits- und Gesundheitsanforderungen zwischen **allgemeinen Sicherheits- und Gesundheitsanforderungen**, für alle in den Anwendungsbereich der Richtlinie fallenden Maschinen (siehe Anhang I zur Maschinenrichtlinie, Punkt 1: „Grundlegende Sicherheits- und Gesundheitsanforderungen bei Konzipierung und Bau von Maschinen“) und **besonderen Sicherheits- und Gesundheitsanforderungen** für bestimmte Maschinengattungen (siehe Anhang I zur Maschinenrichtlinie, Punkt 2: „Grundlegende Sicherheits- und Gesundheitsanforderungen für bestimmte Maschinengattungen“). Hinzu kommen Anforderungen zur Ausschaltung der speziellen Gefahren aufgrund der Beweglichkeit von Maschinen (Punkt 3), zur Ausschaltung der speziellen Gefahren durch Hebevorgänge (Punkt 4), für Maschinen, die im Untertagebau eingesetzt werden (Punkt 5) sowie zur Vermeidung der speziellen Gefahren beim Heben oder Fortbewegen von Personen (Punkt 6).[1482]

849 **§ 4 Abs. 2 Satz 1 bis 3 GPSG** beschränkt sich im nicht-harmonisierten Bereich auf eine abstraktere Regelung und verweist anders als die Richtlinien im harmonisierten Bereich nicht auf einen Anhang mit detaillierten Sicherheitsanforderungen:

[1481] Zur Einteilung der Richtlinien nach dem New Approach Teil 1 Rn. 148.

[1482] Siehe Anhang I der Richtlinie 98/37/EG des Europäischen Parlaments und des Rates vom 22.6.1998 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für Maschinen, ABl. EG L 207 vom 23.7.1998, S. 1.

§ 4

(2) Ein Produkt darf, soweit es nicht § 4 Abs. 1 unterliegt, nur in den Verkehr gebracht werden, wenn es so beschaffen ist, dass bei bestimmungsgemäßer Verwendung oder vorhersehbarer Fehlanwendung Sicherheit und Gesundheit von Verwendern oder Dritten nicht gefährdet werden. Bei der Beurteilung, ob ein Produkt der Anforderung nach Satz 1 entspricht, sind insbesondere zu berücksichtigen

1. die Eigenschaften des Produkts einschließlich seiner Zusammensetzung, Verpackung, der Anleitungen für seinen Zusammenbau, der Installation, der Wartung und der Gebrauchsdauer,

2. seine Einwirkungen auf andere Produkte, soweit seine Verwendung mit anderen Produkten zu erwarten ist,

3. seine Darbietung, Aufmachung im Handel, Kennzeichnung, Warnhinweise, Gebrauchs- und Bedienungsanleitung und Angaben für seine Beseitigung sowie alle sonstigen produktbezogenen Angaben oder Informationen,

4. die Gruppen von Verwendern, die bei der Verwendung des Produkts einer größeren Gefahr ausgesetzt sind als andere.

Bei der Beurteilung, ob ein Produkt den Anforderungen nach Satz 1 entspricht, können Normen und andere technische Spezifikationen zugrunde gelegt werden. [...]

(2) Vermutungswirkung bei Normkonformität

850 Schlüsselelement des New Approach ist die Normungsarbeit der europäischen Normungsorganisationen CEN, CENELEC und ETSI (harmonisierter Bereich, § 2 Abs. 16 GPSG) sowie des Ausschusses für technische Arbeitsmittel und Verbraucherprodukte (nicht harmonisierter Bereich, §§ 4 Abs. 2 Satz 3, 4, 13 GPSG). Zum den Normungsverfahren siehe ausführlich Teil 1 Rn.145 ff.).

851 Wie bereits in Teil 1 zum GPSG dargestellt, ist die Anwendung der technischen Normen durch den Hersteller **freiwillig**. Rechtlich verbindlich ist allein das in der Harmonisierungsrichtlinie geforderte Sicherheitsziel, d.h. die grundlegenden Sicherheitsanforderungen wie sie beispielsweise im Anhang zur Maschinenrichtlinie näher konkretisiert werden. Dem Hersteller bleibt es unbenommen, das geforderte Sicherheitsniveau durch eine von den technischen Normen abweichendes Sicherheitskonzept zu verwirklichen. In diesem Fall ergibt sich aus Sicht des Herstellers die Schwierigkeit die Gleichwertigkeit seiner Sicherheitslösung mit den abstrakten Sicherheitsanforderungen der Richtlinien bzw. des Gesetzes zu beweisen.

852 Bei Konformität mit technischen Normen, die bestimmten Anforderungen an Normgeber und Verfahren entsprechen, gilt eine **Vermutungswirkung** zugunsten des Herstel-

lers für die Einhaltung der in den Richtlinien festgelegten Sicherheitsanforderungen. Der Hersteller kann sich dann auf die Darlegung der Übereinstimmung seines Produkts mit den konkreten Vorgaben der technischen Norm beschränken und steht nicht vor dem Problem, abstrakte gesetzliche Sicherheitsanforderungen durch eigene Lösungen konkretisieren zu müssen. Im **harmonisierten Bereich** wurde die Vermutungswirkung in § 4 Abs. 1 Satz 2 GPSG in deutsches Recht umgesetzt:

§ 4

(1) [...] [2]Entspricht eine Norm, die eine harmonisierte Norm umsetzt, einer oder mehreren Anforderungen an Sicherheit und Gesundheit, wird bei einem entsprechend dieser Norm hergestellten Produkt vermutet, dass es den betreffenden Anforderungen an Sicherheit und Gesundheit genügt.

853 Die Regelung setzt Art. 5 Abs. 2 der Maschinenrichtlinie bzw. die entsprechenden Vorschriften der anderen Harmonisierungsrichtlinien in deutsches Recht um[1483]:

Art. 5

(2) Entspricht eine nationale Norm in Umsetzung einer harmonisierten Norm, deren Fundstelle im *Amtsblatt der Europäischen Gemeinschaften* veröffentlicht worden ist, einer oder mehreren grundlegenden Sicherheitsanforderungen, wird bei nach dieser Norm hergestellten Maschinen oder Sicherheitsbauteilen davon ausgegangen, daß sie den betreffenden grundlegenden Anforderungen genügen. Die Mitgliedstaaten veröffentlichen die Fundstellen der nationalen Normen, die harmonisierte Normen umsetzen.

854 Die zunächst nur im harmoniserten Bereich angewandte Vermutung wird durch § 4 Abs. 2 GPSG nunmehr auf den **nicht harmonisierten Bereich** übertragen.

§ 4

(2) [...] [4]Entspricht eine Norm oder sonstige technische Spezifikation, die vom Ausschuss für technische Arbeitsmittel und Verbraucherprodukte ermittelt und von der beauftragten Stelle im Bundesanzeiger bekannt gemacht worden ist, einer oder mehreren Anforderungen an Sicherheit und Gesundheit, wird bei einem nach dieser Norm oder sonstigen Spezifikation hergestellten Produkt vermutet, dass es den betreffenden Anforderungen an Sicherheit und Gesundheit genügt.

855 Die Regierungsbegründung zum GPSG verspricht sich von der Übernahme des Vermutungsprinzips eine Stärkung der Normung auch im nicht harmonisierten Bereich.[1484]

b) Übertragung auf ein IT-Sicherheitsgesetz

[1483] Wilrich, § 4 GPSG Rn. 27.
[1484] BT-Drucks. 15/1620, S. 28.

856 Die beschriebene Regelungstechnik des New Approach findet bereits breitflächig auf EU-Ebene und neuerdings auch im nationalen Recht (s. § 4 Abs. 2 Satz 4 GPSG) Anwendung. Ihre Übertragung auf ein IT-Sicherheitsgesetz würde **Kontinuität im Hinblick auf eine mögliche künftige Regelung auf europäischer Ebene** gewährleisten.

(1) Grundlegende Anforderungen an die IT-Sicherheit

857 Übertragen auf ein IT-SicherheitsG bedeutet eine Orientierung am Regelungsmodell des New Approach, dass sich das IT-Sicherheitsgesetz auf die Festlegung der angestrebten **wesentlichen Sicherheitsanforderungen** in Bezug auf IT-Produkte, IT-Dienstleistungen, IT-Anlagen und das IT-Riskmanagement beschränkt. Die Normen des IT-Sicherheitsgesetzes selbst sollten hierbei aufgrund der Komplexität und Verschiedenheit der zu regelnden technischen Systeme und der daran zu richtenden IT-Sicherheitsanforderungen möglichst knapp gehalten werden.

858 Gesetzgebungstechnisch könnte dies zunächst durch eine generalklauselartige Regelung erfolgen, wonach IT-Produkte, IT-Dienstleitungen, IT-Anlagen und IT-Riskmanagementsysteme entsprechend den **allgemein anerkannten Regeln der Sicherheitstechnik** zu gestalten und zu betreiben sind; alternativ wäre auch entsprechend dem früheren § 87 TKG 1996 ein Verweis auf den **Stand der Technik** möglich, was allerdings in der Regel nur für besonders gefahrenträchtige Anlagen oder Produkte gefordert wird (z.B. im Immissionsschutz). Sofern bereits auf der gesetzlichen Ebene – etwa aufgrund technischer Erfordernisse – eine stärkere Ausdifferenzierung und Konkretisierung erforderlich sein sollte, könnte eine gesetzliche Regelung in Anlehnung an das Modell der Maschinenrichtlinie so formuliert werden, dass die in einem **Anhang des IT-Sicherheitsgesetzes** näher beschriebenen Sicherheitsanforderungen erfüllt werden müssen. In einem Anhang zum IT-Sicherheitsgesetz könnten die grundlegenden Anforderungen an die IT-Sicherheit technikneutral umschrieben werden (s. das Regelungsbeispiel Rn. 828 ff.).

859 **Differenziertheit der Regelung** und **Regelungstiefe** auf Ebene des Anhangs zum IT-Gesetz wären primär aus technischer Sicht zu klären. Die Sicherheitsanforderungen müssten in jedem Fall **hinreichend bestimmt** formuliert werden, so dass sie Pflichten der Normadressaten begründen können, deren Nichteinhaltung verwaltungsrechtliche (und ggf. zivilrechtliche) Sanktionen nach sich ziehen kann und die zuständigen Behörden in die Lage versetzt werden, auch Einhaltung der Sicherheitsanforderungen auch unabhängig von den zu erarbeitenden technischen Normen zu beurteilen. Wie das Bei-

spiel des § 4 Abs. 2 Satz 1 bis 3 GSPG zeigt (Rn. 849), genügt hierbei jedoch ggf. auch die Bezugnahme auf die anerkannten Regeln der Technik.

860 In Anlehnung an das Vorbild der Maschinenrichtlinie könnte erforderlichenfalls bereits in einem Anhang nach **allgemeinen Sicherheitsanforderungen** und besonderen Anforderungen für bestimmte Produkte, Dienste, Anlagen und IT-Risk-Management bzw. besondere Gefährdungslagen unterschieden werden. Im Einzelnen wäre an eine Regelungsstruktur zu denken, die **bestimmten IT-Produkten, IT-Dienstleistungen und IT-Anlagen** bzw. besonders **gefährdeten Bereichen** durch spezielle Anforderungen Rechnung trägt. In welcher Weise allgemeine Sicherheitsanforderungen zu einem allgemeinen Basisschutz zusammengefasst werden können oder segmentspezifische Einzelanforderungen erforderlich sind, bleibt wiederum primär aus technischer Sicht zu klären.

861 Eine **Änderung oder Anpassung der Sicherheitsanforderungen** des IT-Sicherheitsgesetzes kann im Unterschied zu den technischen Normen ohne Rechtsnormqualität nur im Wege eines formellen Gesetzgebungsverfahrens erfolgen.

(2) Technische Normen und Vermutungswirkung

862 Zentrales Element des Gesamtkonzepts eines kodifizierten IT-Sicherheitsrechts ist die Erarbeitung von Standards für IT-Produkte, IT-Dienstleistungen, IT-Anlagen und das IT-Riskmanagement, welche **keine Rechtsnormqualität** aufweisen, sondern auf freiwillige Beachtung angelegt sind. Den Normadressaten des IT-Sicherheitsgesetzes bleibt es unbenommen alternative Lösungen zu entwickeln, welche den gleichen Sicherheitsstandard aufweisen. Ebenso wie im europäischen Produktsicherheitsrecht sichert die Verweisung auf technische Normen die notwendige Flexibilität bei der Überarbeitung und Aktualisierung der Standards und entlastet die gesetzliche Regelung von technischen Details. Zugleich wahrt der rechtlich unverbindliche Charakter der technischen Normen den notwendigen unternehmerischen Freiraum für technische Innovationen.

863 Die Sicherheitsstandards wären zur **Konkretisierung der Sicherheitsanforderungen des IT-Sicherheitsgesetzes** geeignet und hätten insoweit – ebenso wie DIN-Normen – Empfehlungscharakter für die Adressaten des IT-SicherheitsG. Um einen Anreiz zur Einhaltung der Standards zu schaffen, sollte an die Konformität mit den Standards entsprechend dem geschilderten New Approach im Produktsicherheitsrecht (Rn. 862 ff.) eine **widerlegliche Vermutung** für die Wahrung der Sicherheitsanforderungen des IT-

Sicherheitsgesetzes geknüpft werden. Dadurch würde nicht nur die Rolle der Normung im Bereich der IT-Sicherheit deutlich gestärkt.[1485] Für die Unternehmen würde der Nachweis der Einhaltung der Sicherheitsanforderungen des IT-Sicherheitsgesetzes aufgrund der Vermutung deutlich erleichtert und zugleich ein hohes Maß an Rechtssicherheit für die Wirtschaft geschaffen, da nur die Übereinstimmung mit den technischen Normen dargelegt werden muss. Zu den verwaltungs- und zivilrechtlichen Konsequenzen der Vermutung näher unten Rn. 880, 888 ff..

864 Die Vermutungswirkung sollte nach dem Vorbild des europäischen New Approach (dazu §§ 2 Abs. 16, 4 Abs. 1 Satz 2 GPSG) und des nationalen New Approach (§ 4 Abs. 2 Satz 4 GPSG)[1486] nur bei Einhaltung von technischen Normen zugebilligt werden, welche in einem bestimmten geordneten Verfahren aufgestellt wurden und hinsichtlich der **Qualität der Normung** eine Gewähr für die Wiedergabe der im IT-Sicherheitsgesetz normierten Sicherheitsstandards bieten. Im Einzelnen müssen hierbei insbesondere eine angemessene fachlich-personellen und technischen Infrastruktur bei der normierenden Stelle, die Beteiligung von Behörden und betroffenen Kreisen der Wirtschaft und der Gesellschaft sowie die **Bekanntmachung der Normen**[1487] sichergestellt werden. Das IT-Sicherheitsgesetz könnte hierzu allgemeine verfahrensmäßige Vorgabe hinsichtlich der Aufstellung der technischen Normen und der staatlichen Anerkennung dieser Normen vorsehen. Zu den Möglichkeiten der **Gestaltung der Normungsarbeit** und zu Möglichkeit der **Zertifizierung** und **Akkreditierung** unten Rn. 914 ff.

(3) Regelungsbeispiel: Sicherheitsanforderungen des IT-Sicherheitsgesetzes für Authentisierungsverfahren im eCommerce

865 Konkret bedeutet das vorgeschlagene Regelungsmodell beispielsweise für eine IT-sicherheitsrechtliche Regelung für Authentisierungsverfahren im eCommerce, dass sich das **IT-Sicherheitsgeset**z auf die Festlegung der grundlegenden Sicherheitsanforderung beschränkt:

> IT-Dienstleistungen müssen entsprechend den allgemein anerkannten Regeln der Sicherheitstechnik gestaltet und erbracht werden.

[1485] S. auch BT-Drucks. 15/1620, S. 28, zur Einführung des Vermutungsprinzips im nicht harmonisierten Bereich durch § 4 Abs. 2 Satz 4 GPSG.

[1486] Ausführlich Teil 1 Rn. 238.

[1487] Z.B. im Bundesanzeiger entsprechend dem Vorbild des § 4 Abs. 2 Satz 4 GPSG.

866 **Alternativ** hierzu könnte sich das IT-Sicherheitsgesetz auch auf einen Anhang verweisen:

> IT-Dienstleistungen müssen die im Anhang zu diesem Gesetz aufgeführten Sicherheitsanforderungen erfüllen.

867 In einem **Anhang zum IT-Sicherheitsgesetz** könnten die spezifischen Anforderungen technikneutral weiter spezifiziert und das zu erreichende Sicherheitsziel rechtlich verbindlich formuliert werden. Beispiel:

> Authentifizierungsverfahren müssen gegen ein Ausspähen der Legitimationsdaten des Kunden besonders gesichert sein.

868 Die eigentlichen technischen Anforderungen sind Inhalt der von Fachleuten erarbeiteten **technischen Norm für Authentisierungsverfahren**, welche die in Fachkreisen anerkannten Regeln der Technik widerspiegeln, für den Adressaten des IT-Sicherheitsgesetzes jedoch rechtlich – im strengen Sinne – nicht verbindlich sind, wohl aber Vermutungswirkungen auslösen. Dabei können die Anforderungen im einzelnen auch entsprechend den jeweiligen Anwendungsfeldern von Authentisierungsverfahren im eCommerce differieren. Für das Beispiel des Online Banking könnte der einschlägige Standard etwa vorsehen:

> Sicherungsverfahren für Online-Banking-Systeme müssen auf dem Prinzip des Medienbruchs beruhen bzw. über einen zweiten Kanal verfügen.

869 Auch insoweit ist wieder bevorzugt von einer technik-neutralen Umschreibung gebrauch zu machen. Die eben entworfenen Anforderungen könnten z.B. durch mehrere derzeit bekannte Verfahren erfüllt werden, etwa das mTAN-Verfahren, das Verfahren mit TAN-Generator oder das HBCI-Verfahren.

870 An die Einhaltung der in technischen Norm beschriebenen Sicherheitslösung knüpft das IT-Sicherheitsgesetz eine **Vermutung der Wahrung der bindenden Sicherheitsanforderungen** an. Nach dem Vorbild des § 4 GPSG könnte eine Vermutungsregelung folgenden Wortlaut haben:

> Entspricht eine technische Norm, die von [zum Erlass der technischen Normen zuständige Stelle] ermittelt und von [zuständige Stelle] im Bundesanzeiger bekannt gemacht worden ist, einer oder mehreren Anforderungen an die IT-Sicherheit, wird bei einer nach dieser Norm konzipierten IT-Dienstleistung vermutet, dass sie den betreffenden Anforderungen an die IT-Sicherheit genügt.

c) Sicherheitsanforderungen an Produkte, Dienstleistungen und Anlagen im IT-Bereich

(1) Anforderungen an Produkte und Dienste

871 Die Anforderungen an Produkte und Dienste ließen sich weitgehend zusammenfassen, da ihre materiellen (untergesetzlichen) Standards zwar unterschiedlich sein mögen, aus verfahrensrechtlicher Sicht aber ähnliche Strukturen eingreifen, etwa durch die Zertifizierung von Diensten oder Produkten. Eine Gleichbehandlung rechtfertigt sich ferner vor dem Hintergrund, dass mehr und mehr IT-Produkte, insbesondere Software, durch netzgestützte Dienstleistungen (zumindest teilweise) ersetzt werden, wie z.B. durch sog. Web-Services oder durch Application Providing – selbst Hardware kann zunehmend durch softwarebasierte Lösungen substitutiert werden. Eine strikte Trennung von Produkten und Diensten wäre daher gerade im IT-Bereich nicht ratsam. Dementsprechend wären in diesem Bereich die Fortentwicklungen der Standards zu Protection Profiles und der Common Criteria, aber auch anderer, auf das Internet bezogener Standards anzusiedeln.

872 Auch bezüglich der Anforderungen an die Standards für IT-Produkte und IT-Dienste lassen sich möglicherweise allgemeine, für alle IT-Produkte bzw. Dienste geltende Sicherheitsanforderungen von bestimmten, nur für besondere Kategorien geltenden unterscheiden, etwa für Authentisierungsverfahren im eCommerce (z.B. im Online-Banking). Eine Standardisierung könnte hierauf Rücksicht nehmen durch die Formulierung von Basisanforderungen, auf die dann bestimmte Module aufbauen – auch hier kann das Produktsicherheitsrecht der EU als Vorbild dienen, kennt es doch ebenfalls bestimmte Module, die aufeinander aufbauen.

873 Werden die Anforderungen an IT-Dienstleistungen eingehalten, können sich auch in anderen Konstellationen, insbesondere in zivilrechtlichen Streitigkeiten weitere beweisrechtliche Wirkungen anschließen.

874 Als Beispiel sei hier wieder die bereits in Teil 1 modellhaft untersuchte Konstellation im Online Banking aufgegriffen: Wie in Teil 1 ausführlich dargelegt kann ein Anscheinsbeweis für eine Pflichtverletzung des Bankkunden nur angenommen werden, wenn ein Sicherungsverfahren mit Medienbruch oder zweitem Kanal verwendet wird (Teil 1 Rn.520 ff.). Sofern – was die Bank ggf. durch Vorlage eines Zertifikats zu beweisen hat – diesem Sicherheitsstandard genügt wird, ließe sich aufgrund der technischen Sicherheit des Systems ein Erfahrungssatz formulieren, dem zufolge ein Anscheinsbeweis dafür spricht, dass eine Transaktion im Online-Banking entweder vom Kunden selbst vorgenommen worden ist oder aber der Bankkunde im Umgang mit den Legitimationsmedien seine Sorgfaltspflichten verletzt hat (dazu sogleich unten 940)

(2) Organisatorische und anlagenbezogene Anforderungen

875 Einem zweiten Abschnitt des Besonderen Teils würden dagegen alle anlagenbezogenen Vorschriften enthalten sein, die sich zum einen auf materielle Anforderungen, wie z.B. strikte **Personenkontrollen**[1488], **Brandschutz, Einbruchshemmung** usw. beziehen könnten, zum anderen aber generelle organisatorische Pflichten zur Einführung und Unterhaltung eines **IT-Riskmanagements** entsprechend dem Ansatz des IT-Grundschutzes des BSI (bzw. der ISO 27001 ff.) vorsehen könnten.

876 Flankiert werden können die auf untergesetzliche Normierungen verweisenden Pflichten zur Einrichtung eines IT-Sicherheitsmanagements durch die zwingend erforderliche Bestellung eines **IT-Sicherheitsbeauftragten**, wie er jetzt schon im Rahmen der Best Practice bei vielen Unternehmen als CIO (Chief Information Officer oder Chief IT Officer) vorzufinden ist. Eine Teilregelung hierzu findet sich zudem in § 109 Abs. 3 TKG 2006 über den „Telekommunikationssicherheitsbeauftragten“ und § 4f BDSG über den „Datenschutzbeauftragten“, deren Aufgaben aufgrund ihrer Sachnähe schon nach derzeitiger Rechtslage ein und derselben Person übertragen werden können.[1489] Aus Verhältnismäßigkeitsgründen könnte diese Pflicht erst ab einer bestimmten Größe oder ab einem bestimmten Datenflusses der IT-Anlage eingreifen. Sie sollte den Vorbildern des Datenschutzbeauftragten des BDSG folgen und Stellung, Rechte und Pflichten des Beauftragten regeln, im günstigsten Fall direkt der Geschäftsführung unterstellt werden und ähnlich dem Störfallbeauftragten nach § 1 Abs. 2 der 5. BImSchV in besonderen (Stör-) Fällen selber mit Kompetenzen zur Anordnung von Sicherheitsmaßnahmen befugt.

d) Vollzug

(1) Eingriffsgrundlagen, Anordnungen

877 Der Vollzug eines solchen IT-SicherheitsG wäre den für die Produktsicherheit und für die Anlagensicherheit **zuständigen Behörden** (Gewerbeaufsicht) zu überantworten, gegebenenfalls neu zu schaffenden Vollzugsbehörden. In diesem Rahmen können die klassischen aus dem Produktsicherheitsrecht bekannten Vollzugsstrukturen der Aufsicht Anwendung finden.

878 Die beschriebenen öffentlich-rechtlich fundierten Pflichten können im Wege von Anordnungen auf der Grundlage einer allgemeinen Befugnisnorm umgesetzt werden, ver-

[1488] Vergleichbar etwa § 9 BDSG.

[1489] Beck’scher TKG-Kommentar-*Bock*, § 109 TKG Rn. 44; Säcker-*Klesczewski*, § 109 TKG Rn. 23; Scheurle/Mayen-*Zerres*, § 87 TKG Rn. 29.

gleichbar etwa § 6 I, II KWG, der die BaFin ermächtigt, bei Missständen einzuschreiten. Zudem können aber auch dem Vorbild des GPSG folgend bestimmte spezifische Anordnungsmöglichkeiten im IT-SicherheitsG vorgesehen werden. Insbesondere wären auch **öffentliche Produktwarnungen** möglich, entsprechend den allgemeinen Regelungen im GPSG (s. § 8 Abs. 4 GPSG und Teil 1 Rn. 128 ff.).

879 Darüber hinaus sollte vor allem eine Art **Eilkompetenz** für die Behörden im Benehmen mit einer Bundesbehörde, wie z.B. dem BSI, vorgesehen werden, um Konstellationen zu erfassen, in denen noch kein Standard vorhanden ist. Denkbar wäre auch bei fehlendem Standard eine Eilkompetenz zur Standardsetzung, mit der Maßgabe, dass diese Eil-Standards binnen einer bestimmten Frist von vornherein ihre Wirkung verlieren, um ein ordnungsgemäßes Standardssetzungsverfahren nicht zu unterlaufen.

(2) Vermutungswirkung im Vollzug

880 Entsprechend dem Vorbild des § 8 Abs. 2 Satz 4 GPSG (GS-Zeichen)[1490] könnte an die Erteilung eines Zertifikats durch eine akkreditierte unabhängige Stelle eine Vermutungswirkung gegenüber der Verwaltung geknüpft werden. Die Vermutung würde dahingehend lauten, dass IT-Produkte, IT-Dienstleistungen, IT-Riskmangagementsysteme usw. den **gesetzlichen Anforderungen an die IT-Sicherheit genügen**. Die Verwaltung kann gegenüber einem zertifizierten Produkt, Dienst usw. daher nur dann vorgehen, wenn sie nachweist, dass die erforderliche Sicherheit entgegen dem Zertifikat nicht gewahrt ist, was für Unternehmen wiederum einen Anreiz zu Normkonformität und Zertifizierung setzt.

3. Konsequenzen für andere öffentlich-rechtliche Regelungen

881 Wie oben dargelegt[1491] enthalten zahlreiche andere öffentlich-rechtliche Aufsichtsnormen Ansätze zur Regulierung von IT-Risiken, am deutlichsten etwa § 9 BDSG, § 25a KWG oder § 33 WpHG. So wird im Gefolge der Umsetzung der MiFID-Richtlinie § 25a KWG in Zukunft für die Fragen des Outsourcing von Funktionen das auslagernde Kreditunternehmen dazu verpflichten, auf die Gewährleistung der nötigen EDV-Sicherheit zu achten.[1492] Ebenso überlappen sich einige Anforderungen des § 9 BDSG mit Standardsetzungen etwa des IT-Grundschutzhandbuchs des BSI, das für Standards

[1490] Dazu Teil 1 Rn.. 250 ff.
[1491] Teil 1 Rn. 404 ff. (BDSG), Rn. 439 ff. (KWG) etc.
[1492] Näher dazu *Spindler/Kasten*, AG 2006, 785 ff.

eines IT-Sicherheitsgesetzes für Anlagen herangezogen werden könnte. Gleiches gilt für den bereits erwähnten Komplex der TK-Netzsicherheit (§ 109 TKG).

882 Die Frage liegt daher auf der Hand, ob und wie ein etwaiges IT-SicherheitsG mit den Spezialgesetzen verzahnt werden kann. Hier bieten sich mehrere Möglichkeiten an:

- die jeweiligen Spezialnormen könnten aufgehoben und durch das IT-SicherheitsG ersetzt werden
- die jeweiligen Spezialnormen könnten sich auf einen Verweis auf das IT-Sicherheitsgesetz beschränken (materiell-rechtliche Lösung), hilfsweise durch einen Verweis auf die nach dem IT-Sicherheitsgesetz erlassenen Standards
- die zuständigen Behörden könnten verpflichtet werden, alle öffentlich-rechtlichen Belange zu berücksichtigen, insbesondere nur im Einvernehmen mit dem BSI als zuständiger IT-Standardisierungsbehörde entsprechende Festlegungen zu treffen (verfahrensrechtliche Lösung)

883 Vorzugswürdig erscheint demgegenüber eine **gemischte materiell-rechtliche Lösung einschließlich einer verfahrensrechtlichen Flankierung**. Demnach wäre im IT-SiG zu regeln, dass die Einhaltung der IT-spezifischen Anforderungen in anderen Vorschriften ebenfalls durch die Einhaltung der Standards vermutet wird. Die derzeit von dieser Regelung vorrangig betroffenen Vorschriften (etwa: §§ 9 BDSG, § 25a KWG, § 33 WpHG) könnten in der Begründung in einer – nicht abschließenden – Liste zur Verdeutlichung aufgeführt werden.

884 Auf jeden Fall sollte aber zur **Vermeidung von Dopplungen** in der Regulierung und zur Schaffung von Rechtssicherheit bei den IT-Herstellern, Dienstleistern und Anwendern eine verfahrensrechtliche Regelung geschaffen werden, die die jeweiligen Spezialaufsichtsbehörden dazu verpflichtet, IT-relevante Anordnungen nur im Einvernehmen mit der IT-Standardsetzenden Behörde – hier dem BSI – zu treffen. So würde durch verfahrensrechtliche Absicherungen gewährleistet, daß etwa die BaFin in Umsetzung der Pflichten aus § 25a KWG nicht über die IT-Standards des BSI hinausgehende Anforderungen ohne besondere Rechtfertigung anordnen dürfte.

885 Schließlich ist auch an **Erleichterungen der Überwachung gegenüber IT-Unternehmen** zu denken, die Zertifizierungen ihrer IT-Anlagen aufweisen können. Ähnlich dem Vorbild der EU-Öko-Audit-VO, deren Befolgung und Zertfizierung in fast allen Bundesländern gem. § 58e BImSchG zu Erleichterungen bei der Überwachung der entsprechenden Unternehmen führt, könnten auch im IT-Bereich derartige Rechtsfolgen in Betracht kommen – etwa für § 9 BDSG, für das KWG, WpHG etc.

4. Zivil- und gesellschaftsrechtliche Wirkungen des IT-Sicherheitsgesetzes

886 Auch wenn es sich beim IT-Sicherheitsgesetz um öffentliches Sicherheitsrecht handelt, hätte die Regelung beträchtliche zivil- und gesellschaftsrechtliche Auswirkungen, insbesondere im Rahmen des Haftungsrechts, Vertragsrechts sowie des gesellschaftsrechtlichen Risikomanagements. Für die Praxis von ausschlaggebender Bedeutung sind in allen diesen Bereichen die beweisrechtlichen Wirkungen,welche im IT-Sicherheitsgesetz an die Einhaltung der Standards geknüpft werden können.

a) Regelungsvorschlag: Kodifizierung eines Anscheinsbeweises im Zivilrecht

887 Zur Stärkung der Anreizwirkung des IT-Sicherheitsgesetzes sollte an die Einhaltung der IT-Standards im zivilrechtlichen Bereich ein **querschnittsartiger Anscheinsbeweis für alle Rechtsgebiete** geknüpft werden, der jeweils eingreift, wenn die Einhaltung von Sicherheitspflichten im IT-Bereich in Rede stehen, sei es für einen Unternehmer oder für einen privaten Nutzer (§ 254 BGB). Unter Berücksichtigung der oben für die öffentlich-rechtlichen Eingriffsbefugnisse vorgeschlagenen gesetzlichen Vermutungsregelung ergäbe sich danach folgendes beweisrechtliches Regelungskonzept im IT-Sicherheitsgesetz:

(1) Grundlage: Gesetzliche Vermutung im öffentlichen IT-Sicherheitsrecht

888 Für die **öffentlich-rechtlichen Eingriffsbefugnisse** der Behörde würde das IT-Sicherheitsgesetz eine gesetzliche Vermutung für die Einhaltung der **Sicherheitsanforderungen *des IT-Sicherheitsgesetzes*** vorsehen (dazu oben Rn. 870). Eine entsprechende Regelung wäre für IT-spezifische Anforderungen in **anderen Vorschriften** wie beispielsweise BDSG, KWG und WpHG vorzusehen (zu den gesetzestechnischen Gestaltungsmöglichkeiten oben Rn. 881 ff.) Da die behördlichen Eingriffsbefugnisse auf die Nichteinhaltung der gesetzlichen Vorgaben abstellen, können Unternehmen Verwaltungsmaßnahmen durch Standardkonformität regelmäßig vermeiden. Den zuständigen Behörden obläge in diesem Fall der Beweis, dass die in den Standards niederlegten Sicherheitsmaßnahmen nicht (mehr) den allgemein anerkannten Regeln der IT-Sicherheitstechnik entsprechen.

(2) Mittelbare Wirkung im Zivilrecht

889 Diese gesetzliche Vermutung käme über die Verweisung des **§ 823 Abs. 2 BGB** auch im Rahmen der deliktischen Haftung für **Schutzgesetzverletzungen** zum Tragen. Die Beweislast für die Verwirklichung aller Tatbestandsmerkmale des Schutzgesetzes trägt

– vorbehaltlich einer abweichenden Regelung der Beweislast im Schutzgesetz selbst – grundsätzlich der Geschädigte.[1493] Im Falle des IT-Sicherheitsgesetzes bedeutet dies, dass der Geschädigte Nichteinhaltung der Sicherheitsanforderungen des IT-Sicherheitsgesetzes darzulegen und zu beweisen und folglich bei Standardkonformität des Unternehmens die an die Einhaltung der Standards geknüpfte (öffentlich-rechtliche) gesetzliche Vermutung des IT-Sicherheitsgesetzes zu widerlegen hat. Konkret muss der Geschädigte damit beispielsweise zur vollen Überzeugung des Gerichts darlegen und beweisen, dass *die Standards* die gesetzlichen Sicherheitsanorderungen nicht wiedergeben, weil sie beispielsweise nicht ordnungsgemäß erarbeitet oder überaltert sind.

890 In der praktischen Anwendung ist zu erwarten, dass für die Unternehmen schon aufgrund der Unsicherheiten bei der Konkretisierung der abstrakten Sicherheitsanforderungen ein starker **Anreiz zur Einhaltung der technischen Normen** und zur Zertifizierung besteht. Diese Anreizwirkung wird noch verstärkt, indem sich der Unternehmer aufgrund der gesetzlichen Vermutung unter der Voraussetzung der Normkonformität (und ggf. der Zertifizierung) im Ergebnis quasi von der Haftung für primäre Vermögensschäden vollständig freizeichnen kann.

(3) Anscheinsbeweis im Zivil- und Gesellschaftsrecht

891 Für die verbleibenden Bereiche des Zivil- und Gesellschaftsrechts – insbesondere die rechtsgutsbezogene Haftung nach § 823 Abs. 1 BGB, das Vertragsrecht sowie gesellschaftsrechtliche IT-Riskmanagementanforderungen (z. B. § 91 Abs. 2 AktG) – könnte zudem ein **querschnittsartiger Anscheinsbeweis** für die Einhaltung der **zivil- und gesellschaftsrechtlichen IT-Sicherheitsanforderungen** im Rahmen des IT-Sicherheitsgesetzes eingeführt werden.

892 Ein gesetzliches Vorbild für einen solchen Anscheinsbeweis findet sich im deutschen Recht bereits in **§ 371a Abs. 1 Satz 2 ZPO** für den Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich aufgrund der Prüfung nach dem **Signaturgesetz** (durch Überprüfung der Zuordnung des Signaturprüfschlüssels) ergibt.[1494] Dieser Anschein kann vom Beweisgegner nur durch Tatsachen erschüttert werden, die

[1493] BGH, NJW 2002, 1123 (1124); BGH, NJW 1987, 2008 (2009); Palandt-*Sprau*, § 823 BGB Rn. 81; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 166; MünchKommBGB-*Wagner*, § 823 BGB Rn. 354.

[1494] S. BT-Drucks. 14/4987, S. 24; Musielak-*Huber*, § 371a ZPO Rn. 12; *Fischer-Dieskau/Gitter/Paul/Steidle*, MMR 2002, 709 (711).

ernstliche Zweifel daran begründen, dass die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.

893 Grundlage dieses Anscheinsbeweises ist die **gesetzliche Bestätigung des Sicherheitsstandards**. Der Anschein der Echtheit beruht abweichend von den von der Rechtsprechung für den Beweis des ersten Anscheins entwickelten Grundsätzen nicht auf einem Erfahrungssatz, sondern auf gesetzlicher Vorgabe.[1495] Die Bundesregierung nahm zu entsprechenden Bedenken des Bundesrats im damaligen Gesetzgebungsverfahren wie folgt Stellung:

> „Es bleibt dem Gesetzgeber [...] unbenommen, anstelle eines Erfahrungssatzes einen gesetzlich verbrieften Sicherheitsstandard als Grundlage einer Beweisregel vorzusehen.[1496]

894 In vergleichbarer Weise könnten auch **andere IT-Standards** für den Nachweis der technischen Sicherheit und der dadurch sicheren Kommunikation im Rahmen von § 371a ZPO fruchtbar gemacht werden, ohne dass allein die digitale Signatur hierfür herangezogen werden müsste.

895 Anders als bei der öffentlich-rechtlichen Vermutung (oben Rn. 862 ff.) wäre **Bezugspunkt** des Anscheinsbeweises nicht nur die Einhaltung der Sicherheitsanforderungen des IT-Sicherheitsgesetzes – diese stellen nach allgemeinen Grundsätzen im Zivilrecht nur den Mindeststandard dar, so dass ein Anscheinsbeweis für die Einhaltung der öffentlich-rechtlichen Anforderungen des IT-Sicherheitsgesetzes zivilrechtlich nicht weiterführend wäre (ausführlich Teil 1 Rn. 563 ff.) – , sondern die **Wahrung der (zivil- bzw. gesellschaftsrechtlich) erforderlichen IT-Sicherheitsvorkehrungen** selbst, welche im Einzelfall über das IT-Sicherheitsgesetz hinausgehen können.

896 Im Ergebnis besteht damit beweisrechtlich ein ein **Unterschied zwischen der rechtsgutsbezogenen Haftung nach § 823 Abs. 1 BGB und der Haftung für Schutzgesetzverletzung**, da der Anscheinsbeweis bereits durch die ernsthafte Möglichkeit eines abweichenden (atypischen) Geschehensablaufs im konkreten Einzelfall erschüttert werden kann, wohingegen die Widerlegung der gesetzlichen Vermutung zur vollen Überzeugung des Gerichts feststehen muss. Wertungsmäßig lässt sich dies indes rechtfertigen, da die hochrangigen Rechtsgüter des § 823 Abs. 1 BGB gleichsam den deliktischen Minimalschutz markieren, während an die Befreiung von der Haftung für primäre Vermö-

[1495] Gegenäußerung der Bundesregierung, BT-Drucks. 14/4987, S. 44; Musielak-*Huber*, § 371a ZPO Rn. 7; MünchKomm-ZPO-*Prütting*, § 292a ZPO Rn. 10..

[1496] Gegenäußerung der Bundesregierung, BT-Drucks. 14/4987, S. 44.

gensschäden – welche durch § 823 Abs. 2 BGB abgedeckt werden soll – geringere Anforderungen gestellt werden können.

897 Ein Anscheinsbeweis für die Wahrung der zivilrechtlichen Sorgfalt bewegt sich zudem im Rahmen der Diskussion um die haftungsrechtliche Bedeutung technischer Normen. In der Literatur wurde schon seit jeher ein Anscheinsbeweis bei die Wahrung der im Verkehr erforderlichen Sorgfalt diskutiert,[1497] auch wenn die gegenwärtig herrschende Meinung wohl von einer Indizwirkung der Einhaltung technischer Normen ausgeht (dazu Teil 1 Rn. 539 ff.).[1498] Als **Grundlage des erforderlichen Erfahrungssatzes** lassen sich danach die fachliche Qualifikation und Autorität der Normungsverbände, die Art der Regelaufstellung in einem geordneten Verfahren unter Mitwirkung fachkundiger Vertreter aller beteiligten Interessen, das hohe Ansehen und der hohe Verbreitungsgrad der Regeln sowie die empirisch nachweisbare Tatsache, dass die Beachtung der Regeln der Entstehung von Schäden im allgemeinen wirksam vorbeugt.[1499]

898 Zwar entfaltet ein IT-SicherheitsG zusammen mit untergesetzlichen Standards sowie Zertifizierungen und den damit verbundenen Indizwirkungen bereits eine erhebliche Haftungserleichterung für diejenigen Unternehmen, deren IT-Produkte und –Dienstleistungen zertifiziert worden sind. Im Hinblick auf die angestrebte **Anreizwirkung** des IT-Sicherheitsgesetzes kommt einer Kodifizierung eines Anscheinsbeweises indes eine entscheidende Signalwirkung gegenüber den Unternehmen zu, da er dem Bedürfnis der Wirtschaft nach **Rechtssicherheit** Rechnung trägt.

899 Schließlich wäre noch als Ergänzung daran zu denken, den Anscheinsbeweis nicht nur zugunsten des Pflichtigen bei Einhaltung der vom IT-Sicherheitsgesetz definierten Standards vorzusehen, sondern auch zu dessen Lasten, wenn er diese Standards nicht einhält. Diese könnte besonders in denjenigen Fällen relevant werden, in denen sich noch keine einheitliche Rechtsprechung – anders als etwa im Produkthaftungsrecht bzw. Deliktsrecht (s. Teil 1 Rn. 169 ff.) - herausgebildet hat, die dem Schädiger quasi einen Entlastungsbeweis dafür aufbürdet, daß seine Sicherheitslösungen den Standards gleichwertig sind, wenn feststeht, daß er einen Standard nicht eingehalten hat. Wenn

---

[1497] Siehe dazu Lipps, NJW 1968, 279 (282); *Marburger*, Die Regeln der Technik im Recht, 1979, S. 464; *Marburger*, VersR 1983, 597 (602 f.) mwN.; *Vieweg*, in: Schulte, Handbuch des Technikrechts, 2002, S. 361 f. (im Ergebnis ablehnend)

[1498] Ausdrücklich OLG Celle, NJW 2003, 2544; Soergel-*Krause*, Anh III § 823 Rn. 16; *Foerste*, in: v. Westphalen, ProdHaftHdB, § 24 Rn 41; *Vieweg*, in: Schulte, Handbuch des Technikrechts, 2002, S. 362; *Reiff*, Technische Regeln im Umwelt- und Technikrecht, UTR Band 86, 2006, S. 167.

[1499] So *Marburger*, Die Regeln der Technik im Recht, 1979, S. 464.

daher den Geschädigten die volle Beweislast trifft, daß der Schädiger pflichtwidrig gehandelt hat, kann ein Anscheinsbeweis zu seinen Gunsten im Fall, daß der Schädiger einen Standard nicht eingehalten hat, eingreifen.

900 Eine denkbare Norm sähe etwa wie folgt aus:

"Hängt eine Rechtsfrage vom Erreichen eines in einem [nach dem IT-SiG staatl. akzeptierten und veröffentlichten] Standard festgelegten Sicherheitsziels ab, so greift ein Beweis des Ersten Anscheins zugunsten desjenigen ein, der die Einhaltung der Vorgaben des Standards nachweisen kann, daß er die ihm obliegenden IT-bezogenen Sicherheitspflichten eingehalten hat; andernfalls hat der Pflichtige zu beweisen, daß er das betreffende Sicherheitsziel eingehalten hat".

(4) Auswirkungen auf die Haftung Dritter

901 An die Einhaltung von IT-Sicherheitsstandards können abgesehen von einem Anscheinsbeweis für die Einhaltung der das Unternehmen selbst treffenden Sorgfaltsanforderungen weitere beweisrechtliche Wirkungen anknüpfen. So kommt – abhängig von der technischen Sicherheit des verwendeten Sicherungssystems – insbesondere im Bereich der **Authentifizierungsverfahren im E-Commerce** ein Anscheinsbeweis dahingehend in Betracht, dass der Inhaber der Legitimationsdaten Urheber einer elektronischen Erklärung war oder aber im Umgang mit den Legitimationsdaten die notwendige Sorgfalt nicht beachtet hat. Eine Teilregelung zu diesem Problemkreis findet sich derzeit in § 371a Abs. 1 Satz 2 ZPO für den Anschein der Echtheit einer mit elektronischer Signatur versehenen Erklärung.

902 Beispielhaft lässt sich hier der Bereich des **Online-Banking** anführen, wo ein Anscheinsbeweis für die Urheberschaft des Online-Bankkunden bzw. dessen Pflichtverletzung unter der Voraussetzung bejaht werden kann, dass ein Verfahren mit Medienbruch bzw. zweitem Kanal verwendet wird (dazu ausführlich Teil 1 Rn.582 ff.). Die gesetzliche Regelung eines Anscheinsbeweises ist dem deutschen Recht nicht fremd wie das bereits erwähnte Beispiel des § 371a Abs. 1 Satz 2 ZPO zeigt, wo ebenfalls ein gesetzlich verbriefter Sicherheitsstandard als Grundlage einer Beweisregel gewählt wurde. Die Begründung zu § 292a ZPO a.F. (jetzt § 371a Abs. 1 Satz 2 ZPO) hob damals unter Bezugnahme auf die uneinheitliche instanzgerichtliche Rechtsprechung zum Anscheinsbeweis bei ec-Kartenmissbrauch ausdrücklich hervor, dass eine derartige Beweisregelung insbesondere dann in Betracht kommt, wenn die Rechtsprechung das Vor-

liegen von Erfahrungssätzen ungterschiedlich bewerten könnte.[1500] Gerade die anhaltende Diskussion um die Sicherheit des Online-Banking zeigt, dass ein gesetzlicher Anscheinsbeweis nach dem Modell des § 371a Abs. 1 Satz 2 ZPO, welcher an einen bestimmten technischen IT-Sicherheitsstandard anknüpft hier Rechtssicherheit für die beteiligten Verkehrskreise schaffen kann. Allerdings ist zu beachten, daß hier grundsätzlich Überschneidungen zwischen § 371a Abs. 1 Satz 2 ZPO und einem neuen Anscheinsbeweis bestehen können; anders formuliert, würde ein Anscheinsbeweis zu Lasten des Kunden bei Verwendung sicherer IT-Verfahren seitens des Vertragspartners dazu führen, daß quasi spiegelbildlich zur digitalen Signatur der Kunde sich entlasten müßte.

(5) Zusammenfassung

903 Zusammengefasst ergibt sich damit folgendes beweisrechtliches Gesamtkonzept:

- **Gesetzliche Vermutung** der Wahrung der Sicherheitsanforderungen des IT-Sicherheitsgesetzes bei Einhaltung von sicherheitstechnischen Standards (Bedeutung für behördliche Eingriffsbefugnisse und Schutzgesetzverletzung i. S. v. § 823 Abs. 2 BGB).
- **Querschnittsartiger Beweis des ersten Anscheins** für die Wahrung der zivilrechtlich und gesellschaftsrechtlichen IT-Sicherheitsanforderungen an Unternehmen bei Einhaltung von sicherheitstechnischen Standards (Bedeutung für Vertrags- und Deliktsrecht, IT-Riskmangement).
- **Anscheinsbeweis bei Verwendung von Authentifizierungsverfahren** im E-Commerce (anknüpfend an die Einhaltung von sicherheitstechnischen Standards) für die Urheberschaft Dritter für Erklärung bzw. Pflichtverletzung Dritter im Umgang mit den Legitimationsdaten (Beispiel: Online-Banking).

b) Auswirkungen auf materiell-rechtliche Anforderungen

(1) Haftungsrecht

(a) Rechtsgutsbezogene deliktische Haftung (§ 823 Abs. 1 BGB)

904 Ein IT-Sicherheitsgesetz und in diesem Zusammenhang erarbeitete technische Normen hätten als öffentliches Sicherheitsrecht unmittelbare Auswirkungen auf die Haftung nach § 823 Abs. 1 BGB, da sie zur **Konkretisierung von deliktsrechtlichen Pflichten** herangezogen werden können. Wie an anderer Stelle ausgeführt (Teil 1 Rn. 637) umschreiben Regelungen des öffentlichen Sicherheitsrechts den einzuhaltenden **Mindeststandard**, wobei in der Praxis die Einhaltung der in öffentlich-rechtlichen Regelungen und technischen Normen festgelegten Anforderungen jedoch oftmals gleichbedeutend mit der Wahrung der im Verkehr erforderlichen Sorgfalt ist. Im Einzelfall ist auch die Einhaltung technischer Normen jedoch kein Garant für eine Haftungsentlastung, da der

[1500] Gegenäußerung der Bundesregierung, BT-Drucks. 14/4987, S. 44.

Pflichtige dazu angehalten sein kann, besondere Gefahren im Einzelfall zu berücksichtigen.

905 Zwar entfaltet ein IT-SicherheitsG zusammen mit untergesetzlichen Standards sowie Zertifizierungen und den damit verbundenen **Indizwirkungen** im Rahmen des § 823 Abs. 1 BGB schon nach allgemeinen Grundsätzen erhebliche Haftungserleichterung für diejenigen Unternehmen, deren IT-Produkte und –Dienstleistungen zertifiziert worden sind (dazu Teil 1 Rn. 156 ff.). Die Bedeutung des IT-Sicherheitsgesetzes würde indes durch **ausdrückliche Regelung eines Anscheinsbeweis** erheblich aufgewertet. Dazu ausführlich oben Rn. 891 ff..

(b) Deliktische Haftung für Schutzgesetzverletzungen (§ 823 Abs. 2 BGB)

906 Die größte haftungsrechtliche Bedeutung würde das IT-Sicherheitsgesetz im Rahmen des § 823 Abs. 2 BGB als Schutzgesetz entfalten. Ausgehend von der Qualifikation als Schutzgesetz im Sinne mit individualschützendem Charakter hätte das IT-Sicherheitsgesetz unter Berücksichtigung des oben Rn. 830 ff. beschriebenen Schutzbereichs die **Ersatzfähigkeit primärer Vermögensschäden** zur Folge. Wie in Teil 1 dargelegt (dort Rn.112) ist eines der Defizite der derzeitigen Haftungsregelung die Problematik des Ersatzes von Vermögensschäden.[1501] Die Bedeutung des IT-Sicherheitsgesetzes ginge damit weit über § 4 GPSG hinaus, welcher von der h.M. ebenfalls als Schutzgesetz qualifiziert wird[1502], da der Schutzbereich des GPSG grundsätzlich nur Personenschäden erfasst und damit weitgehend parallel zu § 823 Abs. 1 BGB verläuft.

907 Maßstab der Haftung nach § 823 Abs. 2 BGB für primäre Vermögensschäden wäre die **Einhaltung der Sicherheitsanforderungen des IT-Sicherheitsgesetzes**, nicht aber ein unter Umständen darüber hinausgehender zivilrechtlicher Sorgfaltsmaßstab. Wird der öffentlich-rechtliche Mindeststandard des IT-Sicherheitsgesetz eingehalten, so befreit dies auch zivilrechtlich regelmäßig von der Haftung für primäre Vermögensschäden nach § 823 Abs. 2 BGB, wenn die Vermutung nicht widerlegt werden kann. Zur Darlegungs- und Beweislast oben Rn. 888 ff.

(c) Schaffung einer eigenen Haftungsnorm

[1501] Teil 1 Rn. 112.
[1502] Teil 1 Rn. 222.

908 Im Rahmen eines IT-Sicherheitsgesetzes könnte alternativ eine eigene Haftungsnorm – vergleichbar etwa der Regelung in § 33 GWB – vorgesehen werden. Ein Bedürfnis zur Schaffung einer besonderen Anspruchsgrundlage besteht indes allenfalls dann, wenn an die Ausgestaltung als international zwingendes Recht (Eingriffsnorm) gedacht wird (unten Rn. 1068 ff.). Unsicherheiten bei der Qualifikation des IT-Sicherheitsgesetzes als Schutzgesetz im Sinne des § 823 Abs. 2 BGB können auch durch die ausdrückliche Anordnung der Schutzgesetzeigenschaft im IT-Sicherheitsgesetz, einen Verweis auf § 823 Abs. 2 BGB oder aber eine entsprechend deutliche Äußerung in der Gesetzesbegründung vermieden werden.

(d) Weitere haftungsrechtliche Einzelfragen

(i) Mitverschulden (§ 254 BGB)

909 Festlegungen und Konkretisierungen von IT-Sicherheitsstandards dürften sich auch darauf auswirken, wie der **Mitverschuldenseinwand** nach § 254 BGB konkretisiert wird. Je nachdem, ob die Einhaltung eines solchen IT-Sicherheitsstandards für jedermann zumutbar ist, werden auch entsprechende IT-Standards im Rahmen von § 254 BGB von der Rechtsprechung berücksichtigt.[1503] Auch hier könnte wiederum ein zu schaffender **Anscheinsbeweis** für die Einhaltung den Geschädigten treffenden Obliegenheiten zur Schadensvermeidung und – begrenzung bei Einhaltung bestimmter Standards sprechen. Ein solcher Anscheinsbeweis käme auch Privaten zugute, wenn sie etwa zertifizierte Software verwenden; zwar bezöge sich das IT-SicherheitsG auf Unternehmen und nicht auf Private, doch könnte der Anscheinsbeweis neutral dahingehend formuliert werden, daß zugunsten jedermann, der Pflichten zur IT-Sicherheit unterliegt, ein Anscheinsbeweis der Pflichteinhaltung eingreift, wenn zertifizierte IT-Produkte oder IT-Dienstleistungen verwandt werden.

(ii) Haftungshöchstgrenzen

910 Unabhängig von der konkreten Anspruchsgrundlage können die Haftungsrisiken für Unternehmen ggf. durch Haftungshöchstgrenzen im IT-Sicherheitsgesetz begrenzt werden. Dies hätte vor allem im Hinblick auf die angestrebte Verschärfung der Haftung für primäre Vermögensschäden durch das IT-Sicherheitsgesetz Bedeutung, da Haftungsrisiken für Unternehmen überschaubar und die Versicherbarkeit erleichtert würden.

(2) Vertragsrecht

1503 S. oben Teil 1 Rn. 314 ff.

911 Auch wenn ein IT-SicherheitsG sich nicht unmittelbar auf vertragliche Pflichten bezieht, würde es dennoch mittelbar auf Vertragsbeziehungen einwirken, indem beispielsweise Standards für IT-Produkte die vertragliche geschuldete Beschaffeneheit im Rahmen der §§ 434 Abs. 1 Satz 2, 633 Abs. 2 BGB mitbestimmen.[1504] Ebenso hätten das IT-Sicherheitsgesetz und technische Normen Einfluss auf die Auslegung vertraglicher Sorgfaltsanforderungen (§ 276 BGB). Denn die Festlegung von Minimumstandards erweist sich häufig als klauselfest in dem Sinne, dass sie allenfalls durch eine Individualvereinbarung abbedungen werden dürfen (s. Teil 1 Rn.100). Ein querschnittsartiger **Anscheinsbeweis** für die Einhaltung der erforderlichen IT-Sicherheit würde sich auch im Rahmen des Vertragsrechts bei der Bestimmung der Mangelhaftigkeit oder aber der Konkretisierung vertraglicher Sorgfaltsanforderungen auswirken.

(3) Spezielle Anforderungen an kommerzielle Unternehmen (Riskmanagement;

912 Neben den genannten zivilrechtlichen Konsequenzen können sich durch ein IT-Sicherheitsgesetz auch Auswirkungen auf das Gesellschaftsrecht ergeben, insbesondere im Rahmen der Konkretisierung der nur allgemein vorgegebenen Anforderungen an ein Riskmanagement. Da der Vorstand (bzw. alle anderen geschäftsführenden Organe) aber auch verpflichtet ist, alle öffentlich-rechtlichen Normen einzuhalten,[1505] würde per se auch ein IT-SicherheitsG mit seinen untergesetzlichen Standardisierungen dazu gehören.

913 Eine querschnittsartig angelegte Regelung des **Anscheinsbeweis** im IT-Sicherheitsgesetz würde sich in diesem Zusammenhang auch im Gesellschaftsrecht auswirken. Prima facie wäre danach nicht nur von der Einhaltung der gesellschaftsrechtlichen Anforderungen zum IT-Riskmanagement in Bezug auf die Gesellschaft auszugehen. Vielmehr wäre auch im Rahmen einer möglichen Geschäftsleiterhaftung nach § 43 Abs. 2 GmbHG bzw. § 93 Abs. 2 AktG ein Anscheinsbeweis für die Wahrung der erforderlichen Sorgfalt gegeben. Der dem Geschäftsleiter nach § 93 Abs. 2 Satz 2 AktG obliegende Entlastungsbeweis[1506] würde damit im Falle der Einhaltung der Standards deutlich erleichtert.

[1504] Dazu BGH, NJW 1985, 1769 ff.; *Reiff*, Technische Regeln im Umwelt- und Technikrecht, UTR Band 86, 2006, S. 160.

[1505] S. dazu *Raiser/Veil*, Recht der Kapitalgesellschaften, § 14 Rn. 66.

[1506] Der dort zum Ausdruck kommende Rechtsgedanke gilt grundsätzlich auch für den GmbH-Geschäftsführer, Baumbach/Hueck-*Zöllner/Noack*, § 43 GmbHG Rn. 36, 38.

5. Die mögliche Rolle des BSI

914 Aus dem Vorstehenden werden bereits die verschiedenen potentiellen Rollen und Funktionen des BSI im Rahmen eines IT-SicherheitsG deutlich:

- Erarbeitung der Standard durch das BSI
- Standardsetzung in technischem Ausschuss beim BSI und amtliche Einführung der Standards durch das BSI
- Erteilung von Normungsaufträgen und amtliche Einführung der Standards durch das BSI
- Erteilung von Zertifikaten für die Einhaltung von Standards bzw. die Akkreditierung von Zertifizierungsstellen durch das BSI
- Beteiligung des BSI an Verfahren anderer Behörden

a) Erarbeitung der Standards

(1) BSI als standardsetzende Stelle

915 Das BSI könnte selbst als standardsetzende Behörde tätig werden oder gar zu entsprechenden Verordnungen ermächtigt werden – vergleichbar etwa der BaFin. Aufgaben der Standardsetzung werden dem BSI künftig beispielsweise durch § 4 Abs. 1 Nr. 4 SatDSiG übertragen. Hierbei handelt es sich indes um einen verpflichtend einzuhaltenden technischen Standard, welcher dem Adressaten des SatDaSiG keine Alternativlösungen erlaubt. § 4 SatDSiG[1507] lautet auszugsweise:

> § 4
>
> Genehmigungsvoraussetzungen
>
> (1) Die Genehmigung ist zu erteilen, wenn [...]
>
> 3. die Übermittlung der Daten durch das Orbital- oder Transportsystem an ein Bodensegment des Betreibers oder einer nach § 11 zugelassenen Person, die Übermittlung der Daten zwischen verschiedenen Standorten des Bodensegmentes des Betreibers und die Übermittlung der Daten vom Betreiber an eine nach § 11 zugelassene Person durch ein vom Bundesamt für Sicherheit in der Informationstechnik geprüftes und für geeignet erklärtes Verfahren gegen unbefugte Kenntnisnahme geschützt sind, und [...]

916 Für eine umfassende Erarbeitung von Standards durch das BSI selbst, müssten umfangreiche **personelle und technische Mittel** zur Verfügung stehen. Denkbar wäre in diesem Zusammenhang zwar auch die Delegation der Erarbeitung von Standards durch das BSI an Subunternehmer, welche vom BSI überwacht werden – auch zu diesem Zweck müsste das BSI allerdings auch mit den dafür erforderlichen Ressourcen ausgestattet

[1507] Entwurf eines Gesetzes zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten (Satellitendatensicherheitsgesetz - SatDSiG), BR-Drucks. 65/07 vom 26.1.2007.

werden. Zudem bliebe in beiden Fällen die Veranwortung für das Normungsergebnis beim BSI.

(2) Kooperative Standardsetzung

(a) Standardsetzung in technischem Ausschuss beim BSI und amtliche Einführung der Standards durch das BSI

917 Standards könnten wie bereits oben angedeutet (Rn. 820) durch einen **neu zu schaffenden technischen Ausschuss** unter federführender Beteiligung des BSI (und ggf. anderer Behörden wie beispielsweise der BaFin sowie Vertretern der Wirtschaft, Verbraucher usw.) aufgestellt werden. Wegen des internationalen Bezugs der IT-Sicherheit müsste aber auch dann, wenn die Normen durch ein nationales Gremium ermittelt werden, die internationale Akzeptanz und Kompatibilität der Normungsergebnisse sichergestellt sein. Dies gilt insbesondere hinsichtlich der Abstimmung mit bereits bestehenden Regelwerken auf internationaler Ebene (z.B. ISO, IEC, s. oben Rn. 45 ff.). Die erarbeiteten Standards würden vom BSI (beispielsweise im Bundesanzeiger) amtlich eingeführt, woran wiederum die Vermutungswirkung bei Normkonformität anknüpft.

918 Entsprechend dem Vorbild des Ausschusses für technische Arbeitmittel und Verbraucher Produkte (AtAV) könnte sich die Funktion des beim BSI einzurichtenden Ausschusses aber auch auf die bloße **Ermittlung vorhandener Standards** beschränken, welche dann vom BSI amtlich eingeführt werden.

(b) Erteilung von Normungsaufträgen und amtliche Einführung der Standards durch das BSI

919 Alternativ könnte dem BSI die Aufgabe der Erteilung von **Normungsaufträgen** an private Normungsorganisationen übertragen werden – vergleichbar der Stellung der EU-Kommission gegenüber den europäischen Normungsorganisationen bei europäischen Normungsvorhaben.[1508] Die Verantwortlichkeit für die Richtigkeit der Normen läge in diesem Fall bei den Normungsorganisationen. Bei der Normung durch private Organisationen könnte auf **bestehende Infrastrukturen** zurückgegriffen werden. So besteht im Rahmen des DIN schon gegenwärtig ein Normungsausschuss Informationstechnik NI-27 „IT-Sicherheitsverfahren“, welcher mit der Ausarbeitung von technischen Normen

[1508] Dazu oben Rn. 148 ff.

im IT-Sicherheitsbereich befasst ist.[1509] Der NI-27 repräsentiert auf nationaler Ebene das internationale Komitee ISO/IEC JTC 1/SC 27 "Information Technology – Security Techniques"[1510], an dessen Programm sich die Arbeit des NI-27 orientiert.

920 Zu beachten ist in diesem Zusammenhang das Erfordernis der **Notifikation von Normungsvorhaben** bei der Europäischen Kommission sowie der Mitteilung an die europäischen Normungsorganisationen CEN und CENELEC nach dem Verfahren der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften.[1511]

921 Im Hinblick auf eine Vermutungswirkung im IT-Sicherheitsgesetz bei Einhaltung technischer Standards ist die **amtliche Einführung der Normen** durch das BSI zentraler Bestandteil der Standardsetzung (zum europäischen Produktsicherheitsrecht oben Rn. 850 ff). Dem BSI könnte in diesem Zusammenhang die Kompetenz Bekanntmachung der Standards in öffentlichen Publikationen wie beispielsweise dem Bundesanzeiger übertragen werden, verbunden mit der Befugnis zur vorausgehenden Prüfung der Standards im Hinblick auf Erreichung des gesetzlichen Sicherheitsniveaus sowie Einhaltung eines geordneten Normungsverfahrens. Es muss sichergestellt werden, dass die technischen Normen der tatsächlich die **gesetzlichen Sicherheitsanforderungen wiedergeben** und das **Normungsverfahren objektiv und neutral** durchgeführt wird.[1512] Dies könnte vergleichbar den Allgemeinen Leitlinien auf europäischer Ebene[1513] durch entsprechende Vereinbarungen mit privaten Normungsorganisationen geschehen. Auch ohne förmliche Vereinbarung bestünde aufgrund der an die amtliche Einführung anknüpfenden Vermutungswirkung zumindest ein starker Anreiz für Normungsorganisationen in den von ihnen erarbeiteten Normen das gesetzliche Sicherheitsniveau abzubilden und entsprechende Verfahrensanforderungen einzuhalten. Zu erwarten ist überdies, dass von Seiten der Wirtschaft (welche auch im Normungsverfahren vertreten ist) ent-

[1509] http://www.nia.din.de/sixcms/detail.php?id=22008.

[1510] Siehe http://www.nia.din.de/sixcms/list.php?template=na_index_redirect&query=nania_redirect_q&_nakurz=nia&sv%5balias%5d=sc27

[1511] Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften, ABl. EG L 204, S. 37 und Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20. Juli 1998 zur Änderung der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften.

[1512] Siehe dazu *Marburger*, Die Regeln der Technik im Recht, 1979, 402; BMU, Umweltgesetzbuch (UGB-KomE), 1998, S. 495, 497, 498 f. und oben Rn. 809, 810 und 864.

[1513] Siehe Rn. 148.

sprechender Druck ausgeübt würde, um bei Normkonformität in den Genuss der gesetzlichen Vermutung zu kommen.

b) Mögliche Standards für IT-Sicherheit (Module)

922 Im folgenden werden einige Standards bzw. Module benannt, die durch das BSI in verschiedenen Bereichen bereits betreut, verabschiedet oder gesteuert werden könnten und die sich bereits auf entsprechende Vorarbeiten stützen können. In allen genannten Feldern hat sich in der Praxis ein Handlungsbedarf ergeben, ohne dass diese Beispiele abschließend wären. Alle Beispiele wären Teil einer umfassenden Strategie, die im Wege einzelner Standardisierungen rechtlich akzeptierte Mindestanforderungen aufstellt:

923 An übergreifenden Vorhaben sind zu nennen:

- IT-Riskmanagementsysteme: aufbauend auf BSI-IT-Grundschutz bzw. Teile daraus oder Abwandlungen davon
- Private IT-Nutzung: Benennung der Standardmaßnahmen bezüglich der Abwehr von Viren etc. (aufbauend auf Kompetenz in der Internetsicherheit)
- Sektorspezifische Standards könnten für folgende Bereiche entwickelt werden:
- Weiterentwicklung digitaler Ausweispapiere: Erstellung von Protection Profiles und Technischer Richtlinien für eingesetzte IT-Produkte
- Mautsysteme: Erstellung Protection Profiles und Technischer Richtlinien für eingesetzte IT-Produkte
- Überweisungsterminals: Protection Profiles und Technischer Richtlinien für eingesetzte IT-Produkte
- Online-Banking: Benennung (und damit Standardisierung) hinreichend sicherer Verfahren, bei denen sich ein Anscheinsbeweis zugunsten der Bank bejahen ließe
- Gesundheitswesen: Protection Profiles und Technische Richtlinien für eingesetzte IT-Produkte
- WLAN (IT-Intermediäre): Protection Profiles und Technischer Richtlinien für eingesetzte IT-Produkte (Hersteller) sowie Richtlinien für Anwender zur Sicherung der WLANs
- Meldewesen: Erstellung von PP/TR für eingesetzte IT-Produkte
- Transparente Programmgestaltung und Dokumentation; Geregelte Vorgaben für Funktionen von Programmen betrifft, die ohne Wissen des Nutzers Informationen abrufen, einschließlich von sog. ad-ware oder spyware oder DRM-Systeme.

924 Die gegenwärtig bestehenden IT-Sicherheitsstandards wurden vom Bundesverband Informationswirtschaft, Telekommunikatiopn und neue Medien e. V. (BITKOM) in Zusammenarbeit mit dem DIN Normenausschuss Informationstechnik (NI-27) in einem Leitfaden zusammengestellt[1514]. Einige einschlägige Normungen sind im **Anhang** aufgeführt.

c) Zertifizierung und Akkreditierung

[1514] Abrufbar unter http://www.bitkom.org/files/documents/Kompass_der_IT_28.06.06.pdf.

(1) Derzeitige Zertifizierungs- und Akkreditierungspraxis des BSI und Ausbaumöglichkeiten

925 Neben der Funktion des BSI im Rahmen der Standardsetzung ist an einen Ausbau schon bestehenden Kompetenz des BSI im Bereich Zertifizierung und Akkreditierung zu denken.[1515] So ist das BSI gegenwärtig für die **Akkreditierung**, d.h. die formelle Anerkennung der Kompetenz einer Prüfstelle, bestimmte Prüfungen oder Prüfungsarten durchzuführen, zuständig. Die Akkreditierung erfolgt auf Grundlage der international anerkannten Standards DIN EN ISO/IEC 17025 und DIN EN 45000 ff..[1516]

926 Rechtliche Grundlage für die Vergabe von **Sicherheitszertifikaten für IT-Systeme und Komponenten** durch das BSI ist das BSIG[1517] und die Ausführungsbestimmungen der BSIZertV.[1518] Die Zertifizierung durch das BSI erfolgt aufgrund Antrags des Herstellers oder Vertreibers des IT-Produkts. Die Evaluierungen werden grundsätzlich von den durch das BSI anerkannten Prüfstellen durchgeführt; im Einzelfall führt das BSI selbst die Evaluierung durch. Die eigentliche Zertifizierung erfolgt durch die Zertifizierungsstelle des BSI durch Zertifizierungsbescheid.

927 Gegenstand der Zertifizierung durch das BSI sind derzeit **IT-Produkte**[1519], welche anhand der Common Criteria for Information Technology Security Evalutation (Common Criteria), welche nunmehr als ISO Standard 15408 veröffentlicht wurden, geprüft und bewertet werden.[1520] Daneben bietet das BSI gegenwärtig eine **IT-Grundschutzzertifizierung**, anhand der IT-Grundschutzkataloge des BSI an, welche nunmehr auch die Zertifizierung nach der Norm ISO 27001 abdeckt. Durch das Grundschutzzertifikat können Unternehmen und Behörden ihr IT-Sicherheitsmanagement gegenüber Kunden und Vertragspartnern nachweisen.

[1515] Siehe http://www.bsi.de/zertifiz/akkred/index.htm.

[1516] Eine Liste der vom BSI akkreditierten Zertifizierungsstellen ist abrufbar unter http://www.bsi.de/zertifiz/zert/pruefst.htm.

[1517] BSI-Errichtungsgesetz vom 17. Dezember 1990, BGBl. I, S. 2834, zuletzt geändert durch Artikel 11 der Verordnung vom 25.11.2003, BGBl. I, S. 2304

[1518] Verordnung über das Verfahrender Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung – BSIZertV) vom 7.7.1992, BGBl. I, S. 1230.

[1519] Beispiele: Software-Produkte (z. B. Betriebssysteme, Datenbanksysteme) Firmware (z. B. Smart Card-Betriebssyteme), Hardware-Produkte (z. B. Smart Card Integrated Circuits), Kombinationen aus Software und Hardware (z. B. HW einer Smart Card zusammen mit einem Betriebssystem), IT-Systeme, die aus mehreren Produkten bestehen sowie Werkzeuge zur Produktentwicklung, siehe BSI, BSI-Zertifizierung und BSI-Produkt-Bestätigung, 2004, S. 7 f., abrufbar unter http://www.bsi.bund.de/zertifiz/zert/7138.pdf..

[1520] BSI, BSI-Zertifizierung und BSI-Produkt-Bestätigung, 2004, S. 7, abrufbar unter http://www.bsi.bund.de/zertifiz/zert/7138.pdf.

928 Um die mehrfache Zertifizierungen des gleichen Produktes und des gleichen Schutzprofils in verschiedenen Staaten zu vermeiden, wurde eine **gegenseitige Anerkennung von IT-Sicherheitszertifikaten** vereinbart, welche auf ITSEC oder Common Criteria beruhen. Zertifikate der Unterzeichnerstaaten werden damit in den jeweils anderen Sicherheitszertifikate anderer anerkannter Prüfstellen aus dem Bereich der Europäischen Gemeinschaft werden vom BSI anerkannt soweit sie eine den Zertifikaten des BSI gleichwertige Sicherheit ausweisen (§ 4 Abs. 4 BSIG).

929 Die schon bestehenden Bereiche, in denen eine Zertifizierung erfolgt, könnte ggf. auf bislang **noch nicht abgedeckte Bereiche** wie beispielsweise die Zertifizierung von **IT-Dienstleistungen** erstreckt werden. Antragsberechtigt wären in diesem Fall die Betreiber der entsprechenden Online-Plattformen. Hierbei wäre beispielsweise an die Zertifizierung der Gestaltung von Websites etwa für das Online-Banking (z.B. Verzicht auf aktive Elemente), aber auch in anderen (sensiblen) Bereichen des E-Commerce zu denken. Bei der praktischen Umsetzung könnte auf die beim BSI schon bestehenden Akkreditierungs- und Zertifizierungsinfrastrukturen zurückgegriffen werden, so dass die vorangehende Prüfung zur Entlastung der öffentlichen Hand wie bisher auf private Prüfstellen übertragen würde.

930 Nur angedeutet werden können an dieser Stelle die **technischen Grenzen der Zertifizierung** im IT-Bereich: eine Zertifizierung kann stets nur den sicherheitstechnischen Zustand des Prüfungsgegenstandes im Zeitpunkt der Überprüfung bescheinigen, was beispielsweise bei adaptiver, also anpassungsfähiger Software den Aussagegehalt des Zertifikats hinsichtlich der Wahrung der IT-Sicherheitsanforderungen in der Folgezeit erheblich mindern kann, mit entsprechenden Auswirkungen auf die (beweis-) rechtliche Bedeutung des Zertifikats. In die gleiche Richtung gehen Bedenken aufgrund des rasanten Wandels der Software und neuerer Entwicklungen, auch im Rahmen von Updates. Denkbar wäre hier die Zertifizierung der Systeme oder des Softwareengineering-Prozesses selbst, was indes weiterer technischer und rechtlicher Analyse bedarf. Überdies zeigt die Praxis der großen Softwarehäuser, daß häufig bestimmte grundlegende Releases (bzw. grundlegende Neuentwicklungen wie Windows XP oder Vista) sich über mehrere Jahre hinweg erstrecken, sei es etwa bei Adobe, Microsoft, SAP oder anderen Softwarefirmen.

(2) Rechtliche Wirkungen einer Zertifizierung

931 Auf etwaige beweisrechtliche Wirkungen von Zertifikaten würde bereits im Zusammenhang mit den öffentlich-rechtlichen Eingriffsbefugnissen nach dem IT-Sicherheitsgesetz sowie den zivil- und gesellschaftsrechtlichen Wirkungen des IT-Sicherheitsgesetzes hingewiesen (oben Rn. 880, 888 ff. und 891 ff.).

932 Nur am Rande sei an dieser Stelle erwähnt, dass eine die Einführung eines Zertifizierungsmodells ein klassisches **Problem des Nachweises sicherer Verfahren im Prozess** lösen könnte: Denn die Darlegung und der Beweis von Sicherungsverfahren, insbesondere interner organisatorischer Vorkehrungen, können immer dazu führen, dass die nötige **Geheimhaltung** durchbrochen und die Sicherungsvorkehrungen damit ineffektiv werden.[1521] Der IT-Dienstleister und Anlagenbetreiber sieht sich hier zwischen Scylla und Charybdis: Offenbart er die Sicherungsmechanismen, riskiert er deren Nutzlosigkeit in Zukunft – unterlässt er dies, bleibt er im Prozess beweisfällig. Aus diesem Dilemma können Gütesiegel, Testate oder eben auch Zertifikate herausführen, indem bei einem zertifizierten Sicherungsverfahren keine Notwendigkeit der Offenbarung der Sicherungsvorkehrungen besteht. Allerdings ist einzuräumen, dass dies nach wie vor nicht mit der ständigen Rechtsprechung konform ginge, die zum einen den Rechtsschutz der Partei gewährleisten will, das heißt auch hier die Offenlegung jedenfalls des Zertifizierungsverfahrens verlangen würde, zum anderen im Einzelfall strengere Anforderungen stellt als dies die zertifizierte Einhaltung der IT-Sicherheitsnorm verlangen würde.

(3) Kosten der Zertifizierung

933 Die **Kosten** der Zertifizierung würden entsprechend der bestehenden Zertifizierungspraxis die antragstellenden Unternehmen treffen. Sie werden vom BSI auf Grundlage der BSI-Kostenverordnung[1522], von den akkreditierten Prüfstellen aufgrund vertraglicher Vereinbarung mit dem antragstellenden Unternehmen erhoben.

934 Unter Umständen können die Kosten einer Zertifizierung für kleinere Unternehmen eine erhebliche finanzielle Belastung bedeuten, wollen sie an den wirtschaftlichen Vorteilen einer Zertifizierung teilhaben. Die Zertifizierung ist zwar insgesamt freiwillig, doch ist nicht zu verkennen, dass für Unternehmen ein gewisser Druck zur Zertifizierung entstehen kann. (Haftungs-)Rechtlich bewirkt eine Einhaltung von Standards und eine darauf

[1521] Siehe hierzu OLG Brandenburg, MMR 2006, 107 ff. mit Anm. *Spindler* zur Darlegung von Sicherheitsmaßnahmen gegen Namensanmaßung durch ein Internet-Auktionshaus.

[1522] Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung – BSI-KostV), BGBl. I 1992 S. 1838.

aufbauende Zertifizierung einen starken Anreiz durch Durchführung entsprechender Verfahren – sei es einer gesetzlichen Vermutung im öffentlichen IT-Sicherheitsgesetz, sei es um einer Indizwirkung im Zivilrecht Willen. Hinzu kommt die wirtschaftliche Bedeutung einer Zertifizierung im Hinblick auf Werbung, Vergabe von Aufträgen usw.. Zur Lösung dieses Problems ließe sich an die Einführung einer Gebührenordnung für Zertifizierungen denken, womit indes eine generelles Problem des Zertifizierungssystems angesprochen ist, welches an dieser Stelle nicht vertieft werden kann.

d) Einvernehmenslösungen mit anderen Behörden

935 Das BSI kann die öffentlich-rechtlichen Belange der IT-Sicherheit auch im Rahmen anderer Verfahren wahrnehmen etwa in Gestalt einer Einvernehmensregelung gegenüber anderen Behörden, wenn es um die Berücksichtigung von IT-spezifischen Anforderungen bei Genehmigungen oder Anordnungen geht. Entsprechende spezialgesetzliche Befugnisse des BSI im Rahmen von Einvernehmens-/Benehmens-Lösungen finden sich derzeit beispielsweise in § 24c Abs. 6 KWG, § 2 Abs. 4 KapMuG, § 303c Abs. 2 SGB V, § 151a Abs. 3 SGB VI, § 21 Abs. 4 KHEntgG, § 1 Abs. 2 StDÜV, früher auch in § 87 Abs. 1 TKG 1996[1523]. Die § 24c KWG lauten auszugsweise:

> § 24c: Automatisierter Abruf von Kontoinformationen
>
> (6) Das Kreditinstitut und die Bundesanstalt haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der abgerufenen und weiter übermittelten Daten gewährleisten. Den Stand der Technik stellt die Bundesanstalt im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik in einem von ihr bestimmten Verfahren fest.

6. Zusammenfassung: Die Struktur eines IT-SicherheitsG

936 Ziel eines IT-Sicherheitsgesetzes sollte es sein, eine allgemeine Erhöhung des IT-Sicherheitsniveaus herbei zu führen. Dies kann auf Dauer nur durch gemeinsame Anstrengungen auf internationaler, insbesondere aber europäischer Ebene gelingen. Gerade mit der Schaffung eines IT-Sicherheitsgesetzes könnte eine Vorreiterrolle in Europa und im internationalen Bereich eingenommen werden. Die vorgeschlagene Einbettung des IT-Sicherheitsgesetzes in das öffentliche Sicherheitsrecht trägt vor allem der Tatsache Rechnung, dass zivilprozessualen Beweisproblemen im Internetverkehr nicht völlig auf gesetzlicher Ebene begegnet werden kann und private Anreize zur Erhöhung des IT-

[1523] Das TKG enthält heute in § 109 keine explizite Regelung mehr des Benehmens mit dem BSI.

Sicherheitsniveaus nicht immer in ausreichendem Maße vorhanden sind. Ein IT-Sicherheitsgesetz kann aber sehr wohl quasi querschnittsartig greifen, indem über das öffentliche Recht für alle anderen Rechtsgebiete – verbunden mit entsprechenden Vermutungswirkungen – Standards festgesetzt werden könnten. Vorbildfunktion kann hier etwa das SigG (zusammen mit dem FormAnpassG) entfalten, das ebenfalls hinsichtlich der Gleichstellung der elektronischen mit der schriftlichen Form querschnittsartig zahlreiche Rechtsmaterien harmonisiert hat.

937 Zusammengefaßt ergeben sich folgende **Vorteile** durch ein allgemeines IT-SicherheitsG:

- Durch ein IT-Sicherheitsgesetz kann ein allgemein höheres Niveau im Bereich der IT-Sicherheit erreicht werden, wodurch indirekt nicht nur der Verbraucherschutz, sondern auch der Kriminalprävention durch eine höhere Schutzdichte Rechnung getragen wird.
- Eine Regelung der IT-Sicherheitsanforderungen in einem einheitlichen Gesetz verbunden mit Standards für eine Basissicherheit schafft Rechtssicherheit und Rechtsklarheit für Unternehmen gegenüber der derzeitigen rechtlichen Zersplitterung.
- Das vorgeschlagene IT-Sicherheitsgesetz bewirkt Kontinuität mit dem auf europäischer Ebene im Produktsicherheitsrecht verfolgten Regelungsmodell des New Approach durch gesetzliche Regelung grundlegender Sicherheitsanforderungen, Verweis auf technische Standards und Vermutungswirkungen bei Normkonformität; das IT-Sicherheitsgesetz kann damit eine Vorreiterrolle für eine künftige europaweite Harmonisierung einnehmen.
- Der Verweis auf technische Standards unter Beteiligungsmöglichkeit der öffentlichen Hand erlaubt eine im Prinzip hohe Flexibilität sowie einen hohen Detaillierungsgrad. Die erstellten Standards würden sich zudem in ein bereits bestehendes System internationaler Standards einfügen.
- Durch die Entwicklung rechtlich unverbindlicher Standards mit daran anknüpfender Vermutungswirkung gewährleistet den notwendigen rechtlichen Freiraum um technische Innovationen voranzutreiben.
- Es würde für IT-Produkte, IT-Dienstleistungen sowie IT-Riskmanagementsysteme ein Standard für die Basissicherheit definiert werden, der auch öffentlich-rechtlich durchgesetzt werden könnte, zum einen breitflächig mit Hilfe privater Zertifizierungsinstitutionen, die wiederum der staatlichen Kontrolle durch Akkreditierungen unterlägen, zum anderen in besonderen Fällen punktuell durch die Befugnis zur Anordnung im Einzelfall. Im Rahmen des Wettbewerbs ist zu vermuten, dass sich nur solche Produkte am Markt halten können, die den entsprechenden Standards entsprechend und zertifiziert sind.
- Es könnten IT-spezifische Schäden erfasst werden, gleichzeitig auch Beweiserleichterungen für Geschädigte aufgrund der Vermutungswirkung geschaffen werden, insbesondere in zivilprozessualer Hinsicht.

938 Die öffentlich-rechtliche Verankerung der IT-Sicherheitsanforderungen ermöglicht deren Durchsetzung unabhängig von prozessualen Nachweisproblemen im Zivilrecht.

- Die Ausgestaltung des IT-Sicherheitsgesetzes als Schutzgesetz im Sinne von § 823 Abs. 2 BGB und das daran anknüpfende Risiko der Haftung für primäre Vermögensschäden, schaffen Anreize für die Unternehmen IT-Sicherheitsstandards einzuhalten und die Normkonformität zertifizieren zu lassen. Durch die Beschränkung auf bestimmte Gefährdungstypen und Schäden werden übermäßige Haftungsrisiken vermieden, andererseits aber bestimmte sonst kaum oder nicht erfasste Schäden denjenigen belastet, die sie am besten beherrschen können.

- Durch die Beschränkung auf bestimmte Gefährdungstypen und Schäden werden übermäßige Haftungsrisiken vermieden, andererseits aber bestimmte sonst kaum oder nicht erfasste Schäden denjenigen belastet, die sie am besten beherrschen können.

939 Ein IT-SicherheitsG würde sich demnach wie folgt strukturieren:

- *Anwendungsbereich*:
- Persönlicher Anwendungsbereich (IT-Hersteller, IT-Dienstleister, Intermediäre, kommerzielle IT-Anwender)
- Sachlicher Anwendungsbereich (Herstellung von IT-Produkten, Erbringung von IT-Dienstleistungen, Netze, Organisation/Management von IT-Einsatz)
- *Pflichtenprogramm*
- Basis-Sicherheitsanforderungen (ggf. differenziert nach Anwendungsbereich (IT-Produkte, IT-Dienstleistungen, Netze, IT-Organisation)
- Sektorspezifische Anforderungen mit Verweis auf Anhang (z.B. nach obigem Bsp. für Authentisierungsverfahren)
- Klarstellung, dass Pflichtenprogramm des IT-SiG (grds.) alle weiteren IT-bez. Anforderungen aus sonstigen Gesetzen harmonisiert
- *Standards und Standardsetzung*
- Verweis auf Standards zur Konkretisierung der gesetzlichen Vorgaben aus 2.
- Beschreibung der Normungsarbeit
- Beschreibung des Verfahrends der amtlichen Einführung der Standards]
- *Prozessuale Wirkungen der Standards*
- Vermutungswirkung der Wiedergabe der allgemein anerkannten Regeln der IT-Sicherheit durch vom Staat akzeptierte Normen (für Vollzug des IT-SiG)
- Querschnittsregelung eines Anscheinsbeweises für die Einhaltung der erforderlichen IT-Sicherheit auch in anderen Rechtsgebieten
- Nachweis der Einhaltung des Standards (Vermutung) durch Zertifikat des BSI (bzw. vom BSI akkreditierte Prüfer)
- *Öffentlich-rechtliche Flankierung*
- Ermächtigungen zum Vollzug bzw. Ausführungsbestimmungen
- ggf. IT-Sicherheitsbeauftragter
- *Sonstiges*
- ggf. Haftungshöchstgrenzen

V. Einführung einer IT-Gefährdungshaftung

940 Schließlich ist in die Überlegungen noch ein weiterer Schritt einzubeziehen: Die Einführung einer Gefährdungshaftung für IT-Anlagen – wiederum vergleichbar anderen Gefährdungshaftungstatbeständen wie den Regelungen des UmweltHG, des StVG oder des GenTG. Gegenüber dem grundsätzlich verschuldensabhängigen Deliktsrecht des BGB (§§ 823 ff. BGB) bietet eine Gefährdungshaftung für den Geschädigten die Erleichterung, keinen objektiven Sorgfaltspflichtverstoß und kein Verschulden des Schä-

digers beweisen zu müssen. Ob die Regelung einer Gefährdungshaftung notwendig und empfehlenswert ist, muss anhand des hypothetischen Anwendungsbereichs einer solchen verschuldensunabhängigen Einstandspflicht im IT-Verkehr überprüft werden.

1. Grundlinien der bestehenden Gefährungshaftungstatbestände

941 Das Recht der Gefährdungshaftung setzte sich erst im 20. Jahrhundert als eigenständiges Rechtsinstitut durch. Im BGB nimmt das Verschuldenspinzip eine zentrale Stellung ein,[1524] auch wenn sich seit jeher in § 833 S.1 BGB die Gefährdungshaftung des Tierhalters findet. Die neueren (spezialgesetzlichen) Gefährdungshaftungstatbestände sind primär **Reaktionen auf die Gefahren der modernen Technik** der industriellen Gesellschaft.[1525] So finden sich gegenwärtig verschuldensunabhängige Haftungstatbestände für Schienenfahrzeuge (§ 1 HaftPflG) und Elektrizitäts- und Gasanlagen (§ 2 HaftPflG), für Fahrzeuge im Straßenverkehr (§ 7 StVG), für Kernenergieanlagen (§§ 25 ff. AtG), für Umweltschäden (§ 1 UmweltHG), für Bergschäden (§ 114 BBergG), für Arzneimittel (§ 84 AMG), für fehlerhafte Produkte (§ 1 ProdHaftG), für gentechnische Anlagen (§ 32 GenTG), sowie für Einwirkungen auf das Wasser (§ 22 WHG). In allen diesen Fällen handelt es sich um bereichsspezifische Regelungen, die eine Ausnahme vom Verschuldensprinzip des BGB darstellen.[1526] Eine einheitliche Kodifikation des Rechts der Gefährdungshaftung – etwa in einer Generalklausel – fehlt. Vielmehr ist die gegenwärtige Rechtslage zersplittert, auch wenn sich gewisse zugrundeliegende Regelungsmuster und Grundprinzipien herausarbeiten lassen:

a) Charakteristika der geltenden Regelungen

942 Für das Recht der Gefährdungshaftung gilt wegen der spezialgesetzlichen Regelung nur für bestimmte Sachverhaltskonstellationen das **Enumerationsprinzip**.[1527] Die einzelnen Tatbestände können nur unter äußerst strengen Voraussetzungen[1528] analog auf gesetzlich nicht geregelte Sachverhalte angewendet werden.[1529] Hintergrund des Enumerationsprinzips ist die Überlegung, dass der potentielle Schädiger wegen der strengen Haf-

[1524] Soergel-*Spickhoff*, Vor § 823 BGB Rn. 46.

[1525] *Deutsch/Ahrens*, Deliktsrecht, Rn. 355; *Kötz/Wagner*, Deliktsrecht, Rn. 494; *Larenz/Canaris*, § 84 I 1 a, S.600.

[1526] *Deutsch*, Allgemeines Haftungsrecht, Rn. 656 f.; *Larenz/Canaris*, § 84 I, S.600.

[1527] BGHZ 54, 332; BGHZ 55, 229; *Deutsch/Ahrens*, Deliktsrecht, Rn. 363; *Deutsch*, Allgemeines Haftungsrecht, Rn. 651; *Larenz/Canaris*, § 84 I 1 b, S. 601 f.; Staudinger-*Hager*, Vorbem zu §§ 823 ff Rn. 29.

[1528] Dazu *Deutsch*, Allgemeines Haftungsrecht, Rn. 652 ff.; *Larenz/Canaris*, § 84 I 1 b, S. 601.

[1529] Siehe etwa BGH, NJW 1960, 1345: keine Gefährdungshaftung für Schlepp- oder Sesselliftе;OLG Hamburg, VersR 1982, 561: keine Gefährdungshaftung für Hochsitze; OLG Karlsruhe, VersR 2003, 752: keine Gefährdungshaftung für schnelle Binnenschiffe.

tung von seiner möglichen verschuldensunabhängigen Einstandspflicht wissen muss, damit er gegebenenfalls Vorsorge durch Abschluss einer Haftpflichversicherung treffen kann. Das Erfordernis nach Rechtssicherheit im Bereich der Gefährdungshaftung führt letztlich dazu, dass Gefährdungshaftungstatbestände praktisch in der alleinigen Entscheidungsgewalt des Gesetzgebers liegen (s. auch unten Rn. 948 f. (besondere Gefahr)).[1530]

943 Allen Gefährdungshaftungstatbeständen gemeinsam ist – parallel zu § 823 Abs.1 BGB – die **Beschränkung des Schutzbereiches** auf die Verletzung der Rechtsgüter Leben, Körper, Gesundheit und Eigentum.1531 Nicht erfasst werden dagegen sonstige Rechte im Sinne des § 823 Abs. 1 BGB, insbesondere nicht das Recht am eingerichteten und ausgeübten Gewerbebetrieb, sowie primäre – d.h. nicht durch eine Rechtsgutsverletzung vermittelte – Vermögensschäden. Einzige **Ausnahme** hierzu ist **§ 22 WHG**, welcher ausnahmsweise auch primäre Vermögensschäden erfasst,[1532] was indessen auf die Besonderheiten des Wasserrechts zurückzuführen.[1533] So unterliegt etwa das Grundwasser einer vom Oberflächeneigentum losgelösten öffentlich-rechtlichen Benutzungsordnung.[1534] Trotz fehlender Eigentumsverletzung gewährt § 22 Abs.1 WHG dem Nutzungsberechtigten im Falle einer ihn schädigenden Verunreinigung des Grundwassers einen Ersatzanspruch.[1535] Nach § 22 WHG ersatzfähig sind daher beispielsweise die Kosten zur Schadensbeseitigung oder der Verhinderung einer Verschmutzung des Wassers, selbst wenn das in seiner Beschaffenheit nachteilig veränderte Gewässer nicht im Eigentum des Geschädigten steht.[1536] Nicht ersatzberechtigt sind dagegen Dritte, auf deren Vermögen sich die nachteilige Veränderung des Wassers nur mittelbar auswirkt.[1537] Letztlich ist auch die Regelung des § 22 Abs. 1 WHG zumindest in gewisser Weise rechtsgutsbezogen, als sie dem Schutz des Wassers als Lebensgrundlage und damit dem Schutz der hochrangigen Schutzgüter Leben und Gesundheit dient. Als Ausnahmerege-

[1530] BGHZ 55, 229 (234); *Deutsch/Ahrens*, Deliktsrecht, Rn. 363; *Kötz/Wagner*, Deliktsrecht, Rn. 492, 514; *Larenz/Canaris*, § 84 I 1 b, S.601 f.

[1531] *Larenz/Canaris*, § 84 I 1 c, S. 602; *Schäfer/Ott*, Ökonomische Analyse des Zivilrechts, S.204.

[1532] BGHZ 103, 129 (140); *Deutsch/Ahrens*, Deliktsrecht, Rn. 396; *Deutsch*, Allgemeines Haftungsrecht, Rn. 648, 883; *Medicus*, Schuldrecht-BT, Rn. 896; *Czychowski/Reinhardt*, § 22 WHG Rn. 29; Sieder/Zeitler-*Schwendner*, § 22 WHG Rn. 55; aA *Kotulla*, § 22 WHG Rn. 15.

[1533] Dazu *Larenz/Canaris*, § 84 I 1 c, S. 603, V 1 f, S. 636.

[1534] BVerfGE 58, 300 (328 f., 344).

[1535] BGHZ 103, 129 (133, 140); Sieder/Zeitler-*Schwendner*, § 22 WHG Rn. 48.

[1536] BGHZ 103, 129 (133, 140).

[1537] Sieder/Zeitler-*Schwendner*, § 22 WHG Rn. 48.

lung dürfte sich § 22 WHG indes kaum als Regelungsmodell für eine Gefährdungshaftung für primäre Vermögensschäden im IT-Bereich eignen.

944 Im Unterschied zur deliktischen Haftung unterliegt die Gefährdungshaftung regelmäßig einer betragsmäßigen **Haftungshöchstgrenze**, was die Versicherbarkeit der gefährlichen Tätigkeit erleichtern soll. Hinzu kommen besondere **Haftungsausschlussgründe** im Falle höherer Gewalt oder unabwendbarer Ereignisse (so noch § 7 Abs. 2 StVG a.F.). Als begleitende Regelungen zur Einführung von Gefährdungshaftungstatbeständen sind vielfach **Pflichtversicherungen** und **Entschädigungsfonds** (z.B. §§ 1, 12 PflVG für Kraftfahrzeuge) oder Pflichten zur **Deckungsvorsorge** (z.B. §§ 13 AtG, 19 UmweltHG, 36 GenTG, 94 AMG).

945 Im Ergebnis lassen sich bestimmte Grundtypen der Gefährdungshaftung ausmachen. Von der Halter-, Anlagen- und Zustandshaftung (z.B. StVG, AtG, UmweltHG) ist die Haftung für gefährliche Handlungen zu unterscheiden (z.B. § 1 ProdHaftG, § 84 AMG, § 32 GenTG). Das Gesetz knüpft hierbei zum Teil an die generelle Gefährlichkeit der Anlage oder Handlung, zum Teil aber auch an die konkrete Fehlerhaftigkeit an (z.B. § 1 ProdHaftG).

b) Gerechtigkeitskriterien

946 Alle Gefährdungshaftungstatbestände können trotz ihres Charakters als nur punktuelle Spezialregelung auf bestimmte gemeinsame Gerechtigkeitserwägungen zurückgeführt werden.[1538] Zentrale Kriterien sind hierbei die **Gefahrveranlassung** und **Gefahrbeherrschung**.[1539] Den Gefährdungshaftungstatbeständen gemein ist die Schaffung einer besonderen Gefahr, welche über die Gefahren hinausgehen, welche mit den meisten anderen Handlungen verbunden sind.[1540] Anknüpfungspunkt für die Haftung des jeweiligen Akteurs ist dabei nicht die konkrete Gefahrbeherrschung, sondern die bloß **abstrakte Veranlassung und Beherrschung** der Gefahr durch Schaffung und Aufrechterhaltung der Gefahrenquelle.[1541] Abzustellen ist folglich nicht auf die einzelne (Betriebs-)Handlung, sondern auf die Herbeiführung einer allgemeinen Risikosituation.[1542] Hinzu kommt, dass der Halter der gefährlichen Anlage bzw. der Handelnde durch überobliga-

[1538] *Deutsch*, Allgemeines Haftungsrecht, Rn. 635; *Larenz/Canaris*, § 84 I 2, S. 604 ff.

[1539] *Blaschczok*, S. 53 ff., 65 ff., 70 ff.; *Deutsch*, Allgemeines Haftungsrecht, 355;*Kötz*, AcP 170 (1970), 1 (20f.); *Larenz/Canaris*, § 84 I 2 a, S. 605; Staudinger-*Hager*, Vorbem zu §§ 823 ff Rn. 28.

[1540] *Blaschczok*, Gefährdungdshaftung und Risikozuweisung, 1993, S. 53; *Larenz/Canaris*, § 84 I 2 a, S.605; *Kötz*, AcP 170 (1970), 1 (29).

[1541] *Deutsch*, Allgemeines Haftungsrecht, Rn. 641; *Larenz/Canaris*, § 84 I 2 a, S.605.

[1542] *Deutsch*, JuS 1981, 317 (318).

tionsmäßige Sicherungsmaßnahmen das Risikopotential seiner Anlage steuern kann. Insbesondere im unternehmerischen Bereich wird die strenge Gefährdungshaftung überdies von der Überlegung getragen, dass der **Vorteilsziehung** aus der gefährlichen Anlage, das **Risiko** der Haftung in daraus resulierenden Schadensfällen entsprechen muss, welches der Unternehmer über eine Haftpflichtversicherung oder die Preisgestaltung für seine Leistungen wiederum auf seine Kunden abwälzen kann.[1543] In Bereichen, welche einer Gefährdungshaftung unterliegen, sind überdies die Möglichkeiten des Selbstschutzes oftmals stark eingeschränkt, wenn nicht sogar ausgeschlossen (z.B. bei Atomunfällen), so dass eine verschuldensunabhängige Haftung auch durch die **Unausweichlichkeit der Gefahr** gerechtfertigt wird.[1544]

947 Kein tragfähiges Argument ist indessen die Verknüpfung der Gefährdungshaftung mit der **Erlaubtheit des Risikos**. Mit anderen Worten ist die Regelung einer verschuldensunabhängigen Einstandspflicht nicht die Voraussetzung dafür, dass die mit einer Gefährdungshaftung belegte Tätigkeit überhaupt durchgeführt werden darf.[1545]

c) Zentralbegriff: Die „besondere Gefahr“

948 Alle Gefährdungshaftungstatbestände beruhen auf der ungeschriebenen Voraussetzung der Verwirklichung einer **besonderen Gefahr**.[1546] Schon ein Überblick über die zersplitterten Regelungen der Gefährdungshaftung in einer Vielzahl von Einzelgesetzen macht indes deutlich, dass nicht jede besondere Gefahr durch eine Gefährdungshaftung aufgefangen wird.[1547] So fehlt beispielsweise eine Gefährdungshaftung für Schusswaffen und Gifte.[1548] Diese unterliegen zwar einer strikten verwaltungsrechtlichen Präventivkontrolle anhand des WaffG und sonstiger öffentlich-rechtlicher Regelungen. Wie aber das Beispiel Atomrecht und Gentechnikrecht zeigt, substituiert eine behördliche Aufsicht nicht zwangsläufig eine strenge zivilrechtliche Haftung.

[1543] *Blaschczok*, Gefährdungshaftung und Risikozuweisung, 1993, S. 60 ff.; *Deutsch*, JuS 1981, 317 (319); *Larenz/Canaris*, § 84 I 2 a, S. 605; MünchKommBGB-*Wagner*, Vorbemerkung § 823 BGB Rn. 17; Soergel-*Spickhoff*, Vor § 823 BGB Rn. 45; Staudinger-*Hager*, Vorbem zu §§ 823 ff Rn. 28.

[1544] *Blaschczok*, Gefährdungshaftung und Risikozuweisung, 1993, S. 58 ff.; *Larenz/Canaris*, § 84 I 2 a, S. 606.

[1545] *Blaschczok*, Gefährdungshaftung und Risikozuweisung, 1993, S. 46 ff.; *Kötz/Wagner*, Deliktsrecht, Rn. 499; *Larenz/Canaris*, § 84 I 2 a, S. 606; anders *Deutsch*, JuS 1981, 317 (319).

[1546] *Blaschczok*, Gefährdungshaftung und Risikozuweisung, 1993, S. 53 ff., 69 ff.; *Deutsch/Ahrens*, Deliktsrecht, Rn. 355; *Deutsch*, Allgemeines Haftungsrecht, Rn. 634, 639 ff.; *Canaris*, VersR 2005, 577 (578); *Kötz*, AcP 170 (1970), 1 (28 ff.); *Larenz/Canaris*, § 84 I 2 b, S.607.

[1547] S. dazu *Blaschczok*, Gefährdungshaftung und Risikozuweisung, 1993, S. 54 f.; *Kötz*, Gefährdungshaftung, in: Gutachten und Vorschläge zur Überarbeitung des Schuldrechts Bd. II, 1779 (1786 f.).

[1548] *Deutsch/Ahrens*, Deliktsrecht, Rn. 363; *Medicus*, Schuldrecht-BT, Rn. 869.

949 Wann eine besondere Gefahr vorliegt, welche die Regelung einer Gefährdungshaftung erfordert, kann kaum anhand abstrakter Kriterien bestimmt werden. Im Ergebnis lassen sich drei große Gruppen von Gefahren unterscheiden[1549]: Im Falle des StVG ist Wahrscheinlichkeit des Schadenseintritts besonders hoch, das AtG erfasst demgegenüber Sachverhalte, in denen die Höhe des Schadens und die Schadensfolgen apokalyptische Ausmaße annehmen kann, wohingegen im Bereich der Gentechnik das Risikopotential als solches kaum abschätzbar ist. Weitgehend übereinstimmend wird gefordert, dass es sich um eine Gefahr handelt, welche **durch die Aufwendung der im Verkehr erforderlichen Sorgfalt nicht hinreichend beherrschbar** ist (s. auch Rn. 954, 978).[1550] Angesichts der Unbestimmtheit der Voraussetzungen einer „besonderen Gefahr", wird man die Entscheidung über die Statuierung einer Gefährdungshaftung im Ergebnis allein in die Hände des Gesetzgebers legen müssen,[1551] der hierbei an die verfassungsrechtlichen Schranken, insbesondere das Verhältnismäßigkeitsprinzip gebunden ist. Angesichts der fragmentarischen Regelung der derzeitigen Gefährdungshaftungstatbestände ist jedoch bereits an dieser Stelle festzuhalten, dass der Gesetzgeber nicht gezwungen ist, in Bereichen mit erhöhtem Risikopotential eine Gefährdungshaftung einzuführen; ein verfassungsrechtlicher Zwang, etwa aus Schutzpflichten heraus, besteht nicht.

d) Rechtsökonomischer Hintergrund der Gefährdungshaftung

950 Aus rechtsökonomischer Sicht ist Ziel des Haftungsrechts die **Steuerung des Verhaltens der Bürger**, so dass Schadensfälle verhindert werden, welche wegen des damit einhergehenden Gewinns an gesamtgesellschaftlicher Wohlfahrt sinnvoller Weise verhindert werden sollen.[1552] Mit anderen Worten geht es um die Optimierung des Aufwandes zur Schadensvermeidung in Relation zum Gewinn an Sicherheit. Hierbei ist zwischen der Optimierung der Sicherheitsvorkehrungen und der Optimierung des Aktivitätsniveaus zu unterscheiden (ausführlich oben Rn. 23 ff.).

951 Zunächst ist festzuhalten, dass der Umfang in dem**.** **Maßnahmen zur Schadensverhütung** getroffen werden, durch die Einführung einer Gefährdungshaftung nicht ab-

[1549] *Larenz/Canaris*, § 84 I 2 b, S. 607; ähnlich *Blaschczok*, Gefährdungshaftung und Risikozuweisung, 1993, S. 54; *Deutsch*, Allgemeines Haftungsrecht, Rn. 641.

[1550] *Blaschczok*, Gefährdungshaftung und Risikozuweisung, 1993, S. 54; *Deutsch*, JuS 1981, 317 (319); *Kötz*, AcP 170 (1970), 1 (29).

[1551] *Deutsch*, Allgemeines Haftungsrecht, Rn. 640; *Larenz/Canaris*, § 84 I 2 b, S. 607; § 84 I 1 b, S. 601.

[1552] *Kötz/Wagner*, Deliktsrecht, Rn. 64.

nimmt.[1553] Zwar entlastet die Wahrung der erforderlichen Sorgfalt den Schädiger nicht von seiner Einstandspflicht. Ein vernünftiger Halter, Betreiber usw. wird aber aus wirtschaftlichen Erwägungen heraus bemüht sein einen Sicherungsaufwand zu betreiben, dessen Kosten die durch Schadensfälle verursachten Kosten nicht überschreitet.[1554] Voraussetzung ist allerdings die **Vorhersehbarkeit**[1555] von Schadenswahrscheinlichkeit und Schadenshöhe, aus dem sich die in die Kalkulation einzusetzenden Schadenskosten ergeben. Mit einem Schaden den er nicht voraussieht, kalkuliert der Akteur auch nicht. Weitere Voraussetzung ist auch, dass der Aktuer die Möglichkeit hat, die Situation „planend zu überdenken".[1556] Muss der Aktuer spontane Entscheidungen treffen, ist nicht gewährleistet, dass er eine adequate Kosten/Nutzen-Rechnung durchführt.

952 Eine Gefährdungshaftung bewirkt aber keinen ökonomischen Anreiz zur Ergreifung jeder nur denkbaren Sicherungsmaßnahme ohne Ansehung der aufzuwendenden Kosten. Sicherungsmaßnahmen rechnen sich für den Schädiger dann nicht mehr, wenn er mehr an Sicherungskosten investiert, als er im Gegenzug an Schadenskosten erspart. Diese Situation ist **Kaldor-Hicks** optimal.[1557] Auch mit einer Gefährdungshaftung werden also die externen Effekte **internalisiert** durch eine Angleichung der privaten an die gesellschaftlichen Kosten.[1558]

953 Nur durch eine Gefährdungshaftung, aber ist die **Steuerung des Aktivitätsniveaus**, also der Häufigkeit, mit der eine gefährliche Aktivität nachgefragt wird, möglich.[1559] Die Internalisierung der negativen externen Effekte hat eine Verteuerung der gefährlichen Aktivität zur Folge, mit der Folge, dass die Nachfrage wegen steigender Preise sinkt.[1560] Bei der **Verschuldenshaftung** treffen Schäden, welche trotz Einhaltung der im Verkehr erforderlichen Sorgfalt eintreten, das Opfer oder die Allgemeinheit. Unabhängig vom jeweiligen Aktivitätsniveau muss der Schädiger stets denselben Sicherungsaufwand betreiben. So sind im Straßenverkehr etwa Art und Umfang der zur Abwehr des Fahrlässigkeitsvorwurfs erforderlichen Sicherheitsvorkehrungen nicht davon

[1553] Anders aber *Rohe*, AcP 201 (2001), 117 (151); *Cosack*, VersR 1992, 1439 (1441); *Steffen*, NJW 1990, 1817 (1818).

[1554] MünchKommBGB-*Wagner*, Vorbemerkung § 823 BGB Rn. 43.

[1555] *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, S. 214.

[1556] *Weyers*, Unfallschäden, S. 466 ff.

[1557] Zum Kaldor-Hicks-Kriterium bei Meilenstein I, Rn. 21.

[1558] Diese Definition für Internalisierung findet sich auch bei *Schumann*, Grundzüge der Mikroökonomischen Theorie, 1999, S. 38 und S. 492 ff.; *K. Mathis*, Effizienz statt Gerechtigkeit?, 2003, S. 70.

[1559] *Kötz/Wagner*, Deliktsrecht, Rn. 72 ff., 503; MünchKommBGB-*Wagner*, Vorbemerkung § 823 BGB Rn. 17, 45 f.

[1560] MünchKommBGB-*Wagner*, Vorbemerkung § 823 BGB Rn. 45; ausführlich *Schäfer/Ott*, Ökonomische Analyse des Zivilrechts, S. 208 ff.

abhängig, in welchem Umfang die Teilnahme am Straßenverkehr erfolgt. Zur Maximierung seines privaten Wohlfahrtsgewinns wird der Schädiger daher ein hohes Aktivitätsniveau wählen.[1561]

954 Demgegenüber trägt unter Geltung einer **Gefährdungshaftung** der Schädiger alle ihm zurechenbaren Schäden, selbst wenn er alle Sorgfaltsanforderungen erfüllt hat. Er wird daher unter ökonomischen Gesichtspunkten ein optimales Aktivitätsniveau wählen, welches den persönlichen Nutzen des Schädigers mit seinen Sicherungskosten und den Schadenskosten in das wünschenswerte Verhältnis setzt.[1562] Anders als eine Verschuldenshaftung bewirkt eine Gefährdungshaftung somit eine Steuerung der gefährlichen Aktivität auf ein sozial nützliches Niveau. Aus diesem Zusammenhang erklärt sich, warum sich Gefährdungshaftungstatbestände in Lebensbereichen Anwendung finden, in denen selbst bei Beachtung der im Verkehr erforderlichen Sorgfalt noch in beträchtlichem Umfang Schäden eintreten (zum Begriff der besonderen Gefahr oben Rn. 948 f.) und in denen daher Anreize für eine Steuerung des Aktivitätsniveaus erforderlich sind.[1563] Dieser positive Effekt der Gefährdungshaftung tritt in der Praxis jedoch aufgrund von Haftungsobergrenzen und Versicherungsmöglichkeiten nur bedingt ein.[1564]

955 **Nachteile** der Gefährdungshaftung sind jedoch eine höhere Anzahl abzuwickelnder Schadensfälle und damit verbunden ein höherer administrativer Aufwand, welcher beispielsweise bei der Abwicklung von Versicherungsfällen oder Gerichtsprozessen entsteht.[1565] Auch geht die Steuerung durch eine Gefährdungshaftung fehl, wenn dem Akteur die Informationen zur Risikoeinschätzung fehlen, die in diesem Fall nützliche „zentrale Steuerung“[1566] des Sorgfaltsniveaus durch die Gerichte durch Setzung der Fahrlässigkeitsgrenze bietet die Gefährdungshaftung nicht.

956 Des weiteren sind gerade im IT-Sektor Schutzmaßnahmen häufig nur wirksam, wenn sie von allen Teilnehmern eines Netzwerkes ergriffen werden. Wenden nur wenige

---

[1561] *Schäfer/Ott*, Ökonomische Analyse des Zivilrechts, S.208 f.; *Shavell*, Strict Liability versus Negligence, Journal of Legal Studies, Bd. 9 (1980), S. 1 ff.; *Polinsky*, Strict Liability versus Negligence in a Market Setting, American Economic Review, Bd. 70 (1980), S. 363 ff.

[1562] Ausführlich MünchKommBGB-*Wagner*, Vorbemerkung § 823 BGB Rn. 46; *Kötz/Wagner*, Deliktsrecht, Rn. 503-506.

[1563] *Shavell*, Economic Analysis of Accident Law, S. 31; *Shavell*, Strict Liability versus Negligence (1980) 9 J. Legal. Stud. 1; *Cooter/Ulen*, Law & Economics, S. 312; *Schäfer/Ott*, Ökonomische Analyse des Zivilrechts, S. 119 ff.; 194 ff.; *Kötz/Wagner*, Deliktsrecht, Rn. 74, 500 ff.; MünchKommBGB-*Wagner*, Vorbemerkung § 823 BGB Rn. 21, 46.

[1564] Dazu bei Meilenstein 1, Rn. 31 und 33.

[1565] *Kötz/Wagner*, Deliktsrecht, Rn. 506.

[1566] *Finsinger, J. / v. Randow, P.*, Neue Aktivitäten und Haftungsregeln, in: Ökonomische Probleme des Zivilrechts, 1991, S. 89.

Teilnehmer solche Schutzmaßnahmen an, sind diese also wirkungslos und verursachen für sie nur Kosten – im Ergebnis pendeln sich die Teilnehmer bei einem suboptimal niedrigen Schutzniveau dauerhaft ein (Nash Gleichgewicht).[1567] Ein solcher Zustand kann nicht von einer Gefährdungshaftung, wohl aber von einer Verschuldenshaftung aufgebrochen werden, in dem derjenige vom Verschuldensvorwurf befreit wird, der unilateral die Schutzmaßnahmen einsetzt.[1568]

957 Wie bei der deliktischen Haftung kommt auch eine Gefährdungshaftung zudem um eine Mitverschuldensprüfung nicht umhin. Eine solche ist bei der Gefährdungshaftung sogar noch essentieller, denn ohne Mitverschuldensregelung hätte der Geschädigte auf Grund der verschuldensunabhängigen und damit häufiger bestehenden Ansprüche noch geringere Anreiz eigene Sorgfaltsmaßnahmen zu treffen.[1569]

958 Mitverschuldensregelungen führen zu einem weiteren Nachteil der Gefährdungshaftung. Durch Mitverschuldensregelungen bedingt werden die Schadenskosten auf die Parteien verteilt, keine der Parteien hat mehr den gesellschaftlichen Gesamtkosten entsprechende Aufwendungen: Als Folge steigt das Aktivitätsniveau sowohl von Schädiger als auch Geschädigtem steigt über das gesellschaftliche Optimum.[1570] Durch die bei einer Gefährdungshaftung stärkere Kostenverlagerung auf den Schädiger steigt das Aktivitätsniveau beim Geschädigten sogar noch deutlicher über das Optimum.

959 Eine Gefährdungshaftung ist folglich nur dann ratsam, wenn trotz der genannten Nachteile auch eine Steuerung des Aktivitätsniveaus gerade des Schädigers in dem von der Regelung erfassten Bereich tatsächlich erforderlich ist.[1571]

2. Übertragbarkeit auf den IT-Sektor

960 Nach den bisherigen Ausführungen kann den bestehenden Regelungen der Gefährdungshaftung kein zwingendes Erfordernis nach Einführung einer IT-Gefährdungshaftung entnommen werden. Nur bedingt tragfähig ist die Ableitung eines Erfordernisses für eine IT-Gefährdungshaftung aus einer Parallele von Straßenverkehr und IT- (Internet-) verkehr. Vielmehr wird man die Entscheidung über eine IT-Gefährdungshaftung allein anhand der Eigenheiten des IT-Sektors bestimmen müssen,

---

[1567] Vgl. zum Nash-Gleichgewicht *Osborne, Martin J.*, An Introduction to Game Theory, New York 2003, S. 21ff.

[1568] Vgl. auch bei Meilenstein 1, Rn. 36.

[1569] Ebenso *Miceli*, Economics of the Law, 1997, S. 29; Details bei Meilenstein 1, Rn. 35.

[1570] *Shavell, S.*, Strict Liability versus Neglicence, S.1 ff.; *ders.*, Economic Analysis of Accident Law, 1987, S. 29; vgl. Auch bei Meilenstein 1, Rn. 35.

[1571] *Kötz/Wagner*, Deliktsrecht, Rn. 506.

wobei die unter Rn. 860 ff. dargestellten Grundsätze zu berücksichtigen sind. Im Einzelnen:

a) IT-Anlagen als besondere Gefahrenquelle

961 Für den IT-Verkehr könnte eine Gefährdungshaftung in Form der Haftung für IT-Anlagen als Gefahrenquelle in Betracht kommen. An offene Netze angeschlossene Rechner bergen eine gewisse generelle Gefährlichkeit in sich, als sie beispielsweise zur Weiterverbreitung von Viren und Trojanern beitragen können, welche zu Datenschäden, Systemausfällen, Fehlfunktionen usw. führen können. Insbesondere der an das Internet angeschlossenen Computer weist damit eine gewisse „Betriebsgefahr“ auf. Auch kann eine besondere Gefahr unter dem Gesichtspunkt der Schadenshäufigkeit und Schadenshöhe angenommen werden. Hinzu kommt, dass die Gefahren des Internet gerade für private Nutzer durch eigene Sicherungsmaßnahmen nur eingeschränkt abgewehrt werden können und somit durchaus eine Unausweichlichkeit der IT-Risiken zu konstatieren ist.

(1) Veranlassung und Beherrschung der Gefahren im IT-Verkehr

962 Maßgeblicher Zurechnungsgrund für eine Gefährdungshaftung ist die Veranlassung und Beherrschung der besonderen Gefahr durch den Betreiber oder Halter der gefährlichen Anlage. Hierbei kommt es gerade nicht darauf an, ob im Einzelfall die Gefahren konkret beherrschbar sind. Eine Gefährdungshaftung scheidet für den IT-Nutzer nicht zwangsläufig deshalb aus, weil er – anders etwa als der Halter und Fahrer im Straßenverkehr – mangels entsprechenden Wissens und vor allem mangels Zugangs zu Sicherheitslücken seines Systems (der Source Code bzw. Code ist in der Regel nicht zugänglich) „Unfälle“ nicht in demselben Maße zu beherrschen vermag. Für eine Gefährdungshaftung genügt schon die bloß ***abstrakte*** **Veranlassung und Beherrschung** der Gefahr durch Schaffung und Aufrechterhaltung der risikobehafteten Anlage.[1572] Gefährdungshaftung bewirkt eine Haftungszuweisung gerade auch in Fällen, in denen der Schaden durch den Haftungsadressaten im Einzelfall auch bei äußerster Sorgfalt nicht vermeidbar, die Gefahrenquelle m.a.W. also konkret nicht beherrschbar war. Eine Gefährdungshaftung im IT-Verkehr wäre danach auch nicht von der Einführung eines irgendwie gearteten „Internet-Führerscheins“ und der daran anknüpfenden Erhöhung der konkreten Gefahrbeherrschungsmöglichkeiten der IT-Nutzer abhängig.

[1572] *Deutsch*, Allgemeines Haftungsrecht, Rn. 641; *Larenz/Canaris*, § 84 I 2 a, S. 605.

963 Genügt aber eine bloß abstrakte Gefahrbeherrschung als Zurechnungsgrund für die Gefährdungshaftung, trägt der private oder kommerzielle IT-Nutzer beispielsweise auch das Risiko lückenbehafteter Software. In diesem Zusammenhang ist dann fraglich, ob es **rechtspolitisch** wünschenswert ist, dem Nutzer auch die Folgen lückenhafter Software sowie das Risiko des Rückgriffs gegen den Hersteller aufzuerlegen, obwohl die eigentliche Schadensursache im Verantwortungsbereich des IT-Herstellers gesetzt wird. Entsprechende Risikozuweisungen an den Privaten würden wohl bedingen, dass Regress- und Haftungsausschlüsse der Softwarehersteller unzulässig wären – was zwar gerade im Verbrauchsgüterkaufrecht durchaus der Fall ist, jedoch schnell an Grenzen stößt, wenn die Software nur für einen Händler bezogen worden ist, der selbst mangels Vertretenmüssens nicht für Mangelfolgeschäden der Software einstehen muss (s. Teil 1 Rn 102). Auch dies hilft indessen nicht, wenn der Rückgriff an Beweisproblemen des Nutzers scheitert.

(2) Erfasste Risiken des IT-Verkehrs

964 Wie oben ausgeführt beruht die Gefährdungshaftung auf der Schaffung und Beherrschung einer **besonderen Gefahr für ein Rechtsgut oder Interesse**, welche über die Gefahr hinaus geht, welche durch andere Tätigkeiten hervorgerufen werden.[1573] Die Gefahr darf mithin nicht isoliert gesehen werden, sondern kann nur in Bezug auf ein gefährdetes Rechtsgut oder rechtliche geschütztes Interesse bestimmt werden. Hält man sich die gegenwärtigen Gefährdungshaftungstatbestände vor Augen, zeigt sich deutlich, dass die mit verschuldensunabhängiger Einstandspflicht sanktionierten Aktivitäten stets eine besondere Gefahr für die dort aufgeführten Rechtsgüter Leben, Körper, Gesundheit und Eigentum darstellen (Ausnahme: § 22 Abs. 1 WHG).

(a) Risiken für Leben, Körper, Gesundheit und Eigentum

965 Übertragen auf den IT-Sektor kann eine besondere Gefahr durch am Internet angeschlossene Rechner für Leben, Körper und Gesundheit nicht ernstlich bejaht werden. Eine **Eigentumsverletzung** kommt indes unter dem Gesichtspunkt der Datenlöschung oder Datenvernichtung in Frage (Teil 1 Rn. 117). Nachteil der Rechtsgutszentrierung einer künftigen IT-Gefährdungshaftung nach dem Modell der bestehenden Regelungen wäre indessen, dass viele Schadenszenarien mit der Dogmatik der Eigentumsverletzung nicht hinreichend oder nicht mit der nötigen Sicherheit erfassbar sind (dazu bereits Rn.

[1573] *Larenz/Canaris*, § 84 I 2 a, S. 605.

108 ff.). Dies gilt insbesondere für den Fall der Störung der bestimmungsgemäßen Verwendbarkeit des Eigentums (Hardware) und der Betriebs- und Produktionsausfallschäden, wo die Grenze zwischen Eigentumsverletzung und primärem Vermögensschaden besonders schwierig auszumachen ist. Eine IT-Gefährdunghaftung für Leben, Körper und Gesundheit hätte daher praktisch keinen, eine Gefährdungshaftung für Eigentumsverletzung nur einen eingeschränkten Anwendungsbereich – mit allen Schwierigkeiten der Abgrenzung von Rechtsgutsverletzungen von bloßen Vermögensschäden, wie sie von § 823 Abs. 1 BGB und § 1 ProdHaftG bekannt sind.

966 Auf das **Recht am eingerichteten und ausgeübten Gewerbebetrieb** kann in diesem Zusammenhang nicht ausgewichen werden, da regelmäßig kein betriebsbezogener Eingriff vorliegen wird (s. Teil 1 Rn. 117). Überdies wäre eine Einbeziehung des Rechts am Gewerbebetrieb angesichts der bestehenden Regelungen als Bruch im Gesamtsystem der Gefährdungshaftung anzusehen.[1574] Zudem setzt sich immer mehr die Erkenntnis durch, dass das Recht am Gewerbebetrieb eine richterrechtlich begründete Haftung für primäre Vermögensschäden darstellt, welche mit dem Gesamtsystem des deutschen Deliktsrechts nicht in Einklang steht.[1575] Eine verschuldensunabhängige Haftung für die Verletzung des Rechts am Gewerbebetrieb wäre auch im Lichte der Wertung der Grundentscheidung des deutschen Rechts im Hinblick auf den Ersatz primärer Vermögensschäden in § 823 Abs. 2, 826 BGB, 3 UWG kaum vertretbar.

(b) Gefährdungshaftung für primäre Vermögensschäden?

967 Eine Gefährdungshaftung für primäre Vermögensschäden ist dem deutschen Haftungsrecht fremd (einzige Ausnahme § 22 WHG, oben Rn. 943). Das deutsche Deliktsrecht hat eine bewusste **Entscheidung gegen den Ersatz jedes Vermögensschadens** getroffen und stellt grundsätzlich auf die Verletzung von Rechtsgütern die Leben, Körper, Gesundheit, Freiheit und Eigentum ab. Unstreitig ist das Vermögen kein sonstiges Recht im Sinne des § 823 Abs. 1 BGB.[1576] Nicht durch eine Rechtsgutsverletzung vermittelte Vermögensschäden werden nach der gesetzlichen Grundkonzeption nur ausnahmsweise ersetzt, wenn die Art der Beeinträchtigung des Vermögens missbilligenswert

[1574] *Deutsch*, Allgemeines Haftungsrecht, Rn. 648; *Larenz/Canaris*, § 84 I 1 c, S. 603.

[1575] Dezidiert *Larenz/Canaris*, § 81 I 1 a, S. 539, § 81 II 2, S. 545; dazu auch Bamberger/Roth-*Spindler*, § 823 BGB Rn. 113; *Deutsch*, Allgemeines Haftungsrecht, Rn. 873; Staudinger-*Hager*, § 823 BGB D Rn. 2.

[1576] S. nur MünchKommBGB-Wagner, § 823 BGB Rn. 176 mwN.

ist.[1577] So beispielsweise bei Verletzung eines Schutzgesetzes (§ 823 Abs. 2 BGB), bei vorsätzlich sittenwidriger Schädigung (§ 826 BGB) oder im Fall des unlauteren Wettbewerbs (§ 3 UWG).

968 Für die nur eingeschränkte Ersatzfähigkeit primärer Vermögensschäden gibt es mehrere **Gründe**.[1578] So ist die Schädigung des Vermögens – anders als die Verletzung der hochrangigen und absolut schutzwürdigen und schutzbedürftigen Rechtsgüter Leben, Körper, Gesundheit und Eigentum[1579] – nicht per se unerwünscht, wie insbesondere die Schädigung von Konkurrenten im (lauteren) Wettbewerb zeigt.[1580] Hier steht dem Schaden des Einzelnen oftmals kein gesamtwirtschaftlicher Schaden gegenüber, da es sich um eine bloße Umverteilung von Vermögen handelt.[1581] Dem Gesetzgeber ging es vor allem auch um die Kanalisierung der Haftung auf den unmittelbar Verletzten.[1582] Dieses Ziel erreicht er einerseits durch die Verknüpfung der außervertraglichen Haftung mit einer Rechtsgutsverletzung, andererseits dadurch, dass er den Ersatz primärer Vermögensschäden an besondere Tatbestandsvoraussetzungen bindet. Bei reinen Vermögensschäden muss damit stets im Einzelfall geprüft werden, ob ein haftungsrechtlicher Schutz zu gewähren ist oder nicht.[1583] Andernfalls droht eine uferlose Haftung für jeden auch nur mittelbar verursachten Vermögensschaden, was der Entscheidung gegen eine große deliktische Generalklausel widerspricht.

969 Durch die bestehende Gesetzeslage ist der Gesetzgeber nicht gehindert, den Vermögensschutz weiter auszudehnen. Er kann dies einerseits durch die Normierung **vermögensschützender Schutzgesetze** im Sinne von § 823 Abs. 2 BGB oder durch **spezielle Haftungstatbestände** tun. Jüngstes Beispiel hierfür sind die durch das 4. Finanzmarktförderungsgesetz einführten §§ 37b, 37c WpHG, welche im Falle von Vorsatz oder grober Fahrlässigkeit (§ 37b Abs. 2, 37c Abs. 2 WpHG) eine Haftung des Emittenten von Finanzinstrumenten wegen unterlassener unverzüglicher Veröffentlichung von Insiderinformationen bzw. der Veröffentlichung unwahrer Insiderinformationen begründen. Das geplante „Kapitalmarktionformationshaftungsgesetz“ (KapInHaG) ist bislang noch

[1577] *Larenz/Canaris*, § 75 I 3 b, S. 357; vgl. auch *Kötz/Wagner*, Deliktsrecht, Rn. 99.

[1578] Ausführlich *Kötz/Wagner*, Deliktsrecht, Rn. 256 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 176 f.

[1579] *Deutsch*, Allgemeines Haftungsrecht, Rn. 857; *Kötz/Wagner*, Deliktsrecht, Rn. 97, 255; MünchKommBGB-*Wagner*, § 823 BGB Rn. 176 f.

[1580] *Larenz/Canaris*, § 75 I 3 b, S.356 f.; *Kötz/Wagner*, Deliktsrecht, Rn. 97, 258.

[1581] *Kötz/Wagner*, Deliktsrecht, Rn. 97, 258; MünchKommBGB-*Wagner*, § 823 BGB Rn. 176.

[1582] MünchKommBGB-*Wagner*, § 823 BGB Rn. 176

[1583] MünchKommBGB-*Wagner*, § 823 BGB Rn. 177.

nicht weiter verfolgt worden.[1584] Weitere Normen in diesen Bereich sind der Schadensersatzanspruch wegen unlauterer Wettbewerbshandlungen (§ 3 UWG) und der Schadensersatzanspruch wegen Verstoßes gegen kartellrechtliche Vorschriften oder Verfügungen (§ 33 Abs. 3 Satz 1 GWB).

970 Auch im IT-Sektor ist wäre es durchaus denkbar die außervertragliche Haftung für primäre Vermögensschäden zu erweitern. In Betracht kommt hierbei vor allem die Regelung eines IT-Sicherheitsgesetzes als Schutzgesetz gemäß § 823 Abs. 2 BGB. Denkbar wäre aber auch ein spezieller Haftungstatbestand. Um eine Verzerrung des im Gesamtsystems der außervertraglichen Schadenshaftung zu vermeiden müssen, müssen die haftungsbegründenden Voraussetzungen indes klar abgrenzbar umschrieben werden, um die ersatzfähigen von den nicht ersatzfähigen Vermögensschäden zu trennen. Eine große Generalklausel hätte auch im IT-Bereich unübersehbare Haftungsrisiken zur Folge, da praktisch jeder nur mittelbar verursachte Vermögensschaden ersatzfähig wäre.

971 Ausgehend von den oben Rn. 964 dargestellten Grundsätzen ließe sich eine **IT-Gefährdungshaftung** für primäre Vermögensschäden wohl nur dann rechtfertigen, wenn die Teilnahme am IT-Verkehr eine **besondere Gefahr gerade für das Vermögen** als Schutzgut schafft, welche über die Gefahren für Vermögen hinausgeht, die mit anderen Aktivitäten verbunden sind. So drohen beispielsweise auch im Straßenverkehr nach einem Unfallereignis erhebliche Vermögensschäden, wenn etwa als Folge eines Staus Geschäftstermine nicht wahrgenommen werden können, Transporte verspätet ankommen, Züge und Flüge verpasst werden usw. In diesem Zusammenhang werden Vermögensschäden indessen nicht ersetzt (vgl. § 7 StVG). Hier wie dort droht eine uferlose Haftung, welche zudem kaum mehr durch eine bezahlbare (Pflicht-) Versicherung aufgefangen werden könnten.

b) Mögliche Haftungsadressaten

972 Soweit man für IT-Anlagen eine besondere Gefahr bejaht, kommt eine daran anschließende Gefährdungshaftung grundsätzlich für private und kommerzielle IT-Nutzer gleichermaßen in Betracht.

973 Die Anknüpfung an die IT-Anlage als Gefahrenquelle legt es nahe, diese Haftungsform auch und gerade auf **private Nutzer** zu erstrecken, deren Rechner in der Regel weit

[1584] Zum Diskussionsentwurf eines Gesetzes zur Verbesserung der Haftung für falsche Kapitalmarktinformationen s. NZG 2004, 1042.

weniger gegen Bot-Netze, Virenbefall usw. geschützt sind. Man wird den ungeschützten privaten Rechner als eine der Hauptgefahrenquellen im Internet identifizieren müssen. Eine auf **kommerzielle Nutzer** beschränkte Regelung müsste dagegen erklären, warum private Nutzer privilegiert werden, obwohl von ihren Rechnern die Hauptgefahr im Internet ausgeht. Zwar gibt es Gefährdungshaftungstatbestände, welche de facto nur Unternehmer treffen. Dies beruht indes auf der Tatsache, dass bestimmte Anlagen nur von Unternehmern betrieben (z.B. Atomanlagen, Anlagen im Sinne des UmweltHG, gentechnische Anlagen) und bestimmte Handlungen nur von Unternehmern vorgenommen werden (z.B. Herstellung und Inverkehrgabe von Produkten). Dagegen trifft die Haftung nach dem StVG grundsätzlich jeden Fahrzeughalter und niemand käme auf die Idee nach privater und kommerzieller Nutzung zu unterscheiden.

974 Liegt aber der eigentliche Anwendungsbereich einer IT-Gefährdungshaftung im privaten Bereich, stellt sich sogleich die Frage nach der Erforderlichkeit einer verschuldensunabhängigen Haftungsregelung im IT-Verkehr. Für das Verhältnis *zwischen Privaten* dürfte eine verschuldensunabhängige Haftung kaum größere praktische Bedeutung erlangen als die derzeit schon mögliche Haftung nach § 823 Abs. 1 BGB. Soweit privaten Nutzern überhaupt ein ersatzfähiger Schaden entsteht, ist vordringlichstes Problem der Inanspruchnahme des Täters nicht das Verschulden, sondern der Beweis der **Identität des Schädigers** und der **Kausalität** des Handelns des Schädigers für den eingetretenen Schadens (s. Rn. 827), welches durch eine verschuldensunabhängige Haftung alleine aber nicht gelöst wird.

975 Denkbar wäre hier zwar eine Kombination einer verschuldensunabhängigen Haftung mit einer **Beweislasterleichterung** nach dem Vorbild der Ursachenvermutung des § 6 UmweltHG. In der praktischen Umsetzung stellt sich jedoch die Frage, woran eine Kausalitätsvermutung im IT-Verkehr anknüpfen sollte. § 6 UmweltHG stellt darauf ab, ob die (im Anhang zum UnweltHG genannten) Anlage nach den Gegebenheiten des Einzelfalles abstrakt geeignet ist, den entstandenen Schaden zu verursachen. Dieses Kriterium dürfte im IT-Verkehr von vornherein ausscheiden, da theoretisch jeder am Netz angeschlossene Computer die schädigende Anlage sein kann; dies würde zu dem absurden Ergebnis führen, daß ein Geschädigter sich willkürlich einen PC-Besitzer heraussuchen könnte, der sich dann hinsichtlich des Kausalitätsbeweis zu entlasten hätte.

976 Sofern *Unternehmen geschädigt* werden, kommt zum Problem des Kausalitätsnachweises das der mangelnden **Liquidität** des privaten Nutzers, da hier immense Schadens-

summen drohen. Die strenge Haftung wäre hier nur dann durchsetzbar, wenn die Gefährdungshaftung mit einer **Pflicht-IT-Haftpflichtversicherung** kombiniert wird. Um die Versicherungsprämien bezahlbar zu halten, müßten jedoch Haftungshöchstbeträge geregelt werden.

c) Rechtsökonomische Erwägungen

977 Unter rechtsökonomischen Gesichtspunkten ist entscheidendes Kriterium für und wider die Einführung einer IT-Gefährdungshaftung die Notwendigkeit der Steuerung des Aktivitätsniveaus im IT-Verkehr, d.h. der Menge der Internet-Teilnahme. Der Umfang der zur Schadensverhütung getroffenen Maßnahmen kann durch eine Gefährdungshaftung gegenüber einer bloßen Verschuldenshaftung dagegen nicht gesteigert werden. Während es im Straßenverkehr somit durchaus Sinn macht, die „Menge des Autofahrens" durch die Haftung nach § 7 StVG zu reduzieren, um die Unfallzahlen zu senken, stellt sich die Frage, ob diese Überlegung auch im IT-Verkehr greift.

978 Gefährdungshaftungstatbestände bieten sich vor allem für Tätigkeiten an, bei deren Vornahme trotz der Aufwendung der im Verkehr erforderlichen Sorgfalt erhebliche Schäden eintreten können (s. auch Rn. 949, 954).[1585] Da die Bedeutung der IT-Sicherheit derzeit vor allem im privaten, zum Teil aber auch im unternehmerischen Bereich noch nicht hinreichend erkannt ist, kann noch nicht abschließend beurteilt werden, inwieweit das Gefährdungspotential des Internetverkehrs bereits durch klar definierte und praktisch durchsetzbare Sorgfaltsanforderungen und –maßstäbe reduziert wird

979 Da *Unternehmen* aufgrund ihrer personellen, finanziellen und technischen Ressourcen deutlich mehr an IT-Sicherheitsmaßnahmen abverlangt werden kann, wäre denkbar, dass bei kommerziellen Nutzern effektiv durchgesetzte IT-Sicherheitsvorschriften in weitem Umfang zur Reduzierung von Schadensfällen beitragen. Derzeit finden sich aber nur sektorspezifische Anforderungen an die IT-Sicherheit für einzelne Wirtschaftssektoren (Teil 1 Rn. 658). In vielen Bereichen fehlen derzeit dagegen noch flächendeckende Vorgaben für die IT-Sicherheit.

980 *Private Nutzer* sind regelmäßig nur wenig versiert im Umgang mit IT-Technologie, so dass gegenüber kommerziellen Nutzern deutlich niedrigere Sorgfaltsmaßstäbe anzulegen sind (dazu ausführlich Teil 1 Rn. 329 f.). Es ist zu erwarten, dass selbst bei Einhal-

[1585] *Shavell*, Economic Analysis of Accident Law, S. 31; *Cooter/Ulen*, Law & Economics, S. 312; *Kötz/Wagner*, Deliktsrecht, Rn. 74; MünchKommBGB-*Wagner*, Vorbemerkung § 823 BGB Rn. 21, 46.

tung aller dem privaten Nutzer zumutbaren Sorgfalt eine Vielzahl von Schadensfällen eintreten können. Drohen aber trotz Wahrung der privaten Sorgfaltsanforderungen erhebliche Schäden durch private Rechner, erweist sich wiederum der private Nutzer als der eigentlich legitime Adressat einer IT-Gefährdungshaftung.

981 Zudem ist folgender Zusammenhang ist zu bedenken: Als einer der Vorteile des Internet und insbesondere des E-Commerce gilt die jederzeitige Verfügbarkeit. Insbesondere bei Unternehmen mit Internet-Auftritt dürfte kaum gewünscht sein, die Menge der Teilnahme am Internetverkehr zu steuern und damit im Zweifel zu reduzieren. Denn diese sollen gerade rund um die Uhr online erreichbar sein. Unter rechtsökonomischen Gesichtspunkten dürfte eine IT-Gefährdungshaftung somit zumindest ein zweifelhaftes Signal für die Fortentwicklung des Mediums Internet setzen.

3. Ergebnis

982 Der Vorteil einer IT-Gefährdungshaftung liegt in der Entlastung des Geschädigten (und des Gerichts) vom Nachweis des Verschuldens des Schädigers. Eine effektive Ausgestaltung des Haftungstatbestandes müsste sich indessen auch des im Internetverkehr vordringlichen Problems des Beweises der Identität des Schädigers und der Kausalität seiner Tätigkeit für den eingetretenen Schaden annehmen, was indessen auf praktische Umsetzungsprobleme stößt.

983 Die Begründung einer Gefährdungshaftung für Gefahren des Internet ist zwar theoretisch möglich, wenn mit dem Internet verbundene IT-Anlagen als besondere Gefahr angesehen werden. Die Bejahung einer besonderen Gefahr liegt weitgehend in der Entscheidung des Gesetzgebers. Ein praktischer Anwendungsbereich bestünde für eine IT-Gefährdungshaftung indessen nur eingeschränkt in den Fällen der Eigentumsverletzungen durch Datenvernichtung und Datenveränderung. Eine verschuldensunabhängige Haftung für primäre Vermögensschäden wäre mit den bestehenden Grundsätzen der Gefährdungshaftung und dem Gesamtsystem der außervertraglichen Schadenshaftung nur schwer vereinbar.

984 Eine IT-Gefährdungshaftung müsste private wie kommerzielle Nutzer erfassen, da der vernetzte Computer unabhängig vom Nutzungszweck als Gefahrenquelle eingestuft werden kann. Gerade ungesicherte private Rechner dürften im Internet derzeit die größte Schutzlücke darstellen. Hierbei stellt sich jedoch die rechtspolitische Frage, ob eine Gefährdungshaftung zu Lasten privater Nutzer im IT-Bereich gewollt ist, da dem privaten Nutzer damit auch das Risiko fehlerhafter Software auferlegt würde, der indessen

oftmals (insbesondere wegen der Schwierigkeiten des Kausalitätsnachweises) keine Rückgriffschance gegen den Hersteller haben wird.

985 Eine auf kommerzielle Nutzer beschränkte strenge IT-Haftung ließe sich über eine Haftung für die Verletzung eines IT-Sicherheitsgesetzes als Schutzgesetz im Sinne von § 823 Abs. 2 BGB begründen. Abhängig von der konkreten Ausgestaltung eines solchen Gesetzes wäre damit auch die Ersatzfähigkeit primärer Vermögensschäden gewährleistet.

986 Rechtsökonomisch bewirkt eine IT-Gefährdungshaftung im Vergleich zu einer Verschuldenshaftung (etwa nach § 823 Abs. 2 BGB) keine stärkeren Anreize zur Erhöhung des Sicherheitsstandards bei IT-Anlagen. Der Vorteil der Gefährdungshaftung gegenüber einer Verschuldenshaftung liegt aber in der Steuerung des Aktivitätsniveaus.

VI. Europarechtliche Zulässigkeit

987 Ein Sicherheitsgesetz, das bestimmte Anforderungen an die IT-Sicherheit stellt, um Vermögens- bzw. Eigentumsschäden vorzubeugen, müsste aufgrund des Anwendungsvorrangs des Europarechts vor nationalem Recht[1586] insbesondere gemeinschaftskonform sein. In Betracht kommt hierbei nur ein Verstoß gegen die Grundfreiheiten des EG-Vertrags, welche die Freiheit des Waren-[1587], des Personen-[1588], des Dienstleistungs-[1589] und des Kapitalverkehrs[1590] zwischen den Mitgliedstaaten garantieren. Betreffend einzelner IT-Sicherheitsanforderungen wäre in einem öffentlich-rechtlichen IT-Sicherheitsgesetz hinsichtlich solcher, die an bestimmte Produkte[1591] (z.B. beim Vertrieb von Hard-/ Software), an Dienstleistungen[1592] (z.B. beim Online – Banking) bzw.

[1586] St. Rspr. seit EuGH, Rs. 6/64, *Costa Enel,* Slg. 1964, 1251, 1269; Rs. 106/77, *Simmenthal II,* Slg. 1978, 629, 643 Rn. 14 ff.; aus Sicht des BVerfG s. BVerfGE 73, 339 - Solange II; BVerfGE 89, 155 – Maastricht; aus dem Schrifttum statt vieler *Streinz,* Europarecht, S. 73 Rn. 168 ff.; *Haratsch/Koenig/Pechstein,* Europarecht, S. 66 ff. Rn. 150 ff.

[1587] Art. 28 ff. EG.

[1588] Die Personenverkehrsfreiheiten untergliedern sich in die Freizügigkeit der Arbeitnehmer (Art. 39 ff. EG) und die Niederlassungsfreiheit (Art. 43 ff. EG), s. hierzu *Ehlers,* Jura 2001, 266, 267; *Nettesheim,* NVwZ 1996, 342; *Ohler,* WM 1996, 1801, 1802; *Mülbert/Schmolke,* ZvglRWiss 100 (2001), 233, 237 f.; *Kilian,* Europäisches Wirtschaftsrecht, S. 128 Rn. 281.

[1589] Art. 49 ff. EG.

[1590] Art. 56 Abs. 1 EG. Die Freiheit des Zahlungsverkehrs gem. Art. 56 Abs. 2 EG wird als die notwendige Annexfreiheit zu den verwirklichten Grundfreiheiten verstanden, da letztere ohne den freien Transfer von Gehältern, Erlösen und Gewinnen wirkungslos wären, s. hierzu EuGH, Rs. 286/82 u. 26/83, *Luisi und Carbone,* Slg. 1984, 377, 404 Rn. 21 f.; Rs. C-358 u. 416/93, *Bordessa,* Slg. 1995, I-361, 383 Rn. 13 f.; *Streinz,* Europarecht, S. 281 Rn. 656; *Frenz,* europäische Grundfreiheiten, S. 1052 Rn.2792 f.; *Steinberg,* EuGRZ 2002, 13, 14; *Ohler,* WM 1996, 1801, 1801 f.; *Spindler,* RIW 2003, 850 ff.

[1591] S.u. G.VI.1

[1592] S.u. G.VI.2

an die Anlage selbst[1593] (z.B. Sicherheitsanforderungen hinsichtlich des Server- Betriebs) gestellt werden, zu unterscheiden.

988 Generell muß hier jedoch im Hinblick auf die E-Commerce-Richtlinie zwischen offline und online vertriebenen Produkten und Dienstleistungen unterschieden werden: Denn für die online vertriebenen Produkte und Dienstleistungen gelten die Regelungen des Herkunftslandprinzips nach Art. 3 ECRL, wie Erwägungsgrund Nr. 18 deutlich zeigt:

> „Die Dienste der Informationsgesellschaft umfassen einen weiten Bereich von wirtschaftlichen Tätigkeiten, die on-line vonstatten gehen. Diese Tätigkeiten können insbesondere im Online-Verkauf von Waren bestehen. Tätigkeiten wie die Auslieferung von Waren als solche oder die Erbringung von Offline-Diensten werden nicht erfaßt."

989 Daran zeigt sich, dass die EG – ob zu Recht oder nicht – klar zwischen der offline und online-Welt unterscheidet, was sich auch in anderen Richtlinien, etwa der InfoSoc-Richtlinie im Bereich der Erschöpfung niederschlägt. Damit unterfallen aber auch sämtliche IT-Produkte und –Dienstleistungen aus dem EU-Ausland dem Herkunftsland nach der ECRL, so dass nationale Regelungen allenfalls in den Ausnahmebereichen der Art. 3 ECRL gerechtfertigt sein können.

1. IT-Sicherheitsanforderungen an Produkte

990 Wenn ein öffentlich-rechtliches IT-Sicherheitsgesetz bestimmte IT-spezifische Sicherheitsanforderungen an die Produkte stellt, sind die Grenzen der Warenverkehrsfreiheit des Art. 28 EG ebenso wie diejenigen des sekundären Gemeinschaftsrechts (Richtlinien, Verordnungen) zu beachten.

a) Offline-Produkte

(1) Vorrang sekundärrechtlicher Regelungen

991 Ist ein Rechtsgebiet durch sekundäres Gemeinschaftsrecht vollständig harmonisiert worden, ist die Übereinstimmung eines nationalen Rechtsaktes mit dem sekundären Gemeinschaftsrecht vorrangig (vor den primären Grundfreiheiten) zu prüfen. Sofern daher ein bestimmter Bereich der Warenverkehrsfreiheit durch Richtlinien abschließend harmonisiert ist, verfügen die Mitgliedstaaten nicht mehr über die Kompetenz, nationale Maßnahmen zur Beschränkung der durch das sekundäre Gemeinschaftsrecht festge-

[1593] S.u. G.VI.3.

schriebenen Rechtspositionen zu erlassen.[1594] Der Anwendungsbereich eines öffentlich-rechtlichen IT-Sicherheitsgesetz könnte insofern bereits abschließend durch die Produktsicherheits-Richtlinie 2001/95/EG[1595] geregelt sein. Ob und inwieweit eine Gemeinschaftsregelung insoweit abschließend oder nicht abschließend ist, muss sich aus deren Formulierung, Zwecksetzung und Kontext beurteilen.[1596]

992 Der Anwendungsbereich der Produktsicherheits-RL umfasst jedoch nur den Schutz der Gesundheit und die Sicherheit der Verbraucher[1597], nicht hingegen Vermögens- und Eigentumsschäden.[1598] Bereits dadurch, dass in Erwägungsgrund Nr. 12 der RL 2001/95/EG auf die Anwendung von spezielleren Gemeinschaftsvorschriften verwiesen wird, sofern diese bestimmte Risiken oder Risikostrategien abdecken,[1599] zeigt sich, dass die Produktsicherheits-RL insoweit keinen abschließenden Charakter hat. Die RL 2001/95/EG stellt daher für ein öffentlich-rechtliches IT-Sicherheitsgesetz, das nur im Fall eines reinen Vermögens- oder Eigentumsschadens greifen würde, keine vollständige Harmonisierung und damit auch keine abschließende Regelung dar. Für Gesundheitsschäden ist allerdings ihr Anwendungsbereich eröffnet, den sie auch abschließend regelt. Für die Regelung dieses Bereichs besteht also, anders als im Fall eines Vermögens- und Eigentumsschadens, keine Regelungskompetenz der Mitgliedstaaten mehr. Auch sonstige RL im Bereich der Produktsicherheit sind für die Vermögens- bzw. Eigentumsschäden hier nicht einschlägig, da sie lediglich Anforderungen an bestimmte Produktgruppen stellen und die Vermögens- bzw. Eigentumsschäden jeweils nicht mit abdecken.[1600] Eine abschließende Regelung hinsichtlich der Produktsicherheit für Vermögens- und Eigentumsschäden besteht folglich nicht und eine europarechtliche Prüfung kann sich insofern auf die Warenverkehrsfreiheit konzentrieren.

(2) Schutzbereich

[1594] EuGH, Rs. 5/77, *Tedeschi,* Slg. 1977, 1555, 1575 f. Rn. 33, 35; Rs. 190/87, *Moormann,* Slg. 1988, 4689, 4720 Rn. 10; Rs. C-37/92, *Vanacker und Lesage,* Slg. 1993, I-4947, 4978 Rn. 6 ff.; *Schroeder,* in: Streinz, Art. 28 Rn. 14; *Everling,* ZLR 1994, 221, 222.

[1595] Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit, ABl EG L 11, S.4; umgesetzt in nationales Recht in Deutschland durch Gesetz über technische Arbeitsmittel und Verbraucherprodukte (GPSG) vom 6. Januar 2004, BGBl. I 2004, S. 2, ber. BGBl. I 2004, S. 219.

[1596] EuGH, Rs. C-1/96, *Compassion,* Slg. 1998, I-1251, 1298 Rn. 54; *Müller-Graff,* in: von der Groeben/Schwarze, Art. 28 Rn. 202.

[1597] S. Erwägungsgrund Nr. 11 der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit, ABl EG. L 11/4, 5.

[1598] S. auch oben Teil I Rn. 236.

[1599] S Erwägungsgrund Nr. 12 der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit, ABl EG Nr. L 11/4, 5.

[1600] S. oben Teil I Rn. .222.

993 Ihren Schutz entfalten die Grundfreiheiten nur, wenn ein Tun, Dulden oder Unterlassen in sachlicher, personeller, räumlicher und zeitlicher Hinsicht in den jeweiligen Schutzbereich fällt.[1601] Erforderlich ist immer ein grenzüberschreitendes Element, rein interne Sachverhalte mit ausschließlichem Bezug zu einem Mitgliedstaat werden nicht erfasst.[1602]

(a) Begriff der Ware

994 Unter „Waren" werden gemeinhin körperliche Erzeugnisse verstanden, die einen Geldwert haben und deshalb Gegenstand von Handelsgeschäften sein können.[1603] Unproblematisch ist insofern der körperliche Gegenstand Hardware (wie z.B. Computer, Laptop, Drucker, Monitor, Keyboard und anderes Zubehör) als Ware i.S.d. Art. 28 EG anzusehen. Fraglich ist aber, wie Software als „geistige Leistung" einzustufen ist. Dabei scheidet selbstverständlich eine nationale Auslegung[1604] des europarechtlichen Begriffs der „Ware" aufgrund des „effet-utile"-Grundsatz und der Erforderlichkeit einer gemeinschaftseinheitlichen Auslegung aus.

995 Nach Ansicht des EuGH unterfallen zwar rein immaterielle Güter wie Verfahrensweisen, Dienstleistungen oder „know-how", die schon ihrer Natur nach zolltechnisch schwer zu erfassen sind, dem Warenbegriff;[1605] zu beachten ist aber, dass der EuGH den Begriff der Körperlichkeit einer Ware sehr weit auslegt und hierfür insbesondere aus dem Zollwert Rückschlüsse zieht.[1606] Auch in Bezug auf Datenträger mit eingespeicherter Software hielt der EuGH bereits eine Trennung des Datenträgers und darauf eingespeicherte Software für nicht durchführbar und schloss sich in *Brown Boveri* der Meinung der Kommission an, die für die Berechnung des Zollwerts den Wert des Datenträgers mit dem der Software addierte.[1607] Ebenfalls sah der Gerichtshof jüngst in einer

[1601] Zu der allg. Bestimmung des Schutzbereichs *Ehlers,* Jura 2001, 482, 482 f.; *Frenz,* europäische Grundfreiheiten, S. 140 Rn. 355 f.; *Schultz,* Verhältnis von Gemeinschaftsgrundrechten und Grundfreiheiten des EGV, 2005, S. 94 ff.; s. auch *Streinz*, Europarecht, S. 283 ff. Rn. 660 ff., der von „Anwendungsbereich" spricht.

[1602] St. Rspr des EuGH, s. nur EuGH, Rs. 35/82 und 36/82, *Morson,* Slg. 1982, 3723, 3736 Rn. 15 f.; Rs. C-112/91, *Werner,* Slg. 1993, I-429, 468 f. Rn. 11; Rs. C-132/93, *Steen II,* Slg. 1994, I-2715, 2722 Rn. 7 f.

[1603] St. Rspr. seit EuGH, Rs. 7/98, *Kunstschätze,* Slg. 1968, 633, 642; aus der Lit. *Schroeder,* in: Streinz, Art. 28 Rn. 19; *Frenz,* europäische Grundfreiheiten, S. 245 ff. Rn. 637 ff.

[1604] Zur Diskussion im Rahmen des GPSG s. oben unter Rn. 208 ff..

[1605] EuGH, Rs. 1/77, *Bosch/HZA Hildesheim,* Slg. 1977, 1473, 1482 Rn. 4; *Frenz,* europäische Grundfreiheiten, S. 249 Rn. 648.

[1606] EuGH, Rs. C-393/92, *Almero,* Slg. 1994, I-1477; Rs. C-379/98, *Preussen Elektra,* Slg. 2001, I-2099: elektrischer Strom als Ware.

[1607] EuGH, Rs. C-79/89, *Brown Boveri,* Slg. 1991, I-1853, 1890 Rn. 21; *Frenz,* europäische Grundfreiheiten, S. 260 Rn. 676 f.

Rechtsfrage zu Computerspielen den Begriff der Ware ausdrücklich als gegeben an.[1608] Sofern die Software daher auf einem Datenträger verkörpert ist, wird sie nach der Rechtsprechung des EuGH als eine einheitliche Ware angesehen, die insgesamt dem Zollrecht unterliegt.[1609] Der sachliche Schutzbereich des Art. 28 EG ist also einschlägig.

(b) Grenzüberschreitender Sachverhalt

996 Wenn in dem IT-Sicherheitsgesetz allgemein IT-spezifische Anforderungen an den Vertrieb von Hard- und Software gestellt werden, gelten diese nicht nur für den innerdeutschen Vertrieb, sondern auch für den ausländischen Anbieter aus einem EU-Mitgliedstaat, sofern er die genannten Produkte auf dem deutschen Markt vertreibt. Der erforderliche grenzüberschreitende Sachverhalt wäre daher gegeben.

(3) Beeinträchtigung

997 In erster Linie begründen die Grundfreiheiten ein Diskriminierungsverbot[1610] und statuieren insofern das Verbot, Waren oder Personen aufgrund ihrer Herkunft anders zu behandeln als inländische Personen oder Waren.[1611] Daneben legt der EuGH aber inzwischen sämtliche Grundfreiheiten auch als Beschränkungsverbote aus.[1612]

(a) Offene Diskriminierung

998 Eine offene[1613] Diskriminierung liegt vor, wenn eine innerstaatliche Regelung ausdrücklich an die Staatsangehörigkeit anknüpft und zwischen in- und ausländischen Sachverhalten zum Nachteil der die Grenze überschreitenden Produkte oder Personen differenziert.[1614] Das IT-Sicherheitsgesetz stellt aber unabhängig von der Staatsangehörigkeit Anforderungen an die Produkte und würde daher keine Ungleichbehandlung als offene Diskriminierung statuieren.

(b) Versteckte Diskriminierung

[1608] EuGH, Rs. C-65/05, *Kommission/Griechenland,* noch nicht veröffentlicht, Rn. 23 f. (abrufbar unter http://curia.europa.eu/de/content/juris/index_form.htm).

[1609] *Frenz,* europäische Grundfreiheiten, S. 260 Rn. 676.

[1610] *Jarass,* EuR 1995, 105, 211; *ders.,* EuR 2000, 705, 709; *Thiele,* JA 2005, 621, 623 f.; *Classen.* EWS 1995, 97; *Streinz,* Europarecht, S. 286 Rn. 667; *Frenz,* europäische Grundfreiheiten, S. 46 Rn. 105 f.; *Eberhartinger,* EWS, 43, 44 f.; *Plötscher,* Begriff der Diskriminierung, 2003, S. 40.

[1611] EuGH, Rs. C-80/94, *Wielockx,* Slg. 1995, I-2493, 2515 Rn. 17; Rs. C-107/94, *Asscher,* Slg. 1996, I-3089, 3124 f. Rn. 40.

[1612] *Streinz,* Europarecht, S. 288 Rn. 671; *ders.,* in: FS für Röhricht, 2005, S. 1239, 1243; *Borchardt,* Die rechtlichen Grundlagen der EU, S. 301 Rn. 682; *Thiele,* JA 2005, 621, 624; *Jarass,* EuR 2005, 705, 711 f.; *Füßer,* DÖV 1999, 96, 97 f.; *Nettesheim,* NVwZ 1996, 342, 342 f.; *Klinke*, ZGR 1996, 567, 575; *Ehlers,* Jura 2001, 266, 270; *Skouris,* DÖV 2006, 89, 90; *Brigola,* System der EG-Grundfreiheiten, 2004, S. 123 ff.

[1613] Als Synonym werden die Begriffspaare unmittelbare, formale und rechtliche Diskriminierung verwendet, hierzu *Ehlers,* Jura 2001, 266, 271.

[1614] *Ehlers,* Jura 2001, 266, 271; *Thiele,* JA 2005, 621, 624; *Oppermann,* Europarecht, S. 638 Rn. 1521; *Frenz,* europäische Grundfreiheiten, S. 53 Rn. 123.

999 Versteckte[1615] Diskriminierungen sind gegeben, wenn die betroffene Regelung zwar nicht ausdrücklich an die Staatsangehörigkeit anknüpft, jedoch die Produkte oder Personen ausländischer Herkunft typischerweise stärker als inländische Produkte oder Personen betrifft.[1616] Da durch ein IT-Sicherheitsgesetz aus- und inländische Produkte gleichermaßen die IT-Anforderungen erfüllen müssten, wäre auch diese Voraussetzung nicht erfüllt.

(c) Beschränkung

1000 Seit der *Dassonville*-Entscheidung im Jahr 1974 legt der EuGH die Warenverkehrsfreiheit jedoch nicht nur als Diskriminierungsverbot, sondern auch als allgemeines Beschränkungsverbot aus.[1617] Nach der *Dassonville*-Formel ist als Maßnahme gleicher Wirkung i.S.d. Art. 28 EG jede Maßnahme anzusehen, die geeignet ist, den innergemeinschaftlichen Handel unmittelbar oder mittelbar, tatsächlich oder potentiell zu behindern.[1618] Diese extrem weite Auslegung des Art. 28 EG, welche dazu führte, dass jegliche Bestimmung dem Anwendungsbereich des Art. 28 EG unterfiel und daher einer Rechtfertigung bedurfte,[1619] korrigierte der EuGH 1993 mit seiner Entscheidung *Keck und Mithouard*[1620]. Seither ist zwischen „Verkaufsmodalitäten" und „produktbezogenen Regelungen" zu differenzieren, wobei die „Verkaufsmodalitäten" nicht dem Beschränkungsbegriff des Art. 28 EG unterfallen sollen, sofern diese Bestimmungen für alle betroffenen Wirtschaftsteilnehmer gelten, die ihre Tätigkeit im Inland ausüben (1. Keck-Kriterium), und sofern sie den Absatz der inländischen Erzeugnisse und Erzeugnisse aus anderen Mitgliedstaaten rechtlich wie tatsächlich in gleicher Weise berühren (2. Keck-Kriterium).[1621] Verkaufsmodalitäten sind Regelungen, die festlegen, wer, wann, was, wo und wie verkaufen darf und die somit nur in mittelbarem Zusammenhang mit den Einfuhren stehen, während produktbezogene Vorschriften Regelungen hinsichtlich

---

[1615] Versteckte Diskriminierungen werden auch mittelbare, materielle, faktische bzw. verschleierte Diskriminierungen genannt, s. *Ehlers,* Jura 2001, 266, 271; *Thiele,* JA 2005, 621, *Müller-Graff,* in: GTE, Art. 30 Rn. 196; *Streinz,* in: FS für Rudolf, 2001, S. 199, 218; *Kilian,* Europäisches Wirtschaftsrecht, S. 146 Rn. 333.

[1616] EuGH, Rs. 152/73, *Sotgui,* Slg. 1974, 153, 164 f. Rn. 11.; Rs. 31/87, *Beentjes,* Slg. 1988, 4635, 4659 Rn. 30; Rs. C-266/95, *Merino Garcia,* Slg. 1997, I-3279, 3313 Rn. 3313; Rs. 327/94, *O'Flynn,* Slg. 1996, I-2617, 2637 f. Rn. 17.

[1617] EuGH, Rs. 8/74, *Dassonville,* Slg. 1974, 837, 852 Rn. 5.

[1618] EuGH, Rs. 8/74, *Dassonville,* Slg. 1974, 837, 852 Rn. 5.

[1619] *Frenz,* europäische Grundfreiheiten, S. 306 Rn. 796; *Hammer,* Handbuch zum freien Warenverkehr, 1998, S. 15; *Brigola,* System der EG-Grundfreiheiten, 2004, S. 8; *Bleckmann,* Europarecht, S. 554 Rn. 1500; *Herdegen,* Europarecht, S. 255 Rn. 5; *Zuleeg,* in: FS für Everling, 1995, Bd. II, S. 1717, 1719; *Bernhard,* EWS 1992, 403, 405; *Stuyck,* WRP 1994, 578; *Ress,* EuZW 1993, 745; *Moench,* NJW 1982, 2689, 2690.

[1620] EuGH, Rs. C-267 u. 268/91, *Keck,* Slg. 1993, I-6097. Aus der umfangreichen Literatur s. nur *Hammer,* Handbuch zum freien Warenverkehr, 1998, S. 108 ff.; *Bernhard,* EWS 1995, 404, 405; *Müller-Graff,* in: von der Groeben/Schwarze, Art 28 Rn. 239 je mwN.

[1621] EuGH, Rs. C-267 u. 268/91, *Keck,* Slg. 1993, I-6097, 6131 Rn. 16.

der Bezeichnung der Ware, ihrer Form, ihrer Abmessungen, ihres Gewichts, ihrer Zusammensetzung, ihrer Aufmachung, ihrer Etikettierung und ihrer Verpackung treffen.[1622]

1001 Bei den produktbezogenen Vorschriften handelt es sich nach der EuGH-Definition um Regelungen, welche die Beschaffenheit von Waren im weitesten Sinne zum Gegenstand haben und an diese konkrete Beschaffenheit die Erlaubnis zum Marktzugang knüpfen, so dass das physische Erscheinungsbild des Produktes über dessen Verkehrsfähigkeit entscheidet.[1623] Der Gerichtshof hat bereits in diversen Urteilen nach *Keck* verschiedene Maßnahmen den produktbezogenen Regelungen zugeordnet.[1624] Darunter fallen u.a. Vorschriften, welche die Bezeichnung eines bestimmten Produktnamens,[1625] deren Herkunftsbezeichnung,[1626] die Etikettierung,[1627] die Zusammensetzung[1628] und die damit zusammenhängenden erlaubten Produktbezeichnungen[1629] sowie entsprechende Kontrollen[1630] betreffen.

1002 IT-spezifische Anforderungen nach einem öffentlich-rechtlichen Sicherheitsgesetz sind keine Regelungen, die festlegen, wer, wann, was, wo und wie verkaufen darf, sondern knüpfen an die konkrete Beschaffenheit der Hard- bzw. Software (z.B. hinsichtlich einer erfolgten Zertifizierung) die Erlaubnis zur Verkehrsfähigkeit auf dem deutschen Markt. Insofern stellen sie produktbezogene Regelungen dar, die i.S.d. Keck-Formel nach wie vor dem Rechtfertigungszwang der Art. 28 ff. EG unterliegt.

(4) Rechtfertigung

[1622] *GA Tesauro,* Rs. C-292/92, *Hünermund,* Slg. 1993, I-6787, 6803 ff. Rn. 9 ff. mit ausführlicher Anm. von *Petschke,* EuZW 1994, 107, 109 ff.

[1623] *Schimming,* Konvergenz der Grundfreiheiten des EGV, 2002, S. 127; *Körber,* Grundfreiheiten und Privatrecht, 2004, S. 176 f.

[1624] Zu einem guten Überblick s. *Frenz,* europäische Grundfreiheiten, S. 323 ff. Rn. 844 ff.

[1625] EuGH, Rs. C-315/92, *Clinique,* Slg. 1994, I-317, 335 ff. Rn. 13 ff.; Rs. C-313/94, *Graffione,* Slg. 1996, I-6039, 6057 Rn. 15 f., Rs. C-184/96, *Kommission/Frankreich,* Slg. 1998, I-6197, 6224 Rn. 18; Rs. C-448/98, *Guimont,* Slg. 2000, I-10663, 10689 Rn. 26.

[1626] EuGH, Rs. C-321 bis 324/94, *Pistre,* Slg. 1997, I-2343, 2377 Rn. 54; EuGH, Rs. C-87/97, *Consorzio per la tutela del formaggio Gorgonzola,* Slg. 1999, I-1301; Rs. C-325/00, *Kommission/Deutschland,* Slg. 2002, I-9977; Rs. C-108/01, *Consorzio del Prosciutto di Parma,* Slg. 2003, I-5121; Rs. C-469/00, *Société Ravil,* Slg. 2003, I-5053.

[1627] EuGH, Rs. C-317/92, *Kommission/Deutschland,* Slg. 1994, I-2039, 2060 Rn. 12; Rs. C-51/93, *Meyhui,* Slg. 1994, I-3879; Rs. C-33/97, *Colim,* Slg. 1999, I-3175; Rs. C-293/93, *Houtwipper,* Slg. 1994, I-4249, 4267 Rn. 11 f.; Rs. C-240/95, *Schmit,* Slg. 1996, I-3179; Rs. C-55/99, *Kommission/Frankreich,* Slg. 2000, I-11499; Rs. C-30/99, *Kommission/Irland,* Slg. 2001, I-4169.

[1628] EuGH, Rs. C-17/93, *van der Veldt,* Slg. 1994, I-3537, 3558 f. Rn. 9 ff.; Rs. C-358/95, *Moratello,* Slg. 1997, I-1431, 1449 Rn. 12; Rs. C-123/00, *Bellamy,* Slg. 2001, I-2795; EuGH Rs. C-184/96, *Kommission/Frankreich,* Slg. 1998, I-6197; EuGH, Rs. C-383/97, *van der Laan,* Slg. 1999, I-731, 759 Rn. 19 ff.; EuGH, Rs. C-192/01, *Kommission/Dänemark,* Slg. 2003, I-9693; EuGH, Rs. C-24/00, *Kommission/Frankreich,* Slg. 2004, I-1306.

[1629] EuGH, Rs. C-12/00, *Kommission/Spanien,* Slg. 2003, I-459; Rs. C-14/00, *Kommission/Italien,* Slg. 2003, I-515.

[1630] EuGH, Rs. C-105/94, *Celestini,* Slg. 1997, I-2971; Rs. C-390/99, *Canal Satélite Digital,* Slg. 2002, I-607.

1003 Nicht jede festgestellte Beeinträchtigung stellt auch einen Verstoß gegen die Grundfreiheiten dar, in Betracht kommt bei Vorliegen der jeweiligen Voraussetzungen immer auch eine Rechtfertigung.[1631] Zu differenzieren ist grundsätzlich zwischen den geschriebenen Rechtfertigungsgründen des Vertrages und den ungeschriebenen, die vom EuGH in der *Cassis-de-Dijon*-Entscheidung[1632] in Rechtsfortbildung entwickelt wurden.[1633]

(a) Geschriebene Rechtfertigungsgründe, Art. 30 EG

1004 Art. 28 EG steht zunächst ausdrücklich solchen Maßnahmen nicht entgegen, die aus Gründen der öffentlichen Sittlichkeit[1634], Ordnung[1635] und Sicherheit[1636],[1637] zum Schutze der Gesundheit und des Lebens von Menschen[1638], Tieren oder Pflanzen[1639], des nationalen Kulturguts von künstlerischem, geschichtlichem oder archäologischem Wert[1640] oder des gewerblichen und kommerziellen Eigentums[1641] gerechtfertigt sind (Art. 30 EG). Die Auslegung der genannten Schutzgüter erfolgt gemeinschaftsrechtlich

[1631] *Jarass,* EuR 1995, 295, 220 f.; *ders.,* EuR 2000, 705, 716; *Ehlers,* Jura 2001, 482, 486; *Thiele,* JA 2005, 621, 625; *Frenz,* europäische Grundfreiheiten, S. 176 Rn. 464; *Streinz,* Europarecht, S. 297 Rn. 692 ff.

[1632] EuGH, Rs. 120/78, *Cassis de Dijon,* Slg. 1979, 649.

[1633] *Frenz,* europäische Grundfreiheiten, S. 176 Rn. 464; *Streinz,* Europarecht, S. 297 f. Rn. 692 ff.; *Jarass,* EuR 1995, 202, 220 ff.; *ders.,* EuR 2000, 705, 717 ff.; *Hartje,* Jura 2003, 160, 165; *Epiney,* in: Ehlers, Grundfreiheiten, S. 241 ff. Rn. 51 ff.; *Ehlers,* Jura 2001, 482, 486.

[1634] Zum Begriff der öffentlichen Sittlichkeit s. EuGH, Rs. 34/79, *Henn und Darby,* Slg. 1979, 3795, 3813 Rn. 15 f.; Rs. 121/85, *Conegate,* Slg. 1986, 1007, 1022 Rn. 14; *Becker,* in: Schwarze, Art. 30 Rn. 9.

[1635] Zur öffentlichen Ordnung s. EuGH, Rs. 30/77, *Bouchereau,* Slg. 1977, 1999, 2013 Rn. 33 f.; Rs. 7/78, *Thompson,* Slg. 1978, 2247, 2275 f. Rn. 32 ff.; Rs. 154/85, *Kommission/Italien,* Slg. 1987, 2717, 2738 f. Rn. 13 f.

[1636] EuGH, Rs. C-367/89, *Richardt,* Slg. 1991, I-4621, 4652 Rn. 22; Rs. 72/83, *Campus Oil,* Slg. 1984, 2727, 2752 Rn. 35; Rs. C-124/95, *Centro-Com,.* Slg. 1997, I-81, 127 Rn. 44; Rs. C-398/98, *Kommission/Griechenland,* Slg. 2001, I-7915, 7941 Rn. 29; *Becker,* in: Schwarze, Art. 30 Rn. 12.

[1637] Eine Auslegung der öffentlichen Ordnung und Sicherheit anhand der Generalklausel des deutschen Polizei- und Ordnungsrechts kommt nach ganz h.M. nicht in Betracht, s. hierzu ausführlich *Millarg,* Schranken des freien Warenverkehrs, 2001, S. 141 f.

[1638] EuGH, Rs. 53/80, *Eyssen,* Slg. 1981, 409, 421 f. Rn. 13 f.; Rs. 87/83, *Melkunie,* Slg. 1984, 2367, 2386 Rn. 19; Rs. 98/83, *Heijn,* Slg. 1984, 3263, 3280 Rn. 19; Rs. 54/85, *Mirepoix,* Slg. 1986, 1067, 1079 Rn. 15.

[1639] EuGH Rs. 40/82, *Kommission/Vereinigtes Königreich II,* Slg. 1984, 283, 299 Rn. 14 ff.; Rs. 74/82, *Kommission/Irland,* Slg. 1984, 317, 342 Rn.31 ff.; Rs. 131/93, *Kommission/Deutschland,* Slg. 1994, I-3303, 3320 f. Rn. 13 ff.; *Frenz,* europäische Grundfreiheiten, S. 367 ff. Rn. 965 ff. mwN.

[1640] Zu dem Schutz des nationalen Kulturguts s. *Müller-Graff,* in: von der Groeben/Schwarze, Art. 30 Rn. 62 ff. mwN.

[1641] EuGH, Rs. 16/74, *Centrafarm,* Slg. 1974, 1183, 1195 Rn. 8 f.; Rs. 55 u. 57/80, *GEMA,* Slg. 1981, 147, 161 Rn. 9; Rs. 258/78, *Nungesser,* Slg. 1982, 2015, 2063 Rn. 35; Rs. 144/81, *Keurkoop,* Slg. 1982, 2853, 2870 Rn. 14; Rs. C-47/90, *Delhaize,* Slg. 1992, I-3669, 3709 Rn. 16; Rs. C-3/91, *Exportur,* Slg. 1992, I-5529, 5562 Rn. 28.

und nicht aus nationaler Sicht.[1642] Als Ausnahmetatbestände werden sie vom EuGH in ständiger Rechtsprechung eng ausgelegt.[1643]

1005 Schutzziele eines öffentlich-rechtlichen Sicherheitsgesetzes sind der Verbraucherschutz sowie allgemeine volkswirtschaftliche Überlegungen. In Betracht kommt insoweit gem. Art. 30 EG allenfalls eine Rechtfertigung aus Gründen der öffentlichen Sicherheit. Gründe der öffentlichen Sicherheit liegen jedoch erst dann vor, wenn die Existenz eines Mitgliedstaats gefährdet ist, insbesondere bei Gefährdung der erforderlichen Einrichtungen und wichtiger öffentlicher Dienste.[1644] Eine Gefährdung elementarer, existenzsichernder staatlicher Interessen liegt bei einer Vermögensgefährdung durch gefährliche IT-Produkte in der Regel nicht vor. Allenfalls bei Gefährdung besonders kritischer Infrastrukturen wäre eine solche Rechtfertigung denkbar.[1645]

(b) Ungeschriebene Rechtfertigungsgründe

1006 Neben den ausdrücklich geschriebenen Rechtfertigungsgründen hat der EuGH in seiner *Cassis*–Rechtsprechungaber auch weitere, ungeschriebene Rechtfertigungsgründe anerkannt (sog. zwingende Gründe des Allgemeinwohls). [1646] Diese gelten im Unterschied zu den geschriebenen Rechtfertigungsgründen jedoch nicht für alle Arten der Beeinträchtigungen: Während umstritten ist, ob sie auch auf versteckte Diskriminierungen angewandt werden können,[1647] steht fest, dass sie jedenfalls keine Anwendung auf offene Diskriminierungen finden dürfen.[1648] Bei einer – wie hier vorliegenden - Beschränkung i.S.v. *Dassonville* können sie jedoch immer eine Rechtfertigung ermöglichen.[1649]

1007 Genannt waren in dem *Cassis*-Urteil selbst als „zwingende Gründe des Allgemeinwohls“ lediglich der Verbraucherschutz, die wirksame steuerliche Kontrolle, der Schutz

---

[1642] *Frenz,* europäische Grundfreiheiten, S. 358 Rn. 941; *White,* CMLR 1989, 235, 249; *Mayer,* EuR 2003, 793, 797 f.

[1643] Grundlegend EuGH, Rs. 41/74, *van Duyn,* Slg. 1974, 1337, 1350 Rn. 19; seitdem mehrfach bestätigt in EuGH, Rs. 46/76, *Bauhuis,* Slg. 1977, 5, 15 Rn.12/15; Rs. 113/80, *Kommission/Irland,* Slg. 1981, 1625, 1638 Rn. 7; Rs. C-205/89, *Kommission/Griechenland,* Slg. 1991, I-1361, 1377 Rn. 9.

[1644] EuGH, Rs. 7/78, *Thompson,* Slg. 1978, 2247 Rn. 32/42; *Schroeder,* in: Streinz, Art. 30 Rn. 11; *Frenz,* europäische Grundfreiheiten, S. 359 Rn. 945 mwN.

[1645]. Zu kritischen Infastrukturen siehe *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, 2005 (die Problematik wird dort nicht diskutiert).

[1646] EuGH, Rs. 120/78, *Cassis de Dijon,* Slg. 1979, 649, 662 Rn. 8.

[1647] Ausführlich *Steinberg,* EuGRZ 2001, 13, 21 ff.; *Müller-Graff,* in: von der Groeben/Schwarze, Art. 28 Rn. 196 ff.; *Gundel,* Jura 2001, 79, 80 ff. mwN.

[1648] EuGH, Rs. 113/80, *Kommission/Irland,* Slg. 1981, 1625, 1639 Rn. 11; Rs. 59/82, *Weinvertriebs-GmbH,* Slg. 1983, 1217, 1227 Rn. 11; Rs. 19/92, *Kraus,* Slg. 1993, I-1663, 1697 Rn. 32; Rs. C-55/94, *Gebhard,* Slg. 1995, I-4165, 4197 Rn. 23; Rs. C-434/97, *Haim,* Slg. 2000, I-5123, 5166 Rn. 57.

[1649] EuGH, Rs. C-55/94, *Gebhard,* Slg. 1995, I-4165, 4197 Rn. 23; Rs. 19/92, *Kraus,* Slg. 1993, I-1663, 1697 Rn. 32; Rs. C-434/97, *Haim,* Slg. 2000, I-5123, 5166 Rn. 57; *Epiney,* in: Ehlers, Grundfreiheiten, S. 244 f. Rn. 60 f.; *Hakenberg,* in: Lenz/Borchardt, Art. 49/50 Rn. 25; *Schroeder,* in: Streinz, Art. 38 Rn. 71; *Becker,* in: Schwarze, Art. 28 Rn. 43.

der öffentlichen Gesundheit sowie die Lauterkeit des Handelsverkehrs.[1650] Die zwingenden Gründe des Allgemeininteresses sind primärrechtlich weder geregelt noch begrenzt; insofern wird in der Literatur darauf hingewiesen, dass die Mitgliedstaaten einen gewissen Spielraum besitzen, um Schutzanliegen zu definieren.[1651] Es handelt sich bei den zwingenden Gründen des Allgemeinwohls nicht um einen abschließenden Numerus clausus, sondern diese sind beliebig erweiterbar.[1652] Anerkannt wurden bisher vom EuGH der Umweltschutz, die Verbesserung der Lebens- und Arbeitsbedingungen der Arbeitskräfte, die Verkehrssicherheit, die Kulturpolitik, die Aufrechterhaltung der Medienvielfalt, der Schutz landesweiter oder regionaler sozialer und kultureller Besonderheiten, der Erhalt des finanziellen Gleichgewichts der Sozialsysteme sowie der Schutz der Nahversorgungsbedingungen und des öffentlichen Fernmeldewesens.[1653] Lediglich rein wirtschaftliche Gründe scheiden hingegen nach ständiger Rechtsprechung zur Rechtfertigung aus, es darf sich nicht lediglich um Wirtschaftslenkung, die Erreichung wirtschaftspolitischer Zielsetzungen oder die Abwendung wirtschaftlicher Nachteile handeln.[1654]

1008 Das von einem IT-Sicherheitsgesetz verfolgte primäre Ziel des Verbraucherschutzes stellt somit unzweifelhaft einen „zwingenden Grund des Allgemeininteresses“ i.S.d. Cassis-de-Dijon-Rechtsprechung dar. Allgemeine Erwägungen der Volkswirtschaft als rein wirtschaftliche Gründe können hingegegen nach Ansicht des EuGH keinen ungeschriebenen Rechtfertigungsgrund bilden und scheiden vorliegend aus.[1655] Als Schutzzweck des Gesetzes kämen aber nicht nur ganz allgemeine volkswirtschaftliche Erwägungen in Betracht, sondern in concreto etwa auch der Schutz eines Finanzsystems,um dieses durch IT-Sicherheitsanforderungen vor einem etwaigen Zusammenbruch zu bewahren. Explizit wurde dieser Schutzzweck vom EuGH jedoch bisher noch nicht anerkannt. Zu beachten ist jedoch einerseits, dass der Katalog der ungeschriebenen Rechtfertigungsgründe kein abschließender ist, sondern erweiterbar[1656] und andererseits, dass

[1650] EuGH, Rs. 120/78, *Cassis de Dijon,* Slg. 1979, 649, 662 Rn. 8.

[1651] *Randelzhofer/Forsthoff,* in: Grabitz/Hilf, vor Art. 39-55 Rn. 160; *Frenz,* europäische Grundfreiheiten, S. 859 Rn. 2280.

[1652] *Frenz,* europäische Grundfreiheiten, S. 396 Rn. 1042.

[1653] Ausführlich mwN. zur Rspr. *Müller-Graff,* in: von der Groeben/Schwarze, Art. 28 Rn. 224 f.; *Frenz ,* europäische Grundfreiheiten, S. 379 ff. Rn. 998 ff.

[1654] St. Rspr, s. nur EuGH, Rs. C. 120/95, *Decker,* Slg. 1998, I-1831, 1884 Rn. 39; Rs. C-203/96, *Dusseldorp,* Slg. 1998, I-4075, 4127 Rn. 44; *Müller-Graff,* in: von der Groeben/Schwarze, Art. 28 EG Rn. 204; *Epiney,* in: Calliess/Ruffert, Art. 30 Rn. 14 f. je mwN.

[1655] EuGH, Rs. C. 120/95, *Decker,* Slg. 1998, I-1831, 1884 Rn. 39; Rs. C-203/96, *Dusseldorp,* Slg. 1998, I-4075, 4127 Rn. 44; *Epiney,* in: Calliess/Ruffert, Art. 30 Rn. 14 f.

[1656] *Frenz,* europäische Grundfreiheiten, S. 396 Rn. 1042; *Müller-Graff,* in: von der Groeben/Schwarze, Art. 28 Rn. 224 f.

es in der Praxis regelmäßig zu Überschneidungen wirtschaftlicher und nichtwirtschaftlicher Gründe kommt.[1657] Nach Rechtsprechung des EuGH darf es sich aber lediglich nicht nur um *rein* wirtschaftliche Gründe handeln, sobald ein Ziel ein Zwischenziel darstellt, dass letzlich der Erreichung eines nicht ökonomischen Gemeinwohlziels dient und in seiner Bedeutung hinter dieses zurücktritt, kommt eine Rechtfertigung mithilfe der „zwingenden Gründe“ wiederum in Betracht.[1658] Insofern könnte anzunehmen sein, dass auch der Schutz der Finanzsysteme als zumindest nicht *rein* wirtschaftlicher Grund eine Rechtfertigungsmöglichkeit darstellen könnte. Jedoch genügt zur Rechtfertigung bereits ein „zwingender Grund des Allgemeinwohls“ und mangels gefestigter Rechtsprechung zu dem Schutz der Finanzsysteme sollte aus Gründen der Rechtgssicherheit auf den bereits vom EuGH anerkannten Rechtfertigungsgrund des Verbraucherschutzes abgestellt werden.

(c) Verhältnismäßigkeitsgrundsatz

1009 Nachdem festgestellt wurde, dass die staatliche Regelung einem der genannten Ziele der *Cassis*-Formel entspricht, muss immer auch eine Prüfung der Verhältnismäßigkeit erfolgen.[1659] Während dieser im deutschen Recht aus Geeignetheit, Erforderlichkeit und Angemessenheit der Maßnahme besteht,[1660] prüft der EuGH hingegen neben der Geeignetheit regelmäßig im Schwerpunkt nur die Erforderlichkeit, während die Angemessenheit der nationalen Regelung keinen eigenständigen Prüfungspunkt bildet.[1661]

(i) Geeignetheit

1010 Geeignet ist eine nationale Maßnahme, wenn sie das erstrebte Ziel irgendwie fördern kann.[1662] Eine Maßnahme ist nur dann ungeeignet, wenn sie den angestrebten Schutz oder Vorteil überhaupt nicht gewährt, wobei die Teilgeeignetheit bereits genügt.[1663] Nationale Maßnahmen sind selten ungeeignet, da sie in der Regel in diesem Sinne zumin-

---

[1657] *Schroeder,* in: Streinz, Art. 28 Rn. 48.

[1658] EuGH, Rs. Rs. C-120/95, *Decker,* Slg. 1998, I-1831 Rn. 39 (erhebliche Störungern des finanziellen Gleichgewichts der Sozialversicherungssysteme); Rs. 72/83, *Campus Oil,* Slg. 1984, 2727 Rn. 35 (Störungen der Versorgung eines Mitgliedstaats mit Erdölerzeugnissen); s. *Schroeder,* in: Streinz, Art. 28 Rn. 48 mwN. zur Rspr.

[1659] Ausführlich hierzu *Koch,* Grundsatz der Verhältnismäßigkeit, 2003, S. 290 ff.; *von Danwitz,* EWS 2003, 393, 394 ff.; *Mayer,* EuR 2003, 793, 817.

[1660] BVerfGE 65, *Volkszählung,* 1, 48 ff.; s. auch *Koch*, Grundsatz der Verhältnismäßigkeit, 2003, S. 49 ff. mwN.

[1661] EuGH, Rs. C-19/92, *Kraus,* Slg. 1993, I-1663, 1697 Rn. 32; Rs. C-55/94, *Gebhard,* Slg. 1995, I-4165, 4197 f. Rn. 37; Rs. C-424/97, *Haim,* Slg. 2000, I-5123, 5166 Rn. 57; Rs. C108/96, *Mac Quen,* Slg. 2001, I-837, 866 f. Rn. 26.

[1662] EuGH, Rs. 152/78, *Kommission/Frankreich,* Slg. 1980, 2299, 2315 Rn. 15 ff.; *Frenz,* europäische Grundfreiheiten, S. 200 Rn. 528.

[1663] *Kingreen,* Struktur der Grundfreiheiten, 1999, S. 169; *Tiedje/Troberg,* in: von der Groeben/Schwarze, Art. 43 Rn. 106; *Müller-Graff,* in: Streinz, Art. 43 Rn. 79, Art. 46 Rn. 17.

dest möglicherweise zur Zielerreichung taugen.[1664] Allgemeine IT-Sicherheitsstandards für IT-Produkte dürften aber ohne weiteres grundsätzlich geeignet sein, den Verbraucherschutz durch Vermeidung von Vermögens- und Eigentumsschäden zu fördern, da sie den Verbraucher von entsprechenden Kosten und Schäden entlasten können.

(ii) Erforderlichkeit

1011 Damit eine Maßnahme als erforderlich qualifiziert werden kann, darf kein weniger stark eingreifendes Mittel existieren, welches den erstrebten Zweck in der gleichen Weise zu erreichen oder zu fördern geeignet ist.[1665] In diesem Rahmen besagt das Herkunfts- oder Ursprungslandprinzip, dass ein in einem Mitgliedstaat rechtmäßig hergestelltes und in den Verkehr gebrachtes Erzeugnis auch in allen anderen Mitgliedstaaten eingeführt werden darf; unzulässig sind daher insbesondere Doppelkontrollen.[1666] Hintergrund des Herkunftslandprinzips ist der Gedanke, dass alle Mitgliedstaaten mit ihren Rechtsordnungen im Wesentlichen gleiche Interessen verfolgen; basierend auf gegenseitigem Vertrauen ist daher die Entscheidung eines Mitgliedstaates, ein Erzeugnis in seiner konkreten Gestalt zum Verkehr zuzulassen, von allen anderen Mitgliedstaaten zu akzeptieren.[1667] Die anderen Mitgliedstaaten, in welche das betreffende Produkt eingeführt werden soll, haben demnach davon auszugehen, dass es auch ihren nationalen Rechtsvorschriften entspricht (sog. Prinzip der gegenseitigen Anerkennung).[1668] Eine Folge des „Herkunftslandsprinzips“ ist daher die gegenseitige Anerkennung von Standards aus unterschiedlichen Mitgliedstaaten.[1669] So ist nach Rechtsprechung des EuGH das erneute Erbringen eines Befähigungsnachweises im Aufnahmestaat nicht erforderlich, sofern ein äquivalentes Testat bereits im Herkunftsland erworben worden ist.[1670]

[1664] Statt vieler *Schroeder,* in: Streinz, Art. 28 Rn. 52.

[1665] St. Rspr., s. nur EuGH, Rs. 302/86, *Dänische Pfandflaschen,* Slg. 1988, 4607, S. 4630 Rn. 11; *Tesauro,* in: ZEW 1996, S. 1, 8.

[1666] *Classen,* EWS 1998, 97, 98; *Hammer,* Handbuch zum freien Warenverkehr, 1998, S. 27; *Frenz,* europäische Grundfreiheiten, S. 70 Rn. 168; *Santos Lorenzo,* in: Illescas Ortiz/ Moreiro González (Hrsg.), Derecho Comunitario Económico, 2001, S. 55, 66 f.; *Martin-Ehlers,* in: Sandrock/Wetzler (Hrsg.), Deutsches Gesellschaftsrecht im Wettbewerb der Rechtsordnungen, 2004, S. 1, 21 f.

[1667] *Drasch,* Herkunftslandprinzip, 1997, S. 206; *Leible,* in: Grabitz/Hilf, Art. 28 Rn. 26; *Krebber,* in: Jahrbuch junger Zivilrechtswissenschaftler 1997, S. 129, 142; *Feiden,* Bedeutung der „Keck“-Rechtsprechung, 2003, S. 50; *Oppermann,* Europarecht, S. 456 Rn. 1180.

[1668] Zu dem Prinzip der gegenseitigen Anerkennung ausführlich *Bangemann,* EuZW 1993, 7, 7 f.; *Chalmers,* ICLQ 1993, 269, 281; *ders.,* ELR 1994, 385, 396, 402; *Streinz,* Europarecht, S. 414 ff. Rn. 973 ff.; *Drasch,* Herkunftslandprinzip, 1997, S. 205 ff. mwN.

[1669] *Martin-Ehlers,* in: Sandrock/Wetzler (Hrsg.), Deutsches Gesellschaftsrecht im Wettbewerb der Rechtsordnungen, 2004, S. 1, 22; *Becker,* in: Schwarze, Art. 30 EGV Rn. 71 ff.

[1670] EuGH, Rs. C.340/89, *Vlassopoulou,* Slg. 1991, I-2357, 2383 f. Rn.; *Frenz,* europäische Grundfreiheiten, S. 201 Rn. 531.

1012 Sofern im europäischen Ausland daher bereits vor Einfuhr der Hard- bzw. Software nach Deutschland eine angemessene, qualitativ gleichwertige IT-Sicherheitskontrolle durch Vergabe nationaler Zertifikate erfolgt, wäre eine erneute Prüfung nach einem deutschen IT-Sicherheitsgesetz nicht erforderlich und damit unzulässig. Einmal gewährte Produktsicherheitsstandards für Hard- oder Software (wie etwa Zertifizierungen) eines EU-europäischen ausländischen Anbieters sind auch in Deutschland bei qualitativer Gleichwertigkeit anzuerkennen. Dieses müsste in einem nationalen IT-Sicherheitsgesetz zur Vermeidung von Vermögens- und Eigentumsschäden durch Ausnahmeregelungen auch deutlich gemacht werden. Voraussetzung wären indes qualitativ gleichwertige Standards und Kontrollen.

1013 Ansonsten ist bei den einzelnen IT-Sicherheitsanforderungen hinsichtlich der Auswirkung auf den Marktzutritt zum Aufnahmestaat zu differenzieren. So wäre ein absolutes Verkaufsverbot (in Deutschland) bei Produkten aus anderen EU-Staaten, auch wenn sie zu einem erheblichen Vermögens- oder Eigentumsschaden führen, nie erforderlich sein; angenommen wurde dieses in der Rechtsprechung des EuGH bisher lediglich für Gesundheitsschäden.[1671] Da es sich bei der Vermeidung von Vermögens- bzw. Eigentumsschäden nicht um die Beeinträchtigung überragend wichtiger Gemeinschaftsgüter wie etwa Gesundheitsschutz, Verletzungen von Leib oder Leben, handelt, wäre ein Verkaufsverbot als absolute Marktzutrittsschranke und damit als schwerster Eingriff in den Art. 28 EG nie zu rechfertigen. Hier würden nach ständiger Rechtsprechung des EuGH, der im Gegensatz zum deutschen Recht auf das Leitbild des „mündigen Verbrauchers“ abstellt,[1672] statt vollständigen Vermarktungsverboten auch entsprechende Warnhinweise auf dem Produkt genügen.[1673] Zu beachten ist zudem, dass die Zertifizierung nach Rechtsprechung des EuGH nicht derart ausgestaltet sein darf, dass sie eine Negativbewertung speziell der eingeführten Waren vorgibt.[1674] Sicherheitsstandards für Produk-

[1671] EuGH, R. C-473/98, *Toolex,* Slg. 2000, I-5681, 5714 f. Rn. 40 ff., für ein Verbot von Erzeugnissen mit dem Zusatzstoff Trichlorethylen, der eine Gefahr für Nierenkrebsentstehung birgt.

[1672] EuGH, Rs. C-220/98, *Estée Lauder Cosmetics,* Slg. 2000, I-117, 146 Rn. 27; *Schanze/Jüttner,* AG 2003, 661, 663; *Ziemons,* ZIP 2003, 1913, 1916; *Eidenmüller/Rehm,* ZGR 2004, 159, 171 f.; *Körber,* Grundfreiheiten und Privatrecht, 2004, S. 570.

[1673] Zum nicht erforderlichen Verbot der Einfuhr von unter Verwendung von Zusatzstoffen hergestelltem Bier s. EuGH, Rs. 178/94, *Kommission/Deutschland,* Slg. 1987, 1227; *Müller-Graff,* in: von der Groeben/Schwarze, Art. 28 Rn. 218 mwN.

[1674] So EuGH, Rs. 178/84, *Kommission/Deutschland,* Slg. 1987, 1227, 1271 Rn. 35 zum Etikettierungserfordernis; *Müller-Graff,* in: von der Groeben/Schwarze, Art. 28 Rn. 219.

te[1675] sowie Zulassungsverfahren für Produkte müssen außerdem leicht zugänglich und dürfen nicht mit übermäßigen Kosten verbunden sein.[1676]

1014 Bei sonstigen Vermarktungsbeschränkungen sollte insofern hinsichtlich der Schwere der Gefahr eines drohenden Vermögensschadens bzw. sogar einer Eigentumsverletzung unterschieden werden. Hohe IT-Sicherheitsanforderungen können zur Vermeidung kleinerer Bagatellschäden grundsätzlich nicht, hingegen bei der Gefahr eines schweren Vermögens- bzw. Eigentumsschadens eher erforderlich sein. Die Rechtfertigung von Eigentumsschäden sollte wiederum leichter möglich sein als die von bloßen Vermögensschäden. Daher gilt: Je höher die Gefahr eines Schadenseintritts, desto höher können auch die Anforderungen an die IT-Sicherheit sein. Aufwendige Maßnahmen einer Zertifizierung zur Vermeidung von kleinen Schäden scheiden daher eher aus als zur Vermeidung von Schäden größeren Umfangs. Das Gesetz müsste dementsprechend bei den verschiedenen IT-Sicherheitsmaßnahmen im Einzelfall hinsichtlich der Schwere des Schadens sowie zwischen Vermögens- und Eigentumsschäden differenzieren. Sofern Sicherheiten für Produkte verlangt werden würden, mit deren Hilfe strafbare Handlungen durchgeführt werden können (etwa Software, die ein Ausspähen von fremden Daten ermöglicht bzw. erleichtert oder Sicherheitslücken im Internet Explorer, die einen Eingriff Dritter erleichtern) könnten aufgrund der erhöhten Wertigkeit des Verbraucherschutzes, der hier sogar durch ein strafrechtliches Verbot gewährt ist, leichter Sicherheitsanforderungen an derartige Produkte gestellt werden als an solche, die von vorneherein weniger gefährlich sind. Abhängig dürfte dieses jedoch wiederum auch von der Höhe und der Gefahr des drohenden Schadens sein.

b) Online-Produkte

1015 Wie oben schon hervorgehoben, unterfallen Softwareprodukte, die online angeboten werden, prinzipiell dem Herkunftslandprinzip der ECRL (Art. 3). Diese regelt querschnittsmäßig alle Rechtsgebiete, mithin auch das Produktsicherheitsrecht, so dass Deutschland allenfalls nach Art. 3 Abs. 4 lit. a (i) 4. Spiegelstrich zum Schutz der Verbraucher abweichende Regelungen geltend machen könnte. Aber auch dann darf es sich nur um Einzelmaßnahmen handeln; komplette Rechtsgebiete unter den Schutz der Ausnahme nach Art. 3 Abs. 4 lit. a ECRL zu unterstellen, würde dem Notifizierungs- und

[1675] EuGH, Rs. 188/84, *Kommission/Frankreich,* Slg. 1986, 419, 439 Rn. 32 zur Zulassung von Holzbearbeitungsmaschinen.
[1676] EuGH, Rs. C-293/93, *Houtwipper,* Slg. 1994, I-4249 Rn. 19; *Schroeder,* in: Streinz, Art. 30 Rn. 54.

Einzelgenehmigungsverfahren von Art. 3 Abs. 4 ECRL widersprechen.[1677] Auch der Anhang zu Art. 3 ECRL führt hier nicht weiter, da er keine entsprechende Ausnahme hinsichtlich der Produktsicherheit enthält. Immerhin würden hinsichtlich einer Einzelfallmaßnahme die oben beschriebenen Rechtfertigungsgründe eingreifen. Dieses Ergebnis ist zwar rechtspolitisch bedauerlich, aber durch die Trennung zwischen offline- und online-Welt bei der EU derzeit unausweichlich – Abhilfe schafft hier nur eine Harmonisierung in Gestalt einer Produktsicherheits-Richtlinie, wie sie hier explizit favorisiert wird.

2. IT-Sicherheitsanforderungen an Dienstleistungen

a) Grundsätze: Der Einfluß der E-Commerce-Richtlinie

1016 Sofern in dem Gesetz auch IT-Sicherheitsanforderungen an Dienstleistungen gestellt werden, ist an sich die Dienstleistungsfreiheit des Art. 49 EG der entscheidende Maßstab. Indes ist der Anwendungsbereich des Art. 49 EG angesichts der Regelungen in der E-Commerce-Richtlinie nur von marginaler Bedeutung; denn die meisten IT-Dienstleistungen dürften online angeboten werden, so dass von vornherein das Herkunftslandprinzip nach Art. 3 der ECRL eingreift, mit der Folge, dass Deutschland keine Anforderungen stellen kann, die über das Niveau des jeweiligen Herkunftslands des Online-Dienstleisters hinausgehen würden. Ein deutsches IT-SicherheitsG würde daher von vornherein keine Anwendung finden können (bzw. keine über das Niveau des Herkunftslandes hinausgehende Anforderungen stellen können) auf Dienste, die aus dem EU-Ausland erbracht werden.

1017 Die nachfolgenden Ausführungen, die sich vor allem auf die Frage der Primär-Freiheiten beziehen, haben dennoch Geltung, etwa wenn es um die Frage von Rechtfer-

[1677] Die Mitteilung der Kommission an den Rat, das Europäische Parlament und die Europäische Zentralbank betreffend die Anwendung von Artikel 3 Absätze 4 bis 6 der Richtlinie über den elektronischen Geschäftsverkehr auf Finanzdienstleistungen, KOM (2003) 259 endgültig vom 14.5.2003, nennt als Beispiele für Maßnahmen nach Art. 3 Abs. 4 bis 6 ECRL „Sanktionen“ oder „Verfügungen“, also Einzelfallanordnungen (Punkt 2). Weiter führt sie unter Punkt 2.1.2. aus: „Durch die Bezeichnung "bestimmter" Dienst soll klargestellt werden, dass die Mitgliedstaaten im Rahmen von Artikel 3 Absatz 4 keine allgemeinen Maßnahmen gegenüber einer Kategorie von Finanzdienstleistungen als Ganzes - wie z. B. Investmentfonds oder Kredite – ergreifen dürfen. Um unter Artikel 3 Absatz 4 zu fallen, muss sich eine Maßnahme also auf einen konkreten Fall beziehen, d. h. gegenüber einer ganz bestimmten Finanzdienstleistung ergriffen werden, die von einem bezeichneten Anbieter erbracht wird. Es könnte sich z. B. um eine Mahnung oder ein Zwangsgeld von Seiten eines Mitgliedstaats (Bestimmungsmitgliedstaats) gegenüber einer Bank handeln, die von dem Mitgliedstaat aus, in dem sie niedergelassen ist (Herkunftsmitgliedstaat), in seinem Hoheitsgebiet nicht harmonisierte Investmentdienste anbietet. Derartige Maßnahmen könnten damit begründet werden, dass die Bank bestimmte Verhaltensregeln missachtet, die im Bestimmungsmitgliedstaat dem Verbraucherschutz dienen. Nicht zulässig wäre es hingegen, wenn ein Mitgliedstaat auf der Grundlage von Artikel 3 Absatz 4 die Gesamtheit seiner Rechtsvorschriften für nicht harmonisierte Investmentfonds allgemein und horizontal auf alle Dienste anwendet, zu denen die Einwohner dieses Staates Zugang haben.“

tigungen von Ausnahmen nach Art. 3 IV ECRL geht, die sich nach denselben Maßstäben wie die Rechtfertigung bei Beeinträchtigungen der Primär-Freiheiten beurteilen:

b) Andere sekundärrechtlicher Regelungen

1018 Die Produktsicherheits-RL 2001/95/EG findet gem. Art. 1 Abs. 2 der RL lediglich auf die in Art. 2 lit. a) der RL genannten Produkte Anwendung und ist damit für Dienstleistungen nicht einschlägig.[1678] Auch die E-Commerce-RL[1679] sowie der Entwurf der Zahlungsdienste-RL[1680] stellen keine eigenen Anforderungen für Dienstleistungen im Anwendungsbereich von Vermögens- oder Eigentumsschäden auf; erst recht werden keine Sicherheitsstandards definiert. Der vor kurzem verabschiedete Entwurf der Dienstleistungs-RL[1681] erfasst ebenfalls nicht die Vermeidung von Vermögens- und Eigentumsschäden durch Auftstellen von öffentlich-rechtlichen IT-Sicherheitsanforderungen, sondern soll einen „wirklichen Binnenmarkt für Dienstleistungen“ schaffen,[1682] indem die Anforderungen für die Aufnahme oder Ausübung einer Dienstleistungstätigkeit geregelt werden,[1683] Anforderungen an die „Sicherheit von Dienstleistungen“ werden jedoch nicht gestellt. Eine abschließende Harmonisierung besteht daher für IT-Sicherheitsanforderungen an Dienstleistungen zur Vermeidung von reinen Vermögens- bzw. Eigentumsschäden noch nicht.

c) Schutzbereich

(1) Begriff der Dienstleistung

[1678] S. auch Erwägungsgrung Nr. 9 der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit, ABl EG Nr. L 11/4, 5.

[1679] Richtlinie 200/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“), ABl EG Nr. L 178/1.

[1680] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt vom 1.2.2005, KOM (2005) 603 endgültig, abrufbar im Internet unter http://eur-lex.europa.eu/LexUriServ/site/de/com/2005/com2005_0603de01.pdf (zuletzt abgerufen am 23.11.2006); dazu *Burgard*, WM 2006, 2065 ff..

[1681] S. aktueller Richtlinientext (vorläufige Fassung) nach der zweiten Lesung des Europäischen Parlaments vom 15.11.2006, abrufbar im Internet unter http://www.bmwi.de/BMWi/Redaktion/PDF/P-R/richtlinientext-nach-zweiten-lesung-des-europaeischen-parlaments,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf (zuletzt abgerufen am 23.11.2006).

[1682] S. Erwägungsgrund Nr. 18 des aktuellen Richtlinientextes (vorläufige Fassung) nach der zweiten Lesung des Europäischen Parlaments vom 15.11.2006, abrufbar im Internet unter http://www.bmwi.de/BMWi/Redaktion/PDF/P-R/richtlinientext-nach-zweiten-lesung-des-europaeischen-parlaments,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf (zuletzt abgerufen am 23.11.2006), der zudem Finanzdienstleistungen aus dem Anwendungsbereich der RL ausschließt.

[1683] S. Erwägungsgrund Nr. 9, 12 sowie Art. 19 des aktuellen Richtlinientextes (vorläufige Fassung) nach der zweiten Lesung des Europäischen Parlaments vom 15.11.2006, abrufbar im Internet unter http://www.bmwi.de/BMWi/Redaktion/PDF/P-R/richtlinientext-nach-zweiten-lesung-des-europaeischen-parlaments,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf (zuletzt abgerufen am 23.11.2006).

1019 Dienstleistung wird definiert als jede selbständige Leistung, die in der Regel gegen Entgelt erbracht wird; allerdings gilt sie gegenüber den anderen Grundfreiheiten nur subsidiär (Art. 50 Abs. 1 EG). Bei den von einem öffentlich-rechtlichen Sicherheitsgesetz erfassten Dienstleistungen (z.B. Online-Banking Rn. 573 ff.) ist der sachliche Anwendungsbereich der Art. 49 ff. EG daher eröffnet.

(2) Persönlicher Schutzbereich

1020 Der Dienstleistungsfreiheit unterfällt sowohl der Leistungserbinger der Dienstleistung (aktive Dienstleistungsfreiheit) als auch der Leistungsempfänger (passive Dienstleistungsfreiheit).[1684] Beim Online-Banking etwa können sich daher sowohl die Bank als auch die Nutzer auf die Dienstleistungsfreiheit berufen.

(3) Grenzüberschreitendes Element

1021 Sofern die Dienstleistungen von einem EU-Ausländer im deutschen Inland erbracht werden (aktive Dienstleistungsfreiheit), ist das nötige erforderliche grenzüberschreitende Element gegeben. Auch wenn ein EU-Ausländer als Nutzer auf die in Deutschland bereit gestellte Dienstleistung zugreift (passive Dienstleistungsfreiheit), liegt ein grenzüberschreitender Sachverhalt vor, der dem Anwendungsbereich des IT-Sicherheitsgesetzes unterfällt.

(4) Keine Schutzbereichsausnahme

1022 Zudem darf keine Schutzbereichsausnahme vorliegen. Die Dienstleistungsfreiheit erstreckt sich gem. Art. 55 i.V.m. Art. 45 Abs. 1 EG nicht auf Tätigkeiten, die in einem Mitgliedstaat dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt verbunden sind.[1685] Dieses ist bei einem Sicherheitsgesetz, das IT-Sicherheitsanforderungen an Dienstleistungen normiert, ersichtlich nicht der Fall.

d) Beeinträchtigung

(1) Diskriminierung

1023 Da das IT-Sicherheitsgesetz nicht ausdrücklich nach der Staatsangehörigkeit hinsichtlich der Anbieter von Dienstleistungen differenziert und auch nicht typischerweise ausländische Anbieter eher benachteiligt als inländische, ohne jedoch ausdrücklich an die

[1684] EuGH, verb. Rs. 286/82 und 26/83, *Luisi und Carbone,* Slg. 1984, 377; *Müller-Graff,* in: Streinz, Art. 49 Rn. 45 ff.

[1685] EuGH, Rs. 2/74, *Reyners,* Slg. 1974, 631, 655 Rn. 51, 53; *Grüb,* Europäische Niederlassungs- und Dienstleistungsfreiheit für Private mit hoheitlichen Befugnissen, 1999, S. 169 ff.; *Frenz,* europäische Grundfreiheiten, S. 741 ff. Rn. 1974 ff.; *Müller-Graff,* in: Streinz, Art. 45 Rn. 4 ff.

Staatsangehörigkeit anzuknüpfen, liegt weder eine offene noch eine versteckte Diskriminierung vor.

(2) Beschränkung

1024 Spätestens seit der Entscheidung *Säger/Dennemeyer*[1686] legt der EuGH aber auch die Dienstleistungsfreiheit als allgemeines Beschränkungsverbot aus. Umfasst sind daher alle Maßnahmen, die geeignet sind, den zwischenstaatlichen Verkehr unmittelbar oder mittelbar, aktuell oder potentiell zu behindern.[1687] Wenn für EU-Ausländer im Inland bei Ausübung der Dienste spezielle IT-Sicherheitsanforderungen gestellt werden (z.B. beim Online-Banking), die im deutschen Inland erbracht werden müssen, während sie bei einer Tätigkeit im Ausland entbehrlich wären, können dieser Regelungen die Ausübung der Dienstleistungsfreiheit im Inland zumindest weniger attraktiv machen, indem sie potentielle ausländische Anbieter von einem Marktzugang abhalten (Fall der aktiven Dienstleistungsfreiheit). Dieses gilt auch im umgekehrten Fall der passiven Dienstleistungsfreiheit: Auch wenn ein EU-Ausländer als Nutzer auf die in Deutschland bereit gestellten elektronischen Dienstleistungen zugreifen möchte, hierbei aber diverse IT-Sicherheitsmaßnahmen zu beachten hat, ist zumindest nicht auszuschließen, dass er im Zweifel auf einen anderen ausländischen Anbieter, der einen geringeren Aufwand veranschlagt, zugreifen wird. Auch hierdurch kann somit die Dienstleistungsfreiheit zumindest weniger attraktiv gemacht werden.

(3) Einschränkung des Beschränkungsverbot durch Keck analog?

1025 Umstritten ist, ob der EuGH seine Keck-Rechtsprechung i.R.d. Art. 28 EG auf die Dienstleistungsfreiheit übertragen hat. Dann würden „Dienstleistungsmodalitäten", die lediglich das Wer, Was, Wann, Wo und Wie der Ausübung der Dienstleistungsfreiheit erfassen und beide Keck-Kriterien erfüllen würden, nicht dem Beschränkungsverbot des Art. 49 EG unterfallen. Hierfür müssten sie unter analoger Anwendung der Keck-Formel gleichermaßen für alle Wirtschaftsteilnehmer gelten (1. Keck-Kriterium) und die aus- und inländischen Wirtschaftsteilnehmer rechtlich wie tatsächlich gleich berühren (2. Keck-Kriterium). Der EuGH erwähnte die Keck-Formel bei Art. 49 EG ausdrücklich in seinen Entscheidungen *Alpine Investments*[1688] und *Canal Satélite Digi-*

[1686] EuGH, Rs. C-76/90, *Säger/Dennemeyer,* Slg. 1991, I-4221, 4243 Rn. 12.
[1687] EuGH, Rs. 33/74, *Van Binsbergen,* Slg. 1974, 1299 Rn. 10/12; *Müller-Graff,* in: Streinz, Art. 49 Rn. 85.
[1688] EuGH, Rs. C-384/93, *Alpine Investments,* Slg. 1995, I-1141.

tal[1689], unterließ dieses jedoch in der Rechtssache *Laserdrome*[1690], obwohl sich angesichts der ausführlich erörterten Ablehnung der Übertragung von *Keck* durch die Schlussanträge der *GA Stix-Hackl*[1691] hierzu ausreichend die Möglichkeit geboten hätte. Zum Teil wird in der Literatur hieraus gefolgert, dass der EuGH die Keck-Formel in diesen Urteilen auf Art. 49 ff. EG übertragen habe,[1692] andere lehnen hingegen eine Übertragung ab.[1693] Die genannten Entscheidungen des EuGH sind hier im Ergebnis jedenfalls nicht eindeutig.

1026 Der Streit kann an dieser Stelle jedoch dahinstehen, sofern es sich vorliegend bereits nicht um eine „Modalität der Dienstleistung" i.S.d. Keck-Rechtsprechung handelt. Der EuGH stellte im Urteil *Canal Satélite Digital* im Einklang mit den Schlussanträgen der *GA Stix-Hackl*[1694] ausdrücklich fest, dass die Notwendigkeit, die fraglichen Erzeugnisse gegebenenfalls an die im Vermarktungsmitgliedstaat geltenden Vorschriften anzupassen, es bereits ausschließe, dass es sich um Verkaufsmodalitäten i.S.v. Keck handeln könne. [1695] Dieses deckt sich auch mit den Ausführungen des EuGH in der Rechtssache *Alpine Investment,* wo der EuGH unmittelbar auf den Zugang zum Dienstleistungsmarkt in den anderen Mitgliedstaaten abstellte und daher eine Beschränkung annahm.[1696]

Die Pflicht, den IT-Sicherheitsanforderungen des inländischen Gesetzes zu entsprechen, sind für den ausländischen Dienstleistungsanbieter gegebenenfalls mit Anpassungskosten für die Ausübung im deutschen Markt verbunden und würde daher zu einer nicht erwünschten Marktaufsplitterung führen, denn im Zweifelsfall wird der ausländische Anbieter bei erhöhtem Kostenaufwand von seinem Angebot auf dem deutschen Markt absehen. Damit können die IT-Sicherheitsanforderungen nicht den „Dienstleistungs-

[1689] EuGH, Rs. C-384/99, *Canal Satélite Digital,* Slg. 2002, I-607.

[1690] EuGH, Rs. C-36/02, *Laserdrome,* Slg. 2004, I-9609.

[1691] Schlussanträge der *GA Stix-Hackl*, Rs. C-36/02, *Laserdrome,* Slg. 2004, I-9609, 9620 Rn. 36.

[1692] *Frenz,* Europäische Grundfreiheiten, S. 961 f. Rn. 2559 f.; *Randelzhofer/Forsthoff,* in: Grabitz/Hilf, Art. 49/50 Rn. 72; *Epiney,* in: Calliess/Ruffert, Art. 28 Rn. 57; *Kluth,* in: Calliess/Ruffert, Art. 50 EG Rn. 42; *Feiden,* Bedeutung der „Keck"-Rechtsprechung, 2003, S. 147.

[1693] *Holoubek,* in: Schwarze, Art. 49 Rn. 92; *Tiedje/Troberg,* in: von der Groeben/Schwarze, Art. 49 Rn. 105 ff.; *Pache,* in: Ehlers, Grundfreiheiten, S. 335 Rn. 54; *Füller,* Grundlagen und inhaltliche Reichweite der Warenverkehrsfreiheiten, 2000, S. 142 ff.; *Schimming,* Konvergenz der Grundfreiheiten des EGV, 2002, S. 138 ff., 147; *Steinberg,* EuGRZ 2002, 13, 19; *Hansen,* EBLR 2000, 83, 85; *Hatzopoulos,* CMLR 2000, 43, 68; *ders.,* CMLR 1995, 1427, 1438 f.; *ders.,* CMLR 1996, 569, 582; *Ross,* CMLR 1995, 507, 512.

[1694] *GA Stix-Hackl,* Rs. C-384/99, *Canal Satélite Digital,* Slg. 2002, I-607, 624 Rn. 46: nationale Rechtsvorschriften, welche die Rechtmäßigkeit des Inverkehrbringens von Geräten von der Einhaltung bestimmter Registrierungsvorschriften abhängig macht, können keine Vertriebsmodalitäten im Sinne der genannten Rechtsprechung sein.

[1695] EuGH, Rs. C-384/99, *Canal Satélite Digital,* Slg. 2002, I-607, 619 Rn. 30.

[1696] EuGH, Rs. C-384/93, *Alpine Investments,* Slg. 1995, I-1141, 1178 Rn. 38.

modalitäten“ unterfallen und unterliegen, selbst bei analoger Anwendung von Keck, dem Rechtfertigungszwang der Art. 49 ff. EG.

e) Rechtfertigung

(1) Geschriebene Rechtfertigungsgründe, Art. 55 i.V.m. Art. 46 Abs. 1 EG

Durch den Verweis des Art. 55 auf Art. 46 Abs. 1 EG können Beeinträchtigungen der Dienstleistungsfreiheit aus Gründen der öffentlichen Ordnung, Sicherheit oder Gesundheit gerechtfertigt werden. Alle drei Begriffe tauchen auch im Rechtfertigungskatalog des Art. 30 EG auf. Die Auslegung dieses sog. ordre-public-Vorbehalts verläuft insofern deckungsgleich mit den dort genannten Begriffen und liegt hier, wie bereits gezeigt, nicht vor.[1697]

(2) Ungeschriebene Rechtfertigungsgründe

1027 Da es sich vorliegend um eine Beschränkung und nicht um eine Diskriminierung der Dienstleistungsfreiheit handelt, kann aber auch wieder auf die ungeschriebenen Rechtfertigungsgründe zurückgegriffen werden. Der EuGH hat in der Rechtssache *van Binsbergen*[1698] die in *Cassis-de-Dijon* anerkannten „zwingenden Gründe des Allgemeinwohls“ auch als ungeschriebene Rechtfertigungsgründe für die Dienstleistungsfreiheit anerkannt.

1028 Allgemeine Belange des Volkswohls sind als rein wirtschaftlicher Grund auch im Bereich der Dienstleistungsfreiheit nicht anerkannt[1699] - im Gegensatz zum Verbraucherschutz, der auch bei Art. 49 EG einen anerkannten zwingenden Grund des Allgemeinwohls darstellt.[1700]

(3) Verhältnismäßigkeitsgrundsatz

1029 Die nationalen Regelungen müssen aber wiederum dem Grundsatz der Verhältnismäßigkeit genügen. Ein vollständiges Verbot, die entsprechende Dienstleistung anzubieten, wird rein aus Gründen des Vermögensschutzes auch bei Art. 49 EG kaum zu rechtferti-

---

[1697] S.o. Rn. 1004.

[1698] EuGH, Rs. 33/74, *Van Binsbergen,* Slg. 1974, 1299, 1309 ff. Rn. 10/12 ff.

[1699] *Randelzhofer/Forsthoff,* in: Grabitz/Hilf, vor Art. 39 – 55 Rn. 162 ff. mwN.

[1700] EuGH, verb. Rs. C-34/95, C-53/95 und C-36/95, *De Agostini,* Slg. 1997, I-3843 Rn. 53; *Holoubek,* in: Schwarze, Art. 49 Rn. 101 mwN.

gen sein. Denn ein solches wirkt sich unmittelbar auf den Marktzugang der Dienstleistung aus und stellt damit ein erhebliches Handelshindernis dar.[1701]

1030 Wiederum verneint der EuGH die Erforderlichkeit einer Maßnahme, wenn ihr Ziel bereits durch gleichwertige Anforderungen des Herkunftsstaats erreicht wird.[1702] Ein unnötiges Wiederholen gleichwertiger ausländischer Kontrollen ist unzulässig.[1703] Eine nationale Regelung, die gleichwertige Kontrollen hinsichtlich der IT-Sicherheitsanforderungen im Herkunftsland nicht anerkennt, wäre daher auch im Rahmen der Art. 49 ff. EG nicht zu rechtfertigen. In Betracht kommt daher wiederum nur eine nationale Regelung, die Ausnahmeregelungen für Dienstleister aus dem Ausland enthält, um bereits abgedeckte Sicherungen im Hinblick auf Qualität und Leistungsfähigkeit hinreichend zu berücksichtigen.[1704]

1031 Für sonstige Regelungen gilt folgendes: Der EuGH hat als besonders schützenswert bereits die Verbraucherinteressen im Bankensektor eingestuft. Als besonders wichtig sah er es in der Entscheidung *Paroli* an*,* dass Verbraucher gegen eine mögliche Schädigung durch Bankgeschäfte geschützt werden, die von Kreditinstituten durchgeführt werden, welche den Anforderungen an ihre Zahlungsfähigkeit nicht genügen oder deren Geschäftsführer nicht die erforderliche Eignung bzw. erforderliche Zuverlässigkeit besitzen.[1705] Insofern sind die Verbraucher aufgrund des etwa beim Online-Banking betroffenen besonders sensiblen Bereichs besonders schutzwürdig. Wiederum gilt, dass, je höher der drohende einzutretende Schaden ist, desto mehr Anforderungen an die IT-Sicherheit des Anbieters gestellt werden dürfen. Bei Bagatellschäden ist angesichts des Leitbilds des EuGH vom mündigen Verbraucher hingegen davon auszugehen, dass der Bürger sich selbst Informationen hinsichtlich der „Gefährlichkeit“ der Inanspruchnahme einer Dienstleistung beschaffen kann. Je nach den Umständen kann es daher anstelle der Festlegung von kostenintensiven Sicherheitsmaßnahmen auch ausreichen, dass der Verbraucher sich durch geeignete Informationen in die Lage versetzt fühlt, eigenverantwortlich zu entscheiden, ob er eine preisgünstigere, vom Inhalt her sich unterscheidende

[1701] EuGH, Rs. C-384/93, *Alpine Investments,* Slg. 1995, I-1141, 1178 Rn. 38.

[1702] EuGH, Rs. *Säger/Dennemeyer,* Rs. C-76/90, Slg. 1991, I-4221, 4245 Rn. 18 ff.; *Frenz,* europäische Grundfreiheiten, S. 1011 Rn. 2689.

[1703] *Frenz,* Europäische Grundfreiheiten, S. 1011 Rn. 2689.

[1704] So insbesondere zur Anerkennung von Diplomen: EuGH, Rs. C-340/89, *Vlassopoulou,* Slg. 1991, I-2357; *Frenz,* europäische Grundfreiheiten, S. 1009 Rn. 2684.

[1705] EuGH, Rs. C-222/05, *Parodi,* Slg. 1997, I-3499, 3922 ff. Rn. 20 ff.; *Frenz,* europäische Grundfreiheiten, S. 1001 Rn. 2663; *Holoubek,* in: Schwarze, Art. 49 Rn. 101.

Dienstleistung aus dem Ausland in Anspruch nehmen will.[1706] Auch die Höhe der Kosten für derartige IT-Sicherheitsmaßnahmen müsste hierbei aber wohl berücksichtigt werden.

1032 Zu denken wäre im Bereich etwa des Online-Bankings auch, aufgrund der unterschiedlichen Schutzbedürftigkeit zwischen professionellen und privaten Anlegern zu unterscheiden, so dass auf das konkrete Schutzbedürfnis des Dienstleistungsempfängers abzustellen wäre.[1707] Je schutzbedürftiger der Anleger aufgrund mangelnder (Berufs-)Erfahrung ist, desto höhere IT-Sicherheitsanforderungen dürften gestellt werden.

3. IT-Sicherheitsanforderungen an Anlagen

1033 Auch in den vom Gesetz vorgeschriebenen organisatorischen Anforderungen an die Anlage selbst (z.B. durch eine zwingend erforderliche Bestellung eines IT-Sicherheitsbeauftragten) könnte ein Verstoß gegen die Grundfreiheiten vorliegen. Hier ist die E-Commerce-Richtlinie von vornherein nicht anwendbar, da es sich nicht um grenzüberschreitend erbrachte Dienstleistungen der Informationsgesellschaft handelt, sondern um an den Ort von EDV-Anlagen anknüpfende Regelungen.

a) Erfordernis eines grenzüberschreitenden Sachverhalts

1034 Erforderlich ist zur Anwendbarkeit der Grundfreiheiten aber wiederum zunächst ein grenzüberschreitender Sachverhalt. Der EuGH legt dieses Erfordernis aber sehr weit aus: So hat er in dem Urteil *Kraus*[1708] auch in den sog. Rückkehrfällen einen grenzüberschreitenden Sachverhalt angenommen, obwohl ein Inländer eine Beeinträchtigung geltend machte. Der grenzüberschreitende Bezug wurde hier bereits über den Erwerb eines akademischen Grades im EU-Ausland hergestellt.[1709] Diesen Titel wollte der Betroffene anschließend im Inland führen, was ihm jedoch ohne Gehmigungserfordernis von seinem Heimatstaat untersagt wurde. Auch dieses genügte dem EuGH bereits zur Bejahung des Grenzübertritts. Ein solcher Rückkehrfall ist indes bei anlagenbezogenen Regulierungen schwer denkbar, da es nur um die Regulierung von Tätigkeiten auf diesen ortsfesten Anlagen geht. Wenn sich jedoch ein Wirtschaftsteilnehmer lediglich gegen

[1706] *Tiedje/Troberg,* in: von der Groeben/Schwarze, Art. 49 Rn. 100.

[1707] So *Tiedje/Troberg,* in: von der Groeben/Schwarze, Art. 49 Rn. 101, allerdings nicht speziell bezogen auf das Online-Banking.

[1708] EuGH, Rs. C-19/92, *Kraus*, Slg. 1993, I-1663, 1694 Rn. 17; kritisch zu einer derart weiten Auslegung *Randelzhofer/Forsthoff,* in: Grabitz/Hilf, Art. 43 Rn. 62, hierzu auch *Frenz,* europäische Grundfreiheiten, S. 491 Rn. 1283.

[1709] EuGH, Rs. C-19/92, *Kraus*, Slg. 1993, I-1663, 1694 Rn. 17; kritisch zu einer derart weiten Auslegung *Randelzhofer/Forsthoff,* in: Grabitz/Hilf, Art. 43 Rn. 62, hierzu auch *Frenz,* europäische Grundfreiheiten, S. 491 Rn. 1283.

Behinderungen durch seinen eigenen Staat wendet, liegt bloß ein rein interner Sachverhalt vor und der Anwendungsbereich der Grundfreiheiten ist nicht eröffnet.[1710]

b) Kein Grenzübertritt bei Anforderungen an die Anlage selbst

1035 Das öffentlich-rechtliche Sicherheitsgesetz würde bloße organisatorische Sicherheitsanforderungen an den Betrieb der Anlage selbst als den „physischen Standort" stellen.[1711] Sofern etwa in Deutschland durch ein nationales Gesetz spezielle IT-Sicherheitsanforderungen für die in Deutschland stehenden Anlagen gefordert werden würde, läge ein rein interner Sachverhalt ohne Grenzübertritt vor. Dieses gilt gleichermaßen für die durch nationales Gesetz erforderliche Bestellung eines IT-Sicherheitsbeauftragten für eine in Deutschland stehende Anlage. Insofern fehlt hinsichtlich IT-spezifischer Regelungen für die Anlage der notwendige europäische Grenzübertritt. Ein Verstoß gegen die Grundfreiheiten läge daher in IT-Sicherheitsanforderungen hinsichtlich der Anlage nicht vor.

VII. International-privatrechtliche und International-öffentlichrechtliche Konsequenzen

1036 Für den Anwendungsbereich eines deutschen IT-Sicherheitsgesetzes kommt es beim Internet als einem weltweit zugänglichen Medium schließlich auch auf kollisionsrechtliche Fragen an. Hierbei sind beispielsweise Fälle denkbar, in denen Internet-Provider (z.B. Internethandel, Online-Broker, Online-Banken) vom Ausland aus den deutschen Markt bedienen, wobei zwischen Fällen innerhalb der EU und Drittstaatenfällen zu unterscheiden ist. Zu beleuchten ist hier vor allem die Frage, wie sich ein deutsches IT-SicherheitsG auf die Anforderungen an die (Basis-) IT-Sicherheit solcher ausländischer Angebote auswirken könnte, sowohl hinsichtlich der zivilrechtlichen Ansprüche als auch der öffentlich-rechtlichen Anordnungsbefugnisse.

1. Internationales Deliktsrecht

a) Kollisionsrechtliche Grundlagen

1037 Der sachliche Anwendungsbereich des internationalen Deliktsrechts umfaßt nicht nur das Recht der unerlaubten Handlung im Sinne der §§ 823 ff. BGB, sondern das gesamte

[1710] EuGH, Rs. 35/82 und 36/82, *Morson,* Slg. 1982, 3723, 3736 Rn. 15 f.; *Frenz,* europäische Grundfreiheiten, S. 145 Rn. 372 und S. 105 Rn. 259; *Ehlers,* in: ders., Grundfreiheiten, S. 203 Rn. 55; *Borchardt,* Die rechtlichen Grundlagen der EU, S. 302 f. Rn. 686; *Steinberg,* EuGRZ 2002, 13, 18; *Tesauro,* in: ZEW 1996, S. 1, 25 f.; *Classen,* EuR 2004, 416.

[1711] Technische Sicherheitsanforderungen beträfen die Anlage als „Produkt", so dass wiederum die Vorgaben nach Art. 28 EG einschlägig sind.

Recht der außervertraglichen Schadenshaftung.[1712] Das deutsche internationale Deliktsrecht ist in den Art. 40 ff. EGBGB geregelt. Auf europäischer Ebene wird derzeit zwar eine Vereinheitlichung des Kollisionsrechts der Mitgliedsstaaten der EU angestrebt,[1713] die entsprechende Verordnung ist bislang jedoch noch nicht in Kraft getreten.[1714]

1038 Fehlt eine (nur nachträglich mögliche) Rechtswahl (Art. 42 EGBGB), bestimmt sich das Deliktsstatut primär nach dem gemeinsamen gewöhnlichen Aufenthaltsort von Schädiger und Geschädigtem (Art. 40 Abs. 2 EGBGB). Andernfalls ist die ***lex loci delicti commissi*** (Tatortregel) als grundlegende Anknüpfung im internationalen Deliktsrecht einschlägig (Art. 40 Abs. 1 EGBGB).[1715] Anknüpfungspunkt ist danach sowohl der Ort, an dem die schädigende Handlung vorgenommen wurde (Handlungsort), als auch der Ort an dem der Schaden eingetreten ist (Erfolgsort). Nach der durch die IPR-Reform von 1999 eingeführten – vom ursprünglichen Ubiqutätsprinzip abweichenden[1716] – Regelung ist grundsätzlich das Recht des **Handlungsortes** anwendbar, wenn nicht der Geschädigte von seinem Bestimmungsrecht nach Art. 40 Abs. 1 Satz 2 und 3 EGBGB Gebrauch macht und das Recht des **Erfolgsorts** wählt (Nach der geplanten EU-Verordnung soll Grundanknüpfung dagegen das Recht des Erfolgsorts sein, vgl. Art. 4 Abs. 1 Rom-II-Verordnung). Im Einzelfall kommt eine Anknüpfung an engere Beziehung des Sachverhalts zu einer anderen Rechtsordnung über die Ausweichklausel des Art. 41 EGBGB in Betracht. Von besonderer Bedeutung ist hierbei die vertragsakzessorische Anknüpfung nach Art. 41 Abs.2 Nr.1 EGBGB, welche ein Auseinanderfallen von Vertrags- und Deliktsstatut verhindern soll.[1717]

(1) Kollisionsrechtliche Anknüpfung von Internet-Delikten

[1712] Bamberger/Roth-*Spickhoff*, Art. 40 EGBGB Rn. 7; MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 8.

[1713] Ausführlich dazu *Wagner*, IPRax 2006, 372; *Sonnentag*, ZVglRWiss 3 (2006), 256.

[1714] Gemeinsamer Standpunkt (EG) Nr. 22/2006 vom Rat festgelegt am 25. September 2006 im Hinblick auf die Annahme der Verordnung (EG) Nr. …/2006 des Europäischen Parlaments und des Rates vom … über das auf außervertragliche Schuldverhältnisse anzuwendende Recht („ROM II“) (2006/C 289 E/04). Zum Entwurf der Rom-II-Verordnung: *Wagner*, IPRax 2006, 372; *Sonnentag*, ZVglRWiss 105 (2006), 256; *Staudinger*, SVR 2005, 441; *Huber/Bach*, IPRax 2005, 73; *Hamburg Group for Private International Law*, RabelsZ 67 (2003), 1 ff.; MünchKommBGB-*Junker*, Anhang zu Art. 42.

[1715] Ausführlich MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 22.

[1716] Zum Ubiquitätsprinzip s. MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 16, 29.

[1717] *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (93).

1039 Bei Schadensfällen im Zusammenhang mit der Nutzung des Internet kommt ebenfalls im Grundsatz die Tatortregel zur Anwendung.[1718] Spezielle Anknüpfungsregelungen für Internet-Delikte enthält das deutsche autonome IPR ebenso wenig wie die geplante Rom-II-Verordnung. Hierbei sind Schädigungen unter Nutzung des **Internet als bloßem Trägermedium** (z.B. Persönlichkeitsverletzungen, Wettbewerbsverstöße, Verletzung von Immaterialgüterrechten) einerseits und **internet-spezifische Delikte** andererseits zu unterscheiden. Zur letzteren Kategorie zählen etwa die Versendung von Viren und Trojanern, Online-Versand fehlerhafter Software, Denial-of-Servive-Attacken, Hacking, Ausspähen von Daten usw.[1719] Meist handelt es sich um ein sog. **Distanzdelikt**, da Handlungs- und Erfolgsort oftmals in verschiedenen Staaten liegen werden.[1720] Die Feststellung von Handlungs- und Erfolgsort muss hierbei den Besonderheiten des Internet Rechnung tragen:[1721]

(a) Tatortregel: Handlungs- und Erfolgsort

1040 Unter dem **Handlungsort** ist der Ort zu verstehen, an dem der Schädiger die unerlaubte Handlung ganz oder teilweise ausgeführt hat. Abzustellen ist auf eine tatbestandsmäßige Ausführungshandlung mit Außenwirkung.[1722] Bezogen auf schädigende Daten kommt danach allein der **Ort des „Uploading"**, also der Einspeisung der Daten in das Internet als tauglicher Anknüpfungsmoment in Betracht.[1723] Keine maßgebliche Bedeutung hat in diesem Zusammenhang hingegen die Niederlassung des Serverproviders des Einspeisenden (zur Anknüpfung der Haftung von IT-Dienstleistern unten Rn. 1045). Auch der **Serverstandort** ist kein taugliches Anknüpfungskriterium, da der Einspeisende den Serverstandort nicht kennen muss und dieser im Übrigen zu leicht manipulierbar ist.[1724] Als Handlungsort kommt auch nicht in Betracht, der bloße **Durchleitungsort**, da dieser von Zufälligkeiten abhängt und somit kein hinreichend sicheres Anknüpfungsmoment

[1718] KG, NJW 1997, 3321; LG Düsseldorf, NJW-RR 1998, 979.

[1719] Dazu *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (90).

[1720] *Spindler*, ZUM 1996, 533 (555); *Spindler*, in: Hoeren/Sieber, Handbuch Multimediarecht, Teil 29 Rn. 436; *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (95); MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 29.

[1721] *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (97); MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 173.

[1722] Staudinger-*v.Hoffmann*, Art. 40 EGBGB Rn. 18.

[1723] *Mankowski*, RabelsZ 63 (1999), 203 (257 ff.); Bamberger/Roth-*Spickhoff*, Art. 40 EGBGB Rn. 48; Palandt-*Heldrich*, Art. 40 EGBGB Rn. 12; MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 174; Staudinger-*v.Hoffmann*, Art. 40 EGBGB Rn. 18, 58; *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (97).

[1724] *Mankowski*, RabelsZ 63 (1999), 257 f.; Bamberger/Roth-*Spickhoff*, Art. 40 EGBGB Rn. 48; MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 174; Palandt-*Heldrich*, Art. 40 EGGB Rn.12; Staudinger-*v.Hoffmann*, Art. 40 EGBGB Rn. 18; aA LG Düsseldorf, NJW-RR 1998, 979.

darstellt.[1725] Ebenso scheidet der Ort an dem die schadensstiftende Daten (z.B. der Virus oder Trojaner, die fehlerhafte Website) programmiert wurden als Handlungsort aus.[1726] Denn bei der Konzeption als solcher handelt es sich um eine bloße Vorbereitungshandlung.[1727] Diese theoretisch klare Anknüpfung stößt auf praktische Schwierigkeiten, da der Ort der Einspeisung sich oftmals nicht mit hinreichender Sicherheit wird feststellen lassen können. Im Schrifttum wird zur Vermeidung dieser Beweisschwierigkeiten eine Vermutung dafür erwogen, dass das Uploading am Ort des gewöhnlichen Aufenthalts bzw. am Sitz des in Anspruch genommenen Unternehmens erfolgt ist.[1728] Bei einer **Weiterverbreitung von Viren und Trojanern**[1729] – wenn sich die schädigenden Daten also schon in Umlauf im Netz befinden – ist Handlungsort der Ort, an dem die zur Weiterverbreitung erforderliche Handlung (bspw. die Versendung eines virenbehafteten E-Mail-Anhangs) vorgenommen wird, was regelmäßig mit dem Sitz oder Wohnsitz des Schädigers zusammenfallen wird.

1041 Der **Erfolgsort** ist danach zu bestimmen, wo sich das verletzte Interesse befindet. Werden schädigende Informationen verbreitet, kommt im Grundsatz auf den Ort des Abrufs der Information durch den Geschädigten bzw. den Standort des Zielrechners an.[1730] Die Zerstörung oder Veränderung von Daten (z.B. durch Viren), welche als Eigentumsverletzung anzusehen ist (Teil 1 Rn. 108 ff.), tritt am Standort des betroffenen Rechners ein.[1731] Gleiche wird man beim Hacking oder bei gezielten Rechnerblockaden durch „E-Mail-Bomben“ annehmen müssen.[1732] Sind (primäre) Vermögensschäden entstanden, ist

[1725] *Bachmann*, IPRax 1998, 179 (183); *Mankowski*, RabelsZ 63 (1999), 203 (267 f., 281 f.); MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 174; Spickhoff, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (98).

[1726] Bamberger/Roth-*Spickhoff*, Art. 40 EGBGB Rn. 48; Palandt-*Heldrich*, Art. 40 EGBGB Rn. 12; Staudinger-*v.Hoffmann*, Art. 40 EGBGB Rn. 18; anders aber *Mankowski*, RabelsZ 63 (1999), 203 (206 f.); *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (97): Anknüpfung an den Konzeptionsort jedenfalls dann, wenn der Einspeisungsort nicht ermittelbar ist.

[1727] *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (98); Bamberger/Roth-*Spickhoff*, Art. 40 EGBGB Rn. 48; Palandt-*Heldrich*, Art. 40 EGBGB Rn. 12; Staudinger-*v.Hoffmann*, Art. 40 EGBGB Rn. 18.

[1728] *v.Hinden*, Persönlichkeitsrechtsverletzungen im Internet – Das anwendbare Recht, 1999, S. 77, 221; *Lurger*, FS MPI, S. 479 (494); *Mankowski*, RabelsZ 63 (1999), 203 (265 f.); *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (98);

[1729] Dazu *Mankowski*, RabelsZ 63 (1999), 203 (282).

[1730] LG Düsseldorf, NJW-RR 1998, 979; LG München I, RIW 2000, 466; Bamberger/Roth-*Spickhoff*, Art. 40 EGBGB Rn. 48; Palandt-*Heldrich*, Art. 40 EGBGB Rn. 12; MünchKommBGB-Junker, Art. 40 EGBGB Rn. 163.

[1731] MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 175; *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (99).

[1732] *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (99).

auf den Lageort des verletzten Interesses abzustellen.[1733] Im Internet besteht für den Schädiger damit unter Umständen ein weltweites Haftungsrisiko.[1734] Zum Teil wird hierbei jedoch auf die von Persönlichkeitsrechtsverletzungen bekannte sog. „Mosaikbeurteilung“ abgestellt.[1735] Ist der Verletzungserfolg gleichzeitig in mehreren Staaten eingetreten (z.B. infolge Weiterverbreitung von Viren), kann der Geschädigte nur den am jeweiligen Erfolgsort entstandenen Schaden nach dem dort geltenden Haftungsrecht ersetzt verlangen.[1736]

(b) IT-Produkthaftung

1042 Die kollisionsrechtliche Anknüpfung der Produkthaftung ist im deutschen IPR nicht ausdrücklich geregelt, so dass die allgemeinen Rechte der Art. 40 ff. EGBGB anwendbar sind. Das Haager Übereinkommen über da auf die Produkthaftung anzuwendende Recht vom 2.10.1973 ist von Deutschland nicht ratifiziert worden.[1737] Art. 5 Abs. 1 lit. a der Rom-II-Verordnung erklärt für die Produkthaftung im Grundsatz das Recht des Staates für maßgebend, in dem der Geschädigte zum Zeitpunkt des Schadenseintritts seinen gewöhnlichen Aufenthalt hatte.

1043 Im **autonomen deutschen IPR** ist die kollisionsrechtliche Behandlung von Produkthaftungsfällen umstritten.[1738] Gemäß Art. 40 Abs. 1 Satz 1 EGBGB ist grundsätzlich das Recht des Handlungsorts anwendbar.[1739] Als Handlungsort werden hierbei der Sitz des Herstellers, der Ort der Herstellung, der Ort des Inverkehrbringens, sowie der Ort des Erwerbs des Produkts durch den Geschädigten diskutiert.[1740] Der Erfolgsort (dazu oben Rn. 1041) ist nur bei einer entsprechenden Bestimmung durch den Geschädigten anzuwenden (Art. 40 Abs. 1 Satz 2 EGBGB). Die bislang spärliche Rechtsprechung zum internationalen Produkthaftungsrecht sah als Handlungsort den Sitz des Herstellers und als Erfolgsort den Ort der Rechtsgutsverletzung an.[1741] Soweit zwischen Hersteller und

---

[1733] *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (100); MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 175.

[1734] *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (101); Palandt-*Heldrich*, Art. 40 EGBGB Rn. 12.

[1735] Allgemein *Kropholler* IPR, § 52 V 4, S. 531

[1736] *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (102); Bamberger/Roth-*Spickhoff*, Art. 40 EGBGB Rn. 48; *Mankowski*, RabelsZ 63 (1999), 203 (274).

[1737] Abgedruckt bei Staudinger-*v.Hoffmann*, Art. 40 EGBGB Rn. 80.

[1738] Ausführlich MünchKommBGB-*Junker*, Art.40 EGBGB Rn. 152 ff.

[1739] Palandt-*Heldrich*, Art. 40 EGBGB Rn. 10.

[1740] Bamberger/Roth-*Spickhoff*, Art. 40 EGBGB Rn. 40; *Spindler*, in: Hoeren/Sieber, Handbuch Multimediarecht, Teil 29 Rn. 478; Palandt-*Heldrich*, Art. 40 EGBGB Rn. 10; MünchKommBGB-Junker, Art. 40 EGBGB Rn. 154 ff.

[1741] BGH NJW 1981, 1606; OLG München RIW 1996, 955; MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 151, 153.

Geschädigtem vertragliche Beziehungen bestehen, kann eine vertragsakzessorische Anknüpfung nach Art. 41 Abs. 2 Nr. 1 EGBGB erfolgen.[1742] Nach überwiegender Ansicht kann aus der **Warenverkehrsfreiheit** (Art. 28 EG) keine zwingende Anknüpfung an das Recht des Herkunftslandes abgeleitet werden, was an dieser Stelle jedoch nicht weiter vertieft werden kann (s. auch Rn. 1065).[1743]

1044 Ohne auf die Diskussion über die Anknüpfung internationaler Produkthaftungsfälle hier in der gebotenen Tiefe eingehen zu können, gilt es für die **Produkthaftung im Internet** festzuhalten, dass kein Anlass besteht von der Tatortregel des Art. 40 Abs. 1 EGBGB abzuweichen.[1744] Als Handlungsort kommt damit der Herstellersitz, als Erfolgsort sämtliche Orte, an denen Rechtsgutsverletzungen eingetreten sind, in Betracht. Im Gegensatz zum Vertrieb verkörperter Produkte muss der Service-Provider und der Software-Hersteller bei Vertrieb von Software über das Internet stets mit einem potentiell weltweiten Kundenkreis rechnen; dem Unternehmen wird es zudem meist auf die weltweite Vertriebsmöglichkeit ankommen.[1745] Eine Steuerung des Haftungsrisikos, welches durch die anwendbare Rechtsordnung entsteht, ist damit nur in beschränktem Maße möglich.[1746]

(c) IT-Dienstleistungen

1045 Auch für IT-Dienstleistungen gelten im Grundsatz Art. 40 ff.EGBGB, so dass das Recht des Handlungs- oder Erfolgsorts maßgeblich ist. Bei einem vom Ausland aus agierenden **Internet-Provider**, welcher beispielsweise eine wegen Verwendung aktiver Inhalte unsichere Website unterhält, wird man für die Bestimmung des Handlungsorts im Sinne des Art. 40 Abs. 1 EGBGB in Anlehnung an die Auslegung der ECRL auf die **Niederlassung** des Diensteanbieters abstellen können. Nach Erwägungsgrund 19 der ECRL kommt es für die Bestimmung des Ortes der Niederlassung auf die „tatsächliche Ausübung einer wirtschaftlichen Tätigkeit mittels einer festen Einrichtung auf unbestimmte Zeit“ an. Dabei ist ausschließlich auf den Schwerpunkt seiner wirtschaftlichen Aktivitäten abzustellen, d.h. auf die Steuerung der Tätigkeiten des Diensteanbieters, nicht auf

---

[1742] Bamberger/Roth-*Spickhoff*, Art. 40 EGBGB Rn. 40; *Spindler*, in Hoeren/Sieber, Handbuch Mulitmediarecht, Teil 29 Rn. 479.

[1743] S. dazu *v.Hoffmann*, IPR, § 1 Rn. 107-109; Staudinger-*v.Hoffmann*, Vorbem zu Art. 38 EGBGB Rn. 8; Art. 40 EGBGB Rn. 88, 104 mwN; *Kropholler*, IPR § 53 V 3, S. 529; ausführlich *Graziano*, Europäisches Internationales Deliktsrecht, S. 72 f.; *Roth*, GS Lüderitz, S. 635 ff. mwN.

[1744] So schon *Spindler*, ZUM 1996, 533 (561); *Spindler*, in: Hoeren/Sieber, Handbuch Multimediarecht, Teil 29 Rn. 478.

[1745] *Spindler*, ZUM 1996, 533 (561); *Spindler*, in: Hoeren/Sieber, Handbuch Multimedia, Teil 29 Rn. 478; ebenso *Kronke*, RIW 1996, 985 (988) zu Art. 29 Abs. 1 Nr. 1 EGBGB.

[1746] Staudinger-v.Hoffmann, Art. 40 EGBGB Rn. 4,

die eingesetzten technischen Ressourcen. Unbeachtlich ist folglich der Standort des Servers,[1747] da beispielsweise auch im Inland niedergelassene Service-Provider ihre Dienste ausschließlich über ausländische Rechner erbringen können.[1748] Für in einem Mitgliedsstaat der EU ansässigen Provider ergeben sich hierbei Besonderheiten aufgrund des **Herkunftslandsprinzips der ECRL** (dazu unten (d)).

(d) Insbesondere: E-Commerce und Herkunftslandprinzip

(i) Anwendungsbereich und Reichweite des Herkunftslandprinzips

1046 Das Herkunftslandprinzip besagt, dass die Mitgliedsstaaten den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedsstaat nicht aus Gründen einschränken dürfen, die in den koordinierten Bereich fallen. Sein räumlicher und sachlicher Anwendungsbereich ist beschränkt auf Online-Dienste, welche vom Hoheitsgebiet eines Mitgliedsstaates der EU aus geschäftsmäßig[1749] angeboten oder erbracht werden (Art. 3 Abs. 1, 2 ECRL; § 3 Abs. 1, 2 TMG). Zu den Online-Diensten im Sinne der ECRL bzw. des TMG gehören beispielsweise auch Angebote des Telebanking (s. den früheren Beispielskatalog des § 2 Nr. 1 TDG a.F.).[1750]

(a) Koordinierter Bereich

1047 Das Herkunftslandprinzip erfasst den gesamten „**koordinierten Bereich**“ der E-Commere-Richtlinie (s. Art. 3 Abs. 1, 2 ECRL).[1751] Der Ausdruck „koordinierter Bereich“ wird in Art. 2 lit. h ECRL sehr weit definiert als die für die Anbieter von Diensten der Informationsgesellschaft und die Dienste der Informationsgesellschaft *in den Rechtssystemen der Mitgliedstaaten* festgelegten Anforderungen, ungeachtet der Frage, ob sie allgemeiner Art oder speziell für sie bestimmt sind. Der koordinierte Bereich ist nach Erwägungsgrund 21 der ECRL beschränkt auf Anforderungen betreffend **Online-Tätigkeiten** (beispielsweise Online-Informationsdienste, Online-Werbung, Online-Verkauf, Online-Vertragsschluss); Anforderungen an verkörperte Waren wie Computer-

[1747] So aber *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (97).
[1748] *Spindler*, ZUM 1996, 533 (555).
[1749] Dazu *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (110); Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 12.
[1750] Ausführlich Spindler/Schmitz/Geis-*Spindler*, § 2 TDG Rn. 42 ff.
[1751] Dazu *Tettenborn*, K & R 2000, 59 (61); MünchKommBGB-*Martiny*, Art. 34 EGBGB Anh. III Rn. 10.

Hardware, (z.B. (Produkt-)Sicherheitsnormen, Kennzeichnung, Haftung) betrifft er nicht (Art. 2 Lit. h (ii) ECRL und Erwägungsgründe 18 und 21).[1752]

1048 Das Herkunftslandprinzip besitzt danach nicht nur für Anforderungen an **IT-Dienstleistungen**, sondern auch für „virtuelle" **IT-Produkte** Relevanz. So können beispielsweise auch elektronisch erteilte Instruktionen und online übertragene Produkte (z.B. Download von Software, Musik, Videos, Büchern oder sonstiger Informationen) zumindest im B2B-Bereich (zu Verbrauchern s. Rn. 1052[1753]) erfasst werden.[1754]

1049 Gemäß Art. 2 lit. h (i) 1. SpStr. ECRL betrifft der koordinierte Bereich einerseits die **Aufnahme der Tätigkeit** eines Dienstes der Informationsgesellschaft (beispielsweise Anforderungen betreffend Qualifikation, Genehmigung oder Anmeldung). Art. 2 lit. h (i) 1. SpStr. ECRL bezieht darüber hinaus ausdrücklich auch die vom Diensteanbieter zu erfüllenden Anforderungen in Bezug auf die **Ausübung der Tätigkeit** eines Dienstes der Informationsgesellschaft, beispielsweise Anforderungen betreffend das Verhaltens des Diensteanbieters, Anforderungen betreffend Qualität oder Inhalt des Dienstes, sowie Anforderungen betreffend die Verantwortlichkeit des Diensteanbieters in den koordinierten Bereich mit ein.

(b) Durchbrechungen und Ausnahmen

1050 Die ECRL selbst lässt **Abweichungen vom Herkunftslandprinzip** zu. Jedoch kann sich der Empfangsstaat nur auf die in der Richtlinie selbst geregelten Ausnahmen berufen. Die vom EuGH[1755] entwickelten Grundsätze zur Rechtfertigung von Beschränkungen der Grundfreiheiten durch zwingende Erfordernisse finden daneben keine Anwendung.[1756]

1051 Das Herkunftslandprinzip gilt danach nicht in den in Art. 1 Abs. 5 ECRL, sowie im Anhang zur ECRL genannten Bereichen (Art. 3 Abs. 3 ECRL). Diese Vorgaben wurden in § 3 Abs. 4 TMG mit nur redaktionellen Anpassungen im deutschen Recht umge-

[1752] Dazu *Tettenborn*, K&R 2000, 59 (61); Spindler/Schmitz/Geis-*Spindler*,§ 4 TDG Rn. 10.

[1753] *Lurger/Vallant*, RIW 2002, 188 (190); *Spindler*, RabelsZ 66 (2002), 633 (692).

[1754] *Spindler*, RabelsZ 66 (2002), 633 (692); *Spindler*, MMR-Beilage 7/2000, 4 (19); *Mankowski*, ZVglRWiss 100 (2001), 137 (174); Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 11; *Thode*, NZBau 2001, 345 (350); *Tettenborn*, K & R 2000, 59 (61); *Lurger/Vallant*, RIW 2002, 188 (190); *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (116).

[1755] EuGH, Rs. 120/78, *Cassis de Dijon,* Slg. 1979, 649, 662 Rn. 8. Ausführlich oben Rn. 1006 ff..

[1756] *Spindler*, RabelsZ 66 (2002), 633 (653); Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 4.

setzt.[1757] Dieser Katalog enthält einerseits **rechtsgebietsbezogene Ausnahmen** für das Immaterialgüterrecht[1758], Kartellrecht, Versicherungsrecht, Datenschutzrecht, die Freiheit der Rechtswahl, sowie die vertraglichen Schuldverhältnisse in Bezug auf Verbraucherverträge und andererseits **Bereichsausnahmen** für Verteildienste, unerbetene elektronische Kommunikation, Glücksspiele und Lotterien, eletronisches Geld, Notare und andere hoheitlich tätige Berufe, sowie die Vertretung vor Gericht.

1052 Neben dem Katalog genereller Ausnahmen enthält Art. 3 Abs. 4-6 ECRL eine Art **Schutzklauselverfahren für Einzelfälle in bestimmten Bereichen**.[1759] Nach Art. 3 Abs. 4 ECRL können die Mitgliedsstaaten insbesondere Maßnahmen ergreifen, die zum Schutz der öffentlichen Ordnung, Sicherheit und Gesundheit, sowie des Schutzes der Verbraucher und von Anlegern erforderlich sind (Art. 3 Abs. 4 lit. a (i) ECRL). Der Begriff der öffentlichen Ordnung wird durch die nicht abschließenden Beispiele Strafprävention und –verfolgung, Jugendschutz, Hetze aus Gründen der Rasse, des Geschlechts, des Glaubens oder der Nationalität sowie Verletzung der Menschenwürde illustriert. In jedem Fall muss es sich um Umstände handeln, welche in ihrem Unwertgehalt den aufgezählten Beispielen entsprechen. Hierbei kann auf die sehr enge Auslegung des EuGH zu Art. 46 EG zurückgegriffen werden, so dass insbesondere nicht jeder Gesetzesverstoß genügt, sondern ein Grundinteresse des Staates berührt sein muss.[1760] Der Begriff der öffentlichen Sicherheit betrifft auch nationale Sicherheits- und Verteidigungsinteressen.

1053 Voraussetzung für Maßnahmen ist, dass sie einen bestimmten Dienst der Informationsgesellschaft betreffen, der die genannten Schutzziele beeinträchtigt oder eine ernsthafte und schwerwiegende Gefahr einer Beeinträchtigung dieser Ziele darstellt und die Maßnahmen in einem angemessenen Verhältnis zur diese Schutzzielen stehen (Art. 3 Abs. 4 lit. a (ii) (iii) ECRL; § 3 Abs. 5 TMG). Für das Verfahren zur Einleitung derartiger Maßnahmen sieht die ECRL in Art. 3 Abs. 4 und 5 Konsultations- und Informations-

---

[1757] Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 37 ff.; MünchKommBGB-*Martiny*, A. 34 EGBGB Anh. III Rn. 40 ff.

[1758] Siehe BGH, GRUR 2007, 67 zur Anwendbarkeit der §§ 126 ff. MarkenG nach § 4 Abs. 4 Nr. 6 TDG..

[1759] Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 54 ff.

[1760] Mitteilung der Kommission an den Rat, das Europäische Parlament und die Europäische Zentralbank betreffend die Anwendung von Artikel 3 Absätze 4 bis 6 der Richtlinie über den elektronischen Geschäftsverkehr auf Finanzdienstleistungen, KOM (2003) 259 endgültig vom 14.5.2003 (Punkt 2.1.3.); Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 58. Für den EuGH setzt "die Berufung einer nationalen Behörde auf den Begriff der öffentlichen Ordnung [...], wenn er gewisse Beschränkungen der Freizügigkeit von dem Gemeinschaftsrecht unterliegenden Personen rechtfertigen soll, jedenfalls voraus, dass außer der Störung der öffentlichen Ordnung, die jede Gesetzesverletzung darstellt, eine tatsächliche und hinreichend schwere Gefährdung vorliegt, die ein Grundinteresse der Gesellschaft berührt", Rs. 30/77, *Bouchereau*, Slg. 1977, 1999.

pflichten gegenüber der EU-Kommission und dem Mitgliedsstaat der Niederlassung vor (s. auch § 3 Abs. 5 Satz 2 TMG). Die Ausnahmen vom Herkunftslandprinzip stehen unter dem Vorbehalt der Prüfung der Kommission auf ihre Verhältnismäßigkeit.[1761]

(ii) Herkunftslandprinzip und Kollisionsrecht

1054 Im Bereich der ECRL bzw. des deutschen TMG ist das Verhältnis von **Herkunftslandprinzip und Kollisionsrecht** nicht abschließend geklärt.[1762] Zum Teil wird eine kollisionsrechtliche Qualifikation des Herkunftslandprinzips verneint.[1763] Denn Art 1 Abs. 4 der Richtlinie bzw. § 1 Abs. 5 TMG legen ausdrücklich fest, dass keine neuen Regelungen im Bereich des IPR geschaffen werden sollen und Erwägungsgrund 23 der Richtlinie hebt hervor, dass Vorschriften des durch das IPR zur Anwendung berufenen Rechts nicht die Freiheit zur Erbringung von Diensten im Sinne der Richtlinie beschränken dürfen.[1764] Dem Herkunftslandprinzip kommt danach nur auf der Ebene des nach den allgemeinen Regeln des IPR berufenen Sachrechts eine Korrektivwirkung dergestalt zu, dass die anzuwendenden Normen anhand des Art. 3 Abs.2 der ECRL auf einen Beschränkung der Dienstleistungsfreiheit hin zu untersuchen sind. Andere wiederum qualifizieren das Herkunftlandprinzip kollisionsrechtlich, so dass allein das Sachrecht des Herkunftsstaates zur Anwendung kommt, ohne dass es auf einen Günstigkeitsvergleich mit dem Sachrecht ankäme, welches durch das IPR des Forumsstaates berufen wäre.[1765] Hierfür werden inbesondere Art. 3 Abs. 3 ECRL bzw. § 3 Abs. 3 Nr. 1 TMG angeführt, welche ausdrücklich die freie Rechtswahl unberührt lassen, was sich nur unter Einbeziehung des Kollisionsrechts in das Herkunftslandprinzip erklären lasse.[1766]

1055 Eine rein kollisionsrechtliche Einordnung des Herkunftslandprinzips wird man angesichts des Wortlauts von Art. 3 Abs. 2 ECRL verneinen müssen, da hier nur ein Verbot der Einschränkung ausgesprochen wird.[1767] Das Sachrecht des Herkunftsstaates wird

---

[1761] Ausführlich Mitteilung der Kommission an den Rat, das Europäische Parlament und die Europäische Zentralbank betreffend die Anwendung von Artikel 3 Absätze 4 bis 6 der Richtlinie über den elektronischen Geschäftsverkehr auf Finanzdienstleistungen, KOM (2003) 259 endgültig vom 14.5.2003.

[1762] Ausführlich *Spindler*, RabelsZ 66 (2002), 633 ff.; Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 17 ff.; MünchKommBGB-*Martiny*, Art. 34 EGBGB Anh. III Rn. 23 ff.

[1763] *Ahrens*, CR 2000, 835 (837); *Fezer/Koos*, IPRax 2000, 349 (352); *Sonnenberger*, ZVglRWiss 99 (2000), 278 (305 f.); *Sack*, WRP 2001, 1408 (1408 f.); *Sack*, WRP 2002, 271 (273 ff.); *Halfmeier*, ZEuP 2001, 837 (864).

[1764] *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (118). Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 17; MünchKommBGB-*Martiny*, Art. 34 EGBGB Anh. III Rn. 26.

[1765] *Mankowski*, CR 2001, 630 ff.; *Thünken*, IPRax 2001, 15 (21).

[1766] *Mankowski*, ZVglWiss 100 (2001), 136 (143); *Mankowski*, CR 2001, 630 (632); Palandt-*Heldrich*, Art. 40 EGBGB Rn. 11.

[1767] *Spindler*, RabelsZ 66 (2002), 633 (652); Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 20; MünchKommBGB-*Martiny*, Art. 34 EGBGB Anh. III Rn. 36 f.

nur zum Maßstab, innerhalb dessen der Empfangsstaat den freien Dienstleistungsverkehr nicht beschränken darf. Dies wird beispielsweise daran deutlich, dass das Sachrecht des Empfangsstaates angewendet werden kann, wenn es einen gleichen oder milderen Standard gegenüber dem Herkunftsland aufweist.[1768] Ein „kollisionsrechtlicher Gehalt“ wohnt dem Herkunftslandprinzip demnach allenfalls insoweit inne, als es *als Maßstab* für das durch das IPR des Empfangsstaats bestimmte Sachrecht berufen wird.[1769] Ist das Herkunftslandrecht milder als das Recht des Empfangsstaates, hat entweder eine entsprechende Modifikation des Sachrechts des Empfangsstaates anhand des Maßstabs des Herkunftslandsrechts zu erfolgen. Oder aber das IPR des Empfangsstaates enthält für diesen Fall eine von den allgemeinen Regeln des IPR abweichende (ungeschriebene) kollisionsrechtliche Verweisung auf das (mildere) Recht des Herkunftslandes. Das Primärrecht und die ECRL geben keinen der beiden Wege vor: Die dogmatische Umsetzung des Herkunftslandprinzips obliegt allein den Mitgliedsstaaten (genauer: dem Gesetzgeber bzw. den Gerichten).

1056 Im Bereich des **internationalen Deliktsrechts** modifiziert das Herkunftslandprinzip die Wahlmöglichkeit zwischen Handlungs- und Erfolgsort, da allein das Deliktsrecht des Herkunftslandes Maßstab ist.[1770] Das Herkunftslandprinzip verweist gerade auf das Recht der Niederlassung, welches nicht das Handlungsortsrecht und erst Recht nicht das Recht des Erfolgsorts sein muss.[1771] Am Herkunftslandsrecht sind danach nicht nur die Verhaltenspflichten des Anbieters, sondern alle anspruchsbegründenden und –ausfüllenden Merkmale der Norm einschließlich der Rechtsfolgen zu messen.[1772] Erfasst werden sowohl verschuldensabhängige, als auch verschuldensunabhängige Anspruchsgrundlagen.[1773]

(2) Eingriffsnormen und Sicherheits- und Verhaltensregeln im internationalen Deliktsrecht

[1768] *Spindler*, RabelsZ 66 (2002), 633 (652); Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 20; *Höder*, Multistate-Verstöße, S. 197 ff.

[1769] *Spindler*, RabelsZ 66 (2002), 633 (653).

[1770] *Spindler*, RabelsZ 66 (2002), 633 (689); *Mankowski*, ZVglRWiss 100 (2001), 137 (173 f.); Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 73; MünchKommBGB-*Martiny*, Art. 34 Anh III Rn. 51.

[1771] *Spickhoff*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 89 (114 f.); .

[1772] Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 73; MünchKommBGB-*Martiny*, Nach Art. 34 EGBGB Rn. 18.

[1773] *Spindler*, RabelsZ 66 (2002), 633 (690).

1057 Öffentliche Sichheits- und Verhaltensstandards können im internationalen Privatrecht zum einen als Eingriffsnormen (dazu (a)) und als Umstand zur Bestimmung der erforderlichen Verhaltens- und Sicherheitsstandards (dazu (b)) Bedeutung erlangen:

(a) Eingriffsnormen

1058 Unter Eingriffsnormen sind Normen zu verstehen, welche einen Sachverhalt ungeachtet des nach den kollisionsrechtlichen Regeln anwendbaren Rechts zwingend regeln.[1774] Es handelt sich mithin um **international zwingende Normen**,[1775] welche der Wahrung politischer, sozialer oder wirtschaftlicher Belange in dem betreffenden Staat dienen.[1776] *Inländische* Eingriffsnormen sind – anders als ausländische Eingriffsnormen[1777] – stets im Wege der **Sonderanknüpfung** anzuwenden.[1778] Erforderlich ist, dass die Norm im überwiegenden öffentlichen Interesse liegt.[1779] Maßgeblich ist der Anwendungs- und Geltungswille der Norm, welcher auch durch Auslegung ermittelt werden kann, vorzugsweise aber in der Norm ausdrücklich zum Ausdruck kommt.[1780] Beispiele für Eingriffsnormen des deutschen Rechts sind etwa das Außenwirtschaftsrecht, das Devisenbewirtschaftungsrecht, das Kapitalmarktrecht und das Wohnraummietrecht.[1781]

1059 Jedem Staat steht es grundsätzlich frei, bestimmte Normen für international zwingend zu erklären.[1782] Im europäischen Binnenmarkt gelten jedoch auch für international zwingende Normen die Grenzen der Grundfreiheiten und des sekundären Europarechts.[1783] Grundsätzlich erfordert die Anwendung einer Eingriffsnorm eine gewissen **Inlandsbezug**, was sich aus der Nähe der Eingriffsnormen zum ordre public (s. Art. 6 EGBGB) erklärt.[1784] Die erforderliche Stärke des Inlandsbezugs ist hierbei abhängig vom Gewicht der geschützten öffentlichen Interessen.[1785]

[1774] *Kropholler*, IPR, § 3 II, S. 18 ff.; § 52 IX, S. 490; *v.Hoffmann*, IPR, § 10 Rn. 93 ff.

[1775] *Kropholler*, IPR, § 3 II 1, S. 19; Palandt-*Heldrich*, Art. 34 EGBGB Rn. 3.

[1776] *v.Hoffmann*, IPR, § 10 Rn. 94; *Kropholler*, IPR, § 52 IX 1, S. 491; *v.Bar/Mankowski*, IPR, § 4 Rn. 91; Palandt-*Heldrich*, Art. 34 EGBGB Rn. 3. Siehe auch Erwägungsgrund 29 des Gemeinsamer Standpunkt (EG) Nr. 22/2006 vom Rat festgelegt am 25. September 2006 im Hinblick auf die Annahme der ROM-II-Verordnung (2006/C 289 E/04).

[1777] Dazu ausführlich *Schramm*, Ausländische Eingriffsnormen im Deliktsrecht, 2005; *v.Bar/Mankowski*, IPR, § 4 Rn. 104 ff..

[1778] *Kropholler*, IPR, § 3 II 2, S. 19; *v.Hoffmann*, IPR, § 10 Rn. 94.

[1779] *Kropholler*, IPR, § 52 IX 1, S. 491.

[1780] *Kropholler*, IPR, § 3 II 2, S. 19; § 52 IX 1, S. 492; *v.Hoffmann*, IPR, § 10 Rn. 94.

[1781] Siehe Palandt-*Heldrich*, Art. 34 EGBGB Rn. 3.

[1782] *Kropholler*, IPR § 52 IX, S. 490.

[1783] EuGH, RIW 2000, 137; *Jayme/Kohler*, IPRax 2000, 455; ausführlich *Fetsch*. Eingriffsnormen und EG-Vertrag.

[1784] *Kropholler*, IPR, § 3 II 2, S. 19, § 52 IX 1, S. 491; Palandt-*Heldrich*, Art. 34 EGBGB Rn. 3.

[1785] Palandt-*Heldrich*, Art. 34 EGBGB Rn. 3.

1060 Im **deutschen IPR** findet sich eine Teilregelung zu Eingriffsnormen im Vertragsrecht in Art. 34 EGBGB, welche – anders als die zugrundeliegende Vorschrift des Art. 7 EVÜ – aber auf inländische Eingriffsnormen beschränkt ist. Die geplante **Rom-II-Verordnung** enthält in **Art. 16** eine gesonderte Regelung über Eingriffsnormen des Forumstaates. Die Verordnung berührt danach nicht die Anwendung der „nach dem Recht des Staates des angerufenen Gerichts geltenden Vorschriften, die ohne Rücksicht auf das für außervertragliche Schuldverhältnis maßgebende Recht den Sachverhalt zwingend regeln".

1061 Für das Deliktsrecht ist die Wirkungsweise von Eingriffsnormen im EGBGB nicht geregelt und wissenschaftlich bislang kaum untersucht.[1786] Eingriffsnormen können im Deliktsrecht unter folgenden Gesichtspunkten von Bedeutung sein: als international zwingende **Anspruchsgrundlage** für Schadensersatzansprüche oder als international zwingendes **Schutzgesetz** dessen Verletzung eine Schadensersatzpflicht nach § 823 Abs. 2 BGB oder entsprechenden ausländischen Vorschriften nach sich zieht.[1787] Als Beispiel für eine international zwingende Anspruchsgrundlage lässt sich aus dem deutschen Recht § 33 GWB i. V. m. § 130 Abs. 2 GWB anführen.[1788] Nach § 130 Abs. 2 GWB findet das GWB und damit auch § 3 GWB auf Wettbewerbsverstöße Anwendung, die sich im Inland auswirken (also Schädigung deutscher Marktteilnehmer); Art. 40 ff. EGBGB werden insoweit verdrängt.

(b) Sicherheits- und Verhaltensregeln

1062 Sicherheits- und Verhaltensregeln können im Rahmen des anzuwendenden Sachrechts als Verhaltensmaßstab herangezogen werden. Im IPR ist hierbei von besonderer Bedeutung, inwieweit örtliche Verkehrsregeln und Sicherheitsvorschriften anwendbar sind, welche nicht dem vom IPR berufenen Deliktsstatut entstammen. Im kollisionsrechtichen Schrifttum wird dieser Problemkreis vor allem im Zusammenhang mit dem internationalen Straßenverkehrsunfallrecht und dem internationalen Produkthaftungsrecht diskutiert.

1063 Unterliegt beispielsweise ein Verkehrsunfall in einem ausländischen Staat aufgrund gemeinsamen gewöhnlichen Aufenthalts von Schädiger und Geschädigtem nach Art. 40 Abs.2 EGBGB deutschem Recht, können dennoch zur Bestimmung der Verhaltensan-

[1786] *V.Hoffmann*, FS Henrich, 2000, S. 283 ff.; *Schramm*, Ausländische Eingriffsnormen im Deliktsrecht, 2005.
[1787] S. dazu *Schramm*, Ausländische Eingriffsnormen im Deliktsrecht, 2005, S. 11 ff.
[1788] Siehe dazu *v.Hoffmann*, FS Henrich, 2000, S. 283 (289 ff.).

forderungen die Sicherheits- und Verhaltensregeln des Handlungsorts herangezogen werden.[1789] Die betreffende Regelung wird in diesem Fall **nicht** unmittelbar aufgrund eines **kollisionsrechtlichen Anwendungsbefehls** (Sonderanknüpfung) angewandt, sondern es handelt sich vielmehr um eine Konkretisierung der vom Deliktsstatut aufgestellten Verhaltens- und Sorgfaltsanforderungen unter Berücksichtigung der am Tatort geltenden Regeln.[1790] Die Voraussetzungen und die Rechtsfolgen der Haftung bestimmen sich alleine nach dem vom deutschen IPR berufenen Deliktsstatut, jedoch können Verhaltensregeln einer anderen Rechtsordnung **Tatbestandswirkung** entfalten.[1791] Hierbei gilt der Grundsatz, dass Sicherheits- und Verhaltensvorschriften dem **Recht des Handlungsorts** zu entnehmen sind.[1792]

1064 Für die übrigen Bereiche des Haftungsrechts besteht im deutschen Recht keine hinreichende Klarheit über die Anwendung von Sicherheitsvorschriften, welche nicht dem Deliktsstatut entnommen werden. Im Bereich der **Produkthaftung** - wo es sich meist um Distanzdelikte handelt - bestimmen sich die anwendbaren Sicherheitsstandards (z.B. GPSG) nach überwiegender Ansicht nach dem Recht des (ausländischen) **Marktorts für den produziert wird.**[1793] Für Exportware, welche gerade für das Land bestimmt ist, in dem der Schaden eingetreten ist, werden die Pflichten der Hersteller somit der Rechtsordnung dieses Staates auch dann entnommen, wenn das Deliktsstatut einer anderen Rechtsordnung unterliegt. Dies erscheint auch interessengerecht, da andernfalls Hersteller an einem Produktionsort mit niedrigem Schutzniveau bevorzugt würden. Gerade in Internet-Fällen richtet der Hersteller zudem sein Angebot an einen potentiell weltweiten Kundenkreis, so dass sein Vertrauen auf die am Herstellungsort geltenden Sicherheitsregeln nicht gerechtfertigt erscheint.

[1789] *v.Hoffmann*, IPR, § 11 Rn. 58.

[1790] Staudinger-*v.Hoffmann*, Vorbem zu Art. 40 EGBGB Rn. 58.

[1791] *v.Hoffmann*, IPR, § 11 Rn. 58; MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 205; Staudinger-*v.Hoffmann*, Vorbem zu Art. 40 EGBGB Rn. 58.

[1792] BGH, NJW-RR 1996, 732; *Kropholler*, IPR, § 53 V, S. 522; Bamberger/Roth-Spickhoff, Art. 40 EGBGB Rn. 11; MünchKommBGB-*Junker*, Art. 40 EGBGB Rn. 205; Palandt-Heldrich, Art. 40 EGBGB Rn. 8 Staudinger-*v.Hoffmann*, Vorbem zu Art. 40 EGBGB Rn. 58. Vgl. auch MünchKommBGBm-*Junker*, Art. 40 EGBGB Anh. Rn. 80 zu Art. 14 Rom-II-Verordnung.

[1793] OLG Düsseldorf, NJW 1980, 533 (534); *Kreuzer*, IPRax 1982, 1 (3); *Siehr*, RIW 1972, 373 (385); Kullmann/Pfister-*Pfister*, Produzentenhaftung, Kz . 4010, S. 31 f.; *Wilde*, in: v.Westphalen, Produkthaftungshandbuch, § 100 Rn 16; MünchKommBGB-*Junker*, Art.40 EGBGB Rn. 158; Staudinger-*v.Hoffmann*, Vorbem Art. 40 EGBGB Rn. 60, Art. 40 EGBGB Rn. 90, 103. Gemäß Art. 9 des (von Deutschland nicht ratifizierten) Haager Abkommens über das auf die Produkthaftpflicht anwendbare Recht vom 2.10.1973 sollen die Sicherheitsvorschriften des Ortes anzuwenden sein, an dem das Produkt in den Markt eingeführt wurde, abgedruckt bei Staudinger-*v.Hoffmann*, Art. 40 EGBGB Rn. 80.

1065 Auf dem vom EuGH entwickelten (*primärrechtlichen*) „Herkunftslandprinzip“ beruhende **europarechtliche Bedenken** dagegen, die Sicherheitsvorschriften des Marktlandes auch auf in einem Mitgliedsstaat der EU ansässige Hersteller anzuwenden,[1794] werden im Schrifttum unter Berufung auf zwingende Erfordernisse überwiegend verworfen.[1795] Soweit Produkte online übermittelt werden, dürfte dagegen das *sekundärrechtliche* Herkunftslandprinzip des Art. 3 ECRL bzw. § 3 TMG im Verhältnis zu gewerblichen Abnehmern zu beachten sein (Rn. 1048),[1796] da die ECRL nur abschließend aufgezählte Durchbrechungen und Ausnahmen kennt und damit über das unmittelbar aus den Grundfreiheiten abgeleitete Herkunftslandprinzip hinausgeht (s. Rn. 1050 ff.).

1066 Die geplante Regelung des Art. 17 der Rom-II-VO[1797], bestimmt, dass unabhängig vom anzuwendenden Recht bei der Beurteilung des Verhaltens der Person, deren Haftung geltend gemacht wird, faktisch und soweit angemessen die Sicherheits- und Verhaltensregeln zu berücksichtigen sind, die an dem Ort und zu dem Zeitpunkt des haftungsbegründenden Ereignisses in Kraft sind. Ort des haftungsbegründenden Ereignisses im Sinne der Vorschrift ist der **Handlungsort**,[1798] da man davon ausgeht, dass der Schädiger sein Verhalten an den Vorschriften des Handlungsorts auszurichten hat.[1799] Diese Regelung dürfte nach dem Wortlaut „soweit angemessen“ indessen keine zwingende Anwendung allein der Sicherheits- und Verhaltensregeln am Handlungsort festlegen, so dass bei einem Handeln vom Ausland aus grundsätzlich auch deutsche Regelungen herangezogen werden können.

b) Kollisionsrechtliche Bedeutung eines deutschen IT-Sicherheitsgesetzes

1067 Ein IT-Sicherheitsgesetz kann im international-privatrechtlichen Kontext auf mehrere Arten Bedeutung erlangen, wobei unerheblich ist, dass dieses als öffentliches Sicherheitsrecht einzuordnen ist.[1800] Zunächst kann ein IT-Sicherheitsgesetz auch in international gelagerten Fällen als **Anspruchsgrundlage** für Schadensersatzansprüche oder als **Schutzgesetz** zur Anwendung kommen (unten (1)). Weiter können die **Verhaltensan-**

[1794] Dazu *v.Hoffmann*, IPR, § 1 Rn. 107-109; Staudinger-*v.Hoffmann*, Art. 40 EGBGB Rn. 88, 104 mwN.

[1795] Kullmann/Pfister-*Pfister*, Produzentenhaftung, Kz. 4010, S. 32; ebenso wohl Staudinger/*v.Hoffmann*, Art. 40 EGBGB Rn. 104.

[1796] *Spindler*, RabelsZ 66 (2002), 633 (692).

[1797] Siehe oben Fn. 1714.

[1798] Der Verordnungsentwurf bezeichnet als Erfolgsort den *Ort, an dem der Schaden eintritt*, s. Art. 4 Abs. 1 Rom-II-Verordnung.

[1799] MünchKommBGB-*Junker*, Art. 40 EGBGB Anh. Rn. 80.

[1800] Staudinger-*v.Hoffmann*, Vorbem zu Art. 40 EGBGB Rn. 56, 58.

forderungen des IT-Sicherheitsgesetzes zur Konkretisierung des Inhalts und Umfangs von Verkehrspflichten bzw. der Fahrlässigkeit herangezogen werden (unten (2)). Im internationalen Zusammenhang stellt sich hier die Frage, ob allein die Verhaltensnormen des Deliktsstatuts maßgeblich sind oder auch Sicherheitsanforderungen einer anderen Rechtsordnung anwendbar sind. Bei im EU-Ausland niedergelassenen Internet-Dienstleistern ist auf das Herkunftslandprinzip der ECRL Rücksicht zu nehmen (unten (3)).

(1) IT-Sicherheitsgesetz als Anspruchsgrundlage oder Schutzgesetz

1068 Sofern man das IT-Sicherheitsgesetz als **international zwingende Norm** (sog. Eingriffsnorm) ausgestaltet wird, ist das IT-Sicherheitsgesetz unabhängig vom nach den Kollisionsregeln des IPR berufenen Rechts im Wege einer Sonderanküpfung anwendbar. Das IT-Sicherheitsgesetz wäre danach beispielsweise auch dann anwendbar, wenn nach Art. 40 ff. EGBGB ein ausländisches Deliktsrecht zur Anwendung berufen ist.

1069 Sanktioniert das IT-Sicherheitsgesetz selbst einen Verstoß gegen die darin geregelten Verhaltens- und Sicherheitsstandards durch eine Haftungsfolge und enthält es somit eine selbständige **Anspruchsgrundlage**, kommt es für die Haftung der Adressaten des Gesetzes nicht darauf an, ob ein anwendbares ausländisches Recht an die Verletzung von Schutzgesetzen Schadensersatzansprüche (z.B. § 823 Abs. 2 BGB, § 1311 österreichisches ABGB[1801]) knüpft. Regelt das IT-Sicherheitsgesetz nicht zugleich die Haftungsfolgen, kommt eine Einordnung als international zwingendes **Schutzgesetz** in Betracht. Die Anwendung des IT-Sicherheitsgesetzes als Schutznorm bereitet dann keine Schwierigkeiten, wenn deutsches Recht anwendbar ist, da in diesem Fall § 823 Abs. 2 BGB anwendbar ist. Probleme entstehen aber dann, wenn ein ausländisches (Handlungsorts-)Recht anwendbar ist und diese Rechtsordnung keine dem § 823 Abs. 2 BGB vergleichbare Regelung enthält. Ein Ausweg wäre die Berücksichtigung des IT-Sicherheitsgesetzes im Rahmen der Bestimmung der Sorgfaltsanforderungen des ausländischen Deliktsstatuts als international zwingender Verhaltensstandard.

1070 Ist das IT-Sicherheitsgesetz nicht als Eingriffsnorm ausgestaltet, kommt eine **sachrechtliche Berücksichtigung** in Betracht. Dies stößt zumindest im Ausgangspunkt dann wiederum nicht auf Schwierigkeiten, wenn *deutsches Sachrecht* berufen und somit

[1801] Österreichisches Allgemeines Bürgerliches Gesetzbuch (ABGB) vom 1.6.1811 (JGS Nr. 946/1811), zuletzt geändert durch BGBl. I Nr. 113/2006.

§ 823 Abs. 2 BGB anwendbar ist. In diesem Fall ist dann aber zu prüfen, inwieweit die deutschen Verhaltensvorschriften überhaupt auf den ausländischen Provider usw. anwendbar sind. Selbst wenn das IT-Sicherheitsgesetz so auszulegen sein sollte, dass auch Unternehmen mit Sitz im Ausland darunter fallen, wird man im Einzelfall eine schuldhafte Verletzung des Schutzgesetzes verneinen müssen (s. § 823 Abs. 2 Satz 2 BGB). Ist dagegen *ausländisches Recht* Deliktsstatut, kommt es für eine Haftung wegen Schutzgesetzverletzung darauf an, ob der ausländische Haftungstatbestand auch Schutzgesetze aus anderen Rechtsordnungen (hier das deutsche IT-Sicherheitsgesetz) erfasst.

(2) IT-Sicherheitsgesetz als Konkretisierung von Verhaltensregeln

1071 Wird das IT-Sicherheitsgesetz nicht als international zwingende Eingriffsnorm ausgestaltet, kann es dennoch im Rahmen des anzuwendenden Sachrechts als Verhaltens- und Sicherheitsmaßstab herangezogen werden. Das IT-Sicherheitsgesetz wird in diesem Fall nicht unmittelbar aufgrund eines kollisionsrechtlichen Anwendungsbefehls angewandt, sondern es handelt sich vielmehr um eine Konkretisierung der vom Deliktsstatut aufgestellten Verhaltens- und Sorgfaltsanforderungen im Wege einer Tatbestandswirkung.[1802]

1072 Bislang wurde im kollisionsrechtlichen Schrifttum – soweit ersichtlich – die Frage der anwendbaren Verhaltens- und Sicherheitsstandards im IT-Bereich noch nicht diskutiert. Für die Anwendbarkeit des IT-Sicherheitsgesetzes auf vom Ausland aus handelnde Internet-Provider ist damit fraglich, ob die Standards am (ausländischen) Handlungsort oder am (inländischen) Erfolgsort maßgeblich sind. Die Situation ähnelt insoweit der Problematik im Bereich der internationalen Produkthaftung (oben Rn. 1064 f.), wo ebenfalls regelmäßig Distanzdelikte vorliegen. Denkbar wäre es in diesem Zusammenhang allein auf das Recht am Sitz des Providers abzustellen. Dies erscheint im Hinblick auf die Verkehrsinteressen im Internet aber nicht zielführend, da der Provider sein Angebot auf einen potentiell weltweiten Markt ausrichtet und sein Vertrauen auf die Verhaltens- und Sicherheitsstandards am Ort seiner Niederlassung somit nicht schutzwürdig ist. Vielmehr würden Anreize zur Verlagerung der Niederlassung an einen Standort mit niedrigem Sicherheitsniveau geschaffen. Damit müsste sich der Provider aber potentiell auf alle Rechsordnungen weltweit einstellen. Um eine sinnvolle Eingrenzung der anwendbaren Rechtsordnungen zu erreichen erscheint es daher angezeigt die Heranziehung des deutschen IT-Sicherheitsgesetzes davon abhängig zu machen, dass der ausländ-

[1802] Staudinger-*v.Hoffmann*, Vorbem zu Art. 40 EGBGB Rn. 58.

dische Provider **sein Angebot zumindest auch auf den deutschen Markt ausgerichtet** hat (z.B. durch deutschsprachige Websites, Werbung usw.). Diese Lösung liefe auch konform mit der wohl überwiegenden Ansicht im internationalen Produkthaftungsrecht (oben Rn. 1064). Besonderheiten ergeben sich wiederum für IT-Dienstleister innerhalb der EU (dazu sogleich (3)).

(3) Insbesondere: Anwendung des IT-Sicherheitsgesetzes auf EU-Ausländer

1073 Angesichts der Weite des durch die ECRL **koordinierten Bereichs** wird man auch eine Regelung hinsichtlich der sicherheitstechnischen Ausgestaltung der Internet-Dienstleistung bzw. von Online-Produkten als von der ECRL und damit dem Herkunftslandprinzip erfasst ansehen müssen (oben Rn. 1047 ff.). Ein **IT-Sicherheitsgesetz** würde Organisations- und Verhaltensanforderungen für Provider aufstellen, welche letztlich auch für die Bestimmung des Sorgfaltsmaßstabes und damit die Verantwortlichkeit und Haftung der Diensteanbieter entscheidend sind. Denkbar wäre auch den Gesichtspunkt der IT-Sicherheit als Frage der Qualität des Dienstes einzuordnen.

1074 Auch wenn ein IT-Sicherheitsgesetz somit in den Anwendungsbereich der ECRL fällt, wäre der deutsche Gesetzgeber nicht gehindert für Dienste, welche von deutschem Hoheitsgebiet aus erbracht werden, eine innerstaatliche Regelung zur IT-Sicherheit zu erlassen (s. Art. 3 Abs. 1 ECRL). In Bezug auf Dienste der Informationsgesellschaft, welche von einem anderen Mitgliedsstaat aus erbracht werden, gilt es indessen das Herkunftslandprinzip des Art. 3 Abs. 2 ECRL zu beachten. Danach unterliegen die Diensteanbieter grundsätzlich den Vorschriften – und folglich auch den IT-Sicherheitsanforderungen – des Mitgliedsstaates, in dem sie ihre Niederlassung haben.[1803] Ein deutsches IT-Sicherheitsgesetz käme damit grundsätzlich jedenfalls dann nicht zur Anwendung, wenn es strengere IT-Sicherheitsvorschriften enthält als der Mitgliedsstaat der Niederlassung des Diensteanbieters.

1075 Unterfallen die Regelungen eines IT-Sicherheitsgesetzes dem Herkunftslandprinzip, ist seine Anwendung auf Internet-Provider davon abhängig, in welchen Grenzen eine **Abweichung vom Herkunftslandprinzip** zulässig ist (dazu bereits Rn. 1050 ff.). Denkbar wäre es im Zusammenhang mit dem Erlass eines IT-Sicherheitsgesetzes auf europäischer Ebene Anstrengungen zu unternehmen, um dem Anhang zur ECRL eine weitere

[1803] Zum Begriff der Niederlassung ausführlich *Spindler*, RabelsZ 66 (2002) 633 (648 f.); Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 15 f.

rechtsgebietsbezogene Ausnahme für das IT-Sicherheitsrecht hinzuzufügen, wie dies beispielsweise seit jeher für das Datenschutzrecht der Fall ist. Dies könnte in der anstehenden Revision der ECRL angeregt werden. Gleiches müsste auch dann geschehen, wenn sich die EU zu einer gemeinschaftsweiten Regelung der IT-Sicherheit – etwa in einer „IT-Sicherheitsrichtlinie" – entschließen würde.

1076 Ein IT-Sicherheitsgesetz dürfte als abstrakt-generelle Querschnittsregelung nicht unter die Regelung des Art. 3 Abs. 4-6 ECRL bzw. § 3 Abs. 5 TMG fallen, da die Richtlinie ausdrücklich von Maßnahmen „im Hinblick auf einen bestimmten Dienst der Informationsgesellschaft" spricht.[1804] Ein IT-Sicherheitsgesetz würde demgegenüber Regelungen für alle Internet-Dienstleister treffen. Im Ergebnis würde so der abschließende Katalog des Anhangs zur ECRL unter Ausschaltung des Verfahrens zur Richtlinienänderung umgangen. Verwaltungsrechtliche Anordnungen gegenüber Intermediären aus dem EU-Ausland kommen auf Grundlage des IT-Sicherheitsgesetzes allenfalls in Betracht, sofern im Einzelfall die strengen Voraussetzungen des Art. 3 Abs. 4-6 ECRL bzw. § 3 Abs. 5 TMG erfüllt sind (dazu oben Rn. 1052).

1077 Eine Anwendung des IT-Sicherheitsgesetzes auf in einem anderen Mitgliedsstaat niedergelassene Diensteanbieter unter Berufung auf die **Rechtsprechung des EuGH** zur Rechtfertigung von Beschränkungen der Dienstleistungsfreiheit zur zwingende Erfordernisse kommt nicht in Betracht, da die Richtlinie die Ausnahmen vom Herkunftslandprinzip abschließend regelt.[1805] Andernfalls würde die differenzierte Einzelregelung des Art. 3 Abs. 3 und 4 ECRL, sowie das Schutzklauselverfahren des Art. 3 Abs. 4-6 ECRL unterlaufen.[1806] Der Regelung des Herkunftslandprinzips in Art. 3 Abs. 2 ECRL geht folglich wesentlich weiter als die in der Rechtsprechung des EuGH entwickelten Kriterien zur Waren- und Dienstleistungsfreiheit.

2. Internationales öffentliches Recht

1078 Ein IT-SicherheitsG muss ferner das Problem der **aufsichtsrechtlichen Zuständigkeit** hinsichtlich grenzüberschreitender Tätigkeiten zu adressieren. Gerade auf den Feldern des Bank- und Finanzdienstleistungssektors sowie im Versicherungswesen verschwim-

[1804] Vgl. die Mitteilung der Kommission an den Rat, das Europäische Parlament und die Europäische Zentralbank betreffend die Anwendung von Artikel 3 Absätze 4 bis 6 der Richtlinie über den elektronischen Geschäftsverkehr auf Finanzdienstleistungen, KOM (2003) 259 endgültig vom 14.5.2003 (Punkt 2. und 2.1.2.) und oben Fn. 1677.

[1805] *Spindler*, RabelsZ 66 (2002), 633 (653); Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 4.

[1806] Spindler/Schmitz/Geis-*Spindler*, § 4 TDG Rn. 4.

men nationale Grenzen immer mehr.[1807] Sowohl im Bereich der Welthandelsorganisation (WTO) als auch auf europäischer Ebene wird dieser Bereich unter den Begriffen des „grenzüberschreitenden Marktzugangs“ für das GATS[1808] (General Agreement on Trade in Services) sowie des „grenzüberschreitenden Dienstleistungsverkehrs“ lebhaft diskutiert.

1079 Fraglich ist in diesem Rahmen vor allem, inwieweit inländische, nationale Regelungen öffentlich-rechtlich auch zur Geltung kommen können, wenn ein **grenzüberschreitender Marktzugang** vorliegt, etwa wenn ein Anbieter aus dem Ausland heraus einem in Deutschland ansässigen Kunden Dienstleistungen erbringt, etwa Wertpapierdienstleistungen in Form des Onlinebroking.[1809] Im Rahmen der Globalisierung versuchen viele Unternehmen vor allem im Finanzbereich über ihren eigentlichen Heimatmarkt hinaus, sich neue Märkte zu erschließen.[1810] Daher ist es nicht verwunderlich, dass gerade in diesen Rechtsbereichen sich die meisten Anhaltspunkte für Fragen der extraterritorialen Anwendung sowie der Bestimmung von Anknüpfungspunkten (Belegenheit) finden, die auch für ein IT-SicherheitsG herangezogen werden können.

a) Internationaler Anwendungsbereich des öffentlichen Aufsichtsrechts

1080 Nach dem **Territorialitätsprinzip** ist das nationale öffentliche Recht nur auf Tatbestände anzuwenden, die in einer territorialen, d.h. **räumlichen Beziehung** zu dem Staat stehen, der es erlassen hat.[1811] Allerdings sagt das Territorialitätsprinzip selbst nichts darüber aus, wie dieser räumliche Zusammenhang für einen bestimmten Sachverhalt konkretisiert werden soll, ob also beispielsweise die körperliche Belegenheit im Inland erforderlich oder die bloße Auswirkung auf das Inland genügend ist. Für die Frage der Rechtsanwendung sind somit die hinter dem Begriff Territorialitätsprinzip stehenden Anknüpfungsprinzipien ausschlaggebend.[1812]

[1807] So schon *Ohler*, WM 2002, 162; *Steck/Campbell*, ZBB 2006, 354, 355; *Kollhosser* in: Prölss, VAG, 12. Aufl. 2005 § 105 VAG Rz. 2.

[1808] Hierzu monographisch *Volkel*, Der Marktzugang ausländischer Versicherer unter besonderer Berücksichtigung des Allgemeinen Dienstleistungsabkommens (GATS), 2003.

[1809] S. dazu *Steck/Campbell*, ZBB 2006, 354, 355.

[1810] *Bundesanstalt für Finanzdienstleistungsaufsicht*, Hinweise zur Erlaubnispflicht nach § 32 Abs. 1 KWG in Verbindung mit § 1 Abs. 1 und Abs. 1a KWG von grenzüberschreitend betriebenen Bankgeschäften und/oder grenzüberschreitend erbrachten Finanzdienstleistungen, April 2005, S. 2.

[1811] BGHZ 31, 371 = NJW 1960, 1101; BGHZ 64, 189 = NJW 1975, 1220; ausführlich v.Bar/Mankowski, IPR, § 4 Rn. 63 ff.; MünchKommBGB-*Sonnenberger*, Einl IPR Rz. 422.

[1812] *v.Bar/Mankowski*, IPR, § 4 Rn. 63, 66.

1081 Im deutschen Recht finden sich eine Reihe von **Anknüpfungsprinzipien** (dazu Rn. 1082 ff.), welche den als Eingriffsvoraussetzung erforderlichen **Inlandsbezug** konkretisieren. Völkergewohnheitsrechtlich werden *minimum contacts* zum behördlich eingreifenden Staat gefordert (*genuine link*).[1813] Die Fragestellung gleicht hier im Wesentlichen der zu Eingriffsnormen im internationalen Privatrecht erörterten Problematik des hinreichenden Inlandsbezugs (dazu Rn. 1059).

(1) Anknüpfungsprinzipien

1082 Als Voraussetzung für ein Tätigwerden von Behörden kommen verschiedene Anknüpfungsprinzipien in Betracht,[1814] so beispielsweise das Herkunftslandprinzip (in der E-CRL konkretisiert durch den Begriff der Niederlassung, s. Art. 3 ECRL und unten Rn. 1090), das Bestimmungslandprinzip, das Auswirkungsprinzip oder das Marktortprinzip. Öffentliche Aufsichtsbefugnisse im Zusammenhang mit Internet-Aktivitäten sind derzeit vor allem in den Bereiche Banken- und Versicherungsaufsicht, sowie im Kartellrecht relevant, deren Regelungen als Muster für ein IT-SicherheitsG herangezogen werden könnten.

(a) Bankenaufsicht (KWG)

1083 Das Kreditwesengesetz enthält in §§ 32, 53 ff. KWG Regelungen mit internationalem Bezug. Gemäß § 32 Abs. 1 Satz 1 KWG bedarf einer schriftlichen Erlaubnis, wer im Inland gewerbsmäßig oder in einem Umfang, der einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb erfordert, Bankgeschäfte beteiben oder Finanzdienstleistungen erbringen will. Nach der – nicht unumstrittenen[1815] – neuen Verwaltungspraxis det der BaFin ist eine Erlaubnis auch dann erforderlich, wenn der „Erbringer der Dienstleistung seinen Sitz oder gewöhnlichen Aufenthalt im Ausland hat und sich im Inland **zielgerichtet an den Markt wendet**, um gegenüber Unternehmen und/oder Personen, die ihren Sitz oder gewöhnlichen Aufenthalt im Inland haben, wiederholt und geschäftsmäßig Bankgeschäfte oder Finanzdienstleistungen anbietet“,[1816] da bereits dann ein „Be-

[1813] *Dahm/Wolfrum/Delbrück*, Völkerrecht, Bd. I/1, S. 320 ff.; *Ipsen*, Völkerrecht, § 23 Rn. 90 ff..

[1814] Ausführlich *Mankowski*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 51 (54 ff.).

[1815] Gegen eine Anwendbarkeit des KWG etwa Boos/Fischer/Mattler-*Marwede*, § 53 KWG Rn. 111; *Schork*, § 32 KWG Rn. 2.

[1816] *BaFin*, Hinweise zur Erlaubnispflicht nach § 32 Abs. 1 KWG in Verbindung mit § 1 Abs. 1 und Abs. 1a KWG von grenzüberschreitend betriebenen Bankgeschäften und/oder grenzüberschreitend erbrachten Finanzdienstleistungen, April 2005, S. 1; zuvor *BAKred,* Schreiben vom 12.04.2002, S. 1, abrufbar unter http://www.bafin.de/schreiben/92_2002/ba_120402.htm; dazu Boos/Fischer/Schulte-Mattler/*Marwede*, § 53 KWG Rn. 134; dazu auch *Voge*, WM 2007, 381 ff...

treiben“ im Sinne von § 32 Abs. 1 Satz 1 KWG vorliegt.[1817] Da aber grenzüberschreitende Geschäfte ohne Hauptsitz (§ 33 Abs. 1 Satz 1 Nr. 6 KWG) oder Zweigstelle (§ 53 Abs. 1 KWG) im Inland *nicht erlaubnisfähig* sind, führt dies dazu, dass Anbieter aus Nicht-EU-Staaten und Nicht-EWR-Staaten (s. § 53b KWG),[1818] die Bank- und Finanzdienstleistungsprodukte in Deutschland zielgerichtet vertreiben wollen, ein für die Erlaubnis notwendiges Tochterunternehmen oder eine Zweigstelle in Deutschland gründen müssen.[1819]

1084 Hinsichtlich der Erlaubnispflichtigkeit von Internetangeboten differenziert die Bafin nunmehr folglich danach, ob Leistungen aus dem Inland bloß abrufbar sind (dann keine Zuständigkeit der deutschen Bankenaufsicht) oder, ob ein **Angebot gezielt auf inländische Kunden ausgerichtet** ist (dann erlaubnispflichtiger grenzüberschreitender Geschäftsbetrieb).[1820] Die Ausrichtung einer Website auf den Inlandsmarkt ist auf Grundlage des Inhalts der Homepage bzw. der Online-Aktivitäten im Rahmen einer Gesamtbetrachtung zu ermitteln.[1821] Kriterien sind beispielsweise sprachliche Fassung des Angebots, Abstimmung des Angebots auf die Bedürfnisse des deutschen Marktes und die deutsche Rechtsordnung, Verwendung einer deutschen Internetadresse oder Zusammenarbeit mit inländischen Unternehmen bei der Geschäftsabwicklung, festgestellt werden.[1822] Dieses Anknüpfungskriterium wäre auch auf ein IT-SicherheitsG übertragbar (dazu unten Rn. 1088).

(b) Versicherungsaufsicht (VAG)

1085 Im Versicherungsaufsichtsrecht schreibt § 105 VAG vor, dass Versicherungsunternehmen eine Zulassung beantragen müssen, wenn sie Erstversicherungsgeschäfte in Deutschland betreiben wollen – und sei es auch nur durch eine Mittelsperson. Umstritten ist hierbei, ob bei Betrieb einer Internetseite, die von Deutschland aus abgerufen

---

[1817] *Voge*, WM 2007, 381 (382).

[1818] Zu Kreditinstituten mit Sitz in EU- oder EWR-Staaten siehe *Mankowski*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 51 (77 ff.)

[1819] Abrufbar unter http://www.bafin.de/schreiben/92_2002/ba_120402.htm. Boos/Fischer/Schulte-Mattler-*Fischer*, § 32 KWG Rn. 8; Boos/Fischer/Schulte-Mattler-*Marwede*, § 53 KWG Rn. 134, 138.

[1820] *Bafin*, Hinweise zur Erlaubnispflicht nach § 32 Abs. 1 KWG in Verbindung mit § 1 Abs. 1 und Abs. 1a KWG von grenzüberschreitend betriebenen Bankgeschäften und/oder grenzüberschreitend erbrachten Finanzdienstleistungen (Stand April 2005), abrufbar unter http://www.bafin.de/merkblaetter/050400.htm; ebenso *Spindler*, VersR 2002, 1049; Boos/Fischer/Schulte-Mattler/*Fischer*, § 32 KWG Rn. 8; s. auch *Mankowski*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 51 (76 f.).

[1821] *Bafin*, Hinweise zur Erlaubnispflicht nach § 32 Abs. 1 KWG in Verbindung mit § 1 Abs. 1 und Abs. 1a KWG von grenzüberschreitend betriebenen Bankgeschäften und/oder grenzüberschreitend erbrachten Finanzdienstleistungen (Stand April 2005), abrufbar unter http://www.bafin.de/merkblaetter/050400.htm.

[1822] Boos/Fischer/Schulte-Mattler/*Fischer*, § 32 KWG Rn. 9.

werden kann, bereits die Voraussetzung einer „Mittelsperson“ im Sinne des § 105 Abs. 2 VAG angesehen werden kann oder ob eine nicht erlaubnispflichtige Korrespondenzversicherung vorliegt.[1823]

1086 Die BaFin (als Nachfolgebehörde des Bundesaufsichtsamts für das Versicherungswesen) ordnet den Online-Vertrieb von Versicherungen gegenwärtig als Korrespondenzversicherung ein und sieht ihn folglich nicht als von § 105 VAG erfasst an.[1824] Diese Auslegung liegt nach dem Wortlaut des § 105 Abs. 2 VAG, welcher ausdrücklich auf eine Mittelsperson abstellt, nahe. Unter Schutzzweckgesichtspunkten stößt sie indes auf Bedenken, da für Versicherungsnehmer im Internet nicht ohne Weiteres erkennbar ist, dass es sich um ein ausländisches Versicherungsunternehmen handelt (insbesondere bei Verwendung einer de-Domain).[1825] Vergleichbar den Überlegungen zum KWG (oben Rn. 1084) erscheint daher auch im Versicherungsaufsichtsrecht ein auf den **Marktort** bezogener Ansatz zumindest de lege ferenda erwägenswert.[1826] Hierbei können die für Art. 29 EGBGB im Hinblick auf die grenzüberschreitenden Verträge im Internet entwickelten Kriterien herangezogen werden, insbesondere die bestimmungsgemäße Ausstrahlung der Werbung auf den Empfangsstaat bzw. den gewöhnlichen Aufenthaltsort des Versicherungsnehmern sowie dessen Abgabe der relevanten Erklärungen an seinem gewöhnlichen Aufenthaltsort. Damit wäre für die Anwendbarkeit des VAG maßgeblich, ob das **Angebot** im Hinblick auf die verwandte Sprache, die Bereitschaft zum Abschluss mit deutschen Versicherungsnehmern, die verwandten Konditionen und die verwandte Währung, die Ausrichtung auf das belegene Risiko etc. **in einer Gesamtschau auf Deutschland bezogen** ist.

(c) Kartellrecht (GWB)

1087 Als eine Ausprägung des Bestimmungslandprinzips erweist sich das **Auswirkungsprinzip** des Kartellrechts.[1827] Nach § 130 GWB findet deutsches Kartellrecht bei Wettbewerbsbeschränkungen Anwendung, die sich im Geltungsbereich des Gesetzes „aus-

[1823] S. *Götting*, CR 2001, 528; *Spindler*, VersR 2002, 1049; *Winter*, VersR 2001, 1461; *Mankowski*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien , S. 51 (80 f.).

[1824] VerBAV 1998, 140; ebenso *Götting*, CR 2001, 528 (531); *Winter*, VersR 2001, 1461; Fahr/Kaulbach-*Fahr*, § 105 VAG Rn. 35; anders Prölss/Schmidt-*Schmidt*, § 105 VAG Rn. 12.

[1825] *Götting*, CR 2001, 528 (531).

[1826] Ausführlich *Spindler*, VersR 2002, 1049 ff..

[1827] *Mankowski*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien , S. 51 (55).

wirken", auch wenn sie außerhalb des Geltungsbereich des GWB veranlasst werden.[1828] Für die Eingriffsbefugnis der Kartellbehörden erfolgt damit eine Anknüpfung anhand der Folgen der wettbewerbsbeschränkenden Maßnahmen, unabhängig davon, von wo und von wem sie ausgehen,[1829] wobei jedoch eine **Mindestintensität** der Auswirkungen im Inland erforderlich ist.[1830] Bei Sachverhalten mit Internetbezug – beispielsweise elektronischen Marktplätzen – gilt das kartellrechtliche Auswirkungsprinzip ohne Besonderheiten.[1831]

(2) Anwendbarkeit eines künftigen IT-Aufsichtsrechts auf ausländische Anbieter

(a) Anknüpfungspunkte für ein IT-Sicherheitsrecht

1088 Bezogen auf ein künftiges IT-Aufsichts- bzw. Sicherheitsrecht zeigen die bisher existierenden Normen, dass Unklarheiten in der Normstruktur durch inhaltlich zu enge Anknüpfungen (insbesondere im KWG und VAG) keine geeigneten Kollisionsnormen darstellen. Eine Anknüpfung allein an physischen Belegenheiten wird gerade IT-Dienstleistungen oder IT-Produkten nicht gerecht, die ohne Transaktionskosten grenzüberschreitend angeboten und vertrieben werden können. Vielmehr ist eine **Anknüpfung an der Tätigkeit im heimischen Markt** erforderlich, indem er einen umfassenden Marktschutz gewährleistet.

1089 Ein tätigkeitsbezogener Ansatz könnte ähnlich wie § 130 Abs. 2 GWB mittels des **Auswirkungsprinzips** auf die rechtsgeschäftlichen Bindungen der Vertragsparteien bei dem zugrunde liegenden Geschäftsabschluss abstellen. Für Angebote aus dem Internet nahe liegend ist für das öffentliche Aufsichts- bzw. Sicherheitsrecht eine Anknüpfung danach, ob ein **Angebot gezielt auf inländische Kunden ausgerichtet** ist, insbesondere durch in deutscher Sprache abgefasste Angebote, Lieferung nach Deutschland etc. (Rn. 1084, 1086; vgl. auch die zu Art. 29 EGBGB entwickelten Kriterien[1832]). Auch die entsprechenden Anknüpfungskriterien aus dem Internationalen Produkthaftungsrecht

[1828] EuGH, Rs . C-89/85, *Ahlström u.a.*, Slg. 1988, 5233, 5242; BGH WuW/E 1276, 1279 – „*Ölfeldrohre*"; BGH WuW/E 1613, 1614 – „*Organische Pigmente*"; BGH WuW/E 2596 – „*Eisenbahnschwellen*"; KG WuW/E OLG 3051, 3061 – „*Morris/Rothmans*"; OLG Frankfurt, WRP 1992, 331 (332); *Bechtold*, GWB, 4. Aufl. 2006, § 103 GWB Rz. 14.

[1829] BGHSt 25, 208 (209); OLG Frankfurt WuW/E DR-R 801 ff.; *Bechtold*, GWB, 4. Aufl. 2006, § 103 GWB Rz. 14.

[1830] Immenga/Mestmäcker-*Rehbinder*, § 130 Abs. 2 GWB Rn. 30; Langen/Bunde-*Stadler*, § 130 GWB Rn. 126, 128.

[1831] *Immenga/Lange*, RIW 2000, 733 (736); *Köhler*, K & R 2000, 569 (571); *Lambert/Michel*, K & R 2002, 505; *Lange*, Virtuelle Unternehmen, 2001, Rn. 597 f.; *Heinemann*, in: Spindler/Wiebe, Internet-Auktionen und Elektronische Marktplätze, Kap. 8 Rn. 9.

[1832] Bamberger/Roth-*Spickhoff*, Art. 29 EGBGB Rn. 12 ff.; MünchKommBGB-*Martiny*, Art. 29 EGBGB Rn. 33 ff., insbesondere Rn. 36 zu Websites und Internet-Werbung.

könnten auf die Anwendung produktsicherheitsrechtlicher Vorschriften übertragen werden, indem es nur darauf ankommt, ob ein Produkt in den heimischen Markt eingeführt wird. Demgemäß könnte ein IT-SicherheitsG auch hinsichtlich seiner öffentlich-rechtlichen Aufsichtskomponente auf Angebote aus dem Ausland erstreckt werden, sofern sie einen hinreichenden Inlandsbezug aufweisen.

(b) Besonderheiten bei Anbietern aus dem EU-Ausland

1090 Wiederum gelten auch im Bereich des öffentlichen Rechts **Besonderheiten für Anbieter aus dem EU-Ausland** für online-vertriebene Produkte und Dienstleistungen; da das europäische Recht dezidiert offline und online-Vertrieb ungleich behandelt – was insbesondere etwa in der Information-Society-Richtlinie[1833] zum Urheberrecht hinsichtlich des Erschöpfungsgrundsatzes zum Ausdruck kommt[1834], ebenso in Erwägungsgrund 18 der ECRL – muss wohl derzeit angenommen werden, dass die E-Commerce-Richtlinie auch hinsichtlich von Sicherheitsanforderungen für digitalisierte, online vertriebene Produkte gilt. Die Erwägungsgründe 18 und 24 der ECRL stellen ausdrücklich fest, dass die Aufsicht über Online-Dienste, welche der ECRL unterliegen, im Herkunftsland erfolgen soll. Dies hat zur Konsequenz, dass – wie oben schon für das Europarecht und für das Produkthaftungsrecht festgehalten (Rn. 1073 ff.) – Deutschland keine weitergehende Anforderungen an die IT-Sicherheit von online vertriebenen bzw. angebotenen Produkten oder Dienstleistungen aus dem EU-Ausland stellen kann. Zwar sieht die E-CRL einige Durchbrechungen des **Herkunftslandprinzips** vor, insbesondere auch zum Verbraucherschutz; doch bedarf es einer nur im Einzelfall zu erteilenden Ausnahmegenehmigung durch die EU-Kommission, so dass man die Anwendung eines deutschen IT-SicherheitsG in der Anwendung auf online IT-Produkte und –Dienstleistungen nicht hierauf stützen kann.

1091 Die Anwendung eines zu schaffenden IT-Sicherheitsgesetzes wird daher primär für Produkte oder Dienstleistungen aus dem Nicht-EU-Ausland relevant. Für **offline-vertriebene Produkte und Dienstleistungen** aus Mitgliedsstaaten der EU sind die Warenverkehrs- und die Dienstleistungsfreiheit der At. 28 ff., 49 ff. EG zu und das aus ihnen abgeleitete **primärrechtliche Herkunftslandprinzip** zu beachten, so dass im

[1833] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22.5.2001 Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. EG L 167, S. 10.
[1834] Dazu ausführlich *Heinz*, Urheberrechtliche Gleichbehandlung von alten und neuen Medien, 2006.

Verhältnis zur Aufsicht in den jeweiligen Herkunftsstaaten der Grundsatz der gegenseitgen Anerkennung in Bezug auf aufsichtsrechtlichen Standards gilt.

b) Grenzüberschreitende Durchsetzung behördlicher Anordnungen

1092 Hiervon zu trennen ist natürlich die in der Praxis im Vordergrund stehende Frage der internationalen Durchsetzbarkeit. Keine besonderen Schwierigkeiten entstehen hierbei, wenn **verkörperte IT-Produkte** in das Inland eingeführt werden, die den hier geltenden Sicherheitsstandards nicht entsprechen. Denn inländische Behörden können Verwaltungsmaßnahmen zumindest nach Einfuhr der Produkte durchführen.

1093 Anders ist dies bei Standards für **IT-Dienstleistungen** und **online vertriebene IT-Produkte**, da der Anbieter im Ausland sitzt und ein verwaltungsrechtlicher Einfluss unmittelbar auf online bezogenen Dienste und Produkte kaum möglich ist. Auf ausländischem Territorium können behördliche Anordnungen wegen der Souveränität der Staaten nicht einfach hoheitlich durch den erlassenden Staat durchgesetzt werden. **Grenzüberschreitende Amtshilfe** ist – selbst innerhalb der EU – noch immer äußerst kompliziert und zeitaufwändig.[1835]

1094 Somit stellt sich die Frage nach einem wirksamen Instrumentarium für Verwaltungsbehörden, um auf im Ausland ansässige Anbieter im Inland Zugriff nehmen zu können. In Betracht kommt hierbei zunächst der **Zugriff auf inländische Vermögenswerte** ausländischer Anbieter bei der Verwaltungsvollstreckung verhängter Bußgelder oder Geldstrafen.[1836] Dies stellt indes nur soweit eine effektive Handlungsoption dar, als in dem betreffenden Gebiet überhaupt derartige Sanktionen verhängt werden können und der betreffende ausländische Anbieter überhaupt über im Inland belegenes Vermögen (z.B. Warenbestände, Konten, aber auch Forderungen gegen inländische Schuldner) verfügt. In diesem Zusammenhang wäre auch an Sanktionen gegenüber den verantwortlichen Geschäftsleitern zu denken.

1095 Starker Druck auf ausländische Anbieter ließe sich zudem über **behördliche Warnungen** vor ausländischen Anbietern, welche IT-Sicherheitsvorgaben nicht erfüllen, erreichen (s. Rn. 877). Mit behördlichen Warnungen vor eklatanten IT-Sicherheitsrisiken (insbesondere in den Massenmedien) geht regelmäßig ein beträchtlicher Verlust an Un-

[1835] *Mankowski*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien , S. 51 (60 f.)
[1836] *Mankowski*, in: Leible, Die Bedeutung des Internationalen Privatrechts im Zeitalter der neuen Medien, S. 51 (61f.).

ternehmensreputation und Vertrauen im Kunden- und Benutzerkreis einher, welcher in empfindlichen Umsatzeinbrüchen resultieren kann. Auf dem betroffenen Unternehmen lastet dann nicht unerheblicher Druck durch Konvergenz mit den geforderten Sicherheitsstandards verlorenes Vertrauen wieder zu gewinnen. So hat beispielsweise die BaFin die Möglichkeit nach § 37 Abs. 1 KWG ergangene Untersagungs- und Abwicklungsanordnungen bekannt zu machen, um Anleger auf ergangene Verwaltungsanordnungen aufmerksam zu machen.[1837]

1096 Äußerst umstritten sind verwaltungsrechtliche **Anordnungen gegenüber inländischen Zugangsvermittlern oder anderen Providern**, die die Angebote verfügbar machen.[1838] Diese Problematik wurde bislang hauptsächlich im Zusammenhang mit den **sog. Düsseldorfer Sperrverfügungen** diskutiert[1839] und betrifft eine allgemeine Problematik öffentlich-rechtlicher Anordnungen gegenüber ausländischen Angeboten, die nicht spezifisch für ein IT-SicherheitsG sind. Inhalt der auf Grundlage von § 22 Abs. 2, 3 MDStV (jetzt § 59 Abs. 2 bis 5 RStV[1840]) ergangenen Sperrverfügungen der Bezirksregierung Düsseldorf war die Sperrung des Zugangs zu ausländischen Webseiten, welche rechtsradikale Inhalte bereithielten. Entsprechend könnten vorbehaltlich der technischen Realisierbarkeit Sperrverfügungen gegenüber Access-Providern wegen IT-Sicherheitsmängeln ausländischer Webangebote ergehen. Doch stellt sich hier wie dort das verwaltungsrechtliche Problem der Bestimmung des sicherheitsrechtlich Verantwortlichen und der verhältnismäßigen Mittel.

c) Ergebnis

1097 Fasst man die komplexe Rechtslage in internationaler Hinsicht zusammen, kann grob zwischen Nicht-EU-Staaten und dem EU-Ausland unterschieden werden:

1098 Für **Nicht-EU-Staaten** greift das internationale Deliktsrecht ein, so dass der in Deutschland Geschädigte deutsches Recht wählen kann, mit der Folge, dass ein deutsches IT-SicherheitsG Anwendung fände. Auch im öffentlichen Recht könnte Deutschland extra-

[1837] *Voge*, WM 2007, 381 (383).

[1838] Dazu *Spindler/Volkmann*, K & R 2002, 389 (402); *Mankowski*, MMR 2002, 28 (30).

[1839] S. OVG Münster, MMR 2003, 348 ff.; VG Düsseldorf, MMR 2005, 794 ff.; VG Köln, MMR 2005, 399 ff.; VG Düsseldorf, MMR 2003, 205 f.; VG Minden, MMR 2003, 135 ff.; dazu *Spindler/Volkmann*, K&R 2002, 398 ff.

[1840] Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag – RStV) vom 31.8.1991, zuletzt geändert durch Art. 1 des Neunten Staatsvertrages zur Änderung rundfunkrechtlicher Staatsverträge vom 31.7. bis 10.10.2006 (GBl. BW 2007 S. 111) gültig ab 1.3.2007.

territoriale Wirkungen an ein IT-SicherheitsG knüpfen, sofern sich IT-Produkte oder IT-Dienstleistungen auf das Inland spürbar auswirken.

1099 Für **Angebote aus EU-Staaten** gelten diese Grundsätze jedoch nur sehr eingeschränkt, da hier zum großen Teil für online vertriebene IT-Produkte und IT-Dienstleistungen die E-Commerce-Richtlinie und das in ihr verankerte Herkunftslandprinzip eingreift – sowohl für zivilrechtliche/deliktsrechtliche Ansprüche als auch öffentlich-rechtliche Eingriffsbefugnisse.

1100 Für **nicht online vertriebene Produkte** könnte dagegen ein IT-SicherheitsG eingreifen, da hier keine speziellen Vorgaben bestehen – abgesehen von den grundsätzlich eingreifenden europarechtlichen Primärfreiheiten.

1101 Daher sollte ein deutsches IT-SicherheitsG **unbedingt** durch eine **entsprechende europäische Initiative** begleitet werden, etwa in Gestalt einer **IT-Produktsicherheits-Richtlinie**, die sich in das Gesamtkonzept der EU zur Produktsicherheit, aber auch zur Dienstleistungssicherheit einfügt.

VIII. Ergebnisse des zweiten Teils

1102 Zusammengefaßt erscheint die Schaffung eines IT-SicherheitsG ein erfolgversprechender Weg zu sein, um eine übergreifende rechtliche Grundlage für eine Mindestsicherheit im IT-Bereich zu schaffen. Folgende Eckpfeiler sollten dieses Gesetz charakterisieren:

- Geltung für IT-Produkte, IT-Dienstleistungen, IT-Intermediäre sowie IT-Riskmanagement
- Verwendung des europäischen Ansatzes zur Produktsicherheit, mit Hilfe von untergesetzlich festgelegten, aber staatlich akzeptierten Standards sowie damit verknüpften Vermutungswirkungen der Einhaltung der nötigen Sicherheit
- Ausrichtung auf Gefährdung von kritischen Infrastrukturen, Sicherheitslücken bei Software, die die Begehung von IT-spezifischen Straftaten ermöglichen, sowie auf die Schädigung von Daten und Datenbeständen beim Nutzer
- Öffentlich-rechtliche Anordnungsbefugnisse einschließlich von öffentlichen Produktwarnungen
- Zivilrechtliche Flankierung durch Ausgestaltung des IT-SicherheitsG als Schutzgesetz zugunsten Dritter, verknüpft mit Beweiserleichterungen für den Nachweis der Kausalität, die wiederum bei zertifizierten Unternehmen ausgesetzt werden; gleichzeitige Aufhebung von haftungsrechtlichen Privilegierungen im Telekommunikationsbereich, Überführung in das allgemeine Recht der Inhaltskontrolle
- Zivil- und gesellschaftsrechtliche Vermutungswirkungen zugunsten von zertifizierten Herstellern, Dienstleistern, TK-Providern, dass die Sorgfaltspflichten eingehalten werden

1103 Darüberhinaus kann die Einführung einer IT-Gefährdungshaftung sowie eines IT-Führerscheins für jedermann erwogen werden, gekoppelt an den Verkauf von EDV-Produkten (einschließlich von Internet-Anschlüssen).

1104 Das BSI würde in diesem Rahmen im Wesentlichen die Aufgabe zukommen, die Standardentwicklung zu befördern, zu leiten und zu überwachen sowie als Akkreditierungsstelle zu dienen. Zur Struktur eines IT-Sicherheitsgesetzes siehe oben Rn. 939.

1105 Zu empfehlen ist aber aufgrund der nur eingeschränkten Gültigkeit eines solchen IT-Sicherheitsgesetzes, insbesondere für Anbieter von online vertriebenen IT-Produkten und Dienstleistungen aus dem EU-Ausland (Herkunftslandprinzip der E-Commerce-Richtlinie), die **Initiative zu einer entsprechenden EU-Produktsicherheitsrichtlinie**.

IX. Anhang: Normungen

X. Grundlegende Standards zum IT-Sicherheits- und Risikomanagement

1. Informationssicherheits-Managementsysteme (ISMS)

- ISO/IEC 13335 Management of information and communications technology security Management von Sicherheit der Informations- und Kommunikationstechnik (IuK)
- ISO/IEC 27001 Information security management systems – Requirements Informationssicherheits-Managementsysteme – Anforderungen
- ISO/IEC 17799 Code of practice for information security management Leitfaden zum Informationssicherheitsmanagement
- IT-GSHB IT-Grundschutzhandbuch (jetzt – Grundschutzkatalog)

2. Sicherheitsmaßnahmen und Monitoring

- ISO/IEC 18028 IT network security IT Netzwerksicherheit
- ISO/IEC TR 18044 Information security incident management Management von Sicherheitsvorfällen in der Informationssicherheit
- ISO/IEC 18043 Selection, deployment and operation of intrusion detection systems (IDS) Auswahl, Einsatz und Betrieb von Systemen zur Erkennung des Eindringens in Netze und Systeme (IDS)
- ISO/IEC TR 15947 IT intrusion detection systems (IDS) Leitfaden für Systeme zur Erkennung des Eindringens in Netze und Systeme (IDS)
- ISO/IEC 15816 Security information objects for access control. Sicherheitsobjekte für Zugriffskontrolle

3. Standards mit IT-Sicherheitsaspekten

- Cobit Control Objectives for Information and Related Technology. Kontrollziele für Informations- und verwandete Technologie
- ITIL IT Infrastructure Library. IT Infrastruktur Verfahrensbibliothek
- IDW PS 330 Abschlussprüfung bei Einsatz von Informationstechnologie

XI. Evaluierung von IT-Sicherheit

1. Common Criteria

- ISO/IEC 15408 (CC) Evaluation criteria for IT security (Common Criteria). Evaluationskriterien für IT-Sicherheit
- ISO/IEC TR 15443 A framework for IT security assurance. Rahmenrichtlinien für Sicherung von IT-Sicherheit
- ISO/IEC 18045 Methodology for IT security evaluation. Methodik zur Evaluation von IT-Sicherheit
- ISO/IEC TR 19791 Security assessment for operational systems. Bewertung der Sicherheit von Systemen im Betrieb
- ISO/IEC 19790 (FIPS 140-2) Security Requirements for Cryptographic Modules. Anforderungen an kryptographische Module
- ISO/IEC 19792 Security evaluation of biometrics. Evaluierung der IT-Sicherheit biometrischer Technologien

- ISO/IEC 21827 (SSE-CMM) System Security Engineering – Capability Maturity Model. Modell der Ablaufstauglichkeit (auch ISO 21827)

2. Schutzprofile

- ISO/IEC TR 15446 Guide on the production of protection profiles and security targets. Leitfaden zum Erstellen von Schutzprofilen und Sicherheitsvorgaben

XII. Spezielle Sicherheitsfunktionen 1:

1. Normen zu kryptographischen und IT-Sicherheitsverfahren

a) Verschlüsselung

- ISO/IEC 7064 Check character systems. Prüfzeichensysteme
- ISO/IEC 18033 Encryption algorithms. Verschlüsselungsalgorithmen
- ISO/IEC 10116 Modes of operation for an n-bit block cipher. Betriebsarten für einen n-bit-Blockschlüssel-Algorithmus
- ISO/IEC 19772 Data encapsulation mechanisms. Daten verkapselnde Mechanismen

b) Digitale Signaturen

- ISO/IEC 9796 Digital signature schemes giving message recovery. Digitaler Unterschriftsmechanismus mit Rückgewinnung der Nachricht
- ISO/IEC 14888 Digital signatures with appendix. Digitale Signaturen mit Anhang
- ISO/IEC 15946 Cryptographic techniques based on elliptic curves. Auf elliptischen Kurven aufbauende kryptographische Techniken

c) Hashfunktionen und andere Hilfsfunktionen

- ISO/IEC 10118 Hash functions. Hashfunktionen
- ISO/IEC 18031 Random bit generation. Erzeugung von Zufallsbits
- ISO/IEC 18032 Prime number generation. Generierung einer Primzahl

d) Authentifizierung

- ISO/IEC 9798 Entity authentication. Authentisierung von Instanzen
- ISO/IEC 9797 Message Authentication Codes (MACs). Nachrichten-Authentisierungscodes (MACs)

e) PKI-Dienste

- ISO/IEC 15945 Specification of TTP services to support the application of digital signatures. Spezifikation der Dienste eines vertrauenswürdigen Drittens zur Unterstützung der Anwendung von digitalen Signaturen
- ISO/IEC TR 14516 Guidelines for the use and management of Trusted Third Party Services. Richtlinien für die Nutzung und das Management eines vertrauenswürdigen Dritten

f) Schlüsselmanagement

- ISO/IEC 11770 Key management. Schlüsselmanagement

g) Kommunikationsnachweise

- ISO/IEC 13888 Non-repudiation. Nicht-Abstreitbarkeit

h) Zeitstempeldienste

- ISO/IEC 18014 Time-stamping services. Zeitstempeldienste

XIII. Spezielle Sicherheitsfunktionen 2: Physische Sicherheit

- Technische Leitlinie 7500. Produkte für die materielle Sicherheit

1. Brandschutz

- DIN 4102 Brandverhalten von Baustoffen und Bauteilen
- DIN 18095 Rauchschutztüren
- DIN EN 1047 Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand

2. Einbruchshemmung

- DIN EN 1143-1 Widerstandsgrad
- DIN V ENV 1627 Fenster, Türen, Abschlüsse - Einbruchhemmung

3. Gehäuse

- DIN EN 60529 Schutzart durch Gehäuse

XIV. Annex II: Rechtsvergleichende Studien

XV. Rechtsentwicklung in der IT-Sicherheit - Teil Österreich*

1. Pflichten der Hersteller von IT-Produkten

a) Ausdrücklich normierte Pflichten der Hersteller von IT-Produkten, die sich ausschließlich auf den IT-Bereich beziehen

1106 Soweit ersichtlich existieren dazu nur wenige gesetzliche Normen. Zu nennen sind hier folgende Bereiche:

1107 **Bereich Signaturen:** Signaturgesetz (SigG)[1841] sowie als technische Ausführungsnorm die Signaturverordnung (SigV)[1842], die Vorschriften für die technischen Komponenten und Verfahren zur Erzeugung von sicheren Signaturen bzw qualifizierten Zertifikaten (§§ 5-8 SigV) enthält.

1108 Bereich Arbeitnehmerschutz: Bestimmungen und Regelungen betreffend Bildschirmarbeitsplätze sind aufgrund der Umsetzung der Rahmenrichtlinie 89/391/EWG (Sicherheit und Gesundheit am Arbeitsplatz) in folgenden Materien zu finden:

- Bildschirmrichtlinie 90/270/EWG – EU-Bildschirmrichtlinie
- ArbeitnehmerInnenschutzgesetz – ASchG (insbesondere § 67 und 68)[1843]
- Bildschirmarbeitsverordnung – BS-V[1844]

1109 Diese Bestimmungen richten sich primär an den Arbeitgeber, wirken aber indirekt auch auf die Hersteller, etwa in der Gestaltung von Bildschirm (Zeichen, Bild, Helligkeit, Kontrast) und Tastatur sowie in der Software Ergonomie.

1110 Im Übrigen ergeben sich aus den Europäischen Normen (EN), die auch als ÖNORMEN übernommen werden, wichtige Hinweise für die Auslegung der Vorschriften über Bild-

---

* Erstellt von Dr.Markus Fallenböck, Wien/Österreich.

1841 BGBl I 1999/190 idgF.

1842 BGBl II 2000/30 idgF.

1843 BGBl 1994/450 idgF.

1844 BGBl II 1998/124 idgF.

schirmarbeitsplätze. Dabei ist insbesondere auf die ÖNORM EN ISO 9241 über ergonomische Anforderungen für Büroarbeit mit Bildschirmgeräten zu verweisen.

1111 **IT-Normen:** Daneben spielen verschiedene internationale bzw nationale Normen eine große Rolle, die in Streitfällen von den Gerichten (bzw von den berufenen Sachverständigen) als wesentlicher Maßstab für den Stand der Technik herangezogen werden.

1112 Das Österreichische IT-Sicherheitshandbuch[1845] nennt in Teil 2 (Version 2.2, November 2004) folgende Normen:

- ISO/IEC 7816 Identification cards - Integrated circuit(s) cards with contacts
- ISO 8372 Information processing - Modes of operation for a 64-bit block cipher algorithm
- ISO 8732 Banking - Key management (wholesale)
- ISO 9564 Banking - Personal Identification Number management and security
- ISO/IEC 9594-8 Information technology - Open Systems Interconnection – The Directory: Authentication framework
- ISO/IEC 9796 Information technology - Security techniques - Digital signature scheme giving message recovery
- ISO/IEC 9797 Information technology - Security techniques - Message Authentication Codes (MACs)
- ISO/IEC 9798 Information technology - Security techniques - Entity authentication
- ISO/IEC 9979 Data cryptographic techniques - Procedures for the registration of cryptographic algorithms
- ISO/IEC 10116 Information technology - Modes of operation for a n -bit block cipher algorithm
- ISO/IEC 10118 Information technology- Security techniques - Hash functions
- ISO 10126 Banking - Procedures for message encipherment (wholesale)
- ISO/IEC 10181 Information technology - Open systems interconnection – Security frameworks for open systems
- ISO 10202 Financial transaction cards - Security architecture of financial transaction systems using ICCs

[1845] Das IT-Sicherheitshandbuch wird von der „Stabsstelle IKT-Strategie des Bundes“ (eine Dienststelle des Bundeskanzleramtes) sowie vom Zentrum für sichere Informationstechnologie - Austria (A-SIT) herausgegeben. A-SIT wurde als erste Bestätigungsstelle lt. §19 Signaturgesetz (SigG), BGBl. I Nr. 190/1999 idgF durch Verordnung des Bundeskanzlers vom 2.2.2000 (Verordnung - A-Sit, BGBl. II Nr. 31/2000 idgF,) anerkannt.

- ISO/IEC 10536 Identification cards - Contactless integrated circuit(s) cards – Closecoupled cards

- ISO 11568 Banking - Key management (retail)
- ISO/IEC 11770 Information technology - Security Techniques - Key Management
- ISO/IEC TR 13335 Information technology - Guidelines for the management of IT Security
- ISO 13491 Secure Cryptographic devices
- ISO/TR 13569 Banking, securities and other financial services - Information security guidelines
- ISO/IEC 13888 Information technology - Security techniques - Non-repudiation
- ISO/IEC 14443 Identification cards - Contactless integrated circuit(s) cards – Proximity cards
- ISO/IEC 14516 Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services
- ISO/IEC 14888 Information technology - Security techniques - Digital signatures with appendix
- ISO/IEC 15292 Information technology - Security techniques - Protection Profile registration procedures
- ISO/IEC 15408 Information technology- Security techniques- Evaluation criteria for IT security
- ISO/IEC TR 15443 Information technology - Security techniques - A framework for IT security assurance
- ISO/IEC 15446 Information technology - Security techniques - Guide on the production of Protection Profiles and Security Targets
- ISO/IEC 15693 Identification cards - Contactless integrated circuit(s) cards – Vicinity Integrated Circuit(s) Card
- ISO/IEC 15816 Information technology - Security techniques - Security Information Objects
- ISO/IEC 15945 Information technology - Security techniques - Specification of TTP services to support the application of digital signatures
- ISO/IEC 15946 Information technology - Security techniques – Cryptographic techniques based on elliptic curves
- ISO/IEC 18014 Information technology - Security techniques - Time stamping services
- ISO/IEC 18033 Information technology - Security techniques - Encryption algorithms BSI 7799 (Part 1) /
- ISO 17799 Information technology - Code of practice for information security management
- BSI 7799 (Part 2) Information Security Management Systems

1113 Leider verfügt Österreich über keine statistische Erfassung an Gerichtsentscheidungen, in denen technische Normen angewendet werden. Dies liegt insbesondere daran, dass – und dies trifft vor allem auf den IT-Bereich zu – solche Verfahren in der Regel über Sachverständigengutachten auf der Tatsachenebene entschieden werden und es daher an der rechtlichen Erheblichkeit mangelt, die Voraussetzung für ein Verfahren vor dem OGH ist. In Österreich werden jedoch nur Entscheidungen des OGH systematisch publiziert. Insofern kann die Zahl an einschlägigen Verfahren – speziell im IT-Bereich – seriöser Weise nicht geschätzt werden. Der Autor kann jedoch aus seiner beruflichen Erfahrung sagen, dass komplexe IT-Schäden häufig nicht Gegenstand von Verfahren werden, da sich die Parteien im Vorfeld vergleichen. Grundsätzlich kommt technischen Normen insbesondere im Bereich der Produkthaftung große Bedeutung zu. Es ist ständige Rechtsprechung des OGH[1846], dass die normgerechte oder sonstigen technischen Standards entsprechende übliche Herstellungsart die Fehlerfreiheit des Produkts indiziert[1847].

b) Das Recht der Produktsicherheit und IT-Produkte

1114 In Österreich existiert dazu in Umsetzung der einschlägigen EU-Richtlinie das Produktsicherheitsgesetz 2004 (PSG 2004)[1848]. Das Produktsicherheitsrecht wird in der Öffentlichkeit meist nur dann wahrgenommen, wenn es zu größeren Rückrufaktionen kommt: Bekannt sind sie vor allem im Bereich schadhafter Fahrzeuge, die Unfälle verursachen können, und elektronischer Geräte, von denen Brandgefahr ausgeht. Vielfach gehen derartige Rückholaktionen von den Herstellern aus, die damit ihr Haftungsrisiko verringern wollen. Behördlicherseits wurden aber auch Spielwaren zurückgeholt oder Tauchcomputer, die auf Grund von Softwarefehlern die Atemluft falsch berechnen, und Äpfel, die mit unzulässigen Substanzen behandelt waren.

1115 Die Definition des „Produktes“ im PSG wurde weitgehend von der Richtlinie übernommen und mit der Definition aus dem PSG 1994 („bewegliche Sache“ in Anlehnung an das Produkthaftungsgesetz) ergänzt. Abweichend vom PSG 1994 wird die Einschränkung auf „körperliche“ Sachen fallengelassen, da etwa Software durchaus sicherheitsrelevante Eigenschaften besitzen kann und mittlerweile nicht mehr nur auf „körper-

[1846] OGH 6 Ob 73/04k; 3 Ob 547/95; 6 Ob 157/98a.

[1847] Siehe dazu unten Punkt I.3 zur Produkthaftung.

[1848] BGBl I 16/2005; aus der sehr spärlichen Literatur zum PSG seien genannt: *Moser*, Produktsicherheitsgesetz, ecolex 2004, 600; *Schwarz*, Wenn Hautcreme schadet statt pflegt: Rückruf EU-weit möglich, Die Presse RECHTSPANORAMA - 28. 2. 2005; *Linder,* Produktbeobachtung, Rückruf und Versicherungsschutz, wbl 2004, 449.

lichen“ Datenträgern, sondern auch als Download in Verkehr gebracht wird[1849]. Somit sind sowohl Hardware- als auch Softwareprodukte vom PSG erfasst.

1116 Eine wesentliche Neuerung der Richtlinie 2001/95/EG ist die Möglichkeit, Normen zu mandatieren und ihre Fundstelle im Amtsblatt der EG zu veröffentlichen (ein Verfahren, das der Harmonisierung und Referenzierung von Normen bei Richtlinien nach der neuen Konzeption entspricht). Bei Einhaltung dieser Normen wird die Konformität mit den Sicherheitsanforderungen der Richtlinie vermutet. Mit § 5 Abs. 1 und 2 PSG wird diese Bestimmung umgesetzt, Die Fundstellen dieser – trotzdem unverbindlichen – Normen, die als nationale Normen in den Vertragsstaaten des EWR veröffentlicht werden müssen, sowie gegebenenfalls die Streichung dieser Fundstellen sind in Österreich im Bundesgesetzblatt II kundzumachen.

1117 Den auf diese Art in Österreich kundgemachten Normen sind die entsprechenden Normen anderer EU Staaten gleichzuhalten. Dh, dass genauso wie die Einhaltung der entsprechenden ÖNORM EN die Einhaltung z.B. einer identen britischen BS EN oder deutschen DIN EN (wenn auf die zugrunde liegende EN im EG-Amtsblatt verwiesen wurde) die Konformitätsvermutung auslöst.

1118 Eine Nichteinhaltung von solcherart kundgemachten Normen bedeutet nicht automatisch, dass ein Produkt gefährlich ist. Das von solchen Normen vorgegebene Sicherheitsniveau wird aber als wesentlicher Maßstab für die Konformitätsbeurteilung gelten. Dies bedeutet, dass ein Unterschreiten dieses Sicherheitsniveaus in der Regel dazu führen wird, dass das entsprechende Produkt als gefährlich im Sinne des PSG 2004 einzustufen ist. Es bleibt aber jedenfalls den Herstellern/Herstellerinnen unbenommen, wie – also auch abweichend von der Norm - dieses Sicherheitsniveau erreicht wird.

1119 Die Verwendung des CE-Zeichens für Produkte, die ausschließlich dem PSG 2004 unterliegen, ist aber weiterhin nicht zulässig.

1120 Sollte eine entsprechende Norm kein zufrieden stellendes Sicherheitsniveau garantieren, sieht die Richtlinie ein Ausschussverfahren vor, wonach auch eine Streichung dieser Norm möglich ist. Darüber hinaus erfolgt die Konformitätsbeurteilung – sofern nicht ohnehin gesetzliche Vorschriften anzuwenden sind – wie im PSG 1994 nach anderen,

[1849] Siehe dazu die Erläuternden Bemerkungen des Nationalrates, 512 d.B. (XXII. GP).

nicht im Amtsblatt veröffentlichten europäischen Normen, nationalen Normen, in der PS-Richtlinie vorgesehenen Empfehlungen der europäischen Kommission zur Festlegung von Leitlinien, Verhaltenskodizes, dem Stand des Wissens und der Technik (entsprechend der Definition im ArbeitnehmerInnenschutzgesetz), den Sicherheitserwartungen der Verbraucher/innen und den Empfehlungen des Produktsicherheitsbeirates (Abs. 3).

1121 Trotz Übereinstimmung mit den o.a. Anforderungen kann sich ein Produkt als unsicher erweisen. Behördliche Maßnahmen nach dem PSG sind diesfalls trotzdem zulässig.

1122 Zur Vereinfachung der Vollziehung sieht Abs. 5 vor, dass Risikobewertungen durch andere Behörden des EWR oder Testergebnisse von in- und ausländischen Prüf-, Überwachungs- und Zertifizierungsstellen für sich – ohne weitere Untersuchung – ausreichen, um behördliche Maßnahmen bei gefährlichen Produkten zu setzen. Im Hinblick auf kulturelle Unterschiede und abweichende Erfahrungswerte bei der Risikobewertung in anderen Ländern handelt es sich hier bewusst um eine Kann-Bestimmung. Eine neuerliche Prüfung durch die zuständigen Behörden ist jedenfalls zulässig. Im Falle einer RAPEX-Meldung (EU-Produktsicherheitsnotfallsverfahren) wird die Anerkennung der ausländischen Bewertung aber die Regel sein; redundante, kostenintensive und zeitaufwändige Tests werden dadurch vermieden.

1123 Haftungsrechtlich führt die Missachtung der im PSG enthaltenen Vorschriften zu einer Schutzgesetzverletzung, welche bei Schadenersatzforderungen geltend gemacht werden kann.

c) Haftung der Hersteller für die Fehlerhaftigkeit der hergestellten IT-Produkte

(1) Verschuldensunabhängige Haftung

(a) Grundlagen

1124 Primär haftet der Hersteller nach dem Produkthaftungsgesetz (PHG)[1850]. Die Haftung besteht grundsätzlich nur dann, wenn den Schaden nicht ein Unternehmer erlitten hat, der die Sache überwiegend in seinem Unternehmen verwendet hat (§ 2 PHG).

[1850] BGBl ; zur Literatur: *Horwath*, Software - ein Produkt?, ecolex 2000, 784; *Andreewitch*, Zur Anwendbarkeit des Produkthaftungsgesetzes für Softwarefehler, EDVuR 1990, 50; *Holzinger*, Produkthaftpflicht und Software, EDVuR 1988 H 4, 10.

1125 Die Haftung nach dem PHG ist verschuldensunabhängig. Dh, dass nach § 8 PHG die Haftung nicht durch den Mangel eines Verschuldens, sondern durch den Nachweis ausgeschlossen werden, dass

- 1. der Fehler auf eine Rechtsvorschrift oder behördliche Anordnung zurückzuführen ist, der das Produkt zu entsprechen hatte,
- 2. die Eigenschaften des Produktes nach dem Stand der Wissenschaft und Technik zu dem Zeitpunkt, zu dem es der in Anspruchgenommene in den Verkehr gebracht hat, nicht als Fehler erkannt werden konnten oder
- 3. wenn der in Anspruchgenommene nur einem Grundstoff oder ein Teilprodukt hergestellt hat – der Fehler durch die Konstruktion des Produkts, in welches der Grundsstoff oder das Teilprodukt eingearbeitet worden ist, oder durch die Anleitungen des Herstellers dieses Produkts verursacht worden ist.

1126 Schäden nach dem PHG liegen nur vor, wenn ein Mensch getötet, am Körper verletzt oder an der Gesundheit geschädigt oder eine von dem Produkt verschiedene körperliche Sache beschädigt wird (§ 1 PHG).

1127 In Österreich ist die Anwendung des PHG auf Schäden durch IT immer noch nicht endgültig durch die Gerichte geklärt. Nach überwiegender Meinung gelten Hardware und Standard-Software jedenfalls insofern als Produkt iSd PHG, als sie in Hardware "integriert" ist oder als die in der Software gespeicherten Informationen direkt zu Zerstörungen oder Beschädigungen von geschützten Zu denken ist hier insb an Personenschäden, die sich im Bereich computerisierter Diagnostik und Therapie ereignen und sich aus der vom Computer gegebenen falschen Information ergeben.

1128 Von österreichischen Gerichten noch nicht geklärt ist, ob Software auch unabhängig von der Verkörperung auf einem Datenträger ein Produkt iSd PHG ist. Die Produkthaftungsrichtlinie enthält das Merkmal der Körperlichkeit nicht. Daraus könnte abgeleitet werden, dass § 4 PHG im Hinblick auf das dort normierte Erfordernis der Körperlichkeit des Produkts nicht richtlinienkonform sei und die geschilderte Problematik lediglich aus der richtlinienwidrigen Umsetzung entstanden sei. 1989 hat die Kommission auf eine Anfrage folgende Antwort gegeben: "Im Sinne von Art 2 der RL ... über die Haftung für fehlerhafte Produkte gilt als Produkt jede bewegliche Sache, ... auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bildet. Somit findet die RL auf Computer-Software Anwendung, ...". Damit erübrigt sich nach Auffassung der Kommission auch eine gesetzliche Regelung über die Haftung. Auf die-

ser Basis geht die neuere Literatur[1851] davon aus, dass Software unabhängig von ihrer sachenrechtlichen Einordnung dem PGH unterliegt.

1129 Eine Differenzierung nach Individual- und Standardsoftware hinsichtlich der Zuordnung zum Produktbegriff kann nicht aus dem PHG abgeleitet werden. Es kommt nicht darauf an, auf welcher vertragsrechtlichen Grundlage (Kaufvertrag einerseits oder Werk- bzw Dienstvertrag andererseits) Software in Verkehr gesetzt wurde. Auch die im Zuge einer Dienstleistung entstandene bewegliche, körperliche Sache ist Produkt iSd PHG.

1130 Im Rahmen der Haftung für die Fehlerhaftigkeit von IT-Produkten sind vor allem die Rolle von Rechtsvorschriften und technischen Normen zu beleuchten.

(b) Rechtsvorschriften oder behördliche Anordnungen

1131 Eine allgemeine Vorschrift, an die in diesem Zusammenhang zu denken ist, ist das Datenschutzgesetz. Es wäre denkbar, dass eine programmtechnische Maßnahme, die den unbefugten Zugriff auf personenbezogene Daten verhindern soll, zwangsläufig zu einem Fehler im eigentlichen Funktionsbereich der Software führt. Relevanter sind hingegen Vorschriften aus dem jeweiligen Anwendungsgebiet. *Holzinger*[1852] bringt dazu folgendes fiktives Beispiel: So würde eine gesetzliche Vorschrift, die eine Mindestzeit für das Ansprechen einer Autobremse fordert, den Software-Hersteller von der PHG-Haftung befreien, wenn eine computerprogramm-gesteuerte Autobremse bloß deswegen, um die entscheidende Zentelsekunde zu spät angesprochen habe, wenn eine entsprechende Warteroutine in seinem Programm vorgesehen wurde, um dieser Vorschrift genüge zu tun.

(c) Stand der Wissenschaft und Technik

1132 Bei der Beurteilung, ob ein IT-Produkt im Sinn des § 5 PHG fehlerhaft ist, sind die berechtigten Sicherheitserwartungen des Geschädigten maßgebend. Hiefür ist ein objektiver Maßstab anzulegen, dessen Konkretisierung im Einzelfall unter Berücksichtigung aller Umstände vorzunehmen ist. Was im Einzelfall an Produktsicherheit erwartet werden darf, ist eine Rechtsfrage. Bei den Konstruktionsfehlern ist die Enttäuschung der

[1851] *Horwath*, Software - ein Produkt?, ecolex 2000, 784.

[1852] *Holzinger*, Produkthaftpflicht und Software, EDVuR 1988 H 4, 10.

Sicherheitserwartung im technischen Konzept - in der "Konstruktion" des Produkts – begründet.

1133 Der Standard von Wissenschaft und Technik konkretisiert die berechtigten Sicherheitserwartungen des durchschnittlichen Produktbenützers. Die normgerechte oder sonstigen technischen Standards entsprechende übliche Herstellungsart indiziert die Fehlerfreiheit des Produkts[1853]. § 5 Abs 2 PGH stellt klar, dass ein Produkt nicht allein deshalb als fehlerhaft anzusehen ist, weil später ein verbessertes Produkt in den Verkehr gebracht worden ist. "Verbessert" ist ein Produkt, wenn es konstruktiv weiter entwickelt und dadurch sicherer geworden ist[1854].

1134 Gemäß der Regierungsvorlage ist „der Stand von Wissenschaft und Technik der Inbegriff der Sachkunde, die im wissenschaftlichen und technischen Bereich allgemein zur Verfügung steht ... Mindermeinungen, Einzeluntersuchungen und Einzelwissen scheiden grundsätzlich aus ..., weil der Unternehmer das Risiko ihrer Unrichtigkeit nicht auf sich nehmen muss ...; anderes gilt nur, wenn die neue "Einzelerkenntnis" evident richtig, "zwingend" ist."

1135 Die Programmierung erfolgt nach dem gegenwärtigen Stand der Technik in der Weise, dass zuerst das Programm geschrieben wird und dann mit Hilfe von ausgesuchten Testdaten geprüft wird, ob das Programm die gewünschten Funktionen erfüllt. Es liegt auf der Hand, dass ein solches Verfahren immer ein großes Maß an Unsicherheit enthält, da aus Zeitgründen nicht alle Fälle geprüft werden können. Der in § 8 Z 2 PHG normierte Ausschluss des Entwicklungsrisikos scheint, wegen der „Unaustestbarkeit“ von Computerprogrammen die Haftung des Programmherstellers völlig zu beseitigen. Doch diese Norm ist kein Freibrief für den Programmhersteller, unsauber zu testen. Wenngleich das obige Beispiel wohl eindrücklich belegt, dass ein theoretisch vollständiger Test innerhalb wirtschaftlich sinnvoller Zeit nicht möglich ist, kann durch Zusammenfassung

[1853] OGH 6 Ob 73/04k; 3 Ob 547/95; 6 Ob 157/98a. Grundsätzlich interessant ist die OGH Entscheidung zu 6 Ob 73/04 k. Die Klägerin begehrte hier ua nach PHG Schadenersatz, weil sie durch einen von ihr behaupteten Material- oder Konstruktionsfehler des Brillenglases während einer Schneeballschlacht am linken Auge verletzt wurde. Die Beklagte wandte dagegen ein, dass sie bei der Produktion und Qualitätskontrolle die entsprechende EN ISO 14889 einhalte. Der OGH hielt fest, dass das Glas des bei der Brille der Klägerin verwendeten Typs schon längere Zeit am Markt war und den einschlägigen technischen Richtlinien entsprach, die zugleich eine Zusammenfassung üblicher Sorgfaltsanforderungen darstellen. Dass bereits im Zeitpunkt, als das verwendete Kunststoffbrillenglas der Beklagten in den Verkehr gebracht wurde - auf den bei der Prüfung der Produktsicherheit im Sinn des § 5 Abs 1 Z 3 PHG abzustellen ist -, andere technische Konzepte und geeignetere Alternativen zum Mineralglas vorhanden gewesen seien und es der Beklagten aus technischer Sicht möglich gewesen wäre, ein bruchsichereres Glas herzustellen, hatte die hiefür beweispflichtige Klägerin gar nicht behauptet. Der OGH gab jedoch der Klägerin insofern Recht, als dass ein Instruktionsfehler vorliegt. Beim Instruktionsfehler macht die unzureichende Darbietung das Produkt fehlerhaft.

[1854] *Posch* in *Schwimann* Komm zum ABGB[2] Band 8 § 5 PHG Rz 22.

gleichartiger Fälle vom erfahrenen Fachmann doch ein sinnvoller Satz von Testfällen zusammengestellt werden[1855].

1136 Da dem Hersteller gemäß § 8 PHG der Nachweis für das Vorliegen eines Haftungsausschließungsgrundes obliegt, ist den Programmherstellern zu raten, ihre durchgeführten Tests in einer nachzuvollziehenden Weise zu dokumentieren und diese Dokumentation bis zum Ablauf der Verjährungsfrist für die mögliche PHG-Haftung (gemäß § 13 «PHG» 10 Jahre ab Inverkehrbringen durch den betreffenden Haftenden) aus dem zeitlich letzten Geschäftsfall aufzubewahren[1856].

1137 Wenngleich der Haftungsausschluss auf den Zeitpunkt des jeweiligen Inverkehrbringens abstellt, sind später gefundene und dem Programmhersteller bekannt gewordene Programmfehler nicht ohne Belang. Schon aus dem Recht der verschuldensabhängigen Produkthaftung ergeben sich Produktbeobachtungs-, Warn- und Rückholpflichten (siehe dazu im Folgenden).

(d) Rechtliche Wirkung von Normen

1138 Soweit ersichtlich liegen dazu keine Entscheidungen im IT-Bereich vor. Es lassen sich jedoch Grundsätze aus anderen Entscheidungen rund um technische Produkte ableiten. Grundsätzlich gilt, dass dem in Anspruch genommenen Schädiger die Beweislastumkehr und Beweiserleichterung des § 7 Abs 2 PHG zugute kommt. Danach hat er bloß als wahrscheinlich darzutun, dass das Produkt zur Zeit, zu der es in Verkehr gebracht worden war, noch nicht den schadenskausalen Fehler hatte[1857]. Dieser erleichterte Beweis ist grundsätzlich mit den getroffenen Feststellungen, dass das Produkt dem Stand der Technik entspricht und etwa das technische Prüfzeichen einer für die Prüfung anerkannten Anstalt aufweist[1858], als erbracht anzusehen. Dies umfasst auch den Verweis auf die Einhaltung relevanter Normen und Standards (ISO, ÖNORM etc). Insofern kommt es zu einer Beweislastumkehr. Infolge muss der Kläger beweisen, dass entgegen den getroffenen Feststellungen das Produkt schon zum Zeitpunkt des Verkaufs fehlerhaft gewesen ist. Der geschädigte Kläger kann dies dadurch tun, dass er die zu Gunsten des Beklagten erfolgte Indizwirkung erschüttert, etwa indem er dartut, dass eine Norm nicht anwendbar ist, weil sie die Gefahrenlage nicht abdeckt.

[1855] So *Holzinger*, Produkthaftpflicht und Software, EDVuR 1988 H 4, 10.

[1856] *Holzinger*, Produkthaftpflicht und Software, EDVuR 1988 H 4, 10.

[1857] OGH 6 Ob 157/98a.

[1858] Dabei handelte es sich um den Zeichengenehmigungsausweis der VDE-Prüfstelle (Verband Deutscher Elektrotechniker) für einen Elektroofen.

1139 In Österreich ist hier auch die Trennung in Konstruktionsfehler, Produktionsfehler und Instruktionsfehler innerhalb der Produkthaftung relevant zu unterscheiden. Bei den Konstruktionsfehlern ist die Enttäuschung der Sicherheitserwartung im technischen Konzept, eben in der „Konstruktion“ des Produkts, begründet. Beim Produktions-(Fabrikations-)fehler entspricht zwar das Konzept und das danach hergestellte „idealtypische Produkt“ den Erwartungen, nicht aber einzelne Stücke, weil der Produktionsprozess nicht normgerecht war. Beim Instruktionsfehler macht nur die unzureichende Darbietung das Produkt fehlerhaft[1859]. Insofern ist etwa im Falle einer Zertifizierung relevant wofür diese erfolgte (etwa für die Konstruktion eines Gerätetyps oder für das Herstellungsverfahren eines Produktes)[1860]. Dies zeigt sich deutlich in folgender Entscheidung. Darin ging es um eine vollautomatische Kaffeemaschine, die im Standbybetrieb auf Grund eines technischen Defekts in der Maschine in Brand geriet und einen Hausbrand verursacht hat. Die Beklagte versuchte sich hier damit frei zu beweisen, dass die Kaffeemaschine dem Stand der Technik entsprochen habe und das technische Prüfzeichen einer für die Prüfung anerkannten Anstalt aufweise. Dieses Prüfzeichen bezog sich jedoch nicht auf die konkrete Kaffeemaschine oder das Herstellungsverfahren. Festgestellt wurde nur, dass der Espressomaschinentyp zertifiziert wurde. Die Klägerin machte jedoch keinen Konstruktions- sondern einen Produktionsfehler geltend. Der OGH entschied, dass aus der Zertifizierung daher nicht auf eine fehlerfreie Produktion geschlossen werden kann.

(2) Verschuldensabhängige Haftung[1861]

1140 Da § 15 Abs 1 PHG ausdrücklich festhält, dass das übrige Schadensersatzrecht unberührt bleibt, kann neben der PHG-Haftung vom Geschädigten auch die schon bisher von der Lehre entwickelte und von der Judikatur weitgehend anerkannte verschuldensabhängige Produkthaftung ("Vertrag mit Schutzwirkung zugunsten Dritter") geltend gemacht werden. Dies kann insbesondere für Schäden im eigenen Unternehmen (Körperschäden von Angestellten, Kunden und Lieferanten durch im Unternehmen erstellte Programme), für reine Vermögensschäden und hinsichtlich des Selbstbehaltes bei Sachschäden relevant sein.

[1859] Siehe dazu OGH JBl 1996, 188; SZ 70/61; ZVR 2001/71; 10 Ob 19/01v je mwN.

[1860] OGH 10 Ob 98/02p.

[1861] Grundsätzlich zur Haftung im IT-Bereich: *Gantner*, Die Haftung der Krankenanstalten für Computerfehlleistungen, VR 2001, 222; *Welser/Vcelouch*, Haftung für mangelnde „Jahr 2000-Tauglichkeit“ von Hard- und Software ecolex 1998, 829; *Graf*, Wer haftet beim Telebanking?, ecolex 1999, 239; *Gruber*, Computerviren und Schadenersatz, EDVuR 1990, 122.

1141 Besonders relevant ist hier die Produktbeobachtungspflicht. Die Produktbeobachtung ist nicht vom PHG erfasst. Die verschuldensunabhängige Haftung des PHG knüpft an das In-Verkehr-Bringen des fehlerhaften Produkts an (§ 6 PHG); eine Haftung besteht nicht, wenn die haftungsbegründenden Eigenschaften des Produkts nach dem Stand der Wissenschaft und der Technik im Zeitpunkt des In-Verkehr-Bringens nicht erkannt werden konnten (siehe oben). Bei der hier behandelten Produktbeobachtungspflicht geht es dagegen um gefährliche Eigenschaften, die erst nach dem In-Verkehr-Bringen hervortreten und nicht vom PHG erfasst sind. Zur Begründung der Produktbeobachtungspflicht muss auf andere Anspruchsgrundlagen zurückgegriffen werden. In Betracht kommen Ansprüche aus Verschuldenshaftung wegen Verstoß gegen Verkehrssicherungspflichten, Verstoß gegen Schutzgesetze iSd § 1311 ABGB, oder auf Grund vertraglicher Schutzpflichten zugunsten Dritter.

1142 Die Produktbeobachtungspflicht verlangt vom Hersteller, die von ihm auf den Markt gebrachten Produkte auf gefährliche Auswirkungen zu beobachten und beim Auftreten solcher Auswirkungen Maßnahmen zur Gefahrenabwendung zu ergreifen[1862].

1143 Soweit der Hersteller an einen Händler liefert, ist die Produktbeobachtungspflicht aus einem Vertrag mit Schutzwirkungen zugunsten Dritter (also zugunsten des Letztkäufers) abzuleiten. Den Händler selbst trifft grundsätzlich keine Produktbeobachtungspflicht.

d) Technische Normen im Produktsicherheitsrecht, die eine Haftungsprivilegierung nach sich ziehen

1144 In Österreich ist dies nur im Rahmen der oben skizzierten Beweiserleichterung bei Haftungsfällen bekannt.

2. Pflichten der Nutzer von IT-Produkten

a) Private Nutzer

1145 Soweit ersichtlich gibt es nur eine Entscheidung des OGH die sich mit der Haftungsverteilung zwischen Anbieter und Nutzer von IT beschäftigt. Diese stammt aus dem Bereich des Internetbanking: OGH 4 Ob 179/02f[1863]. In der Entscheidung ging es um die

[1862] OGH 2 Ob 309/99a, ecolex 2001/168 = ZVR 2002/31.

[1863] Die Entscheidung wurde weitgehend positiv aufgenommen: *Iro*, OGH: Unwirksame Klauseln in den Allgemeinen Geschäftsbedingungen der Banken, RdW 2/2003, 66 (67); *Graf*, Jetzt schlägts aber (fast) 13!, ecolex 2003, 1 (4f); *Apathy*, Die neuen ABB auf dem Prüfstand – Anmerkungen zu OGH 4 Ob 179/02f, ÖBA 3/03, 177 (180f); schon vor der Entscheidung kritisch zu dieser Klausel *Hofmann*, Bemerkungen zu den neuen Allgemeinen Geschäftsbedingungen für Bankgeschäfte (ABB 2000), ÖBA 5/02, 371 (373f).

Zulässigkeit von Bestimmungen von AGB einer Bank. Unter anderem sahen wie AGB auch einen weitgehenden Haftungsausschluss für IT-Fehler vor, den der OGH für unzulässig erachtete.

1146 Durch die OGH-Entscheidung 4 Ob 179/02f stellt sich die Haftungssituation im Internetbanking nunmehr so dar:

1147 Die Banken haben für Schäden einzustehen, die durch leichte Fahrlässigkeit des Kreditinstitutes entstehen. Bei der Kenntniserlangung der Identifikationsmerkmale durch ein Verschulden des Kunden und bei der Kenntniserlangung aus der Sphäre der Bank ohne ein Verschulden des Kunden und einem jeweiligen - daraus entstehenden - Schaden gibt es keine rechtlichen Änderungen. Bei ersterer Konstellation haftet der Kunde, bei der zweiten die Bank.

1148 Bei Schäden, die durch eine Kenntniserlangung aufgrund von Sicherheitsmängeln des Internetbanking-Systems zustande kommen, lässt die Judikatur keine verschuldensunabhängige Risikohaftung des Kunden zu. Die Haftung hat bei dieser Konstellation die Bank zu tragen.

1149 Erlangt ein unberechtigter Dritter die Identifikationsmerkmale aus der Sphäre des Kunden ohne sein Verschulden, entfällt wiederum die Möglichkeit einer Risikohaftung des Bankkunden. Dabei gelangt man jedoch über die Zuordnung von Gefahren nach Risikosphären zu einer Haftung des Kunden, wenn der Schaden für ihn kalkulierbar war und ihn seine Bank vor Vertragsabschluss ausreichend über das bestehende Risiko beim Internetbanking aufgeklärt hat.

1150 Bei Fehlüberweisungen im Internetbanking trägt die Bank das Haftungsrisiko, sofern sie kein System verwendet, das die Kontonummer mit dem Kontowortlaut abgleicht.

1151 Grundsätzlich besteht hier die allgemeine deliktische Haftung nach § 1295 ABGB. D.h. dass der Privatnutzer für vorsätzlich oder fahrlässig verursachte Schäden haftet. Ein Mitverschulden des Geschädigten führt zu einer entsprechenden Reduktion seines Ersatzanspruches. Entscheidend ist somit die Frage, wann fahrlässiges Verhalten vorliegt. Ist etwa das Fehlen eins Virenfilters und die somit ermöglichte Weiterleitung von Viren durch den Nutzer bereits ein Außerachtlassen der üblichen Sorgfalt? Hier wird sehr viel vom Maßstab abhängen, den die Gerichte an den durchschnittlichen IT-Nutzer stellen.

1152 Die Haftung des Kunden ergibt sich jedenfalls durch die Verletzung des Internetbanking-Vertrages, der die Sorgfaltspflichten des Internetbanking-Kunden beinhaltet.

1153 Nach Meinung der Literatur[1864] können folgende Pflichten durchschnittlichen Usern zugemutet und somit in den Nutzungsbedingungen festgehalten werden:

- Die Geheimzahlen dürfen nicht an leicht zugänglichen Stellen notiert werden.
- Die PIN ist getrennt von der TAN-Liste aufzubewahren und die Identifikationsmerkmale müssen geheim gehalten werden.
- Besteht beim Kunden der Verdacht, dass eine unbefugte Person Kenntnis von den Identifikationsmerkmalen erlangt hat, muss er die Sperre der Zugriffsberechtigung veranlassen.
- Internetbanking-Kunden dürfen die persönlichen Identifikationsmerkmale nicht auf ihrer Festplatte abspeichern.
- Der User hat auf eine sichere Verbindung zu achten, die er an dem Verschlüsselungssymbol in der Statusleiste und an der https:// - Verbindung in der Adresszeile erkennen kann.
- Bei einer umfangreichen Anleitung durch die Bank hat der Kunde seinen Browser sicherheitsoptimal zu konfigurieren.
- Bei einer umfangreichen Anleitung durch die Bank hat der Kunde seinen E-Mail-Client so zu konfigurieren, dass Attachments nicht automatisch geöffnet werden. (Die meisten Angriffe werden über ausführbare Dateien gestartet, die in einer E-Mail enthalten sind.)

1154 Sind Sorgfaltsvereinbarungen aber zu weitreichend und für den Konsumenten nicht erfüllbar oder undurchschaubar, sind sie als nicht wirksam vereinbarte Bestimmungen anzusehen und können auch nicht im Schadensfall von Banken geltend gemacht werden. Hier ist vor allem an umfangreiche technische Sicherheitsvorkehrungen zu denken, die der User ohne eine ausreichende Hilfestellung durch die Bank treffen muss. Nicht wirksam kann unseres Erachtens die Verpflichtung zur Installation eines Virenschutzprogramms vereinbart werden, da der User dadurch zumeist gezwungen ist diese Software käuflich zu erwerben. Ein Hinweis in den AGB darauf, dass ein „Anti-Virus-Programm“ installiert werden sollte, erscheint jedoch sinnvoll. Auch die Implementierung einer persönlichen Firewall, über die man unter anderem auch einzelne Ports sperren kann, wird dem User nicht zugemutet werden können[1865].

b) Kommerzielle Nutzer

[1864] *Krassnigg/Stotter*, Rechtliche Entwicklungen im Internetbanking, wbl 2004, 213.
[1865] *Krassnigg/Stotter*, Rechtliche Entwicklungen im Internetbanking, wbl 2004, 213.

(1) Grundlagen

1155 Grundsätzlich differenziert das allgemeine Haftungsregime des § 1295 ABGB nicht zwischen kommerziellen und privaten Nutzern. Eine Ausnahme bildet hier nur § 1299 ABGB, der die sogenannte Sachverständigenhaftung festlegt.

1156 Relevant ist dieser Unterschied zunächst nur bei etwaigen Haftungsausschlüssen, da hier – insbesondere bei der Verwendung von AGB – Verbraucher stärker geschützt werden als Unternehmer (etwa durch die Klauselkontrolle des § 6 KSchG)[1866].

1157 Die Unterscheidung erfolgt hier nach dem Unternehmer/Verbraucher-Begriff des KSchG. Ausgangspunkt der Definition des Verbrauchergeschäfts ist der Begriff des Unternehmens in § 1 Abs 2 KSchG. Unternehmen ist hiernach „jede auf Dauer angelegte Organisation selbständiger wirtschaftlicher Tätigkeit, mag sie auch nicht auf Gewinn gerichtet sein. Juristische Personen öffentlichen Rechts gelten immer als Unternehmer". Damit ein Verbrauchergeschäft vorliegt, genügt es freilich nicht, dass es von einem Unternehmer geschlossen wurde; es muss überdies zum Betrieb des Unternehmens gehören (§ 1 Abs 1 Z 1 KSchG). Abgestellt wird dabei auf einen funktionalen Zusammenhang zwischen dem Unternehmen und dem Geschäft. Der Verbraucherbegriff wird im KSchG nur negativ definiert; Verbraucher ist, "für den dies" - nämlich der Tatbestand des § 1 Abs 1 Z 1 iVm Abs 2 KSchG - "nicht zutrifft". Verbraucher ist demnach jeder, der kein Unternehmen betreibt, sowie derjenige, für den das Geschäft nicht zum Betrieb des Unternehmens gehört.

1158 Ein Unterschied kann sich jedoch durch die Vorschriften zum Risk Management ergeben, durch die kommerziellen Nutzern grundsätzliche – nicht auf die IT spezialisierte – Pflichten zur Risikoabwehr übertragen werden.

1159 Weiters können sich aus Spezialnormen bestimmte Pflichten zu Schutzmaßnahmen ergeben, welche die Haftung des kommerziellen Nutzers beeinflussen können. So sind dies etwa die besonderen Bestimmungen des DSG zu den Datensicherheitsmaßnahmen (§ 14 DSG) sowie die besondere zivilrechtliche Haftungsbestimmung des § 33 DSG, die auch den Auftraggeber, also den Nutzer einer Datenanwendung trifft[1867]. Dies wird ergänzt durch eine Verwaltungsstrafbestimmung (§ 52 DSG) mit einem Strafrahmen von

[1866] Siehe etwa 4 Ob 98/04x. Darin hat der OGH die AGB-Klausel eines Telekommunikationsanbieters, wonach dieser „…keine Gewähr dafür leistet, dass die Software ununterbrochen bzw fehlerfrei läuft, frei von Produktmängeln ist oder für einen bestimmten Zweck nutzbar ist…" aufgehoben.

[1867] Siehe zum DSG etwa: *Jahnel*, Das Datenschutzgesetz 2000. Wichtige Neuerungen, wbl 2000, 49.

bis zu EUR 9445, wer die Sicherheitsmaßnahmen gemäß § 14 DSG „gröblich außer Acht lässt“. Die Erläuternden Bemerkungen zur Regierungsvorlage zum DSG führen dazu explizit aus[1868]: „Klargestellt sei, dass die Bestimmungen des DSG im Einzelfall auch als Schutzgesetz im Sinne des § 1311 ABGB greifen können.“

(2) Fallbeispiel: Virenschutz

1160 Die grundsätzliche Diskussion zu Sorgfaltspflichten im IT-Bereich lässt sich am besten anhand der Virenproblematik darstellen. In Ermangelung von Rechtsprechung bzw expliziten gesetzlichen Normen stellt dies eine Zusammenfassung der Literaturmeinung dar[1869]:

1161 Wenn ein Virus vorsätzlich eingeschleust wurde, ist die Situation klar: Der Geschädigte hat einen zivilrechtlichen Schadenersatzanspruch. Daneben liegt auch das strafrechtliche Delikt der Datenbeschädigung nach § 126a StGB vor, es kann daher auch der Staatsanwalt eingeschaltet werden. Hingegen ist die Rechtslage unklar, wenn der Virus unwissentlich verschickt wurde und womöglich der Absender nichts von der Virenverseuchung seines eigenen Computers gewusst hat, was bei den weit verbreiteten "E-Mail-Würmern" häufig vorkommt.

(a) Sorgfaltspflichten

1162 Voraussetzung jeder Haftung ist in diesem Fall, dass auf Seiten des Versenders zumindest Fahrlässigkeit vorliegt. Von einer solchen könnte man dann ausgehen, wenn es eine allgemeine Verpflichtung zur Virenvorsorge gibt. Eine solche kann man in gewissem Umfang durchaus fordern. Viren sind heute so verbreitet, dass bei Teilnahme am Internet nicht nur eine Eigengefährdung, sondern aufgrund der spezifischen Eigenschaften vieler E-Mail-Viren auch eine Gefährdung der E-Mail-Partner gegeben ist, wenn man unvorsichtig ist oder kein Virenschutzprogramm verwendet. Dies trifft sowohl für den Sender, als auch für den Empfänger zu.

1163 Ein Virenschutz ist umso wichtiger, je unerfahrener der Computerbesitzer bei der Verwendung von Software (Sicherheits-Updates) und dem Umgang mit potentiell gefährlichen Dateien ist. Ein erfahrener PC-Benutzer kann eher auf ein Virenprogramm verzichten, weil er verdächtige Dateien nicht öffnen wird.

[1868] 1613 d.B. (XX. GP).

[1869] Vgl dazu aus dem Schrifttum: *Rihl*, PC-Viren - eine Bedrohung für Großrechner? Sicherheitsmaßnahmen sollten durch unabhängige Stellen überprüft werden, SWK 1991, C 5; *Gantner*, Die Haftung der Krankenanstalten für Computerfehlleistungen, VR 2001, 222; *Gruber*, Computerviren und Schadenersatz, EDVuR 1990, 122.

1164 Zu einer Haftung des Versenders könnte auch die Aufnahme des Virenopfers in das Adressverzeichnis des Versenders führen, weil man dies als Eröffnung eines (E-Mail-)Verkehrs werten kann, was nach allgemeinen Rechtsregeln Verkehrssicherungspflichten nach sich zieht (ähnlich der Anlage eines Weges). Der Betreiber des Adressbuches könnte dadurch verpflichtet sein, Vorsorge zu treffen, dass die Personen, die in dieses Adressbuch aufgenommen werden, nicht durch Viren, die erfahrungsgemäß auf diese Adressbücher zugreifen und sich an die Adressaten versenden, geschädigt werden. Daneben könnten auch nebenvertragliche Schutzpflichten zum Tragen kommen, wenn der Virus im Rahmen einer Geschäftsbeziehung übermittelt wurde.

1165 Es ist durchaus denkbar, dass die Gerichte die Anforderungen an die Sorgfalt unterschiedlich handhaben, je nachdem, ob es sich um einen Privat-PC mit geringem E-Mail-Aufkommen oder um einen Mail-Server eines Unternehmens handelt. Immerhin unterliegen kommerzielle Nutzer als Unternehmer und Kaufleute auch in anderen Rechtsbereichen strengeren Sorgfaltsmaßstäben (siehe oben etwa DSG).

(b) Beweispflicht des Klägers

1166 Auch wenn nach diesen Kriterien ein vorwerfbarer Sorgfaltsverstoß vorliegt, ist Voraussetzung einer Haftung, dass der Geschädigte nachweist, dass der Virus tatsächlich von jenem stammt, der als Absender aufscheint. Dies wird oft nicht der Fall sein. Viele Viren fälschen nämlich den Absender, um ihre Herkunft zu verschleiern.

(c) Beweispflicht des Beklagten

1167 Gelingt der Nachweis der Verursachung durch den Beklagten, kann dieser den Beweis antreten, dass der Virus auch von einem gängigen Virenschutzprogramm nicht erkannt worden wäre (rechtmäßiges Alternativverhalten) und daher der Schaden auch bei ordnungsgemäßen Vorkehrungen entstanden wäre. Dabei stellt sich dann die Frage, wie aktuell ein Virenprogramm sein muss. Update-Zyklen sind heute meist wochenweise oder noch kürzer (laufendes Live-Update). Das könnte bedeuten, dass ein Virus, der bei üblicher Wartung von einem gängigen Virenprogramm erkannt wird, zur Haftung führen würde, nicht aber ein ganz neuer Virus, der von gängigen Programmen mit üblichem Update noch nicht erkannt wird.

(d) Mitverschulden des Geschädigten

1168 Schließlich stellt sich noch die Frage, ob die Anforderungen beim Absender höher angesetzt werden können als beim Empfänger. Wenn nämlich eine Pflicht zur allgemeinen Viren-Vorsorge bestehen sollte, trifft sie auch den Empfänger. Wenn dieser aber einen

aktuellen Virenschutz gehabt hätte, wie er auf Seiten des Absenders verlangt wird, wäre es gar nicht zur Infektion gekommen und es wäre kein Schaden entstanden. Man wird also auch von einem Mitverschulden des Klägers ausgehen müssen.

1169 Der Umstand, dass der Geschädigte den Schaden mit verursacht und -verschuldet hat, schließt einen Schadenersatzanspruch nicht aus, führt aber zur Reduzierung der Höhe nach.

(e) Das Problem der Rechtswidrigkeit

1170 Die Rechtswidrigkeit ist nach der Kausalität die zweite Haftungsvoraussetzung nach dem ABGB. Ein Verhalten ist rechtswidrig, wenn es gegen Gebote oder Verbote der Rechtsordnung oder gegen die guten Sitten verstößt (deliktische Haftung) oder wenn es vertragswidrig ist (vertragliche Haftung). Neben den ausdrücklich geregelten Geboten und Verboten kommen aber auch solche in Frage, die sich aus der Rechtsordnung als Ganzes ergeben. Daneben indiziert auch noch ein Verstoß gegen so genannte absolute Rechte, die Schutz gegen jedermann genießen, die Rechtswidrigkeit. Das führt teilweise zu einer komplizierten Interessenabwägung, bei der auch das allgemeine gesellschaftliche Interesse, die Zumutbarkeit und die Gefährlichkeit des Verhaltens und der Wert der bedrohten Güter berücksichtigt werden müssen.

1171 Der Schaden, der durch einen Virus ausgelöst wird, ist in der Regel kein Schaden an körperlichen Sachen, sondern ein Schaden an Daten und Programmen. Auch diese sind aber durch die Rechtsordnung geschützt, etwa durch das Strafgesetzbuch [Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB), Beschädigung von Daten und Computersystemen (§ 126a StGB), Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126b StGB), Betrügerischer Datenverarbeitungsmissbrauch (§ 148a StGB), Fälschung von Computerdaten (§ 225a StGB)], aber auch durch das Urheberrechtsgesetz. Dass das Strafgesetzbuch nur die vorsätzliche Datenbeschädigung unter Strafe stellt ändert nichts daran, dass damit Daten grundsätzlich auch zu den geschützten Rechtsgütern zählen.

1172 Damit kommt als nächste Hürde die Interessenabwägung. Dass ein Virus, speziell wenn er in das Netzwerk eines Unternehmens eingeschleust wird, erhebliche Schäden auslösen kann, ist allgemein bekannt. Der Wert der bedrohten Güter ist also erheblich. Aber wie sieht es auf der anderen Seite mit der Zumutbarkeit der Vorsorge aus. Das Internet würde wohl in die Bedeutungslosigkeit verfallen, wenn man verlangen würde, dass nur mehr im Umgang mit Viren ausgebildete Personen daran teilnehmen dürfen. Die Frage

ist aber, ob die technische Vorsorge mittels eines Virenschutzprogrammes zumutbar ist. Derartige Programme sind heutzutage entweder bereits Standardausrüstung eines Privat-PC, in einfacheren Versionen überall gratis zu bekommen und auch in professionellen Ausführungen nicht teuer, wenn man die Kosten von durchschnittlichen PC und Programmen oder PC-Spielen vergleicht. Eine Aufwendung von wenigen Prozenten des Gesamtsystems für die eigene Sicherheit und die aller Kommunikationspartner ist wohl zumutbar.

(f) Haftung des Providers

1173 So wie die Teilnehmer am E-Mailverkehr könnten auch die Betreiber der Mailserver (in der Regel die Provider) eine Virenüberprüfung vornehmen und damit Schäden bei den Verkehrsteilnehmern verhindern. Neben der Verkehrssicherungspflicht könnte ihre Haftung auch noch auf den Providervertrag gestützt werden, soweit nicht in den zugrunde liegenden AGB eine derartige Haftung ausgeschlossen ist. Allerdings sind die Provider und überhaupt alle Anbieter von Diensten der Informationsgesellschaft insofern privilegiert, als ihre Haftung beschränkt ist. Gemäß § 13 E-Commerce-Gesetz (ECG) haften sie nicht für die bloße Durchleitung und kurzzeitige Zwischenspeicherung von Informationen. Die Haftungsfreistellung gilt für den Bereich des Strafrechtes, des Schadenersatzrechtes und auch des Verwaltungsrechtes. Aufgrund der allgemeinen Formulierung und des Zweckes dieser Norm, der in der Förderung dieser Dienste liegt, ist davon auszugehen, dass auch Computerviren unter den Begriff "Information" fallen. Voraussetzung des Haftungsausschlusses ist, dass die Übermittlung der Informationen nicht vom Diensteanbieter selbst veranlasst, der Empfänger nicht ausgewählt und die Information nicht ausgewählt und nicht verändert wird. Diese Voraussetzungen liegen aber beim Betreiber eines Mailservers meist vor.

1174 Ob sich aus dem Providervertrag entsprechende Pflichten des Providers ergeben, wurde bis dato in Österreich noch nicht diskutiert. Stattdessen hat sich die bisherige Diskussion um die datenschutzrechtliche Zulässigkeit des Einsatzes von Filterprogrammen gedreht. Der Einsatz von Filtersoftware für unerwünschte Spam-Mails oder mit schädlichem Code verseuchte E-Mails ist vor dem Hintergrund des straf- und telekommunikationsrechtlichen Vertraulichkeitsschutzes der Telekommunikation sensibel. Die Literatur geht davon aus, dass der Einsatz von Filtersoftware durch den einzelnen User selbst (bzw das Empfänger-Unternehmen) rechtlich unbedenklich ist. Der Einsatz von Filtersoftware durch den Provider setzt dagegen grundsätzlich eine detaillierte Information

und die Einwilligung des betroffenen Kunden als (möglichen) E-Mail-Empfänger voraus. Der strafrechtliche Vertraulichkeitsschutz im StGB und im TKG 2003 erfordert darüber hinaus keine Zustimmung der Absender der von der Filtersoftware betroffenen E-Mails. Aus strafrechtlicher Sicht ist der Einsatz von Filtersoftware durch Internet Provider somit zulässig[1870].

c) Kommerzielle Nutzer mit besonderen Pflichten

(1) Überblick

1175 Soweit ersichtlich gibt es in der österreichischen Rechtsordnung hier nur in ausgewählten Bereichen speziell normierte Pflichten für kommerzielle Nutzer. Dies betrifft die folgenden Bereiche:

(2) Zertifizierungsdiensteanbieter (§ 7 SigG)

1176 Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, hat insbesondere folgende Pflichten:

- die erforderliche Zuverlässigkeit für die von ihm bereitgestellten Signatur- ode Zertifizierungsdienste aufzuweisen,
- den Betrieb eines schnellen und sicheren Verzeichnisdienstes sowie eines unverzüglichen und sicheren Widerrufsdienstes sicherzustellen,
- in qualifizierten Zertifikaten sowie für Verzeichnis- und Widerrufsdienste qualitätsgesicherte Zeitangaben (zB sichere Zeitstempel) zu verwenden und jedenfalls sicherzustellen, dass der Zeitpunkt der Ausstellung und des Widerrufs eines qualifizierten Zertifikats bestimmt werden kann,
- anhand eines amtlichen Lichtbildausweises die Identität und gegebenenfalls besondere rechtlich erhebliche Eigenschaften der Person, für die ein qualifiziertes Zertifikat ausgestellt wird, zuverlässig zu überprüfen,
- zuverlässiges Personal mit den für die bereitgestellten Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Managementfähigkeiten sowie mit Kenntnissen der Technologie elektronischer Signaturen und angemessener Sicherheitsverfahren, zu beschäftigen und geeignete Verwaltungs- und Managementverfahren, die anerkannten Normen entsprechen, einzuhalten,
- über ausreichende Finanzmittel zu verfügen, um den Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen zu entsprechen, sowie Vorsorge für die Befriedigung von Schadenersatzansprüchen, etwa durch Eingehen einer Haftpflichtversicherung, zu treffen.

[1870] *Otto/Parschalk*, Spam- und Virenfilter - eine Notwendigkeit im Graubereich des Rechts, wbl 2005, 10.

1177 Dazu kommt mit § 23 SigG eine besondere Haftungsbestimmung. Ein Zertifizierungsdiensteanbieter, der ein Zertifikat als qualifiziertes Zertifikat ausstellt oder für ein solches Zertifikat nach § 24 Abs. 2 Z 2 einsteht, haftet gegenüber jeder Person, die auf das Zertifikat vertraut, dafür, dass

1. alle Angaben im qualifizierten Zertifikat im Zeitpunkt seiner Ausstellung richtig sind und das Zertifikat alle für ein qualifiziertes Zertifikat vorgeschriebenen Angaben enthält,

2. der im qualifizierten Zertifikat angegebene Signator im Zeitpunkt der Ausstellung des Zertifikats im Besitz jener Signaturerstellungsdaten ist, die den im Zertifikat angegebenen Signaturprüfdaten entsprechen,

3. die Signaturerstellungsdaten und die ihnen zugeordneten Signaturprüfdaten einander bei Verwendung der von ihm bereitgestellten oder als geeignet bezeichneten Produkte und Verfahren in komplementärer Weise entsprechen,

4. das Zertifikat bei Vorliegen der Voraussetzungen unverzüglich widerrufen wird und die Widerrufsdienste verfügbar sind sowie

5. die Anforderungen des § 7 erfüllt und für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung und Speicherung von qualifizierten Zertifikaten technische Komponenten und Verfahren nach § 18 verwendet werden.

1178 Diese Haftung eines Zertifizierungsdiensteanbieters kann im vorhinein weder ausgeschlossen noch beschränkt werden. Bestimmungen des ABGB und anderer Rechtsvorschriften, nach denen Schäden in anderem Umfang oder von anderen Personen als nach diesem Bundesgesetz zu ersetzen sind, bleiben unberührt.

(3) Anbieter von Gesundheitsdienstleistungen (im wesentlichen Spitalserhalter)

1179 Besondere Pflichten nach dem Gesundheitstelematikgesetz (GTelG)[1871] betreffend insbesondere die Datensicherheit (2. Abschnitt) und das Informationsmanagement (3. Abschnitt). Mit dem GTelG werden ergänzende Datensicherheitsbestimmungen für den elektronischen Verkehr mit Gesundheitsdaten festgelegt sowie ein Informationsmanagement für Angelegenheiten der Gesundheitstelematik eingerichtet.

[1871] BGBl I 179/2004.

1180 Im Bereich der Datensicherheit (2. Abschnitt) umfasst dies etwa:

- Nachweis von Identität und Rolle
- Identität
- Rolle
- Vertraulichkeit
- Integrität
- Dokumentation

1181 Im Bereich des Informationsmanagements (3. Abschnitt) umfasst dies etwa:

- eHealth-Verzeichnisdienst
- Registrierungsverfahren
- Registrierungsstellen
- Monitoring
- Qualitätssicherung gesundheitsbezogener Web-Informationen

(4) Kritische Infrastrukturen

1182 Soweit ersichtlich bestehen hier für den IT-Bereich keine besonderen Normen. Österreich beobachtet hier den weiteren Prozess nach Vorstellung des Grünbuches der Kommission zum Schutz kritischer Infrastrukturen, KOM(2005) 576. In den EU-Gremien wird das österreichische Bundesministerium für Inneres (BMI) durch die Abteilung II/4 (Zivilschutz, Krisen- und Katastrophenschutzmanagement) vertreten[1872].

1183 Nach Auskunft des BMI gibt es noch keine auf IT-Risiken spezialisierten Überlegungen. Grundsätzlich lässt sich die Situation aber wie folgt zusammenfassen: Eine Infrastruktur gilt grundsätzlich dann als kritisch, wenn deren Ausfall oder Beeinträchtigung gravierende Folgen auf Staat und Gesellschaft haben können. Die Qualifizierung als kritisch erfolgt nach dem Grad ihrer Vernetzung, der wechselseitigen Abhängigkeit, Größe des Versorgungsgebiets und Bedeutung als Basis der Infrastruktur. In Österreich sind die als kritisch gewerteten zivilen Strukturen in fünf Schutzgruppen mit insgesamt ca. 180 Objekten eingeteilt. Sie umfassen die Organe der Gesetzgebung, oberste Organe der Vollziehung und der Gerichtsbarkeit, Anlagen der Energieversorgungsunternehmen, Informations- und Kommunikationseinrichtungen, Einrichtungen zur Versorgung der Be-

[1872] Siehe dazu http://www.bmi.gv.at/oeffentlsicherheit/2006/05_06/BVT.pdf.

völkerung mit lebensnotwendigen Gütern (z.B. Lebensmittelgroßlager, Wassergroßversorger) sowie Anlagen zur Aufrechterhaltung wesentlicher Verkehrsströme (z.B. Flughäfen, wichtige Donaubrücken, wesentliche Verkehrsknotenpunkte, ÖBB). Zusätzlich werden die zu schützenden Objekte in die Wertigkeitsstufe A bei überregionaler und B bei regionaler Bedeutung eingeteilt. A-wertige Objekte sind in einem Anlassfall unbedingt zu schützen. Die Einstufung der Objekte erfolgt über Vorschlag der zuständigen Sicherheitsdirektion im Einvernehmen mit dem zuständigen Amt der Landesregierung und der betroffenen Struktur beziehungsweise aufgrund einer generellen Bewertung durch das Bundesministerium für Inneres.

1184 In Österreich werden im Rahmen des derzeitigen Schutzkonzepts für Strukturen, deren Schutz vorgesehen ist, von den Sicherheitsdirektionen Objektschutzblätter angelegt. Dabei wird unter anderem untersucht, ob und durch welche baulichen Maßnahmen und technischen Vorsorgen die Sicherheit verbessert werden kann. Die einzelnen Objektschutzblätter werden vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) im „Objektschutzkatalog“ gesammelt. Weiters werden Risiko- und Gefährdungsanalysen erstellt, um festzustellen, welche Objekte einem erhöhten Risiko ausgesetzt sind, um die Prioritätsstufen festzulegen und um gezielte Schutzkonzepte zu erstellen.

3. IT-Intermediäre (insb. Host-/Content-/Access-Provider)

1185 Über die Umsetzung der E-Commerce-Richtlinie hinaus bestehen keine besonderen Privilegierungen. Interessant ist, dass Österreich bei der Umsetzung zusätzlich eine Haftungsprivilegierung für Suchmaschinenbetreiber (§ 14 ECG) sowie für Linksetzer (§ 17 ECG) eingeführt hat.

1186 Betrachtet man die bisherige Rechtsprechung, so bestehen keine Entscheidungen zu Fragen der IT-Sicherheitspflichten von Intermediären sondern ausschließlich zur Frage der möglichen Verantwortung für fremde Inhalte, zB:

- Google Haftung für Adwords: OGH, Beschluss vom 19.12.2005, 4 Ob 194/05s
- Haftung des Host-Providers für Wettbewerbsverletzungen auf Kunden-Websites: OGH, Urteil vom 6.7.2004, 4 Ob 66/04s
- Haftung des Contentproviders für ehrenrührigen Artikel im Online-Archiv: OGH, Urteil vom 19.2.2004, 6 Ob 190/03i

- Haftung des Content-Providers für übernommenes Online-Archiv: OGH, Urteil vom 11.12.2003, 6 Ob 218/03g
- Vorarlberg Online - Haftung für Online-Diskussionsforum: Urteil des OLG Wien vom 4.3.2002, 18 Bs 20/02

1187 Zur allgemeinen Haftung siehe oben unter Rn. 660 ff.

1188 Betreffend besonderer Pflichten von Intermediären ergeben sich hier – abgesehen von den in Umsetzung der E-Commerce-Richtlinie normierten Pflichten in § 18 ECG – nur solche aus dem TKG, das in der Regel auch auf Internet-Provider anzuwenden ist, da diese (auch) TK-Anbieter sind. Die Anbieter treffen nach verschiedenen gesetzlichen Regelungen Auskunfts- und Mitwirkungspflichten (idR betreffend Name, Anschrift und Teilnehmernummer)[1873]; sie sind jedoch nur dann zur Übermittlung von Daten verpflichtet (und berechtigt), wenn hierfür eine gesetzliche Verpflichtung besteht. Die in der Praxis relevanteste und gleichzeitig weitreichendste Bestimmung findet sich in der Strafprozessordnung (StPO): Gemäß § 149a StPO sind die Anbieter unter bestimmten Voraussetzungen zur Auskunft über Stamm-, Verkehrs- und Inhaltsdaten verpflichtet (auch Fangschaltung genannt). Allerdings besteht diese Verpflichtung nur soweit, als diese Daten tatsächlich vorhanden sind; es besteht weder eine Verpflichtung noch eine rechtlich zulässige Möglichkeit zur Speicherung dieser Daten auf Vorrat (für einen etwaigen Anlassfall) oder zur Überwachung dieser Daten. Die rechtlich zulässigen Möglichkeiten zur Speicherung der verschiedenen Datenarten sind wie oben dargestellt sogar stark eingeschränkt.

1189 Zur Überwachung des Fernmeldeverkehrs sind die Anbieter gemäß § 94 Abs 1 TKG 2003 nur im Anwendungsbereich der Überwachungsverordnung (ÜVO) verpflichtet[1874]. Unter die ÜVO fallen ausschließlich Anbieter, die einen öffentlichen Telefondienst erbringen und in deren Netzen physikalische Teilnehmeranschlüsse vorhanden sind. Diese Anbieter haben nach den Bestimmungen der StPO – im Einzelfall (§ 3 Abs 1 ÜVO) - bei konkretem bzw dringendem Verdacht auf die Begehung schwerer strafbarer Vorsatztaten Folgendes zu ermöglichen:

- die Überwachung und Aufzeichnung der von ihren Teilnehmeranschlüssen ein- und abgehenden Verbindungen, samt Verbindungen zu Datenspeichern und

[1873] Vgl zB § 53 Abs 3a SPG, § 90 Abs 6 TKG 2003, § 18 Abs 3 und 4 ECG, § 87b Abs 3 UrhG, § 99 FinStrG, § 22 Abs 2a MBG sowie § 1 Abs 3 und § 26 DSG 2000.

[1874] Siehe dazu *Otto/Seitlinger*, Die "Spitzelrichtlinie": Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG, MR 2006, 227.

- die Bereitstellung von Inhalts-, Vermittlungs- und sonstigen Daten soweit wirtschaftlich und technisch zumutbar.

1190 Eine Überwachung ist nur zulässig, soweit die Verhältnismäßigkeit zum Zweck der Maßnahme bewahrt wird. Für die Anordnungen im Rahmen der StPO ist (je nach Einzelfall) der Untersuchungsrichter oder die Ratskammer bzw im Stadium der Hauptverhandlung das erkennende Gericht zuständig.

4. Organisationspflichten und Risk Management

a) Allgemein: Bereiche (Branchen) mit Organisationspflichten bzw. Risikomanagement

1191 Hier bestehen die allgemeinen Vorschriften zum Risikomanagement durch den Vorstand/Geschäftsführung im Rahmen der Sorgfaltspflicht (§ 84 Abs 1 AktG, § 25 Abs 1 GmbHG). Dies umfasst etwa die Etablierung eines geeigneten Risiko-Monitorings durch ein internes Kontrollsystem (§ 82 AktG, § 22 GmbHG).

1192 Hinzu kommen Prüfpflichten der Überwachungsorgane, v.a. Aufsichtsrat (§ 99 AktG, § 30j GmbHG). Weiters relevant ist der Österreichische Corporate Governance Kodex vom 1.10.2002 (revidiert am 22.2.2005): vorrangig an börsenotierte Gesellschaften gerichtet, doch auch für nicht börsenotierten Aktiengesellschaften relevant

1193 Relevant ist an dieser Stelle auch das in Österreich mit 1.1.2006 eingeführte "Unternehmensstrafrecht" durch das Bundesgesetz über die Verantwortlichkeit von Verbänden für Straftaten[1875].

1194 Unternehmen, deren leitende Angestellte oder Mitarbeiter eine Straftat begehen - zB Datenverwendung in Gewinn- oder Schädigungsabsicht (§ 51 DSG 2000) können in solch einem Fall zu einer Geldstrafe von bis zu EUR 550.000.- verurteilt werden. Dies auch bloß weil das Unternehmen nicht zB durch entsprechende organisatorische oder technische Maßnahmen verhindert hat (siehe solche zB in § 14 DSG 2000), dass solche Straftaten von Mitarbeitern begangen werden können.

b) IT-Bereich: Normen bezüglich Organisationspflichten (inkl. Risk Management)

1195 Der Einfluss von Standards und Normen ist hier wesentlich, da diese im Streitfall herangezogen werden, um den Stand der Technik zu bestimmen.

[1875] BGBl I 151/2005.

1196 Im Auftrag der IKT-Stabsstelle des Bundes wurde das "Österreichische IT-Sicherheitshandbuch" im Jahr 2003 von A-SIT überarbeitet und 2004 aktualisiert[1876]. Dabei wurden die beiden Teile 1 ("IT-Sicherheitsmanagement") und insbesondere Teil 2 ("IT-Sicherheitsmaßnahmen") auf den neuesten Stand der Technik gebracht. Aktuelle E-Government Initiativen und Empfehlungen des IKT-Boards wurden eingearbeitet. Es richtet sich sowohl an die öffentliche Verwaltung, als auch an die Wirtschaft. Zur Unterstützung bei der Etablierung und Umsetzung von IT-Sicherheit umfasst es schwerpunktmäßig:

- die Ermittlung der relevanten IT-Sicherheitsziele und -strategien
- die Erstellung einer organisationsspezifischen IT-Sicherheitspolitik
- die Auswahl und Realisierung geeigneter Sicherheitsmaßnahmen
- die Gewährleistung der IT-Sicherheit im laufenden Betrieb
- eine Sammlung von Best-Practices im Bereich der IT-Sicherheit

1197 Das IT-Sicherheitshandbuch besteht aus zwei Teilen:

1198 Der erste Teil trägt den Titel "IT-Sicherheitsmanagement" und beinhaltet konkret Anleitungen zur Etablierung eines umfassenden und kontinuierlichen IT Sicherheitsprozesses innerhalb einer Behörde, Organisation oder eines Wirtschaftunternehmens.

1199 Der zweite Teil mit dem Titel "IT-Sicherheitsmaßnahmen" beinhaltet die Beschreibung grundlegender Maßnahmen auf organisatorischer, personeller, infrastruktureller und technischer Ebene. Inhaltliches Ziel ist die Gewährleistung angemessener Standardsicherheitsmaßnahmen für IT-Systeme. Besondere Betonung wird dabei einerseits auf die spezifisch österreichischen Anforderungen, Regelungen und Rahmenbedingungen, andererseits auch auf die durchgängige Einbeziehung des gesamten Lebenszyklus der jeweiligen Systeme, von der Entwicklung bis zur Beendigung des Betriebs, gelegt.

5. Genehmigungen und Zertifizierungen

1200 Die (haftungsrechtliche) Wirkung von Zertifizierungen wurde bereits oben unter Rn 156 beschrieben. In Österreich sind soweit ersichtlich folgende Zertifizierungen bzw Zertifizierungsstellen im IT Bereich relevant:

[1876] Abrufbar unter http://www.a-sit.at/de/sicherheitsbegleitung/sicherheitshandbuch/index.php.

a) A-SIT

1201 Das A-SIT ist als Überwachungsstelle tätig. Das A-SIT hat die Akkreditierung als Überwachungsstelle angestrebt und mit Wirksamkeit vom 25. Oktober 2004 gemäß Akkreditierungsgesetz (AkkG) die Bestätigung vom Bundesministerium für Wirtschaft und Arbeit erhalten. Die Akkreditierung entspricht den Anforderungen der ISO/IEC 17020. Die Tätigkeitsfelder (Akkreditierungsumfang) umfassen dabei:

- Überwachung der IT-Sicherheit von elektronischen Zahlungssystemen (siehe im besonderen unten)
- Überwachung der Sicherheit von IT-Produkten und IT-Systemen

1202 Als Ergebnis der Überwachungen stellt A-SIT für den Auftraggeber Inspektionsberichte bzw. Inspektionsbescheinigungen aus. Grundlagen (normative Dokumente) hierfür sind die Aufsichtsgrundsätze für elektronische Zahlungssysteme der Oesterreichischen Nationalbank (OeNB) sowie das IT-Sicherheitshandbuch (Teil 1 und Teil 2)

b) Zertifizierung nach ISO 17799

1203 Im Zentrum steht hier die Zertifizierung nach ISO 17799. Hier erfolgt etwa eine Zertifizierung durch den TÜV mit der Verleihung des TÜV Österreich Zertifikats. Den Schlusspunkt der Einführung eines Informationssicherheitssystems nach ISO 17799 bildet das Zertifizierungs-Audit. Im Rahmen dieser Vor-Ort Überprüfung werden alle Bereiche der Norm von den Auditoren nach einem im Vorhinein festgelegten Auditplan überprüft. Im Rahmen einer Abschlussbesprechung mit allen beteiligten Personen werden die Ergebnisse des Audits vorgestellt. Ein positiver Abschlussbericht des Auditors bildet die Grundlage für die Verleihung des Zertifikats. Anschließend erfolgen jährliche Audits zur Verlängerung des Zertifikats um ein Jahr. Diese umfassen jedoch nicht den Gesamtbereich der Norm sondern es werden gezielt Teilbereiche nach im Vorhinein festgelegten Auditplänen geprüft.

c) Technischen Regelwerk ONR 17700 - „Sicherheitstechnische Anforderungen an Webapplikationen“

1204 Das Österreichische Normungsinstitut bietet mit dem Technischen Regelwerk ONR 17700 - „Sicherheitstechnische Anforderungen an Webapplikationen“ die Grundlage für einen sicheren Betrieb und die Zertifizierung von Webapplikationen. Ausgangsbasis für eine erfolgreiche Zertifizierung sind vor allem der Umgang mit sensiblen Benutzerdaten, sichere Konfigurationseinstellungen, Zugriffsbeschränkungen und der Einsatz von kryptographischen Kontrollen, um die Vertraulichkeit zu gewährleisten.

d) Bescheinigung nach dem SigG

1205 Im österreichischen Signaturgesetz (SigG §18(5) bzw. der EU-Signaturrichtlinie (Art. 3(4)) ist festgelegt, dass die technischen Komponenten und Verfahren für die Erstellung sicherer elektronischer Signaturen nach dem Stand der Technik bescheinigt werden müssen.

1206 Dies hat durch eine Bestätigungsstelle (SigG §19) zu erfolgen. In Österreich ist dies A-SIT.

1207 Von einer Bestätigungsstelle bescheinigungspflichtige Komponenten und Verfahren sind solche, welche die Signaturerstellungsdaten - in der Praxis den privaten (geheimen) Schlüssel - verarbeiten, erzeugen oder speichern (Signaturerstellungseinheiten).

1208 Für Signaturprodukte in der Systemumgebung der Signaturerstellungseinheit ist keine Bescheinigung erforderlich (z.B. "Viewer" und "Chipkartenleser").

1209 Bei Aufnahme oder Änderung eines Zertifizierungsdienstes sind der Aufsichtsstelle für elektronische Signaturen Bescheinigungen vorzulegen. Ein Fehlen derartiger Bescheinigungen stellt einen wesentlichen Sicherheitsmangel dar.

1210 Bescheinigungen werden auf Antrag durch A-SIT gegen Kostenersatz durchgeführt.

1211 Für Signaturkomponenten, welche nicht gemäß § 18(5) SigG bescheinigungspflichtig sind, die aber aufgrund anderer Gesetzesstellen bedeutsam sind, können Bestätigungen gesetzesrelevanter Eigenschaften laut Signaturgesetz, Signaturverordnung , Änderungen der Signaturverordnung bzw. EU-Signaturrichtlinie ausgestellt werden. Das gilt beispielsweise für Signaturerstellungseinheiten von Zertifizierungsdiensteanbietern.

1212 Sie werden auf Antrag durch A-SIT gegen Kostenersatz durchgeführt. Die Tätigkeit seitens A-SIT endet entweder mit dem Ausstellen der Bestätigung oder dem Zurückziehen des Antrags. Bei positivem Abschluss werden die Bestätigung sowie ein Bestätigungsbericht ausgestellt.

e) Überprüfung von Zahlungssystemen

1213 Eine besondere Bestimmung besteht im Bereich der Zahlungssysteme. Die Oesterreichische Nationalbank (OeNB) hat den gesetzlichen Auftrag (§ 44a Nationalbankgesetz), die Aufsicht über die österreichischen Zahlungssysteme auszuüben.

1214 A-SIT wird von der OeNB im Rahmen der Überprüfung der technischen und organisatorischen Sicherheit der Zahlungssysteme in seiner Funktion als Überwachungsstelle für

elektronische Zahlungssysteme im Sinne des Akkreditierungsgesetzes (AkkG) beigezogen.

1215 Die von A-SIT im Zuge dieser Tätigkeit erstellten Inspektionsberichte umfassen insbesondere die Beurteilung der

- Gewährleistung der Betriebssicherheit
- Verfügbarkeit
- Vertraulichkeit und Integrität
- der Zahlungssysteme zum Inhalt.

f) Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen und Anlagen gemäß Informationssicherheitsgesetz (InfoSiG) [1877]

1216 Die Bestimmungen der §§ 11 bis 13 des InfoSiG regeln die Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen, Einrichtungen und Anlagen, die gemäß § 14 zur sicheren Verwendung klassifizierter Informationen für die Teilnahme an industriellen Tätigkeiten und Forschungstätigkeiten verpflichtet sind. Die in Ausführung dazu ergangene Verordnung[1878]regelt die Pflichten bei der elektronischen Verarbeitung klassifizierter Informationen mittels elektronischer Büro- und EDV-Geräte.

6. Hoheitliche Befugnisse

a) Hoheitliche Befugnisse, die staatliches Eingreifen im Falle von Gefahr im Bereich IT-Sicherheit ermöglichen

1217 In diesem Bereich sind folgende rechtliche Bestimmungen zu nennen:

(1) Produktsicherheitsgesetz

1218 Folgende Voraussetzungen müssen nach PSG gegeben sein:

1. die von einem Produkt ausgehende Gefahr für das Leben oder die Gesundheit von Menschen entweder durch ein Gutachten einer in- oder ausländischen akkreditierten Prüfstelle oder eines/r befugten Ziviltechnikers/Ziviltechnikerin festgestellt wurde oder

[1877] BGBl. I 23/2002 idgF.

[1878] BGBl. II 548/2003.

2. der begründete Verdacht besteht, dass die Verwendung eines Produktes eine ernste Gefahr für das Leben oder die Gesundheit von Menschen darstellt oder

3. das Inverkehrbringen eines Produktes offenkundig einer gemäß § 11 angeordneten Maßnahme widerspricht oder

4. das Produkt bereits Gegenstand einer Maßnahme in einem Vertragsstaat des EWR war und diese Maßnahme im Rahmen des RAPEX-Verfahrens aufgrund der Richtlinie 2001/95/EG über die allgemeine Produktsicherheit notifiziert wurde.

1219 Wenn dies vorliegt dann können die Behörden vorläufige Maßnahmen zur Gefahrenabwehr (§ 15 PSG) ergreifen.

(2) Hoheitliche Befugnisse der Aufsichtsstelle für Zertifizierungsdiensteanbieter (§ 13 SigG)

1220 Aufsichtsstelle ist die Telekom-Control-Kommission (§ 110 TKG). Ihr obliegt die laufende Aufsicht über die Einhaltung der Bestimmungen des SigG und der auf seiner Grundlage ergangenen Verordnungen. Die Aufsichtsstelle hat insbesondere

1. die Umsetzung der Angaben im Sicherheits- und im Zertifizierungskonzept zu überprüfen,

2. im Fall der Bereitstellung sicherer elektronischer Signaturen die Verwendung geeigneter technischer Komponenten und Verfahren (§ 18) zu überwachen,

3. Zertifizierungsdiensteanbieter nach § 17 zu akkreditieren und

4. die organisatorische Aufsicht über Bestätigungsstellen (§ 19) durchzuführen.

(3) Kontrollbefugnisse der Datenschutzkommission nach § 30 DSG

1221 Die Datenschutzkommission kann im Fall eines begründeten Verdachtes auf Verletzung der im § 30 Abs. 1 DSG 2000 genannten Rechte und Pflichten Datenanwendungen überprüfen. Hierbei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenanwendungen und diesbezügliche Unterlagen begehren. Zum Zweck der Einschau ist die Datenschutzkommission nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) berechtigt, Räume, in welchen Datenanwendungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträ-

gern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen. Der Auftraggeber (Dienstleister) hat die für die Einschau notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Auftraggebers (Dienstleisters) und Dritter auszuüben.

(4) Allgemeine Regeln (Auffangtatbestände, Generalklauseln), die den hoheitlichen Eingriff erlauben

1222 Hier kommt das Sicherheitspolizeigesetz (SPG)[1879] zur Anwendung. Dieses ermöglicht folgende Eingriffe:

(a) § 32 SPG: Eingriffe in Rechtsgüter im Rahmen der ersten allgemeinen Hilfeleistungspflicht

1223 Soweit es zur Hilfeleistung im Sinne von § 19 erforderlich ist, sind die Organe des öffentlichen Sicherheitsdienstes ermächtigt, in Rechtsgüter einzugreifen, sofern der abzuwendende Schaden die Rechtsgutsverletzung offenkundig und erheblich übersteigt.

(b) § 39 SPG: Betreten und Durchsuchen von Grundstücken, Räumen und Fahrzeugen

1224 Die Organe des öffentlichen Sicherheitsdienstes sind ermächtigt, Grundstücke, Räume sowie Luft-, Land- und Wasserfahrzeuge (Fahrzeuge) zu betreten, sofern dies zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder zur Abwehr eines gefährlichen Angriffs erforderlich ist.

(c) § 42 SPG: Sicherstellen von Sachen

1225 Die Organe des öffentlichen Sicherheitsdienstes sind ermächtigt, Sachen sicherzustellen,

1. wenn dies bei gefährlichen Angriffen dazu dient, eine (weitere) Bedrohung des Lebens, der Gesundheit, der Freiheit oder des Eigentums von Menschen zu verhindern;

2. die sich in der Gewahrsame eines Festgenommenen befinden und besonders geeignet sind, während dessen Anhaltung a) seine eigene oder die körperliche Sicherheit anderer unmittelbar zu gefährden oder b) ihm die Flucht zu ermöglichen oder zu erleichtern;

3. denen unbefugte Beschädigung oder Wegnahme droht, sofern der Eigentümer oder rechtmäßige Besitzer nicht in der Lage ist, selbst für ihren Schutz zu sorgen;

4. die von ihnen aufgefunden werden und sich in niemandes Gewahrsame befinden.

[1879] BGBl I 104/2002 idgF.

7. Konkrete Bedrohungen

a) Grundlagen

1226 Neben den international bekannt gewordenen Bedrohungsfällen (etwa international verbreitete Computerviren) hat es auch einige österreich-spezifische Bedrohungsfälle gegeben. Zu nennen ist hier etwa im Jahr 2004 der Ausfall von großen Teilen des Festnetzes der Telekom Austria und das Mobilfunknetz "A1" der Mobilkom. Als Grund führte die Telekom einen Computerfehler an.

1227 Die Tragweite des Haftungsthemas zeigte sich im September 2004 bei der Bank für Arbeit und Wirtschaft (BAWAG). Im Zuge eines Austausches des Kernbankensystems zur Einführung eines einheitlichen EDV-Systems für die BAWAG und die PSK sind tausende Buchungen verloren gegangen, das heißt, diese Buchungen wurden nicht durchgeführt. Der Fehler wurde erst von einem Kunden entdeckt, als dieser sich einen Kontoauszug holen wollte. Der Grund der Störung lag in einem Computerfehler. Die Behebung des Problems dauerte mehrere Tage. Der Fall gelangte in die Medien[1880]. Abgesehen vom Imageschaden der BAWAG sind bei einzelnen Kunden auch Schäden durch verlorene Überweisungen entstanden (etwa Verrechnung von Verzugszinsen). Laut Medienberichten wurden diese Schäden von der BAWAG ausnahmslos ersetzt. Über die Schadenshöhe wurde nichts bekannt.

1228 Die zentrale Reaktion des österreichischen Gesetzgebers auf Bedrohungen im IT-Bereich war das Strafrechtsänderungsgesetz 2002[1881]. Mit diesem Gesetz (BGBl I 134/2002), das am 1.10.2002 in Kraft getreten ist, wurde in erster Linie die Cyber-Crime-Konvention umgesetzt; hiezu wurden im Strafgesetzbuch (StGB) zum Teil neue Delikte geschaffen und zum Teil bestehende Strafbestimmungen gegen Missbrauch von Computern u.ä. angepasst. Diese sind:

(1) Widerrechtlicher Zugriff auf ein Computersystem § 118a

1229 Danach ist nicht jedes Hacking strafbar. Der nicht über das System verfügungsberechtigte Täter muss zunächst eine Sperre (Passwort beim System oder bei einzelner Datei, Firewall) überwinden und dies muss in der Absicht erfolgen, Daten einem Dritten zu-

[1880] Siehe etwa Tageszeitung Kurier 2.10.2004.

[1881] Siehe dazu allgemein: *Maleczky*, Das Strafrechtsänderungsgesetz 2002, JAP 2002/2003, 115; im besonderen zum Computerstrafrecht: *Ebensperger,* Internet und Strafrecht, in *Brenn*, ECG (2002) 118 (insb 129 ff); *Plöckinger,* Zur Zuständigkeit österreichischer Gerichte bei Straftaten im Internet, ÖJZ 2001, 798.

gänglich zu machen oder sich einen Vermögensvorteil zu verschaffen oder einem anderen einen solchen Nachteil zuzufügen. Der Täter muss auch tatsächlich in das System eindringen und innerhalb des Systems tätig werden können. Unter Computersystem versteht man gem. § 74 Abs. 1 Z 8 sowohl Netzwerke als auch einzelne PC oder Notebooks. Es handelt sich um ein Ermächtigungsdelikt, d.h. der Staatsanwalt wird nur tätig, wenn der Verletzte dies will und seine Zustimmung erteilt.

(2) Verletzung des Telekommunikationsgeheimnisses § 119

1230 Diese Bestimmung schützt das auch unter Grundrechtsschutz stehende Fernmeldegeheimnis (Art. 10a StGG). Die Abhörvorrichtung kann ein Gerät sein, aber auch eine Software, wie ein Trojaner, der zum Zwecke des Ausspionierens des E-Mail-Verkehrs eingeschleust wurde. Nach dieser Bestimmung nicht geschützt sind jedoch gespeicherte oder noch nicht abgeschickte E-Mails (Entwürfe), weil nur der Übertragungsweg geschützt ist. Als Schutz kommt bei solchen aber indirekt § 118a in Frage. Auch dieses Delikt ist ein Ermächtigungsdelikt.

(3) Missbräuchliches Abfangen von Daten § 119a

1231 Nach dieser Bestimmung sind jegliche Daten geschützt (nicht nur Nachrichten wie in § 119. Strafbar ist nicht nur das Abfangen auf dem eigentlichen Übertragungsweg, sondern auch das Ausspionieren über die Abstrahlung (Bildschirm, Tastatur), dafür aber nur bei Gewinnerzielungs- oder Schädigungsabsicht. Auch dieses Delikt ist ein Ermächtigungsdelikt.

(4) Missbrauch von Tonaufnahme- oder Abhörgeräten § 120

1232 Hier ist für den Internetbereich vor allem Abs. 2a interessant. Danach wäre es etwa strafbar (Privatanklagedelikt), wenn jemand irrtümlich eine E-Mail erhält und diese einem Dritten zugänglich macht. Dieses Delikt ist ein Privatanklagedelikt, d.h. der Verletzte muss selbst bei Gericht die Bestrafung beantragen, es geht weder eine Anzeige an die Polizei noch an die Staatsanwaltschaft.

(5) Datenbeschädigung § 126a

1233 Das ist ein Sonderfall der Sachbeschädigung. Werden die Daten samt Datenträger zerstört, kommen § 125 und § 126a parallel zur Anwendung. Voraussetzung ist, dass die Daten zumindest einen gewissen Vermögenswert aufweisen. Eine Veränderung ist nur

strafbar, wenn damit der bestimmungsgemäße Gebrauch verhindert oder beeinträchtigt wird.

(6) Störung der Funktionsfähigkeit von Computersystemen § 126b

1234 Dabei ist der Angriff auf die Störung des Systems selbst gerichtet. So kann etwa ein Computer bei DOS- (Denial of Service) Attacken so mit Datenmengen überfüttert werden, dass er letztlich abstürzt. Voraussetzung für die Strafbarkeit ist eine schwere Störung, die aber im Gesetz nicht definiert ist. Es genügt bedingter Vorsatz, d.h. es genügt, dass der Täter eine schwere Störung ernstlich für möglich hält und sich damit abfindet.

(7) Missbrauch von Zugangsdaten § 126c

1235 Dieses Delikt umfasst Herstellung, Beschaffung und Besitz von Crackprogrammen, Zugangscodes und Passwörtern, aber nur dann, wenn dies zum Zwecke des Verschaffens eines illegalen Zuganges erfolgt.

b) Viren

1236 Siehe oben unter Rn 58.

c) Phishing

1237 Wendet man aus aktuellem Anlass die strafrechtlichen Bestimmungen auf Phishing an, so kommen einige strafrechtliche Tatbestände wie § 108 (1) StGB iVm § 1 (1) DSG, die Datenfälschung des § 225a StGB und ggf der Missbrauch von Zugangsdaten (§ 126c Abs 1 Z 2 StGB) für eine Strafbarkeit des Täters in Betracht kommen. Die Verwertung der erlangten Daten wirft hinsichtlich des Betrugs (§ 146) bzw des betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) keine weiteren Schwierigkeiten auf.

d) Dialer

1238 Nur im Bereich der Dialer gab es eine ausdrückliche normative Reaktion durch die Sechste Verordnung der Rundfunk und Telekom Regulierungs-GmbH, mit der Bestimmungen für Kommunikationsparameter, Entgelte und Mehrwertdienste (KEM-V) festgelegt werden[1882].

1239 Gemäß § 106 KEM-V gilt für die Erbringung eines Mehrwertdienstes unter Verwendung eines Dialers ein Opt-in des Teilnehmers in Richtung des Kommunikationsdienstebetreibers.

[1882] Kundgemacht am 12.Mai 2004 im Amtsblatt zur Wiener Zeitung; dazu: *Wessely*, Neues von der Mehrwertdienste-Front, MR 2004, 149; *Schauhuber*, Übersicht über die Kem-V, MR 2004, 292.

1240 Dialer dürfen nur im Rufnummernbereich 0939 angeboten werden.

1241 Bei der Erbringung eines Mehrwertdienstes unter Verwendung eines Dialers sind sechs Erfordernisse zu erfüllen:

- Vor dem Aufbau einer Verbindung muss der Preis in Euro pro Minute, der Dienstleister und dessen ladungsfähige Anschrift sowie die vollständige Nummer angezeigt werden. Es muss angegeben werden, dass bei Inanspruchnahme des Dienstes eine Telefonverbindung zu einer Mehrwertdiensterufnummer aufgebaut wird und die Bezahlung über die Telefonrechnung erfolgt.
- Die Verbindung darf nur nach einer Aktion aufgebaut werden, durch die der Nutzer die Kenntnisnahme der Informationen bestätigt. Für den Nutzer muss die Möglichkeit bestehen, den Verbindungsaufbau endgültig, einfach und kostenfrei abzulehnen.
- Die Informationen müssen auch in deutscher Sprache in klar lesbarer und zum Hintergrund kontrastreicher Schrift dargestellt werden.
- Über den Dial-Up-Zugang dürfen nur die kostenpflichtigen Inhalte des Dienstleisters abgerufen werden können, die über einen herkömmlichen Internetzugang nicht frei zugänglich sind.
- Die Speicherung des Dialer-Programmes am Endgerät des Nutzers darf nur nach einer zustimmenden Aktion des Nutzers erfolgen und die Entfernung des Dialer-Programmes muss einfach möglich sein.
- Der aktuelle Gesamtpreis und die Verbindungsdauer müssen permanent sichtbar angezeigt werden und über eine permanent sichtbare Schaltfläche muss jederzeit abgebrochen werden können.

8. Internationale Regelungen

1242 Von besonderer Bedeutung ist hier die ISO17799 – „Information technology - Code of practice for information security management". 2003 veröffentlichte das Österreichische Normungsinstitut die ÖNORM ISO/IEC 17799 („Informationstechnologie – Leitfaden für das Management der Informationssicherheit"), womit die internationale ISO-Norm den Status einer Österreichischen Norm erhielt.

1243 Die ISO begründet die Pflicht, alle auf die Sicherheit der Information anwendbaren Gesetze zu befolgen und systematisiert somit das so genannte Recht der Informationstechnologien. Der Schwerpunkt wird jedoch auf die Verwaltung der Sicherheit der Information gesetzt. Die Norm über die Sicherheitsverwaltung der Information setzt in seinem zwölften Kapitel dabei die Voraussetzungen fest, die jede Organisation erfüllen muss, um das gewünschte Zertifikat zu erlangen.

1244 Aus juristischer Sicht werden in der ISO folgende Rechtsgebiete tangiert: Datenschutz, Urheberrecht, E-Commerce, Arbeitsrecht, sowie das Prozessrecht, sofern es die Thematik der Beweiskraft der Information betrifft.

1245 Für kommerzielle Anbieter ist die „Sachverständigenhaftung“ des: § 1299 ABGB zu beachten: „Wer sich zu einem Amte, zu einer Kunst, zu einem Gewerbe oder Handwerke öffentlich bekennet; [...] gibt dadurch zu erkennen, dass er sich den notwendigen Fleiß und die erforderlichen, nicht gewöhnlichen, Kenntnisse zutraue; er muss daher den Mangel derselben vertreten.“ Den Normen kommt bei der Beurteilung, ob eine Sorgfaltspflichtverletzung vorliegt große Bedeutung zu. Die von den Gerichten bestellten Sachverständigen bestimmen anhand der Norm den in einer Branche geltenden Stand der Technik, der wiederum für die besondere Haftung nach § 1299 ABGB als objektiver Maßstab relevant ist.

XVI. IT Security Liability in the UK**

1246 This Report attempts to outline and analyse how UK law[1883] regulates IT security, particularly with respect to liability. Because it is aimed at a non-UK audience, it begins by explaining the basic structure of UK liability law which applies to all products and services. It then examines the statutory obligations which are particularly applicable to IT producers and users – as the reader will see, these are not extensive. The UK has a tradition of regulating activities at the level of the principles to be followed when undertaking those activities, rather than prescribing precisely what must be done, and the regulation of IT security follows this tradition.

1247 The third part of the Report explains the liability regime for suppliers of IT products and services which cause loss to users. The primary legal mechanism for providing redress for such losses is contract, but product liability and tort are also examined, as is the role of technical standards in the UK liability regime. Part four examines the IT security obligations of IT users, distinguishing between private and commercial users and examining in particular IT security in the regulated financial services sector and for IT infrastructure providers.

1248 The Report concludes with a case study of an IT deal involving a bank, which attempts to place the UK regulatory regime in context.

1. Background structure of UK liability law

1249 As in Germany, liability of IT producers and users to those who suffer loss as a result of security failures will derive either from contract, or tort. In this context, tortious liability includes liability for breach of a duty imposed by statute.[1884] To this must be added criminal and regulatory liability[1885], which normally takes the form of criminal or regulatory sanctions such as fines. UK law does not make a clear distinction between private

---

** Prepared by Chris Reed, Professor of Electronic Commerce Law, Centre for Commercial Law Studies, Queen Mary University of London

1883 The UK encompasses three legal systems: England and Wales, Scotland and Northern Ireland. There are substantial differences between these legal systems in relation to land, inheritance and other issues of that type, but for contract and tort the laws are broadly similar. The discussion here focuses on English law as representative of the UK as a whole.

1884 See e.g. the product liability regime under the Consumer Protection Act 1987 at G.XVI.3.a) below.

1885 E.g. under the General Product Safety Regulations 2005 – see G.XVI.2.b) below.

and public law, with the result that infringement of a criminal or regulatory obligation can also give rise to civil (private) liability in some circumstances. The test applied by the courts is whether, in the absence of any clear statement that there is or is not civil liability, the legislature intended the obligation to give rise to private claims as well as public sanctions.[1886] This will be decided by examining the legislation as a whole – it will be decisive if the legislation states specifically that it does not confer a civil law claim on any person.[1887]

1250 Whether a civil claim is in contract or tort, the basis of liability is assessed by reference to the obligation to which the defendant is subject. The question which the courts have to answer is whether this obligation is breached only through fault on the defendant's part, or whether the obligation is absolute or strict, in which case failure to meet that obligation will result in liability whether or not the defendant was at fault.

1251 This is an important difference from German law, which is seen most clearly in relation to breach of a contractual obligation relating to the provision of services. Art 276 of the German Civil Code establishes that if such an obligation has been breached then fault is the basis for granting a contractual remedy, basing the imposition of liability on the defendant's "deliberate acts and negligence". By contrast, English law assesses only whether the defendant was in breach of the promise given to the other party. The fact that it was not the defendant's fault that he was unable to perform the obligation only relieves him from liability in exceptional circumstances[1888], and it is irrelevant to the grant of the remedy of damages.[1889]

> "In relation to a claim for damages for breach of contract it is, in general, immaterial why the defendant failed to fulfil his obligations and certainly no defence to plead that he had done his best."[1890]

[1886] See Percy & Walton, *Charlesworth & Percy on Negligence* (9th ed. Sweet & Maxwell, London 1997) 11-03 to 11-33a.

[1887] See e.g. General Product Safety Regulations 2005 reg. 42, discussed at G.XVI.2.b) below.

[1888] Via the doctrine of frustration, which (summarised very simplistically) states that a contractual obligation ceases to be binding on the promisor if it becomes impossible to perform that obligation for unanticipated reasons which are beyond the promisor's control. Frustration rarely applies because it is usually possible to perform in some other way, though it may be more costly to do so, or because the cause of the impossibility was potentially within the promisor's control (e.g. labour disputes) – see e.g. *Fibrosa Spolka Akcyjna v Fairbairn Lawson Combe Barbour Ltd* [1943] AC 32 and the Law Reform (Frustrated Contracts) Act 1943. For this reason commercial contracts usually contain a "force majeure" clause which specifies the circumstances in which an obligation ceases to be binding because performance is impossible, and also sets out the consequences for the future in relation to those contractual obligations which are still capable of performance.

[1889] Fault might be relevant to some discretionary remedy, such as an order for specific performance (i.e. an order requiring the defendant to fulfil his contractual promise), but a claimant is always entitled to damages for breach of contractual obligations though those damages may be purely nominal if no loss has been suffered.

[1890] *Raineri v Miles* [1981] AC 1050, 1086 per Lord Edmund Davies.

1252 This does not mean that under English law all contractual obligations are strict liability obligations. The relevant question is the content of the obligation.[1891]:If it is a promise to achieve something[1892] then it is broken if the promisor does not achieve that thing. If it is a promise to take care or make efforts to do something, then the question is whether sufficient care[1893] has been taken. In either case, once breach of the obligation has been established in litigation then the promisee is entitled as of right to damages.

1253 In the context of a contract for the provision of an IT *service*, the standard obligation implied by law is one of reasonable care and skill[1894], i.e. it is only breached by fault on the part of the supplier. However, it is common for such contracts between commercial parties to contain contractual terms which are absolute rather than obligations of care. Thus a software supplier will promise that the software meets its specification in all material respects, and an outsourcing service provider will undertake to meet service levels and may promise that security precautions against unauthorised access to data will meet a particular standard. Failure to meet these obligations will give the customer a right to a contractual remedy, irrespective of whether the failure was due to the supplier's fault.

1254 The same analysis is, in broad terms, undertaken for breach of tortious obligations, although in the context of IT security the most common tortious obligation is imposed by the tort of negligence, to take reasonable care to avoid causing harm to those who it is foreseeable might be injured by a failure to take such care.[1895]

1255 Once liability has been established, English law then asks which losses, caused by the breach of obligation, should be compensated by an award of damages. Not all losses are recoverable. In broad terms, a defendant is only liable to compensate the claimant for those losses which are a *foreseeable* result of the breach, though the tests are slightly different in contract and tort.

1256 In contract, the rule in *Hadley v Baxendale*[1896] provides that:

[1891] See further Treitel, *Remedies for Breach of Contact: a comparative account* (Clarendon Press: Oxford 1988) pp 7-8.

[1892] E.g. delivery of goods in a contract of sale.

[1893] In English law, the amount of care required is almost invariably reasonable care – see e.g. Supply of Goods and Services Act 1982 section 13 which imposes on the supplier of services an obligation to perform them using reasonable skill and care..

[1894] Note 1893 above.

[1895] *Donoghue v. Stevenson* [1932] AC 562.

[1896] (1854) 9 Exch 341.

The claimant is entitled to damages for those losses which "arise directly and naturally in the ordinary course of events" from the breach of contract. These might be categorised as the normally expected losses, rather than all foreseeable losses.

1257 However, the claimant is only entitled to damages for other losses if he has made the defendant aware of the special circumstances which make such losses likely to arise. The theoretical basis for this distinction is that the contracting parties promise to confer benefits on each other, and that damages represent the lost benefit. The courts are therefore asking whether the defendant had, implicitly, promised to confer a normally unanticipated benefit on the claimant, in that he contracted to perform in the knowledge that his failure would cause a type of loss which he would not anticipate being suffered by other customers in a similar position.

1258 In tort the test is simpler – is the claimant's loss a foreseeable consequence of the commission of the tort?[1897] For example, suppose that a piece of software, owing to a defect in its design, destroys all the claimant's data. If the software producer owed the claimant a duty of care in the design and was in breach of that duty[1898], then it is clear that some loss of user data is foreseeable. However, if the claimant had failed to back up the data then much of his loss would be unforeseeable as it is standard practice to take regular back-ups. The court would ask how often a reasonable person in the claimant's position could be expected to take backups, and then hold that all the lost data which would have been expected to be backed up was an unforeseeable loss which did not give rise to a damages claim.

2. Statutory Obligations of IT producers and suppliers

a) Legislation on IT security risks

1259 IT technology is subject to a wide range of security risks, such as infection of systems by viruses, Trojans and other malware including rogue diallers and bots generally, remote manipulation of systems via weaknesses in active content technology, compromise of firewalls, etc. Although there have been numerous suggestions that producers and suppliers of such IT technology should bear some liability for guarding against these

[1897] *The Wagon Mound (No.1)* [1961] AC 388. This concept is often described as "remoteness", i.e. that the connection between the tort and the loss is not sufficiently close to justify awarding compensation.

[1898] In most cases a supplier will owe no duty of care, but if the relationship is of the kind explained at G.XVI.3.b) below then tortious liability could arise.

risks[1899], there is currently no UK legislation or case law which imposes legal obligations on producers or users in respect of these matters.

1260 Many of these IT risks will constitute the commission of criminal offences by some person under the Computer Misuse Act 1990. That act creates three basic offences:

- Unauthorised access to computer systems under section 1. This covers all basic hacking.
- Unauthorised access with intent to commit a further offence under section 2, which would cover successful or unsuccessful attempts to e.g. discover information for the purposes of theft, fraud or blackmail.
- Unauthorised modification of the contents of a computer under section 3. This offence would be committed by the author of viruses, Trojans and diallers, and those who use active content to modify data.

1261 DNS spoofing and phishing are likely to constitute criminal offences of theft, fraud etc, or attempts to commit such offences.

1262 However, the UK law in this respect is now 16 years old, and its drafting fails to cover a number of the more recent developments in activity of this type. For example, a denial of service attack has been held not to involve the modification of the contents of a computer[1900] and thus not amount to a section 3 offence. This and a number of other gaps in the law are addressed by the Police and Justice Bill, currently before Parliament.

1263 Of course, these criminal offences will not normally be committed by producers or suppliers of IT technology.

1264 The fact that there are no specific obligations on producers and suppliers does not mean, however, that they can never be liable for technology failures which expose users to the actions of third parties who exploit holes in their IT security. Any such liability will, though, be imposed through the general law of contract or tort (see below).

1265 By contrast, IT *users* are obliged by statute to take reasonable precautions to preserve the security of personal data (though not any other kinds of data). This obligation de-

[1899] See e.g. Edwards, "Dawn of the Death of Distributed Denial of Service: How to Kill Zombies" (2006) 24 Cardozo Arts and Entertainment Law Journal 23, part III.

[1900] *OUT-LAW News* 3 November 2005, http://www.out-law.com/page-6298.

rives from the seventh data protection principle, set out in Schedule 1 to the Data Protection Act 1998[1901]:

> "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

1266 The duty to comply with the data protection principles is imposed by section 4(4) of the 1998 Act, and the relevant questions to be addressed when establishing these security measures are set out in the UK Information Commissioner's *Data Protection Audit Manual*.[1902] It is not obligatory to undertake a data protection audit in accordance with the manual, or even at all, but failure to address the security questions set out in the Manual might be evidence of a failure to take appropriate security measures and thus of a breach of the seventh principle.

b) Product safety rules

1267 The EU Directive on product safety[1903] has been transposed into UK law by the General Product Safety Regulations 2005[1904] (the "GPS Regulations"). These regulations apply to all products which are "intended for consumers or likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them", including second hand products, which are supplied in the course of a commercial activity.[1905] They require any product which is placed on the market, advertised for sale, offered for sale or sold to be safe.[1906] Under Regulation 2, "safe product" means:

> "a product which, under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons."

1268 The GPS Regulations do not apply to:

- Equipment used in the course of providing a service, such as equipment which consumers ride or travel on[1907];

[1901] Implementing Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ No. L 281, 23.11.1995, p.31.

[1902] Available from www.ico.gov.uk.

[1903] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety OJ L11, 15 January 2002 p.4.

[1904] SI 2005/1803.

[1905] GPS Regulations reg. 2 (definition of "product").

[1906] GPS Regulations reg. 5.

[1907] GPS Regulations reg. 2 (definition of "product").

- Any risks covered by specific requirements of Community law other than the Directive, but with the other risks deriving from the product remaining covered by the GPS Regulations[1908]; and
- Second-hand products where the consumer is clearly informed that the product is to be repaired or reconditioned before it is used.[1909]

1269 There are no provisions in the GPS Regulations which apply specifically to IT producers; IT products are subject to exactly the same rules as any other product.

1270 The GPS Regulations are enforced by means of enforcement and other orders, and create a number of criminal offences. Contravention by a supplier of the GPS Regulations does not give the consumer, or any other person, a civil claim for compensation.[1910]

1271 It is important to note that "product" is not defined in a way which clearly includes or excludes software from the definition. It is likely that the courts would look to other definitions of "product" deriving from EU law, and in particular the definition in section 1(2) of the Consumer Protection Act 1987. As explained at 3.a)(1) below, that definition seems likely to exclude software which is not supplied on a tangible medium (such as software downloads).

1272 The GPS Regulations came into force on 1 October 2005. So far as can be ascertained, there have not yet been any prosecutions under the Regulations.

1273 There are few products for which safety certification is compulsory, and no IT products require compulsory certification. The effect of compliance with laws and regulations or with standards on liability under the GPS Regulations is as follows:

- If the product complies with UK health and safety legal requirements, the product is deemed to be safe in respect of those risks which are covered by the legal requirement.[1911] This would mean that the producer of the product could not be in breach of the Regulations unless the risk which rendered it unsafe fell outside the legal requirement. No legal requirements applicable specifically to IT products can be identified which are relevant here.
- If the product meets a voluntary UK standard which implements an EU standard, then the product is *presumed* to be safe in respect of the risks covered by that standard.[1912] The difference in wording from Regulation 6(1) suggests that it should be possible to rebut that presumption by adducing evidence that the product was in fact unsafe, but Regulation 6(2) does not make this clear.

[1908] GPS Regulations reg. 3(1) & (2).
[1909] GPS Regulations reg. 4.
[1910] GPS Regulations reg. 42.
[1911] GPS Regulations reg. 6(1).
[1912] GPS Regulations reg. 6(2).

- Otherwise, compliance with other national or EU standards, or with guidelines and codes of practice, is a factor which the court must take into account in deciding whether the product in question is safe.[1913]

1274 Even if a product is certified or meets a standard, the UK enforcement authorities may still take action to ensure the product is withdrawn from sale or recalled if the product is in fact dangerous.[1914]

c) Sovereign competences

1275 If a serious security flaw is discovered in an IT product, the UK authorities have only a limited range of measures available to deal with the issue.

1276 If the security flaw renders the product dangerous to the health and safety of consumers, then a recall notice can be issued under the GPS Regulations (see part b) above). The Regulations make it possible for the authority to negotiate alternatives to recall with the producer or distributor, and such a condition might include making a patch available (either authored by the producer or by a third party).

1277 Alternatively, if the flaw renders the product dangerous to health and safety more generally then employers could be required by the Health and Safety Executive under the Health and Safety at Work Act 1974 to cease using the product until it is made safe. It would then be for employers to make contractual claims against the supplier of the product as appropriate.

1278 In other cases, there are no statutory powers for public authorities to intervene, other than by publicising the risks and recommending remedial action.

1279 If the IT product is used by a UK authority, the procurement contract may well contain a term requiring the supplier to remedy security defects in the product. However, much will depend on how far the technical specification of the product deals with IT security. The Office of Government Commerce model Technology Supply Agreement v. 1.0 is intended to be used for the procurement of IT products by UK public authorities. However, the model Agreement contains no clause specifically dealing with IT security. Instead the supplier warrants in clause 38 that the product will comply with its technical specification. Thus the contracting UK authority will only have a contractual claim

[1913] GPS Regulations reg. 6(3).
[1914] GPS Regulations reg. 6(4).

against the supplier for IT security defects if it understands the issues well enough to ensure that the specification covers IT security issues.

3. Liability to compensate victims of IT failures

a) Product liability for faulty goods

(1) Is software a product?

1280 UK product liability law is set out in the Consumer Protection Act 1987[1915] which imposes strict (no fault) liability for defective[1916] products. "Product" is defined in section 1(2) as "any goods or electricity" including components. "Goods" are defined in s. 45 as including (amongst other things such as crops and aircraft which clearly do not cover software) "substances", and the same section defines "substance" as "any natural or artificial substance...". In spite of the circularity of this definition, it seems clear that computer software will only qualify as a product if it is a "substance", which suggests that it must have the tangible quality normally associated with goods. This is supported by the text of the Directive which defines "product " as any moveable.[1917]

1281 This question has not been decided by the UK courts, but it seems likely that the Act applies only to software which is marketed on some form of tangible medium (e.g. a CD-ROM or disk) ownership of which is transferred to the purchaser. Software which is installed by downloading it or copying it onto the purchaser's system from a medium that remains the property of the supplier will lack the necessary tangibility to fall within the definition.

1282 The question of whether software is "goods" for the purposes of the Sale of Goods Act 1979 arose in the case of *St. Albans City and District Council v. International Computers Ltd*.[1918] In that case computer software was supplied to the Council by copying it from a disk pack, so that no physical property containing the software was transferred. The issue before the court was whether the terms of satisfactory quality and fitness for purpose were implied into the contract by section 14 of the Act. In the High Court the

[1915] Implementing Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 7.8.1985, p. 29.

[1916] However, the definition of "defective" in the Act allows the court to take into account both the expected ways in which a consumer might use the product and any instructions or warnings given, and the standard expected is that of reasonable safety. Additionally, the "state of the art" defence has been included via s. 4(1)(e). The combined effect of these is to make the theoretical strict liability in fact quite close to negligence liability under general tort law so far as design defects (as opposed to manufacturing defects) are concerned.

[1917] Directive 85/374/EEC art. 7(e).

[1918] [1996] 4 All ER 481.

judge was firmly of the view that software is goods[1919], though the judge was able to decide the case on different grounds. In the Court of Appeal, however, Sir Ian Glidewell held that the contract could not be a sale of goods, because property in the tangible medium of a disk had not been transferred. This does not create a binding precedent because the case was decided on the express terms of the contract, but the opinion of such a senior judge is likely to be very influential on future decisions.[1920]

1283 It therefore seems likely, were the question whether software is a product for the purposes of the Consumer Protection Act to arise, that the court would follow the reasoning of Sir Ian Glidewell and decide that only software supplied on a tangible medium could be a product. However, where software is supplied pre-loaded or embedded in tangible equipment, the courts are likely to treat the combination as a product for these purposes rather than attempting to assess the individual hardware and software elements separately.

(2) Remedies under product liability law

1284 The only remedy available under the Consumer Protection Act is damages, i.e. financial recompense. These damages are limited to compensation for death, physical injury or damage to non-business property.[1921] In deciding whether a particular loss is recoverable, the tort rules on foreseeability discussed above will apply.

1285 Under the GPS Regulations an enforcement authority[1922] may issue various safety notices:

- Suspension notices under reg. 11, prohibiting the marketing or sale of a dangerous product until the authority has completed safety evaluations;
- Requirement to mark notices under reg. 12, requiring that product to be marked with warnings so as to make it safe;
- Requirement to warn notices under reg. 13, requiring notices warning of particular risks to be published and/or supplied with the product;
- Withdrawal notices under reg. 14, prohibiting any further marketing or sale of the product; and

[1919] [1995] FSR 686, 698-9. A strongly influential factor in forming the judge's opinion was his finding that, if software were not goods, it would fall entirely outside any regime of statutorily implied terms.

1920. It has been argued that some civil law jurisdictions may take a purposive approach to the definition of "product", and decide the issue on whether the software in question is effectively mass-marketed or produced only on a one-off basis - see Herschbaeck, *Is Software a Product?* (1989) 5 Computer Law & Practice 154. In the author's view, the UK courts are unlikely to adopt such an approach.

[1921] Consumer Protection Act 1987 section 5.

[1922] Defined in regs 2 and 10, in essence national and local government bodies.

- Recall notices under reg. 15, requiring the person on whom the notice is served to use reasonable efforts to organise the return of the product from consumers.

1286 These notices may be appealed under reg. 17. Failure to comply with a safety notice is a criminal offence.[1923]

1287 There is no specific duty to fix unsafe products, which in the case of software would normally be achieved by distributing a patch. However, an IT producer who does make such a patch available is likely to reduce its liability exposure in two ways:

- The patch may satisfy any duty of care the producer owes under general tort law, so that the producer has no liability at all (see further below); or

- Even if the producer remains liable, e.g. under the strict liability of product liability law, the fact that a patch has been made available may make any losses suffered unforeseeable and thus not recoverable. As we have seen at 1 above, the general principle of UK tort law is that only foreseeable losses are recoverable.[1924] If the patch would have prevented the loss, and it could reasonably be expected that the person suffering loss would apply the patch, then the loss will be unforeseeable and therefore not compensated.

1288 In both cases it will be necessary for the producer to use reasonable efforts to bring the existence of the patch to the attention of software users, which will either discharge the producer's duty of care or make the non-application of the patch, and thus the loss, unforeseeable.

b) Tort law remedies

1289 UK general tort law is the law of negligence, which requires there to be a duty of care owed by the defendant to the claimant, a breach of that duty, and foreseeable loss as a result. The general principle is that a duty of care will be owed if it is foreseeable that the defendant's actions or omissions might cause damage to the claimant.[1925] This means that if an IT product causes physical injury or property damage as a consequence of the producer's negligence, the claimant will be able to seek damages.

1290 However, a duty to avoid causing purely financial losses will only arise in exceptional circumstances.[1926] So far as can be discovered, there have been no cases which establish how general tort law applies to data losses caused by IT products (including software).

[1923] GPS Regulations reg. 20(4).
[1924] *The Wagon Mound (No.1)* [1961] AC 388.
[1925] *Donoghue v. Stevenson* [1932] AC 562.
[1926] *Spartan Steel and Alloys Ltd v. Martin* [1973] QB 27.

The question is therefore whether data loss would be seen by the courts as property damage or as purely financial loss.

1291 This question has not been decided, but it seems likely that the courts would make a distinction between data which is irrevocably lost as a consequence of the defendant's negligence and data which can be recovered or re-created. In the latter case the loss is the financial cost of recovery or recreation, and might be treated as purely financial. In the former case it is the author's opinion (though this cannot be substantiated by reference to any cases) that the courts should recognise the importance of data as a business asset and treat it as a species of intangible property – if so, the loss would be recoverable.

1292 In either event, though, the greatest losses suffered by the victim of negligence would be likely to be the loss of future revenue and profits derived from using that data, and these losses would be purely financial and thus nor normally recoverable via an action in tort.

1293 The UK law on whether a defendant owes a duty of care to avoid causing purely financial losses by negligence is extremely complicated, but can be summarised as follows. The basic principle to be applied was laid down in *Caparo Industries plc v Dickman*[1927], a claim for financial losses caused by negligent misstatements. In that case the court held that liability is based on the defendant's undertaking of responsibility for achieving a particular result, where economic loss is a foreseeable result of failure to meet that responsibility.[1928] Additionally it must be fair and reasonable for the law to impose the duty of care.

1294 In deciding whether it is fair and reasonable to impose a duty of care, commercial arrangements defining liability can be taken into account. This is perhaps most clearly illustrated in *Marc Rich & Co. AG v Bishops Rock Marine Co. Ltd.*[1929] A bulk carrier vessel developed faults and the surveyor acting for the ship's classification society recommended that it could proceed to its next scheduled port for repairs. The following day, the ship sank with a total loss of cargo. The cargo owners claimed in negligence

[1927] [1990] 2 AC 605.

[1928] In negligent misstatement cases an additional requirement, that of reliance on the statement, is also imposed, but *White v Jones* [1995] 2 AC 207, a case in which a solicitor failed to draft a will in time to ensure that the plaintiff beneficiary received a legacy, shows that the requirement of reliance is not essential in non-misstatement cases, as its purpose is only to show a causal link between the negligent misstatement and the loss.

[1929] [1996] AC 211.

against the classification society. The House of Lords held that the same test should apply to physical and financial losses. The question of whether there was sufficient proximity between plaintiff and defendant, which in physical damage cases is normally determined almost exclusively by foreseeability of the likelihood of harm, is decided in economic loss cases by seeking the relevant undertaking of responsibility.[1930]

1295 However, even on the assumption that there was sufficient proximity between the cargo owners and the surveyor, the court also held that on the facts it was not fair, just and reasonable to impose a duty of care because of the agreed contractual structure adopted in the shipping industry which allocates losses of this type between shipowners and cargo owners. This recognition that the imposition of a duty of care can upset carefully crafted contractual arrangements is also found in Lord Nolan's judgment in *White v Jones*[1931], in which he said:

> I would for my part leave open the question whether . . . the defendant who engages in the relevant activity pursuant to a contract can exclude or limit his liability to third parties by some provision in the contract. I would prefer to say that the existence and terms of the contract may be relevant in determining what the law of tort may reasonably require of the defendant in all the circumstances.

1296 It appears from these cases that the kind of circumstances in which a duty of care to avoid economic losses will arise would be where one software producer is employed to devise software specifically for the user, and subcontracts some or all of the work to another software house. In such a case, provided there is evidence that it is the subcontractor rather than the main contractor who is undertaking responsibility for that part of the work, which is likely to require there to have been sufficient discussion between user and sub-contractor to show that the user is relying on the subcontractor's expertise, the user will have an arguable case in tort for the cost of replacement or repair.[1932] However, the role of contracts in determining whether it is just and reasonable to impose a duty of care will need to be examined. If, as is quite likely, the subcontractor has effectively[1933] limited his liability to the main contractor, the fact that imposing direct tortious li-

[1930] See also *Henderson v Merrett Syndicates Ltd* [1995] 2 AC 145; *White v Jones* [1995] 2 AC 207; *Spring v Guardian Assurance plc* [1995] 2 AC 296, all of which stress assumption of responsibility as the test for proximity.

[1931] [1995] 2 AC 207.

[1932] See *Junior Books v. Veitchi* [1983] 1 AC 520, where a nominated subcontractor under a building contract was held to owe a duty of care to the customer.

[1933] If the subcontractor's limitation of liability were ineffective, it would clearly not (for that reason) be unfair, unjust or unreasonable to impose a duty of care on him. This raises the interesting spectacle of a court being required to give judgment on the effectiveness of a contract term which is not actually in dispute.

ability would evade that limit might be sufficient to persuade a court that it would not be fair, just and reasonable to impose a duty.

c) Contract law remedies

1297 The most likely way in which a victim of an IT failure will achieve compensation under UK law is through an action against the supplier of the IT product or provider of the IT service for breach of contract. The main reason for this is that the losses suffered by the victim will, in most cases, be *expectation* losses rather than *reliance* losses.

1298 This distinction is implicit, rather than explicit, in UK law, but has formed the basis of an unarticulated policy debate for at least two centuries.[1934] Expectation losses are those where the defendant is obliged by law to confer a *benefit* on the claimant, and if he fails to do so damages are awarded based on the value of the benefit which should have been conferred. Reliance losses are where the defendant is obliged by law to ensure that the claimant does not suffer a *detriment*, and thus where the claimant does suffer such a detriment the damages are based on the cost of restoring him to his previous position.

1299 In general, tort law only provides compensation for victims of reliance losses. Only in exceptional cases have the courts held that a defendant owes a tortious duty to confer a benefit on a claimant.[1935]

1300 By contrast, contract law allows both expectation and reliance losses to be recovered. This means that there is no restriction on claiming purely financial losses, which will normally be sums of money (such as future profits) which the claimant can demonstrate would have been made had the contract not been breached.[1936]

1301 As explained at part 1 above, a claimant in a breach of contract claim does not need to prove fault on the defendant's part to claim damages. Instead, he has the burden of proving breach of a contractual term, and the causal link between that breach and the loss. It is the nature of the obligation set out in the contractual term which is determinative; some terms require strict compliance, whereas others only required reasonable care or efforts on the defendant's part.

[1934] The distinction between expectation and reliance losses, and the historical development of their differing treatments, is examined at length in Atiyah, *The Rise and Fall of Freedom of Contract* (Clarendon Press, Oxford 1985).

[1935] See e.g. *Junior Books v. Veitchi* [1983] 1 AC 520. It is noteworthy in that case that, had the relationships between the parties been constructed more carefully, the claimant would have had a contractual claim against the defendant, which influenced the court heavily in deciding that a duty of care was owed.

[1936] Subject, of course, to the rules on remoteness (foreseeability) of damage – see G.XVI.1 above

1302 The most common terms in an IT supply contract which require strict compliance are:

- Compliance with specifications;
- Delivery dates and other time obligations, e.g. in a software development contract, submission of the software for acceptance tests;
- Reasonable fitness for purpose of IT products[1937] and other quality terms;
- Compatibility with other IT technology;
- Compliance with technical standards;
- Warranties and indemnities against third party intellectual property rights claims; and
- Obligations to correct defects.

1303 In a business-to-business contract, one would expect to see all these terms set out expressly. It is always possible for a supplier to negotiate a compliance margin, e.g. by promising only "material" compliance with specifications or undertaking not to correct defects absolutely but only to use reasonable efforts to do so.[1938]

1304 Contractual obligations to take reasonable care are most commonly found in relation to the provision of services, such as:

- Software development;
- Technology integration; and
- Software and systems maintenance.

1305 Finally, in relation to business-to-business contracts, it is almost universal to find an express allocation of the risks arising from breach of contract by way of a clause excluding and limiting liability. Some losses may be excluded altogether, most commonly loss of future profits, and the remainder will be subject to an overall financial cap on the supplier's liability. Most clauses of this type will be subject to a test of reasonableness under the Unfair Contract Terms Act 1977, and will be void if they fail that test. However, in contracts between businesses the courts are generally unwilling to substitute their own notions of reasonableness for that of the contracting parties, as evidenced by

[1937] E.g. under Sale of Goods Act 1979 s. 14.

[1938] For a more detailed examination of such contracts see Reed & Angel (eds) *Computer Law* (6th ed, Oxford University Press, Oxford 2007) Chapter 1.

their agreeing to the clause[1939], unless the clause has in effect been forced on the customer.[1940]

1306 In business-to-consumer contracts the position is very different. Because of the combined effect of the Unfair Contract Terms Act and the Unfair Terms in Consumer Contracts Regulations 1999[1941], exclusions and limitations of liability are unlikely to be binding on consumer customers. This means that, in addition to any express terms, consumers will benefit from the terms implied into the contract by the Sale of Goods Act 1979, the Supply of Goods and Services Act 1982 and the Sale and Supply of Goods to Consumers Regulations 2002.[1942] Effectively, consumers will almost always have a breach of contract claim for defective IT products sold or supplied to them, or for defective IT services, but the precise interplay of these implied terms is complex and cannot be analysed in the space available here.[1943]

d) The role of technical standards

1307 The role of technical standards in relation to IT products liability has not yet been addressed by the UK courts, although as explained in part 2.b) above compliance with technical standards may give a complete or partial defence to criminal liability under the GPS Regulations.

1308 Liability under the Consumer Protection Act 1987, discussed at a) above, arises if a product is defective. This means that it does not provide the level of safety which consumers are entitled to expect.[1944] It seems likely that a product which complies with technical standards which address safety issues will be treated by the courts as providing that level of safety which consumers are entitled to expect. If, however, it is dangerous in a way which is not covered by the standard, compliance with the standard would not be a relevant consideration in deciding whether it was defective.

1309 Liability for breach of contract would arise either:

- For breach of an express term that the IT product complied with a particular standard; or

[1939] *Watford Electronics v Sanderson* [2001] All ER 290.

[1940] See e.g. *St Albans City and District Council v International Computers Ltd* [1996] 4 All ER 481.

[1941] SI 1999/2083 implementing Council Directive (EC) 93/13 on unfair terms in consumer contracts [1997] OJ L95, 21 April 1993 p. 29.

[1942] SI 2002/3045.

[1943] See further Reed & Angel (eds) *Computer Law* (6th ed, Oxford University Press, Oxford 2007) Chapter 2.

[1944] Consumer Protection Act 1987 section 3.

- For breach of a term requiring the supplier to exercise reasonable care and skill in selecting the product, installing or integrating it with the customer's IT systems, configuring or operating[1945] it or in providing a service. In this case, failure to comply with the standard might be evidence of a failure to take sufficient care if a reasonable supplier in the same circumstances would be expected to comply.

1310 Liability under the general tort law of negligence is based on breach of the duty of care, i.e. failure to take such care as is reasonable in all the circumstances to avoid causing foreseeable losses. Compliance with a technical standard is likely to be evidence that the defendant has taken reasonable care to avoid those losses unless, as explained above, the standard does not deal with the risks which gave rise to the loss.[1946]

e) National standards

1311 The leading UK standards body is BSI British Standards.[1947] It is the National Standards Body and participates in ISO, IEC, CEN, CENELEC and ETSI standards making. Its status is established by a Memorandum of Understanding with the UK Government, but BSI British Standards does not have any special legal status except in respect of its participation as the UK representative in international standards bodies.

1312 Numerous industry groups also set industry-specific standards, and proprietary standards also exist.

f) International standards

1313 International standards are taken into account in deciding liability in exactly the same way as national standards, as explained above. Compliance with some international standards is directly relevant to liability under the GPS Regulations (see 2.b) above). Other standards will be taken into account by the courts in deciding whether obligations to take reasonable care have been complied with as explained at c) above.

1314 Common international standards will necessarily carry more weight before the courts than differing national standards, but the principles remain unchanged.

[1945] E.g. in an outsourcing contract where the service supplier takes over control of the customer's computer systems and uses them to provide the service.

[1946] The UK courts have held on a number of occasions that failure to comply with a technical standard is evidence (though not conclusive evidence) of negligence – see e.g. *Armstrong v British Coal* [1998] EWCA Civ 1359, *AIC v ITS Testing Services* [2005] EWHC 2122 (Comm) – though this of course does not imply that compliance with a standard is evidence of lack of negligence.

[1947] Formerly the British Standards Institute, www.bsi-global.com.

1315 As there is in general no legal obligation to comply with national or international standards, a common international IT security standard would do no more than reduce the uncertainty which standards it would be advisable for a producer or supplier to meet.

g) Permissions, certificates and audits

1316 There is no general scheme of public authorisations in the UK. Compliance with standards, or certification as compliant, has the effects on general liability explained above. There is no general obligation to audit compliance, though compliance audits are available from professional services organisations.

4. Obligations of IT users

a) Private users

1317 The UK has no specific legislation or judicial decisions which require a private user to take any particular safety measures in respect of their use of IT.[1948] Thus, if a private user's use or misuse of IT technology causes loss to another person, the question whether the private user should compensate that person will be decided either under the general tort law discussed at 3.b) above or as a breach of a contractual obligation.

1318 It is possible to envisage a number of theoretical scenarios where the private user might have liability in tort, though it must be stressed that none of these have ever, so far as can be ascertained, come before the courts:

- The IT user fails to install or update virus protection on his home computer, and as a result sends a Word document to a friend which is infected with a virus. The friend's computer is infected with the virus, causing loss of data and loss of use of the computer system together with the costs of cleaning up the infection. It is arguable that the IT user owes a duty of care in negligence to his friend, as it is foreseeable that failure to operate proper anti-virus precautions could cause the friend loss. A reasonable user would be expected to take such precautions, thus establishing the breach of duty. However, a liability claim under this scenario may fail because the losses are too unforeseeable, and thus too remote. The IT user is entitled to foresee that his friend will behave reasonably, and reasonable behaviour requires taking anti-virus precautions. If those precautions had been in place, the friend would not have suffered the loss. Alternatively, if it is held to be foreseeable that the friend might not have anti-virus precautions in place, the friend's damages will be reduced because his own negligence (in failing to take precautions) contributed to the loss.[1949]

[1948] Except where the private individual is a data controller, in which case the general security obligation in the Data Protection Act 1998 (see G.XVI.2.a) above) will apply.

[1949] If the injured person is guilty of contributory negligence, his or her damages will be reduced by the proportion to which that contributory negligence contributed to the loss under the Law Reform (Contributory Negligence) Act 1945. This prin-

- The IT user fails to install or configure a firewall, and as a consequence his computer is used as part of a Denial of Service attack against a corporation. Although it is foreseeable that this inaction on the user's part might cause loss to a third party in this way, it is in the author's view unlikely that a court would hold that the user owes a duty of care in negligence to the corporation. At the time the user was careless, he could not have foreseen *which* corporation might be injured by his carelessness. The UK courts have consistently been unwilling to impose a duty to take care towards a large and unspecified class of potential victims[1950], which in this case would include every operator of an internet-connected computer world-wide. Even if the IT user were held to owe a duty of care, he would only be responsible for that part of the corporation's loss caused by his own computer, which would be a tiny fraction of the total loss suffered by the corporation.

- The IT user relies on a satellite navigation system when driving his car and, following the system's instructions, turns off the road onto a bridle path and frightens a horse being ridden by the claimant, so that the claimant falls off and is injured. Here the IT user is likely to be liable in negligence. However, the duty of care would be a duty to drive the car carefully, rather than a duty to use the IT technology carefully. His misuse of the technology would be evidence that he was not taking sufficient care in the wider activity of car driving.[1951]

1319 From these scenarios and the principles of general tort law explained at 3.b) above, it seems that such liability will arise only in unusual circumstances.

1320 However, it is increasingly common for the contracts which a private IT user enters into with online service providers to impose security obligations on him. For example, contracts for online banking usually require a private user to take safety measures with regard to preserving the secrecy of passwords and other access devices and not permitting others to know or use them. Thus the Barclays Bank personal account terms[1952] provide:

> 3.2 Before we can act on instructions given to us by telephone or computer we will agree security procedures with you. By "security procedures" we mean the use of a password, security keys, cards, personal identifier(s), codes, Personal Identification Numbers (PINs) or encryption device(s) which may be changed by agreement in the future.
>
> 3.3 You must do all that you reasonably can to make sure that the security procedures are kept secret at all times. If you make a written record of any code or PIN you must make a reasonable attempt to disguise it. Any security-related device must be kept physically secure, which includes making sure that security details are not kept in any form (including by browser or any other software) in such a way that anyone using the same workstation can go through the security procedures using stored details.

---

ciple applies to claims in tort, or to claims in contract where there is concurrent liability in tort – see *Forskringsaktieselskapet Vesta v. Butcher* [1989] AC 879.

[1950] See e.g. *Candler v. Crane Christmas & Co.* [1951] 2 KB 164.

[1951] Over-reliance on technology to avoid collisions has been held to be negligent in the case of radar – see *The Lady Gwendolen* [1965] P 294.

[1952] As at November 2006, http://www.barclays.co.uk/importantinfo/cust_agree.html.

> 3.4 You must tell us as soon as you can if you think someone else may know the security procedures. Until you tell us, you will be responsible for all instructions that we receive and act on even if the instruction was not given by you. Unless we can show that you have been fraudulent, grossly negligent or have not complied with condition 3.3 we will refund your account with any payments we make after you tell us. We will have no further liability to you. We can ask you for all the information you have about the misuse of security procedures, which we may pass to the Police if we think that will be useful.

1321 A breach of these contractual obligations would in theory allow the bank to claim damages from the IT user. In practice, they will be used to defend the bank against a customer's claim that account transactions were not authorised by him.

1322 The imposition of these security obligations will also be important if the customer makes a justified claim against the bank. For example, if the bank's systems are insecure, thus allowing third parties to undertake transactions on the customer's account, the customer will have a damages claim against the bank for breach of its contractual duties to (a) obey the customer's mandate[1953] and (b) take reasonable care and skill in providing the online banking service[1954]. If the claim is purely in contract, e.g. for a strict contractual liability such as the duty to provide goods of satisfactory quality, contributory negligence is not a defence to reduce the amount of damages payable. However, the only damages which can be claimed are those arising directly and naturally from the breach of contract[1955], and thus if the customer's failure to take the required security precautions caused part or the whole of the loss, that would not be recoverable as damages because it was too remote from the breach by the bank.

b) Commercial users

1323 In general, UK law places no different liabilities for IT security on commercial and private users. The general law rules of liability are identical, save that some liabilities (e.g. product liability and some implied terms in contracts) are only imposed on sellers in the course of a business.

1324 However, in practice commercial users will under the general law be obliged to introduce more comprehensive security measures than private users for a number of reasons:

[1953] *Foley v Hill* (1848) 2 HL Cas 28.
[1954] Supply of Goods and Services Act 1982 section 13.
[1955] *Hadley v Baxendale & Ors* [1854] Exch 15.

- A provider of services in the course of the business owes an implied contractual duty to provide those services using reasonable care and skill.[1956] Failure to adopt appropriate security measures could be a breach of this obligation, and a business user has more resources to devote to IT security than a private user. Further, under UK negligence law those who profess to have special skills (such as doctors) will need to exercise greater care and skill than the general public when exercising their special skills[1957]. Thus, for example, a surgeon operating remotely via telemedicine might need to take more stringent security measures in respect of the computer systems involved than a person undertaking a less hazardous and skilled activity.

- Discharge of any general tortious duty of care will, in general, require more from a business than a private individual.

- Some businesses (e.g. in the financial sector – see part c) below) are subject to regulatory obligations both to operate their businesses using reasonable care and skill and sometimes to take security measures against IT systems failure.

1325 There is no universal test for distinguishing between commercial and private users, but the clearest formulation is that set out in section 1 of the Partnership Act 1890, "with a view to profit". In other words, if the activity (taken overall) is intended to make a profit, whether it in fact does so or not, it will be a business. The standard formulation in UK legislation is acting "in the course of a business", which enables the court to distinguish a sole trader's private activities from his business activities.

c) Regulated sectors – banking and financial services

1326 Professionals such as accountants and lawyers are subject to professional codes requiring them to preserve confidentiality of their records, and these codes might be breached if inadequate IT security is used. However, obligations of this type tend to be general obligations to exercise reasonable care and skill rather than specific obligations in respect of IT security.

1327 By contrast, the regulation of financial institutions by the Financial Services Authority (FSA) contains a number of IT-security specific obligations. These are set out in the FSA Handbook[1958], which contains both rules[1959] and guidance.[1960] Guidance has no legal force – a financial institution which follows the guidance may still be in breach of the rules or legislation, whilst failure to follow guidance does not per se amount to a

[1956] Supply of Goods and Services Act 1982 section 13.
[1957] Percy & Walton, *Charlesworth & Percy on Negligence* (9th ed. Sweet & Maxwell, London 1997) Chapter 8.
[1958] http://fsahandbook.info.
[1959] Which have the force of regulation by virtue of Financial Services and Markets Act 2000 sections 138-148.
[1960] The power to give guidance is contained in Financial Services and Markets Act 2000 section 157.

breach. In practice though, following the guidance is likely to enable a financial institution to meet its legal and regulatory obligations.

1328 The section of the FSA Handbook which is most relevant to IT security is *Senior Management Arrangements, Systems and Controls* (SYSC). This contains a general obligation on regulated institutions (firms) to "establish and maintain appropriate systems and controls for managing operational risks that can arise from inadequacies or failures in its processes and systems (and, as appropriate, the systems and processes of third party suppliers, agents and others)."[1961] The FSA undertakes periodic risk assessments of regulated firms, using its own risk-assessment methodology.[1962]

1329 The general obligation is expanded on in SYSC 3A.7.6 to 3A.7.8. SYSC 3A.7.6 sets out general principles for the control of IT risks:

A firm should establish and maintain appropriate systems and controls for the management of its IT system risks, having regard to:

(1) its organisation and reporting structure for technology operations (including the adequacy of senior management oversight);

(2) the extent to which technology requirements are addressed in its business strategy;

(3) the appropriateness of its systems acquisition, development and maintenance activities (including the allocation of responsibilities between IT development and operational areas, processes for embedding security requirements into systems); and

(4) the appropriateness of its activities supporting the operation of IT systems (including the allocation of responsibilities between business and technology areas).

1330 SYSC 3A.7.7 and 3A.7.8 set out further general principles with specific reference to information security, but again do this at the level of general principle rather than mandating particular technological measures:

SYSC 3A.7.7 Failures in processing information (whether physical, electronic or known by employees but not recorded) or of the security of the systems that maintain it can lead to significant operational losses. A firm should establish and maintain appropriate

[1961] FSA Handbook SYSC 3A.7.1.

[1962] See Financial Services Authority, *The FSA's risk-assessment framework* (August 2006) parts 3 and 4.

systems and controls to manage its information security risks. In doing so a firm should have regard to:

(1) confidentiality: information should be accessible only to persons or systems with appropriate authority, which may require firewalls within a system, as well as entry restrictions;

(2) integrity: safeguarding the accuracy and completeness of information and its processing;

(3) availability and authentication: ensuring that appropriately authorised persons or systems have access to the information when required and that their identity is verified;

(4) non-repudiation and accountability: ensuring that the person or system that processed the information cannot deny their actions.

SYSC 3A.7.8 A firm should ensure the adequacy of the systems and controls used to protect the processing and security of its information, and should have regard to established security standards such as ISO17799 (Information Security Management).

1331 Additional principles to manage the rather different risks associated with IT outsourcing are set out at SYSC 3A.9.

1332 It can be seen that the regulatory obligations of firms in respect of IT risks are addressed to the management of the firm, rather than to its technical officers. The regulation is therefore framed in terms of the principles to be considered and addressed by management. This approach follows that of the Basel II process[1963], which takes the view that regulation of operational risks generally, and those arising from IT in particular, is more effective if it requires management to identify, evaluate and guard against the actual risks it faces, rather than mandating particular technical measures which may be inappropriate for the particular institution or become outdated rapidly.

d) IT infrastructure providers

1333 UK legislation does not appear to adopt any general practice of imposing IT security obligations, or indeed any general security obligations, on operators of critical infrastructure. However, the responsible government minister is charged with various duties

[1963] The Basel II initiative is documented extensively at http://www.bis.org/publ/bcbsca.htm. In relation to IT security, see particularly Basel Committee on Banking Supervision, *Risk Management Principles for Electronic Banking* (BIS July 2003); Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk* (BIS February 2003).

to oversee the proper working of critical infrastructure[1964] and, when granting permissions or exemptions to infrastructure providers, is often required to take into account the continuance of a secure supply of services via that infrastructure.[1965]

1334 The more common approach is to incorporate information security provisions into licences. Thus, as examples from telecommunications:

- British Telecom's license under the Telecommunications Act 1984 requires[1966] it to undertake specified measures to safeguard the security of network operations during an emergency.
- Providers of electronic communications services or networks are subject to the conditions set out in the General Conditions of Entitlement, made under section 42 of the Communications Act 2003. Under those Conditions the provider must:
- Comply with any compulsory applicable standards or specifications listed in the EU Official Journal[1967];
- Take account of any non-compulsory ISO, ITC or IEC standards in providing the service[1968]; and
- Comply with any standards direction given by the Director of the Office of Communications.[1969]

1335 To the extent that these standards deal with IT security, the Conditions will require the provider to meet those standards.

1336 Infrastructure providers may also accept contractual liabilities to their customers which have an IT security element. For example, the Demon.net Web hosting standard terms and conditions[1970] provide that:

> 4.6 The Company will implement systems designed to reject certain undesired email (including unsolicited commercial email) or delete them before delivery. The Customer may choose to receive unsolicited commercial email at any time by 'opting out' at https://www.password.uk.demon.net/webpassword.cgi.

1337 In general, infrastructure providers attempt to exclude their liability for service failure (except for partial refunds related to the length of service outage), loss of data, deletion

[1964] E.g. the duty of the Secretary of State to produce an annual report on the security of gas and electricity supplies under the Energy Act 2004 section 172.

[1965] E.g. when granting permission for the construction of offshore gas storage facilities, Petroleum Act 1998 section 17C.

[1966] Condition 53.3A as inserted by Telecommunications (Leased Lines) Regulations 1993/2330 regulation 4(d)(ii).

[1967] Condition 2.1.

[1968] Condition 2.2.

[1969] Condition 2.3.

[1970] http://www.demon.net/helpdesk/producthelp/tandc/webhosting/webhosting.html.

of website files hosted by the provider etc.[1971] However, business customers with sufficient bargaining power will normally expect to negotiate terms which allocate responsibility for some levels of IT security risk to the provider, as discussed in the final part of this Report.

5. Case study – IT security in the financial sector

1338 To illustrate the laws and regulations analysed above, this part of the Report sets out a case study which examines an IT procurement in the financial sector. The study identifies the various liabilities which might arise and how the financial institution would be likely to deal with them.[1972]

1339 Göttingen CreditBank's London subsidiary (Göttingen UK) is a bank regulated by the Financial Services Authority (FSA). It decides to upgrade its UK online banking computer platform. To achieve this, it enters into three deals (all in the UK and relating to UK online banking):

- A website outsourcing agreement, under which FinanceWeb plc will take over the running, development and hosting of the website;
- A software licensing contract with Midware Ltd for the HomeBank suite of online banking software. HomeBank manages all customer communications via the website and enables bank customers to conduct their banking operations online. The contract also requires Midware to write software which integrates HomeBank with both the website and Göttingen's back office systems, so that all three interoperate;
- The purchase of a new array of servers from BankTech Ltd to run HomeBank.
- Göttingen UK's internet connectivity is provided by Incubus Internet Ltd.

a) Main commercial terms relating to IT security

(1) FinanceWeb

1340 The arrangement under which FinanceWeb develops, hosts and operates the Göttingen UK website will be documented in a very detailed contract. In addition to standard commercial terms, there will be a number of specific terms relating to IT security. These are likely to include:

[1971] See e.g. Demon.net Web hosting standard terms and conditions 9.2 and 9.4 (://www.demon.net/helpdesk/producthelp/tandc/webhosting/webhosting.html); Yahoo! UK terms of service 17 and 18 (http://uk.docs.yahoo.com/info/terms.html).

[1972] The case study is based on the author's experience advising financial institutions and their suppliers on transactions of this type. Because commercial contracts are confidential, it is not possible to point to published sources or examples. However, the author's experience is that the issues identified below, and their likely solutions, would be familiar to any UK commercial lawyer practising in this field.

- A term requiring BankTech to implement precautions to secure the website against unauthorised access. This will be an obligation of care, and the commercial discussions will centre around the amount of care to be taken. FinanceWeb will offer "reasonable" care or efforts, whereas Göttingen UK will want "best efforts".[1973] If Göttingen UK can identify applicable technical standards, FinanceWeb may be required to meet those standards.

- FinanceWeb will need to ensure there is a secure communications link to Göttingen UK's back office systems. If this is provided by a third party, Göttingen UK will ideally seek to secure contractually binding obligations from that third party in respect of the link. Alternatively, Göttingen UK's existing ISP Incubus may undertake to provide this link by amendment to its existing contract (see (4) below). FinanceWeb will try to exclude its liability for any communications once they pass from its own systems to the internet or the third party operated communications link. It is likely that Göttingen UK will insist on encryption[1974] of all communications between FinanceWeb and its back office systems.

- FinanceWeb will be obliged to identify Göttingen UK customers using the identification processes (user IDs, passwords, etc) specified by Göttingen UK.

- There will be a general obligation for FinanceWeb to retain communications records and make them available to Göttingen UK for investigating possible security breaches. The parties may negotiate precisely what records are to be maintained and for how long, rather than agreeing a general records retention term.

- FinanceWeb will be a data processor and thus owe a security obligation under the Data Protection Act 1998. The contract will require FinanceWeb to ensure that it complies with this obligation.

- Göttingen UK may well insist on regular reports relating to security (e.g. attempted hacking of the website, data on customer identification failures, etc), as it will need this information to meet its regulatory obligations to the FSA (see b) below). Göttingen UK may also insist on the right to audit FinanceWeb's activities and records.

- FinanceWeb may be required to monitor industry best practice in relation to IT security and to propose improvements to Göttingen UK whenever appropriate and to implement them if required by Göttingen UK (with relevant changes to contract pricing and other obligations).

1341 The liability regime for breaches of the contract, including breaches of security obligations, will be negotiated in detail. Göttingen UK will probably seek an indemnity from FinanceWeb for losses caused by any failure of FinanceWeb to comply with its security obligations under the contract. FinanceWeb will resist this, and try to limit its liability to

[1973] This requires the obligee to do everything possible to achieve security, no matter how expensive, whereas reasonable efforts balances the cost and effort against the risk.

[1974] AES, or whatever other encryption protocols are banking standards and acceptable to the FSA.

damages.[1975] The likely compromise will be to limit the indemnity to some only of the security obligations, and to agree a financial cap on liability (either overall, or for each specified liability). This negotiation will, if conducted properly, allocate all the likely losses between FinanceWeb and Göttingen UK – Göttingen UK will be unable to force FinanceWeb to accept unlimited liability[1976], and will therefore need to examine its own insurance arrangements to make sure that it is covered for losses which it cannot recover from FinanceWeb.

1342 Göttingen UK also has an obligation to plan for failures by its outsourcing suppliers[1977], and thus either the contract with FinanceWeb should require FinanceWeb to provide appropriate disaster recovery services, or Göttingen UK should obtain those services separately or provide them itself.

1343 The decision to outsource in this way has regulatory consequences, and thus Göttingen UK will need to make a risk assessment before entering into the agreement – see b) below.

(2) Midware

1344 When making its decision to purchase the HomeBank software, Göttingen UK will need to satisfy itself that using this software will enable compliance with its regulatory obligations to the FSA (see b) below). Thus Göttingen UK would be sensible to conduct due diligence on this point, investigating other banks' use of the software and any known problems with it.

1345 The agreement with Midware will in the main be a standard software licensing agreement. The primary liability obligation of Midware will be a warranty that the software complies in material respects with its specification, and so Göttingen UK will need to ensure that the specification covers all the necessary IT security functions.

1346 In addition to the licence, it would be normal to enter into a maintenance agreement under which Midware agrees to correct problems with the HomeBank software. Different types of problem will have different priorities and thus fix times, and it would be sensible for IT security problems to be given the highest priority. Göttingen UK should

[1975] As explained at G.XVI.1 above, damages do not compensate for all losses suffered. By contrast, an indemnity will cover unforeseeable losses and other expenses.

[1976] Unless FinanceWeb is so commercially powerless that it has no choice but to agree, in which case it will not have the financial resources to meet Göttingen's claims!

[1977] FSA Handbook SYSC 3A.9.8.

also require Midware to inform it immediately of any reported IT security problems and to work with Göttingen UK to develop solutions to them.

(3) BankTech

1347 Because BankTech is only supplying hardware, this agreement will have the least impact on Göttingen UK's IT security regime. Liability will be based, as for Midware, on compliance with the specification, and so similar terms should be included. There may also be a maintenance obligation, which should contain similar correction and reporting obligations.

(4) Incubus

1348 Incubus is already carrying Göttingen UK's customer communications, and if the pre-existing contract is properly drawn up will have imposed relevant security obligations on Incubus. If Göttingen UK operates logical security controls (such as noting IP addresses from which multiple login attempts are made) it may require Incubus to assist in operating these controls.

1349 If Incubus operates the data link between Göttingen UK's back office servers and the website hosted by FinanceWeb, the agreement will need to be modified to ensure that any additional IT security required is put in place. The liability principles for negotiation will be as for the FinanceWeb contract.

1350 The precise nature of the security obligations in the Incubus contract cannot be predicted, as they will depend on the nature of the service provided. If Incubus merely provides "vanilla" connectivity, leaving security to the technology used at either end of the communication, then the contract may contain little more than an obligation to maintain connectivity and data throughput. Alternatively, Incubus may be able to offer additional security features, monitoring and/or reporting, in which case these will be set out in a specification and the contract will oblige Incubus to meet the specification.

b) Obligations to the regulator

1351 As explained at 4.c) above, the FSA does not mandate specific IT security measures, but instead requires regulated firms to make their own risk assessments and take appropriate measures to guard against them.[1978] Thus under FSA Handbook SYSC 3A.7.6, Göttin-

[1978] "Given the many possible events that could have a negative effect on the financial markets and our limited resources, our risk-based approach is based on a clear statement of the realistic aims and limits of regulation. In other words, we accept that we can never entirely eliminate risks to the statutory objectives we have been set by Parliament – our 'non-zero fail-

gen UK has an obligation to make a risk assessment of this deal and to ensure that it does not pose an unacceptable risk to the financial stability of the bank or the UK financial system, or to its customers.

1352 Göttingen UK may choose to discuss particular risks with the FSA to ensure that the FSA is happy with the approach to IT security risk management which it is taking. The periodic FSA risk assessment review will examine Göttingen UK's IT security policy and, if necessary, the FSA will work with the bank to introduce improves security processes.

1353 A firm cannot contract out compliance with its regulatory obligations[1979], and thus even though the website has been outsourced to FinanceWeb, Göttingen UK remains responsible to the FSA for any failure to mitigate operational risk appropriately. The main operational risk controls are the risk assessment which Göttingen UK must make, the terms of the outsourcing agreement, and the operational controls and checks which Göttingen UK puts in place.[1980] As this is a material outsourcing (because any failure of performance by FinanceWeb would be likely to cause Göttingen UK to be in breach of the Principles for Businesses[1981], Göttingen UK must report the arrangement to the FSA.[1982]

c) Losses suffered by bank customers

1354 If a bank customer suffers loss because of an IT security failure relating to this deal, the customer will claim in contract against Göttingen UK. The claim will be for:

- Failure to undertake transactions in accordance with the customer's mandate, e.g. failing to perform an online banking transaction initiated by the customer; or
- Wrongly debiting the customer's account when it did not have his mandate to do so[1983], e.g. if a security failure allows a third party to initiate payments from the customer's account; or
- Failure to manage the customer's account by exercising reasonable care and skill.[1984]

---

ure' approach. And although the idea that regulation should seek to eliminate all failures may look superficially appealing, in practice this would impose prohibitive costs on the industry and consumers." Financial Services Authority, *The FSA's risk-assessment framework* (August 2006) para 2.7.

[1979] FSA Handbook SYSC 3.2.4 G.

[1980] See generally FSA Handbook SYSC 3A.9.

[1981] FSA Handbook PRIN 2.1.1 R.

[1982] FSA Handbook SUP 15.3.8 G (1)(e).

[1983] *Orr v Union Bank* (1854) 1 Hacq HL 513, *Greenwood v Martin's Bank* [1933] AC 51.

[1984] Supply of Goods and Services Act 1982 s.13; see also *Tai Hing Cotton Mill Ltd. v Liu Chong Hing Bank Ltd.* [1986] AC 519.

1355 The only defence Göttingen UK would have to such a claim, assuming the customer can establish it, is that the contract between the bank and the customer excludes the bank's liability – see e.g. the Barclays Bank terms set out at 4.a) above. Most UK banks are signatories to the Banking Code[1985], and although subscription to the Code is voluntary it is likely that its provisions are in effect mandatory because of the Unfair Terms in Consumer Contracts Regulations 1999.[1986] The Code provides that the customer is not liable for unauthorised "not present" use of payment cards[1987], and although the Code does not specifically cover online banking it seems very likely that a court would hold that any term placing the identical risk on banks customers for their online accounts would be an unfair term, and thus unenforceable. It seems likely, therefore, that a customer's claim would only be rejected by the courts if the loss was caused by the customer's failure to meet his contractual security precautions (as in e.g. the Barclays Bank terms), and was thus in effect either the customer's own fault or not an expected consequence of Göttingen UK's own failure.

1356 Because this would be a contract claim, the customer could claim from Göttingen UK all the losses which would normally be expected to arise from a breach of contract of that kind.

1357 It is unlikely that any of the technology suppliers involved in this deal would owe a duty of care to the customer, on the principles explained at 3.b) above, and so a tortious claim would be unlikely.

d) Losses suffered by Göttingen UK

1358 If a breach of IT security occurs which causes loss to Göttingen UK, it will look to make a claim in contract against the responsible technology supplier. The aim of the contractual framework described at a) above is to identify all foreseeable security (and other risks), and then to allocate responsibility for them expressly between the contracting parties. If, therefore, the contracts have been negotiated properly, it will be clear who is responsible and whether their liability is limited in any way.

[1985] www.bankingcode.org.uk.

[1986] SI 1999/2083. Under those Regulations an unfair contractual term is not binding on the consumer. Given that the Banking Code has been negotiated extensively over many years by banks, building societies and consumer organisations, and that the current version of the Code has been approved by those negotiators, it will be very difficult indeed for a bank to argue that terms which are more onerous to the consumer than those set out in the Code are fair.

[1987] Banking Code section 12.2.

1359 If the loss is not caused by a breach on the part of any of its suppliers, then Göttingen UK itself will have to bear the loss.

H. Literaturverzeichnis

Abel, Ralf Bernd (Hrsg.)	Datenschutz in Anwaltschaft, Notariat und Justiz, 2. Auflage, München 2003 zitiert: *Bearbeiter*, in: Abel, Datenschutz in Anwaltschaft, Notariat und Justiz
Adams, Michael	Ökonomische Analyse der Gefährungs- und Verschuldenshaftung, Heidelberg 1985
Adams, Heinz/ Löhr, Volker	„Bedeutung von Qualitätssicerungssystemen in der entstehenden Haftungsgesellschaft“ in: QZ 36 (1991), 24-26
Altmeppen, Holger	„Die Auswirkungen des KonTraG auf die GmbH“ in: ZGR 1999, 291-313
Altmeppen, Holger	„Haftung der Geschäftsleiter einer Kapitalgesellschaft für Verletzung von Verkehrssicherungspflichten“ in: ZIP 1995, 881-882, 884-891
Angermüller, Niels O./ Eichhorn, Michael/ Ramke, Thomas	„MaRisk - Noch mehr Regulierung in Sicht?“ in: Kreditwesen 2004, 833-834
Angermüller, Niels O./ Eichhorn, Michael/ Ramke, Thomas	„MaRisk - der Nebel lichtet sich“ in: Kreditwesen 2005, 396-398
Anonymous	Der neue Hacker’s Guide, 2. Auflage, München 2001
Arbeitskreis "Externe und Interne Überwachung der Unternehmung" der Schmalenbach-Gesellschaft für Betriebswirtschaft e. V.	„Auswirkung des Sarbanes-Oxley Act auf die Interne und Externe Unternehmensüberwachung“ in: BB 2004, 2399-2407
Arendts, Martin	„Betrügerische Verhaltensweisen bei der Anlagebe-

	ratung und der Vermögensverwaltung“ in: ÖBA 1996, 775-781
Assmann, Heinz-Dieter/ Schneider, Uwe H.	Wertpapierhandelsgesetz, Kommentar, 4. Auflage, Köln 2006 zitiert: Assmann/Schneider-*Bearbeiter*
Assmann, Heinz-Dieter/ Kirchner, Christian/ Schanze, Erich	Ökonomische Analyse des Rechts, Tübingen 1993 zitiert: *Bearbeiter*, in: Assmann/Kirchner/Schanze
Auernhammer, Herbert	Bundesdatenschutzgesetz, 3. Auflage, Köln, Berlin, Bonn, München 1993 zitiert: Auernhammer-*Bearbeiter*
Aufhauser, Rudolf/ Hindinger-Back, Helmut	Bundesdatenschutzgesetz, Kochel am See 1996 zitiert: Aufhauser/Hindinger-Back-*Bearbeiter*
Backu, Frieder	„Pflicht zur Verschlüsselung?“ in: ITRB 2003, 251-253
Balzer, Peter	„Rechtsfragen des Effektengeschäfts der Direktbanken“ in: WM 2001, 1533-1542
Balzer, Peter	„Haftung von Direktbanken bei Nichterreichbarkeit“ in: ZBB 2000, 258-268
Bamberger, Heinz Georg/ Roth, Herbert	Kommentar zum Bürgerlichen Gesetzbuch, Bd. 1-3, München 2003 zitiert: Bamberger/Roth-*Bearbeiter*
Bartl, Harald	Produkthaftung nach neuem EG-Recht: Kommentar zum deutschen Produkthaftungsgesetz, Landsberg (Lech) 1989
Bartsch, Michael	„Software und das Jahr 2000“ in: CR 1998, 193-196

Bartsch, Michael	„Computerviren und Produkthaftung“ in: CR 2000, 721-725
Bartsch, Michael	Rechtsmängelhaftung bei Überlassung von Software, CR 2005, 1-10
Bartsch, Michael	Software und das Jahr 2000 – Haftung und Versicherungsschutz für ein technisches Großproblem, Baden-Baden 1998
Bauer, Axel	„Produkthaftung für Software nach geltendem und künftigem deutschen Recht“, Teile 1 und 2 in: PHi 1989, 38-48, 98-108
Baum, Florian	„Gestaltung von Software-Maintenance-Verträgen in der internationalen Praxis“ in: CR 2002, 705 ff.
Baumbach, Adolf/ Hueck, Alfred	GmbH-Gesetz, 18. Auflage, München 2006 zitiert: Baumbach/Hueck-*Bearbeiter*
Baumbach, Adolf/ Hopt, Klaus J.	Handelsgesetzbuch, Kommentar, München 2006 zitiert: Baumbach/Hopt-*Bearbeiter*
Bäumler, Helmut	„Ein Gütesiegel für den Datenschutz“ in: DuD 2004, 80-84
Baumol, Wiliam J.	Ecomonic Theory and Operations Analysis, 5. Auflage, London 1977
Bayer, Thomas	Auswirkungen eines zertifizierten Qualitätsmanagements nach DIN EN ISO 9000ff. auf die Haftungssituation im Unternehmen, Berlin 1988
Becker, Bernhard/ Janker, Bernd/ Müller, Stefan	„Die Optimierung des Risikomanagements als Chance für den Mittelstand“ in: DStR 2004, 1578-1584

Beckmann, Kirsten/ Müller, Ulf	„Online übermittelte Informationen - Produkte iSd Produkthaftungsgesetzes?“ in: MMR 1999, 14-18
Behnke, Alexander/ Schäffter, Markus	„IT-Entscheider in der Haftung“ in: DSB 2002, Nr 7/8, 10-11
Behrens, Peter	Die ökonomischen Grundlagen des Rechts, Tübingen 1986
Benöhr, Hans-Peter	„Die Entscheidung des BGH für das Vershuldensprinzip“ in: Tijdschrift voor Rechtsgeschiedenis 46, 1978, 1-32
Berndt, Thomas/ Hoppler, Ivo	„Whistleblowing - ein integraler Bestandteil effektiver Corporate Governance“ in: BB 2005, 2623-2629
Bigdoli, Hossein	Handbook of Information Security, Volume 1: Key Concepts, Infrastructure, Standards, and Protocols, 2006
Bigdoli, Hossein	Handbook of Information Security, Volume 2: Information Warfare; Social, Legal, and International Issues; and Security Foundations, 2006
Bigdoli, Hossein	Handbook of Information Security – Volume 3: Threats, Vulnerabilities, Prevention, Detection, and Management, 2006
Bigdoli, Hossein	Encyclopedia of Informationsystems Volume 1, Academic Press, Boston 2002
Bigdoli, Hossein	Encyclopedia of Informationsystems Volume 2, Academic Press, Boston 2002
Bigdoli, Hossein	Encyclopedia of Informationsystems Volume 4,

	Academic Press, Boston 2002
Birkmann, Andreas	„Produktbeobachtungspflicht bei Kraftfahrzeugen - Entwicklung und Weiterentwicklung der Produktbeobachtungspflicht durch die Rechtsprechung des Bundesgerichtshofs“ in: DAR 1990, 124-130
Bizer, Johann	„Bausteine eines Datenschutzaudits“ in: DuD 2006, 5-12
Blaurock, Uwe	„Haftung der Banken beim Einsatz neuer Techniken im Zahlungsverkehr“ in: CR 1989, 561-567
Böcker, Klaus/ Spielberg, Holger	„Basel II und ökonomisches Kapital: Risikoaggregation und Kopulas“ in: Die Bank 2005, 56-59
Bockslaff, Klaus	„Die eventuelle Verpflichtung zur Errichtung eines sicherungstechnischen Risikomanagements durch das KonTraG“ in: NVersZ 1999, 104-110
Bodewig, Theo	Vertragliche Pflichten „post contractum finitum“, JURA 2005, 505-512.
Boecken, Winfried	Deliktsrechtlicher Eigentumsschutz gegen reine Nutzungsbeeinträchtigungen, Berlin 1995
Bohne, Marco	„Zugriffsrechte effizient verwalten“ in: VW 2004, 1583-1584
Bölscher, Jens/ Kaiser, Christian/ v. Schulenurg, Johann-Matthias	„Hacker gibt es wirklich! Wachsende Gefährdung der Versicherungswirtschaft durch Hacker-Angriffe“ in: VW 2002, 565
Bömer, Roland	„Risikozuweisung für unvermeidbare Softwarefeh-

	ler“ in: CR 1989, 361-367
Boos, Karl-Heinz/ Fischer, Reinfried/ Schulte-Mattler, Hermann	Kreditwesengesetz, Kommentar zu KWG und Ausführungsvorschriften, 2. Auflage, München 2004 zitiert: Boos/Fischer/Schulte-Mattler-*Bearbeiter*
Borges, Georg	Rechtsfragen des Phishing – Ein Überblick in: NJW 2005, 3313-3317
Borsum, Wolfgang/ Hoffmeiser, Uwe	„Rechtsgeschäftliches Handeln unberechtigter Personen mittels Bildschirmtext“ in: NJW 1985, 1205-1207
Borsum, Wolfgang/ Hoffmeister, Uwe	„Rechtsgeschäftliches Handeln unberechtigter Personen mittels Bildschirmtext“ in: NJW 1985, 1205-1207
Brandi-Dohrn, Matthias	Gewährleistung bei Hard- und Softwaremängeln: BGB, Leasing und UN-Kaufrecht, 2. Auflage, München 1994
Bräutigam, Peter/ Leupold, Andreas (Hrsg.)	Online-Handel, München 2003 zitiert: *Bearbeiter*, in: Bräutigam/Leupold
Breulmann, Günter	Normung und Rechtsangleichung in der Europäischen Rechtsangleichung, Berlin 1993
Bröcker, Klaus Tim/ Czychowski, Christian/ Schäfer, Detmar	Praxishandbuch Geistiges Eigentum im Internet, München 2003 zitiert: *Bearbeiter*, in: Bröcker/Czychowski/Schäfer
Brown, John Prather	„Toward an Economic Theory of Liability“, in: The Journal of Legal Studies, Bd. 2, 1973, 323-349
Brüggemeier, Gert	Deliktsrecht, Baden-Baden 1986

Brüggemeier, Gert	„Produzentenhaftung nach § 823 Abs. 1 BGB – Bestandsaufnahme und Perspektiven weiterer judizieller Rechtsentwicklung“ in: WM 1982, 1249-1309
Brüggemeier, Gert	„Organisationshaftung“ in: AcP 191 (1991), 33-68
Bruns, Alexander	Informationsansprüche gegen Medien – Ein Beitrag zur Verbesserung des Persönlichkeitsschutzes im Medienprivatrecht, Diss. Iur. Universität Freiburg, Tübingen, 1997
Buchner, Herbert	Die Bedeutung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb für den deliktsrechtlichen Unternehmensschutz, München 1971
Büchting, Hans-Ulrich (Hrsg.)	Beck’sches Rechtanwalts-Handbuch, München 2004 zitiert: *Bearbeiter*, in: RAnwHdb
Büllingen, Franz/ Hillebrad, Annette	„Biometrie als Teil der Sicherungsinfrastruktur?“ in: DuD 2000, 339-343
Bülow, Dieter	„Regulatorische Anforderungen an die IT: Lösungswege einer ITSM/Provisioning-Plattform“ in: DSB 10/2005, 13-14
Bundesamt für Sicherheit in der Informationstechnik (BSI)	IT-Grundschutzhandbuch, Köln 2003
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Einführung von Intrusion-Detection-Systemen, http://www.bsi.bund.de/literat/studien/ids02/dokumente/Rechtv10.pdf
Bundesamt für Sicherheit in der Informationstechnik (BSI)	BSI-Lagebericht 2005, http://www.bsi.de/literat/lagebericht/lageber

	icht2005.pdf
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, Prüfungsschema für ISO 27001 Audits, http://www.bsi.bund.de/gshb/zert/ISO27001/Pruefschema06.pdf
Bundesrechtsanwaltskammer, Ausschuss Datenschutzrecht	Stellungnahme der Bundesrechtsanwaltskammer zu der Frage der Bestellung eines Beauftragten für Datenschutz in Rechtsanwaltskanzleien, BRAK-Stellungnahme-Nr. 31/2004, http://www.brak.de/seiten/pdf/Stellungnahmen/2004/StnBDSinKanzleien.pdf
Burg, Michael/ Gimnich, Martin	„Illegale Dialer im Internet“ in: DriZ 2003, 381-385
Burgartz, Dieter/ Blum, Thomas	QM-Optimizing in der Softwareentwicklung, 2. Auflage, Braunschweig 1998
Bürkle, Jürgen	„Auswirkungen der Unternehmensaufsicht nach dem KWG auf organisatorische Pflichten von Versicherungsunternehmen“ in: WM 2005, 1496-1505
Büssow, Thomas/ Taetzner, Tobias	„Sarbanes-Oxley Act Section 404: Internes Kontrollsystem zur Sicherstellung einer effektiven Finanzberichterstattung im Steuerbereich von Unternehmen - Pflicht oder Kür?“ in: BB 2005, 2437-2444
C & L Deutsche Revision (Hrsg.)	6. KWG-Novelle und neuer Grundsatz I, Frankfurt am Main, 1998
Cahn, Andreas	„Produkthaftung für verkörperte geistige Leistungen“ in: NJW 1996, 2899-2905

Calabresi, Guido	The Cost of Accidents, Yale, 2000
Callies, Christian/ Ruffert, Matthias	Kommentar zu EU-Vertrag und EG-Vertrag, 2. Auflage, Neuwied Kriftel Berlin 2006 zitiert: *Bearbeiter* in: Callies/Ruffert
Canaris, Claus-Wilhelm	Die Vertrauenshaftung im deutschen Privatrecht, München 1971 zitiert: *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht
Canaris, Claus-Wilhelm	Bankvertragsrecht 3. Auflage, Berlin New York 1988 zitiert: *Canaris*, Bankvertragsrecht
Capellaro, Christoph/ Füser, Karsten	„Basel II: IT-Risiken als Ratingkriterium“ in: Die Bank 2005, 68-71
Christiansen, Per	„Wahrheitswidrige Tatsachenbehauptung in einem Internetportal“ in: MMR 2004, 185-186
Cichon, Caroline	Internet-Vertäge, 2. Auflage, Köln 2005
Coase, Ronald H.	„The Problem of Social Cost“ in: The Journal of Law and Economics, Bd. 3, 1960, 1-44
Coase, Ronald H.	“Law and Economics at Chicago” in: The Journal of Law and Economics, Bd. 1, 2, 1993, 239-254
Coleman, James S.	Foundations of Social Theory, 3. Auflage, Cambridge, Mass. 2000
Conrad, Isabell	„Wege zum Quellcode“ in: ITRB 2005, 12-16
Cooter, Robert	“Economic Theories of Legal Liability”

	in: Journal of Economic Perspectives, Summer 1991, Volume 5 Issue 3, 11-30
Cooter, Robert/Ulen, Thomas	Law and Economics, Boston, Mass. 2004
Cosack, Tilman	Umwelthaftung im faktischen GmbH-Konzern, Frankfurt am Main, Berlin, Bern, New-York 1999
Cornelius, Kai/ Tschoepe, Sven	„Strafrechtliche Grenzen der zentralen E-Mail-Filterung und –Blockade“ in: K&R 2005, 269-271
Dauses, Manfred A. (Hrsg.)	Handbuch des EU-Wirtschaftsrechts, 16. Ergänzungslieferung, München 2006 zitiert: *Bearbeiter*, in: Dauses, Handbuch des EU-Wirtschaftsrechts
Dendorfer, Renate/ Niedderer, Sven-Erik	„Spam und andere Belästigungen aus dem Web. Einsatz von Filtertechnologie“ in: AuR 2006, 214-219
Derleder, Peter/ Knops, Kai-Oliver/ Bamberger, Heinz Georg	Handbuch zum deutschen Bankrecht, Wien New York 2004 zitiert: *Bearbeiter* in: Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bankrecht
Deutsch, Erwin/ Spickhoff, Andreas	Medizinrecht, 5. Auflage, Berlin, Heidelberg, New York 2003
Dietrich, Kay	„Typisierung von Softwareverträgen nach der Schuldrechtsreform“ in: CR 2002, 473
Dietrich, Martin	Produktbeobachtungspflicht und Schadenverhütungspflicht der Produzenten, Frankfurt/M 1994
Dörner, Heinrich	„Rechtsgeschäfte im Internet“

	in: AcP 202 (2002), 363-396
Dornseif, Maximillian/ Schumann, Kay H./ Klein, Christian	„Tatsächliche und rechtliche Risiken drahtloser Computernetzwerke“ in: DuD 2002, 226-230
Dreier, Thomas/ Schulze, Gernot	Urhebergesetz, Kommentar, 2. Aufl., München 2006 zitiert: Dreier/Schulze/*Bearbeiter*
Drygala, Tim/ Drygala, Anja	„Wer braucht ein Frühwarnsystem?“ in: ZIP 2000, 297-305
Dustmann, Andreas	Die privilegierten Provider, Baden-Baden 2001
Eckert, Claudia	IT-Sicherheit: Konzepte – Verfahren – Protokolle, 4. Auflage, München 2006
Eder, Klaus	„Die Autorität des Rechts“ in: Zeitschrift für Rechtssoziologie 8, 1987, 193-230
Ehmann, Eugen/ Helfrich, Marcus	EG-Datenschutzrichtlinie, Kurzkommentar, Köln 1999
Ehmann, Horst	„Informationsschutz und Informationsverkehr im Zivilrecht“ in: AcP 1888 (1988), 230 – 380
Eidenmüller, Horst	Effizienz als Rechtsprinzip, Tübingen 2005
Elbel, Thomas	Die datenschutzrechtlichen Vorschriften für Diensteanbieter im neuen Telekommunikationsgesetz auf dem Prüfstand des europäischen und deutschen Rechts, Berlin 2005
Endres, Alfred	Ökonomische Grundlagen des Haftungsrechts, Heidelberg 1991
Endres, Johannes	„Heute ein Admin“

	in: c't – Archiv 23/2005, 112-114
Endres	„Haftungsregeln für gentechnische Unfälle, das Problem der Haftungsobergrenze“ in: Jahrbuch für Sozialwissenschaft, Bd. 24, 1, 51-76
Engel, Friedrich-Wilhelm	„Produzentenhaftung für Software“ in: CR 1986, 702-708
Ensthaler, Jürgen/ Füßler, Andreas/ Nuissl, Dagmar	Juristische Aspekte des Qualitätsmanagements, Berlin 1997
Erben, Meinhard/ Zahrnt, Christoph	„Die Rechtsprechung zur Datensicherung“ in: CR 2000, 88-91
Erfurth, René	„Haftung für Missbrauch von Legitimationsdaten durch Dritte beim Online-Banking“ in: WM 2006, 2198-2207
Erman, Walter	Bürgerliches Gesetzbuch, Kommentar, Bd. 1 und 2, 11. Aufl., Köln 2004 zitiert: Erman/*Bearbeiter*, BGB, Bd.
Ernestus, Walter	„Protection Profile – Formale Beschreibung von Sicherheitsanforderungen“ in: DuD 2003, 68
Ernst, Stefan	„Die Verfügbarkeit des Source Code“ in: MMR 2001, 208-213
Ernst, Stefan	„Wireless LAN und das Strafrecht“ in: CR 2003, 898-901
Ernst, Stefan	„Internet und Recht“ in: JuS 1997, 776-782
Ernst, Stefan	Trojanische Pferde und die Telefonrechnung

	in: CR 2006, 590-594
Ernst, Stefan	Vertragsgestaltung im Internet, München 2003 zitiert: *Ernst*, Vertragsgestaltung im Internet
Ernst, Stefan (Hrsg.)	Hacker, Cracker und Computerviren: Recht und Praxis der Informationssicherheit, Köln 2004 *Bearbeiter,* in: Ernst, Hacker, Cracker & Computerviren
Ertl, Gunter	„Zivilrechtliche Haftung im Internet“ in: CR 1998, 179-185
Faber, Wolfgang	„Elemente verschiedener Verbraucherbegriffe in EG-Richtlinien, zwischenstaatlichen Übereinkommen und nationalem Zivil- und Kollisionsrecht“ in: ZeuP 1998, 854-892
Falke, Josef	Rechtliche Aspekte der Normung in den EG-Mitgliedsstaaten und der EFTA, Luxemburg 2000
Faustmann, Jörg	„Der deliktische Datenschutz“, in: VuR 2006, 260-263.
Fervers, Martin	„Die Haftung der Banken bei automatisierten Zahlungsvorgängen“ In: WM 1988, 1037-1044
Feuerich, Wilhelm E./ Weyland, Dag	Bundesrechtsanwaltsordnung, 6. Auflage, München 2003 zitiert: Feuerich/Weyland-*Bearbeiter*
Finke, Katja	Die Auswirkungen der europäischen technischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht, München 2001
Fischer, Hartmut	„Die rechtliche Bedeutung technischer Normen im

	Telekommunikationsbereich“ in: RDV 1995, 221-230
Fleischer, Holger	„Vorstandsverantwortlichkeit und Fehlverhalten von Unternehmensangehörigen – Von der Einzelüberwachung zur Errichtung einer Compliance-Organisation“ in: AG 2003, 291-300
Fleischer, Holger	„Zur Leitungsaufgabe des Vorstands im Aktienrecht“ in: ZIP 2003, 1-11
Fleischer, Holger (Hrsg.)	Handbuch des Vorstandsrechts, München 2006 zitiert: *Bearbeiter*, in: Fleischer, Handbuch des Vorstandsrechts
Flume, Werner	Allgemeiner Teil des Bürgerlichen Rechts Erster Band, Zweiter Teil – Die juristische Person, Berlin Heidelberg New York Hongkong u.a. 1983 zitiert: *Flume* AT II
Foerste, Ulrich	„Deliktische Haftung für Schlechterfüllung“ in: NJW 1992, 27-28
Foerste, Ulrich	„Zur Rückrufpflicht nach § 823 BGB und § 9 ProdSG – Wunsch und Wirklichkeit“ in: DB 1999, 2199-2201
Foerste, Ulrich	„Nochmals – Persönliche Haftung der Unternehmensleitung – die zweite Spur der Produkthaftung?“ in: VersR 2002, 1-6
Freiwald, Susan	“Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Def-

	amation" in: Harvard Journal of Law and Technology, Vol. 14, 2001, 569-654
Fritz-Aßmus, Dieter/ Tuchtfeld, Egon	„Basel II als internationaler Standard zur Regulierung von Banken" in: ORDO 54 (2003), 269-288
Fritzsche, Jörg/ Malzer, Hans M	„Ausgewählte zivilrechtliche Probleme elektronisch signierter Willenserklärungen" in: DNotZ 1995, 3-26
Frühauf, Karol/ Ludewig, Jochen/ Sandmayr, Helmut	Software-Projektmanagement und – Qualitätssicherung, 4. Auflage, Zürich 2004
Fuhrberg, Kai/ Häger, Dirk/ Wolf, Stefan	Internet-Sicherheit, 3. Auflage, München 2001
Gaumert, Uwe/ Zattler, Michaela	„Basel II: Handelsbuch-Risiken und Double Default-Effekt" in: Die Bank 2005, 55-59
Geiß, Joachim/ Doll, Wolfgang	Geräte- und Produktsicherheitsgesetz, Kommentar und Vorschriftensammlung, Stuttgart 2005
Geppert, Martin/ Piepenbrock, Hermann-Josef/ Schütz, Raimund/ Schuster, Fabian (Hrsg.)	Beck'scher TKG-Kommentar, 3. Auflage, München 2006 zitiert: Beck'scher TKG-Kommentar-*Bearbeiter*
Geppert, Martin/ Ruhle, Ernst-Olav/ Schuster, Fabian	Handbuch Recht und Praxis der Telekommunikation, 2. Aufl., Baden-Baden 2002
Gesmann-Nuissel, Dagmar/ Wenzel, Christian	„Produzenten- und Produkthaftung infolge abfallrechtlicher Produktverantwortung" in: NJW 2004, 117-122
Gliss, Hans	„IT-Sicherheit aus Sicht des Datenschutzbeauftragten" in: DSB 1996, Nr 5, 1-11

Gola, Peter	„Zwei Jahre neues Bundesdatenschutzgesetz - Zur Entwicklung des Datenschutzrechts seit 1991“ in: NJW 1993, 3109-3118
Gola, Peter/ Schomerus, Rudolf	Bundesdatenschutzgesetz, Kommentar, 8. Auflage, München 2005
Gorny, Peter	„Kategorien von Softwarefehlern“ in: CR 1986, 673-677
Göttert, Helmut	„Sicherheit für Datennetze“ in: VW 2001, 1972
Gounalakis, Georgius (Hrsg.)	Rechtshandbuch Electronic Business, München 2003 zitiert: *Bearbeiter*, in: Gounalakis
Grabau, Maik/ Schlee, Klaus	„Die neuen MaRisk – Herausforderungen aus Sicht der Sparkassen-Finanzgruppe“ in: Kreditwesen 2005, 392-394
Grant, Colin	“Whistle Blowers: Saints of Secular Culture” in: Journal of Business Ethics 2002, Vol. 39, Nr. 4, 391 – 399
Greger, Reinhard	„Mitverschulden und Schadensminderungspflicht – Treu und Glauben im Haftungsrecht?“ in: NJW 1985, 1130-1134
Gross, Werner	„Deliktische Außenhaftung des GmbH-Geschäftsführers“ in: ZGR 1998, 551-569
Grundmann, Stefan	„Europäisches Vertragsrechtsübereinkommen, EWG-Vertrag und § 12 AGBG“ in: IPRax 1992, 1-5

Gruson, Michael/ Kubicek, Matthias	„Der Sarbanes-Oxley Act, Corporate Governance und das deutsche Aktienrecht“, http://www.jura.uni-frank-furt.de/ifawz1/baums/Bilder_und_Daten/Arbeitspapiere/paper113.pdf
Gruson, Michael/ Kubicek, Matthias	„Der Sarbanes-Oxley-Act, Corporate Governance und das deutsche Aktienrecht, Teile I und II“ in: AG 2003, 337-352, 393-406
Günther, Andreas	Produkthaftung für Informationsgüter, Köln 2001
Hadding, Walther/ Hopt, Klaus J/ Schimansky, Herbert (Hrsg.)	Entgeltklauseln in der Kreditwirtschaft und E-Commerce von Kreditinstituten – Bankrechtstag 2001, Berlin, New York 2002 zitiert: *Bearbeiter*, in: Hadding/Hopt/Schimansky
Hager, Günter	„Zum Schutzbereich der Produzentenhaftung“ in: AcP 184 (1984), 413-438
Hager, Johannes	„Die Kostentragung bei Rückruf fehlerhafter Produkte“ in: VersR 1984, 799-807
Hammer, Volker/ Bizer, Johann	„Beweiswert elektronisch signierter Dokumente“ in: DuD 1993, 689-699
Hanau, Peter/ Hoeren, Thomas	Private Internetnutzung durch Arbeitnehmer, München 2003 zitiert: Hanau/Hoeren, Private Internetnutzung durch Arbeitnehmer
Härting, Niko	„IT-Sicherheit in der Anwaltskanzlei“ in: NJW 2005, 1248-1250
Härting, Niko	„Unverschlüsselte E-Mails im anwaltlichen Ge-

	schäftsverkehr – Ein Verstoß gegen die Verschwiegenheitspflicht?“ in: MDR 2001, 61-63
Härting, Niko/ Schirmbacher, Martin	„Dialer: Das Urteil fällt und viele Fragen offen“ in: CR 2004, 334-338
Hartung, Wolfgang/ Holl, Thomas	Anwaltliche Berufsordnung, 2. Auflage, München 2001
Hasselblatt, Gordian N.	Die Grenzziehung zwischen verantwortlicher Fremd- und eigenverantwortlicher Selbstgefährdung im Deliktsrecht, Frankfurt/Oder 1996
Hauschka, Christoph E.	„Corporate Compliance – Unternehmensorganisatorische Ansätze zur Erfüllung der Pflichten von Vorständen und Geschäftsführern“ in: AG 2004, 461-475
Häusgen, Frank	„Mit durchgängigen IT-Infrastrukturen die Möglichkeiten des Kapitalanlagemanagements erweitern“ in: VW 2004, 1552-1554
Heckeroth, Klaus	„Die Anforderungen der Jahr-2000-Anpassung an Geschäftsleiter und Abschlussprüfer“ in: DB 1999, 702-707
Heiss, Helmut	„Inhaltskontrolle von Rechtswahlklauseln in AGB nach europäischem Internationalem Privatrecht?“ in: RabelsZ 2001, 634-653
Hellner, Thorwald	„Rechtsfragen des Zahlungsverkehrs unter besonderer Berücksichtigung des Bildschirmtextverfahrens“ in: Hadding, Walther/Mertens, Hans-Joachim/Immenga, Ulrich/Pleyer, Kle-

	mens/Schneider, Uwe W (Hrsg.), Festschrift für Winfried Werner zum 65. Geburtstag am 17. Oktober 1984, Berlin, New York 1984, S. 251-280
Hellner, Thorwald/ Steuer, Stephan	Bankrecht und Bankpraxis – Loseblatt – Stand Oktober 2006, Köln zitiert: *Bearbeiter* in: Hellner/Steuer
Henssler, Martin	„Das anwaltliche Berufsgeheimnis“ in: NJW 1994, 1817-1824
Henssler, Martin/ Prütting, Hanns	Bundesrechtsanwaltsordnung, 2. Auflage, München 2004 zitiert: *Bearbeiter,* in: Henssler/Prütting
Hermeler, Angelika Elisabeth	Rechtliche Rahmenbedingungen der Telemedizin, München 2000
Herrmann, Harald	„Die Rückrufhaftung des Produzenten“ in: BB 1985, 1801-1812
Heun, Sven-Erik	„Die elektronische Willenserklärung“ in: CR 1994, 595-600
Heussen, Benno	„Unvermeidbare Softwarefehler“ in: CR 2004, 1-10
Heussen, Benno/ Damm, Maximilian	„Millennium Bug: Manager- und Beraterhaftung bei unterlassener Systemprüfung und Notfallplanung“ in: BB 1999, 481-489
Heussen, Benno/ Schmidt, Markus	„Inhalt und rechtliche Bedeutung der Normenreihe DIN/ISO 9000 bis 9004 für die Unternehmenspraxis“ in: CR 1995, 321-332

Hilber, Marc/ Hartung, Jürgen	„Auswirkungen des Sarbanes-Oxley Act auf deutsche WP-Gesellschaften: Konflikte mit der Verschwiegenheitspflicht der Wirtschaftsprüfer und dem Datenschutzrecht“ in: BB 2003, 1054-1060
Hilty, Reto M. (Hrsg.)	Information Highway, Bern 1996 zitiert: *Bearbeiter*, in: Hilty, Information Highway
Hinsch, Christian	„Eigentumsverletzungen an neu hergestellten und an vorbestehenden Sachen durch mangelhafte Einzelteile“ in: VersR 1992, 1053-1058
Höckelmann, Eckhard	Die Produkthaftung für Verlagserzeugnisse, Baden-Baden 1994
Hölzlwimmer, Gerhard	Produkthaftungsrechtliche Risiken des Technologietransfers durch Lizenzverträge, München 1995
Hoeren, Thomas	„Die Pflicht zur Überlassung des Quellcodes“ in: CR 2004, 721-724
Hoeren, Thomas	„Produkthaftung für Software - Zugleich eine kritische Erwiderung auf Bauer, PHI 1989, 38ff und 98ff“ in: PHi 1989, 138-144
Hoeren, Thomas	„Virenscanning und Spamfilter - Rechtliche Möglichkeiten im Kampf gegen Viren, Spams & Co“ in: NJW 2004, 3513-3517
Hoeren, Thomas	„Risikoprüfung in der Versicherungswirtschaft“ in: VersR 2005, 1014-1023
Hoeren, Thomas/ Ernstschneider, Thomas	„Das neue Geräte- und Produktsicherheitsgesetz

	und seine Anwendung auf die IT-Branche“ in: MMR 2004, 507-513
Hoeren, Thomas/ Schüngel, Martin (Hrsg.)	Rechtsfragen der digitalen Signatur, Berlin 1999 zitiert: *Bearbeiter*, in: Hoeren/Schüngel
Hoeren, Thomas/ Sieber, Ulrich (Hrsg.)	Handbuch Multimedia-Recht, 13. Ergänzungslieferung, München 2006 zitiert: *Bearbeiter*, in: Hoeren/Sieber
Hörl, Bernhard	„Nachbesserung und Gewährleistung für fehlende Jahr-2000-Fähigkeit von Software“ – Anmerkung zu LG Leipzig, Urteil v. 23.07.1999 – 03 O 2479/99 in: CR 1990, 605-609
Hoffmann, Helmut	„Zivilrechtliche Haftung im Internet“ in: MMR 2002, 284-289
Hofmann, Christof/ Lesko, Michael/ Vorgrimler, Stefan	„Risikomanagement: Eigene EAD-Schätzung für Basel II“ in: Die Bank 2005, 48-52
Hohmann, Harald	„Haftung der Softwarehersteller für das’Jahr-2000’ Problem“ in: NJW 1999, 521-526
Hollmann, Hermann H	„Die EG-Produkthafungslinie, Teile (I) und (II)“ in: DB 1985, 2389-2396 und 2439-2443
Holznagel, Bernd	Recht der IT-Sicherheit, München 2003
Hommelhoff, Peter	„Risikomanagement im GmbH-Recht“ in: Berger, Klaus P./Ebke, Werner F./Elsing, Siegfried H. (Hrsg.), Festschrift für Otto Sandrock zum 70. Geburtstag, Heidelberg 2000, 373-383

Honsell, Heinrich	„Produkthaftungsgesetz und allgemeine Deliktshaftung“ in: JuS 1995, 211-215
Hopt, Klaus J.	„Grundsatz- und Praxisprobleme nach dem Wertpapiergesetz“ in: ZHR 159, 135-163 (1965)
Hüffer, Uwe	Aktiengesetz, 7. Auflage, München 2006
Huth, Rainer	Die Bedeutung technischer Normen für die Haftung des Warenherstellers nach § 823 BG und dem Produkthaftungsgesetz, Frankfurt am Main, Berlin, Bern, New-York 1992
Hütten, Christoph/ Stromann, Hilke	„Umsetzung des Sarbanes-Oxley Act in der Unternehmenspraxis“ in: BB 2003, 2223-2227
Imhof, Ralf/ Wahl, Adalbert	„Auf der Suche nach der verlorenen Zeit: Das Jahr-2000-Problem“ in: WpK-Mitt. 1998, 136-141
Intveen, Michael	„Weitere Einzelheiten zu Haftungsklauseln in Allgemeinen Geschäftsbedingungen im kaufmännischen/unternehmerischen Verkehr“ in: ITRB 2003, 13-15
Jaeger, Lothar	“Grenzen der Kündigung von Softwarepflegeverträgen über langlebige Industrie-Software“ in: CR 1999, 209-213
Janisch, Sonja/ Schartner, Peter	„Internetbanking“ in: DuD 2002, 162-169
Jaskulla, Ekkehard M	“Direct Banking im Cyberspace”

	in: ZBB 1996, 214-224
Jhering, Rudolf	Das Schuldmoment im römischen Privatrecht, Giessen 1867
Johnson, Roberta Ann	Whistleblowing – When it works and why, London 2003
Jungk, Antje	„Haftpflichtfragen“ in: AnwBl 2001, 170-173
Junker, Abbo	„Die Entwicklung des Computerrechts im Jahre 1999“ in: NJW 2000, 1304-1312
Junker, Abbo	„Die Entwicklung des Computerrechts in den Jahren 2003/2004“ in: NJW 2005, 2829-2834
Jürgens, Andreas	Technische Standards im Haftungsrecht, Göttingen 1995
Kahlert, Henning	„Unlautere Werbung mit Selbstverpflichtungen“ in: DuD 2003, 412-416
Karger, Michael	„Kooperation bei komplexer Softwareentwicklung“ in: ITRB 2004, 208-210
Karper, Irene	Sorgfaltspflichten beim Online-Banking – Der bankkunde als Netzwerkprofil? in: DuD 2006, 215-219
Kassebohm, Kristian/ Malorny, Christian	„Auditing und Zertifizierung im Brennpunkt wirtschaftlicher und rechtlicher Interessen“ in: ZfB 1994, 693-716
Kassebohm, Kristian/ Malorny, Christian	„Die strafrechtliche Verantwortung des Managements“ in: BB 1994, 1361-1371

Katko, Peter	„Voice over IP“ in: CR 2005, 189-193
Kaufmann, Bernd	„Neuordnung des Rechts der technischen Anlagensicherheit im Hinblick auf den Europäischen Binnenmarkt“ in: DB 1994, 1033-1038
Keenan, J.P.	“Blowing the Whistle on Less Serious Forms of Fraud: A Study of Executives and Managers” in: Employee Responsibilities and Rights Journal Vol. 12, Nr. 4, 199-217
Keller, Gernot/ Schlüter, Kai Grit	„Peer Review: Perspektiven nach dem Sarbanes-Oxley Act of 2002“ in: BB 2003, 2166-2174
Kilian, Wolfgang	„Vertragsgestaltung und Mängelhaftung bei Computersoftware“ in: CR 1986, 187-196
Kilian, Wolfgang/ Heussen, Benno	Computerrechts-Handbuch : Computertechnologie in der Rechts- und Wirtschaftspraxis, Loseblatt-Ausg., München 1990 – zitiert; *Bearbeiter*, in: Kilian/Heussen
Kind, Michael/ Werner, Dennis	„Rechte und Pflichten im Umgang mit PIN und TAN“ in: CR 2006, 353-360
Kirchgässner, Gebhard	Homo oeconomicus, 2. Auflage, Tübingen 2000
Klapdor, Martin	„IT-Risiken im virtuellen Netzwerk realitätsnah prüfen“ in: VW 2005, 507

Klindt, Thomas	„Der new approach im Produktrecht des europäischen Binnenmarkts - Vermutungswirkung technischer Normung“ in: EuZW 2002, 133-136
Klindt, Thomas	„Das neue Geräte- und Produktsicherheitsgesetz“ in: NJW 2004, 465-471
Klindt, Thomas	Geräte- und Produktsicherheitsgesetz (GPSG), München 2007 zitiert: *Klindt*, GPSG
Klinger, Max	Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, Tübingen 1998
Klutzny, Alexander	Online-Demonstrationen und virtuelle Sitzblockaden – Grundrechtsausübung oder Straftat? in: RDV 2006, 50-59
Knolmayer, Gerhard/ Wermelinger, Thomas	Der Sarbanes-Oxley Act und seine Auswirkungen auf die Gestaltung von Informationssystemen, http://www.ie.iwi.unibe.ch/publikationen/berichte/resource/WP-179.pdf
Koch, Frank A.	Computer-Vertragsrecht, 6. Auflage, Freiburg 2002
Koch, Frank A.	„Rechtsfragen der Nutzung elektronischer Kommunikationsdienste“ in: BB 1996, 2049-2058
Koch, Frank A.	„Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen“ in: CR 1997, 193-203
Koch, Robert	„Haftung für die Weiterverbreitung von Viren durch E-Mails“ in: NJW 2004, 801- 807

Koch, Robert	„»Mängelbeseitigungsansprüche« nach den Grundsätzen der Produzenten-/ Produkthaftung“ in: AcP 203 (2003), 603-632
Koch, Robert	Versicherbarkeit von IT-Risiken, Berlin 2005
Koenig, Christian/ Loetz, Sascha/ Neumann, Andreas	Telekommunikationsrecht, Heidelberg 2004
Köhler, Helmut	„Die haftungsrechtliche Bedeutung technischer Regeln“ in: BB 1985, Beilage 4, 10-15
Köhler, Helmut	„Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen“ in: AcP 182 (1982), 126-270
Köndgen, Johannes (Hrsg.)	Neue Entwicklungen im Bankhaftungsrecht, Köln 1989
Kötz, Hein	Deliktsrecht, 10. Auflage, München 2006
Kötz, Hein/ Schäfer, Hans-Bernd	Judex oeconomicus, Tübingen 2003
Kraft, Dennis/ Meister, Johannes	„Rechtsprobleme virtueller Sit-ins“ in: MMR 2003, 366-374
Kröger, Detlef/ Gimmy, Marc A. (Hrsg.)	Handbuch zum Internet-Recht, 2. Auflage Berlin Heidelberg, New York 2002 zitiert: *Bearbeiter*, in: Kröger/Gimmy
Kropff, Bruno/ Semler, Johannes (Hrsg.)	Münchener Kommentar zum Aktiengesetz, 2. Auflage, München 2000 ff. zitiert: MünchKommAktG-*Bearbeiter*
Krüger, Thomas/ Bütter, Michael	„Elektronische Willenserklärungen im Bankgeschäftsverkehr - Risiken des Online-Banking“

	in: WM 2001, 221-231
Krüger, Thomas/ Büttner, Michael	„Justitia goes online – Elektronischer Rechtsverkehr im Zivilprozess“ in: MDR 2003, 181-189
Kübler, Friedrich	„Effizienz als Rechtsprinzip“ in: Baur, Jürgen F./Hopt, Klaus J./Mailänder, Festschrift für Ernst Steindorff zum 70. Geburtstag am 13. März 1990, 687-704
Kuhn, Matthias	Rechtshandlungen mittels EDV und Telekommunikation, München 1991
Kühne, Hans-Heiner	„Strafbarkeit der Zugangsvermittlung von pornographischen Informationen im Internet“ in: NJW 1999, 188-190
Kühnhauser, Winfried E.	„Root Kits“ in: DuD 2003, 218-222
Kullmann, Hans-Josef	„Die Rechtsprechung des BGH zum Produkthaftungspflichtrecht in den Jahren 1989/90“ in: NJW 1991, 675-683
Kullmann, Hans-Josef	„Die Rechtsprechung des BGH zum Produkthaftungspflichtrecht in den Jahren 1994-1995“ in: NJW 1996, 18-26
Kullmann, Hans-Josef	„Die Rechtsprechung des BGH zum Produkthaftpflichtrecht in den Jahren 1995-1997“ in: NJW 1997, 1746-1753
Kullmann, Hans-Josef	„Die Rechtsprechung des Bundesgerichtshofs zum Produkthaftpflichtrecht in den Jahren 1997/98“ in: NJW 1999, 96-102

Kullmann, Hans-Josef	„Die Rechtsprechung des BGH zum Produkthaft-pflichtrecht in den Jahren 1992-1994“ in: NJW 1994, 1698-1707
Kullmann, Hans-Josef	„Die Rechtsprechung des BGH zum Produkthaft-pflichtrecht in den Jahren 2000 und 2001“ in: NJW 2002, 30-36
Kullmann, Hans-Josef/ Pfister, Bernhard	Produzentenhaftung, 1/05 Ergänzungslieferung, Berlin 2005 zitiert: Kullmann/Pfister-*Bearbeiter*
Kümpel, Siegfried	Bank- und Kapitalmarktrecht, 3. Auflage, Köln 2004
Kümpel, Siegfried/ Veil, Rüdiger	Wertpapierhandelsgesetz, 2. Auflage, Berlin 2006
Kunst, Diana	„Rechtliche Risiken des Internet-Banking“ in: MMR Beilage 9/2001, 23-26
Kunz, Jürgen	„Die Produktbeobachtungs- und Befundsicherungs-pflicht als Verkehrssicherungspflichten des Warenherstellers“ in: BB 1994, 450-455
Kurose, James F./ Ross, Keith, W.	Computer Networking, Second Edition, Boston 2003
Lachmann, Jens Peter	„Ausgewählte Probleme aus dem Recht des Bild-schirmtextes“ in: NJW 1984, 405-408
Lang, Markus	„PC, aber sicher! – Sicherheit beim Einsatz von Personalcomputern“ in: JurPC Web-Dok. 205/2001, Abs. 1-166
Lang, Volker	„Die Beweislastverteilung im Falle der Verletzung von Aufklärungs- und Beratungspflichten bei Wertpapierdienstleistungen“

	in: WM 2000, 450-476
Lange, Hermann/ Schiemann, Gottfried	Schadensersatz, 3. Auflage., Tübingen 2003
Lange, Knut W./ Wall, Friederike (Hrsg.)	Risikomanagement nach dem KonTraG, München 2001 zitiert: *Bearbeiter,* in: Lange/Wall
Langenbucher, Katja	Die Risikozuordnung im bargeldlosen Zahlungsverkehr, München 2001
Lapp, Thomas	„Fax- und E-Mail-Kommunikation“ in: BRAK-Mitt 1997, 106-108
Larenz, Karl	Lehrbuch des Schuldrechts, Erster Band, Allgemeiner Teil, 14. Auflage, München 1987
Larenz, Karl	Lehrbuch des Schuldrechts, Zweiter Band, Besonderer Teil, 1. Halbband, 13. Auflage, München 1986
Larenz, Karl/ Canaris, Claus-Wilhelm	Lehrbuch des Schuldrechts, Zweiter Band, Besonderer Teil, 2. Halbband, 13. Auflage, München 1994
Laufs, Adolf/ Uhlenbruck, Wilhelm (Hrsg)	Handbuch des Arztrechts, 3. Auflage., München 2002 zitiert: *Bearbeiter*, in: Laufs/Uhlenbruck,
Lehmann, Michael (Hrsg.)	Rechtsschutz und Verwertung von Computerprogrammen, 2. Auflage, Köln 1993 zitiert: *Bearbeiter*, in: Lehmann, Rechtsschutz und Verwertung von Computerprogrammen
Leible, Stefan/ Sosnitza, Olaf	„Schadensersatzpflicht wegen Virenbefall von Disketten“ in: K&R 2002, 51-52
Leible, Stefan/ Sosnitza, Olaf	„Neues zur Störerhaftung von Internet-Auktionshäusern“

	in: NJW 2004, 3225
Leible, Stefan/ Sosnitza, Olaf	Versteigerung im Internet, Heidelberg 2004 zitiert: *Bearbeiter* in: Leible/Sosnica, Versteigerung im Internet
Leible, Stefan/ Wildemann, Andree	Kommentar zu BGH, Urteil v. 04.03.2004 – III ZR 96/03 in: K&R 2004, 288-290
Leisinger, Klaus M.	Whistleblowing und Corporate Reputation Management, München, Mering 2003
Lenz, Hansrudi	„Sarbanes-Oxley-Act of 2002 - Abschied von der Selbstregulierung der Wirtschaftsprüfer in den USA“ in: BB 2002, 2270-2275
Lenz, Tobias	„Das neue Geräte- und Produktsicherheitsgesetz“ in: MDR 2004, 918-922
Libertus, Michael	„Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren“ in: MMR 2005, 507-512
Lier, Monika	„Dies und das aus der elektronischen Versicherungswelt“ in: VW 2004, 554-563
Lindacher, Walter F.	„Unlauterer Wettbewerb bei einem DIN-Norm-Verstoß“ in: BB 1981, 144-145
Littbarski, Sigurd	„Herstellerhaftung ohne Ende – Ein Segen für den Verbraucher?“ in: NJW 1995, 217-222

Littbarski, Sigurd	„Kapriolen um die Instruktionspflichten des Herstellers“ in: NJW 2004, 1161-1163
Littbarski, Sigurd	„Das neue Geräte- und Produktsicherheitsgesetz: Grundzüge und Auswirkungen auf die Haftungslandschaft“ in: VersR 2005, 448-458
Litzenburger, Wolfgang	„Das Ende des vollständigen Gewährleistungsausschlusses beim Kaufvertrag über gebrauchte Immobilien“ in: NJW 2002, 1244-1247
Lobinger, Thomas	„Zur vertraglichen Einstandspflicht des Anschlussinhabers für die Annahme von R-Gesprächen durch unbefugte Dritte“ in: JZ 2006, 1076-1080
Loewenheim, Ulrich/Koch, Frank A. (Hrsg.)	Praxis des Online-Rechts zitiert: *Bearbeiter* in Loewenheim/Koch (Hrsg.), Praxis des Online-Rechts
Looschelders, Dirk	Schuldrecht Allgemeiner Teil, 4. Aufl., München 2006
Looschelders, Dirk	Internationales Privatrecht, Art. 3-46 EGBGB, Kommentar, Berlin 2004
Lorenz, Egon	„Zur Haftung für durch einen Stromausfall verursachte Schäden, der durch einen Kurzschluß an einem einer BGB-Gesellschaft gelieferten fehlerhaften Baustromverteiler hervorgerufen worden ist“ in: VersR 1990, 1284- 1285
Löwe, Walter	„Rückrufpflicht des Warenherstellers“

	in: DAR 1978, 288-296
Lüke, Gerhard/ Wax, Peter	Münchener Kommentar zur Zivilprozessordnung Band 1 §§ 1-354, 2. Auflage, München 2000 zitiert: MünchKommZPO-*Bearbeiter*
Lüke, Gerhard/ Wax, Peter	Münchener Kommentar zur Zivilprozessordnung Aktualisierungsband ZPO-Reform 2002, München 2002 zitiert: MünchKommZPO-*Bearbeiter*
Lutter, Markus/ Hommelhoff, Peter	GmbH-Gesetz, 16. Auflage, Köln 2004 zitiert: Lutter/Hommelhoff-*Bearbeiter*
Luttermann, Claus	„Unabhängige Bilanzexperten in Aufsichtsrat und Beirat“ in: BB 2003, 745-750
Malzer, Hans Michael	„Anspruch des Verwenders von Individualsoftware auf Herausgabe des Quellenprogramms (Quellcode) und der Herstellerdokumentation“ in: CR 1989, 991-992
Mankowski, Peter	„Kein Telefonentgeltanspruch für Verbindungen durch ein heimlich installiertes Anwahlprogramm – Dialer“ in: MMR 2004, 312-315
Mankowski, Peter	„Die Beweislastverteilung in 0190er-Prozessen“ in: CR 2004, 185-189
Mankowski, Peter	„Schuldrechtsreform: Werkvertragsrecht - Die Neuerungen durch § 651 BGB und der Abschied vom Werklieferungsvertrag“ in: MDR 2003, 854-860

Mankowski, Peter	„Für einen Anscheinsbeweis hinsichtlich der Identität des Erklärenden bei E-Mails“ in: CR 2003, 44-50
Mankowski, Peter	„Sofort-Option bei E-Bay“ in: MMR 2004, 181-183
Mankowski, Peter	„Überlegungen zur sach- und interessengerechten Rechtswahl für Verträge des internationalen Wirtschaftsverkehrs“ in: RIW 2003, 2-15
Marburger, Peter (Hrsg.)	Technische Regeln im Umwelt- und Technikrecht (UTR), Band 86, Berlin 2006 zitiert: *Bearbeiter*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht
Marburger, Peter	„Herstellung nach zwingenden Rechtsvorschriften als Haftungsausschlussgrund im neuen Produkthaftungsrecht“ in: Leßmann, Herbert/Großfeld, Bernhard/Vollmer, Lothar (Hrsg.), Festschrift für Rudolf Lukes zum 65. Geburtstag, Köln, Berlin, Bonn, München 1989, 97-119
Marburger, Peter	Die Regeln der Technik im Recht, Köln, Bonn, Berlin, München 1979
Marburger, Peter	„Die haftungs- und versicherungsrechtliche Bedeutung technischer Regeln“ in: VersR 1983, 597-608
Marburger, Peter	„Produktsicherheit und Produkthaftung“ in: Ahrens, Hans-Jürgen/v. Bar, Christian/Fischer, Gerfried/Spickhoff, Andreas/Taupitz, Jochen (Hrsg.), Festschrift für Erwin Deutsch

	zum 70. Geburtstag, Köln, Berlin, Bonn, München 1999, 271-289
Marburger, Peter	„Grundsatzfragen des Haftungsrechts unter dem Einfluß der gesetzlichen Regelungen zur Produzenten- und zur Umwelthaftung“ in: AcP 192 (1992), 1-34
Marly, Jochen	Softwareüberlassungsverträge, 4. Auflage, München 2004
Mathis, Klaus	Effiziens statt Gerechtigkeit?, 2. Auflage, Berlin 2006
Maul, Silja/ Lanfermann, Georg	„Europäische Corporate Governance – Stand der Entwicklungen” in: BB 2004, 1861-1868
Mayer, Kurt	„Produkthaftung und Gefahrbeseitigungsanspruch,(Stichwort – ‚Rückrufpflicht’)“ in: DB 1985, 319-326
Medicus, Dieter	Bürgerliches Recht, 20. Auflage, Köln Berlin Bonn München 2004 zitiert: *Medicus*, Bürgerliches Recht
Meier, Klaus/ Wehlau, Andreas	„Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung“ in: NJW 1998, 1585-1591
Meier, Klaus/ Wehlau, Andreas	„Produzentenhaftung des Softwareherstellers“ in: CR 1990, 95-100
Meister, Herbert	Datenschutz im Zivilrecht – Das Recht am eigenen Datum, 2. Aufl., Bergisch-Gladbach 1981
Melullis, Klaus-J.	„Zum Regelungsbedarf bei der elektronischen Willenserklärung“ in: MDR 1994, 109-114

Mertens, Hans-Joachim/ Mertens, Georg	„Zur deliktischen Eigenhaftung des Geschäftsführers einer GmbH bei Verletzung ihm übertragener organisatorischer Pflichten“ – Anmerkung zu BGH Urteil –. 05.12.1989 - VI ZR 335/88 in: JZ 1990, 488-490
Meyer, Andreas	„Die Haftung für fehlerhafte Aussagen in wissenschaftlichen Werken“ in: ZUM 1997, 26-34
Meyer-Sparenberg, Wolfgang	„Rechtswahlvereinbarungen in Allgemeinen Geschäftsbedingungen“ in: RIW 1989, 347-351
Michalski, Lutz	„Produktbeobachtung und Rückrufpflicht des Produzenten“ in: BB 1998, 961-965
Miceli, Thomas J.	Economics of the Law, New York 1997
Mitglieder des Bundesgerichtshofs (Hrsg.)	Das Bürgerliche Gesetzbuch, Kommentar mit besonderer Berücksichtigung des Reichsgerichts und des Bundesgerichtshofes, 12. Auflage, Berlin 2000 zitiert: RGRK-*Bearbeiter*
Möller, Klaus/ Kelm, Stefan	„Distributed Denial-of-Service Angriffe (DDoS)” in: DuD 2000, 292-293
Möllers, Thomas M. J.	Rechtsgüterschutz im Umwelt- und Haftungsrecht: präventive Verkehrspflichten und Beweiserleichterungen in Risikolagen, Tübingen 1996
Möllers, Thomas M. J.	„Qualitätsmanagement, Umweltmanagement und Haftung“

	in: DB 1996, 1455-1461
Möllers, Thomas M. J.	„Versicherungspflichten gegenüber Kindern“ in: VersR 1996, 153-160
Moritz, Hans-Werner	„Quo vadis elektronischer Geschäftsverkehr?“ in: CR 2000, 61-72
Müller-Hengstenberg, Claus D.	„Der Vertrag als Mittel des Risikomanagements“ in: CR 2005, 385-392
Müller-Hengstenberg, Claus D./ Krcmar, Helmut	„Mitwirkungspflichten des Auftraggebers bei IT-Projekten“ in: CR 2002, 549 ff.
Müller-Hengstenberg, Claus D.	„Computersoftware ist keine Sache“ in: NJW 1994, 3128-3134
Müller-Reichart, Matthias/ Dura, Annett/ Fischer, Harry/ Nosty, Filip	„Finanzberater und Versicherungsmakler als Risk Advisors nach Basel II“ in: VW 2002, 625
Münch, Peter	„Harmonisieren – dann Auditieren und Zertifizieren“ in: RDV 2003, 223-231
Musielak, Hans-Joachim	„Beweislastverteilung nach Gefahrenbereichen“ in: AcP 176 (1976), 465-486
Musielak, Hans-Joachim	Zivilprozessordnung, Kommentar (ZPO), 5. Auflage, München 2007 zitiert: Musielak-*Bearbeiter*
Near, J.P./Miceli, M.P.	“Organizational Dissidence: The Case of Whistleblowing” in: Journal of Business Ethics 1985, Nr. 4, 1-16
Neumann, Diana/Bock, Christian	Zahlungsverkehr im Internet, München 2004

Nickel, Friedhelm/Kaufmann, Lars	„Produktsicherheit und Produzentenhaftung“ in: VersR 1998, 948-954
Niebling, Jürgen	Die CE-Kennzeichnung, Stuttgart, Hannover 1995
Niebling, Jürgen	„Gewährleistung und Produkthaftung bei fehlender CE-Kennzeichnung“ in: DB 1996, 80-81
Otto, Franz	„Verkehrssicherungspflichten“ – Anmerkung zu OLG Karlsruhe, Urteil v. 2.10.1996 – 7 U 210/93 in: VersR 1997, 1155-1157
Palandt, Otto	Bürgerliches Gesetzbuch, 66. Auflage, München 2007 zitiert: Palandt-*Bearbeiter*
Paul, Stephan/Stein, Stefan/Kaltofen, Daniel	„Kapitalanforderungen für Retail-Portfolios nach Basel II“ in: Die Bank 2004, 342-349
Pauli, A.	„Die Produktbeobachtungspflichten in der verbraucherpolitischen Auseinandersetzung“ in: PHi 1985, 134 ff.
Pauly, Mark V./Kenneth, J. Arrow	„The Economics of Moral Hazard“ in: The American Economic Review, Nashville, Tenn. Bd. 58, 1968, 531-537
Pawlowski, Hans-Martin	Allgemeiner Teil des BGB, 6. Auflage, Heidelberg 2000 zitiert: *Pawlowski*, Allgemeiner Teil des BGB
Peikari, Cyrus/ Chuvakin, Anton	Kenne Deinen Feind, Köln 2004
Peine, Franz-Joseph	Gesetz über technische Arbeitsmittel, Kommentar, 3. Auflage, Köln 2002

Pellens, Bernhard	„Überregulierung der Kapitalmärkte?“ in: DBW 2003, 473-476
Peters, Falk/ Kersten, Heinrich	„Technisches Organisationsrecht i– Datenschutz - Bedarf und Möglichkeiten“ in: CR 2001, 576-581
Petrasch, Roland	Einführung in das Software-Qualitätsmanagement, Berlin 2001
Pfeifer, Uwe	„Solvency II – ein Thema für die IT?“ in: VW 2005, 1558-1564
Pfeiffer, Thomas	„Vom kaufmännischen Verkehr zum Unternehmensverkehr“ in: NJW 1999, 169-174
Pfingsten, Andreas/ Maifarth, Michael/ Rieso, Sven	„Grundkonzeption und Allgemeine Regelungen der MaRisk“ in: Bank 2005, Nr 6, 34-36, 38-39
Pfister, Bernhard	„Zur Produzentenhaftung wegen Verletzung der Produktbeobachtungspflicht gegenüber fremdem zubehör“ in: EWiR 1987, 235-236
Pieper, Helmut	„Verbraucherschutz durc, Pflicht zum ‚Rückruf’ fehlerhafter Produkte?“ in: BB 1991, 985-992
Podehl, Jörg	„Internetportale mit journalistisch-redaktionellen Inhalten“ in: MMR 2001, 17-23
Polke, Peter	Die darlehensvertragliche Umsetzung der Eigenkapitalgrundsätze nach Basel II, Berlin 2005
Popp, Andreas	„Von Datendieben und Betrügern – Zur Strafbar-

	keit des sogenannten phishing“ in: NJW 2004, 3517-3518
Potinecke, Harald W	„Das Geräte- und Produktsicherheitsgesetz“ in: DB 2004, 55-60
Preußner, Joachim	„Risikomanagement im Schnittpunkt von Bankaufsichtsrecht und Gesellschaftsrecht“ in: NZG 2004, 57-61
Preußner, Joachim	„Deutscher Corporate Governance Kodex und Risikomanagement“ in: NZG 2004, 303-307
Probst, Thomas	„Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik“ in: DSB 2003, Nr 5, 10-12
Probst, Thomas	„Automatisierte Software-Updates“ in: DuD 2003, 508
Prölss, Jürgen	Beweiserleichterungen im Schadensersatzprozess, Karlsruhe 1966 zitiert: *Prölss*, Beweiserleichterungen im Schadensersatzprozeß
Prütting, Hanns	„Die Beweislast im Arbeitsrecht“ in: RdA 1999, 107-112
Quaas, Michael/ Zuck, Rüdiger	Medizinrecht, München 2006 zitiert: Quaas/Zuck-*Bearbeiter*
Quack-Grobecker, Alexander/ Funke, Guido	„Internetrisiken – eine Herausforderung für die Haftpflichtversicherung“ in: VW 1999, 157-160
Raab, Thomas	„Die Bedeutung der Verkehrspflichten und ihre systematische Stellung im Deliktsrecht“

	in: JuS 2002, 1041-1048
Rebmann, Kurt/ Säcker Franz Jürgen/ Rixecker, Roland (Hrsg.)	Münchener Kommentar zum Bürgerlichen Gesetzbuch, 4. Auflage, München 2000 ff. zitiert: MünchKommBGB-*Bearbeiter*
Recknagel, Einar	Vertrag und haftung beim Internet-Banking, München 2005 zitiert: *Recknagel*, Vertrag und Haftung beim Internet-Banking
Redeker, Helmut	„Softwareerstellung und § 651 – Die typischen Vertragsgestaltungen verlangen differenzierte Ergebnisse“ in: CR 2004, 88-91
Redeker, Helmut	„Wer ist Eigentümer von Goethes Werther?“ in: NJW 1992, 1739-1740
Redeker, Helmut	„Geschäftsabwicklung mit externen Rechnern im Bildschirmtextdienst“ in: NJW 1984, 2390-2394
Reese, Jürgen	„Produkthaftung und Produzentenhaftung für Hard- und Software“ in: DStR 1994, 1121-1127
Reiländer, Frank/ Weck, Gerhard	„Datenschutzaudit nach I–-Grundschutz - Konvergenz zweier Welten“ in: DuD 2003, 692-695
Reinicke, Dietrich/ Tiedtke, Klaus	Kaufrecht, 7. Auflage, München 2004
Reiser, Cristof/Werner, Stefan	Rechtsprobleme des Zahlungsverkehrs im Zusammenhang mit EDIFACT in: WM 1995, 1901-1908
Rigamonti, Cyrill P	„Das Jahr-2000-Computer-Problem: Ein Rechts-

	problem?“ in: SJZ 1998, 430-434
Roggenkamp, Jan Dirk	Massenhafter Versand von Werbe-E-Mails, Anmerkung zu Anm. zu OLG Düsseldorf, Urt. v. 24.5.2006 – I 15 U 45/06, jurisPR-ITR 8/2006 Anm. 4
Rolland, Walter	Produkthaftungsrecht, Kommentar, München 1990
Rönck, Rüdiger	Technische Normen als Gestaltungsmittel der europäischen Gemeinschaftsrechts, Berlin 1995
Rösler, Hannes	„Zur Zahlungspflicht für heimliche Dialereinwahlen“ in: NJW 2004, 2566-2569
Rösser, Heinz	„quid! Datenschutzzertifizierung“ in: DuD 2003, 401-405
Roßnagel, Alexander	„Europäische Techniknormen im Lichte des Gemeinschaftsvertragsrechts“ in: DVBl 1996, 1181-1189
Roßnagel, Alexander	„Marktwirtschaftlicher Datenschutz – eine Regulierungsperspektive“ in: Bizer, Johann/Lutterbeck, Bernd/Rieß, Joachim (Hrsg.), Umbruch von Regulierungssystemen in der Informationsgesellschaft, Freundesgabe für Alfred Büllesbach, Stuttgart 2002, S. 131-150
Roßnagel, Alexander	Datenschutzaudit, Braunschweig 2000
Roßnagel, Alexander	„Auf dem Weg zu neuen Signaturregelungen“ in: MMR, 451-461
Roßnagel, Alexander (Hrsg.)	Recht der Multimedia-Dienste, Kommentar, 7. Ergänzungslieferung, München 2005

	zitiert: *Bearbeiter*, in: Roßnagel, Recht der Multimedia-Dienste
Roßnagel, Alexander (Hrsg.)	Handbuch Datenschutzrecht, München 2003 zitiert: *Bearbeiter*, in: Roßnagel, Handbuch Datenschutzrecht
Roth, Birgit/ Schneider, Uwe K.	„IT-Sicherheit und Haftung“ in: ITRB 2005, 19-22
Rücker, Daniel	„Softwareerstellung und § 651 BGB – Diskussion ohne Ende oder Ende der Diskussion?“ in: CR 2006, 361-368
Rühl, Christiane	Rechtswahlfreiheit und Rechtswahlklauseln in allgemeinen Geschäftsbedingungen, Baden-Baden 1999
Runte, Christian/ Potinecke, Harald	„Software und GPSG“ in: CR 2004, 725-729
Runte, Christian/ Potinecke, Harald	„Software und GPSG“ in: CR 2004, 725-729
Rüpke, Giselher	„Ein Beauftragter für den Datenschutz in der Anwaltskanzlei?“ in: AnwBl 2004, 552-555
Sack, Rolf	„Produzentenhaftung und Produktbeobachtungspflicht“ in: BB 1985, 813-819
Säcker, Franz Jürgen (Hrsg.)	Berliner Kommentar zum Telekommunikationsgesetz, Frankfurt am Main 2006 zitiert: Säcker-*Bearbeiter*
Sailer, Kathrin	Prävention im Hatungsrecht, Frankfurt am Main 2005

Salje, Peter	„Ökonomische Analyse des Rechts aus deutscher Sicht“ in: RECHTSTHEORIE 15 (1984), 277-312
Schäfer, Hans-Bernd/ Ott, Claus	Lehrbuch der ökonomischen Analyse des Zivilrechts, 4. Auflage, Berlin, Heidelberg, Bonn, New York 2005
Schenke, Wolf Rüdiger/ Ruthig, Josef	„Amtshaftungsansprüche von Bankkunden bei der Verletzung staatlicher Bankenaufsichtspflichten“ in: NJW 1994, 2324-2329
Scherer, Josef/ Butt, Mark Eric	„Rechtsprobleme bei Vertragsschluss via Internet“ in: DB 2000, 1009-1016
Scheurle, Klaus D./ Mayen, Thomas (Hrsg.)	Telekommunikationsgesetz (TKG), 2. Auflage, München 2006 zitiert: Scheurle/Mayen-*Bearbeiter*
Schieble, Christoph	Produktsicherheitsgesetz und europäisches Gemeinschaftsrecht, Baden-Baden 2003
Schiessl, Maximilian	„Deutsche Corporate Governance post Enron“ in: AG 2002, 593-604
Schimansky, Herbert/ Bunte, Hermann-Josef/ Lwowski, Hans-Jürgen (Hrsg.)	Bankrechts-Handbuch, Band I-III, München 2001 zitiert: *Bearbeiter*, in: Bankrechts-Handbuch
Schläger, Uwe	„Gütesiegel nach Datenschutzauditverordnung Schleswig-Holstein“ in: DuD 2004, 459-461
Schlechtriem, Peter	„Angleichung der Produkthaftung in der EG – Zur Richtlinie des Rates der Europäischen Gemeinschaften vom 25-7-1985“ in: VersR 1986, 1033-1043

Schlutz, Joachim H.	„Deutschland - Rechtliche Auswirkungen der ISO-Zertifizierung, insbesondere auf Produkthaftungsklagen“ in: PHi 1996, 122-135
Schmatz, Hans/Nöthlichs, Matthias	Sicherheitstechnik, Berlin 1969-
Schmid, Viola	Informations- und Datenschutzrecht I, http://www.bwl.tu-darmstadt.de/jus4/lehre/IuD-I_ws_05/ws_0506_vorl_ueb_iud_1_modul_6_060123.pdf
Schmidl, Michael	„Softwareerstellung und § 651 BGB – ein Versöhnungsversuch“ in: MMR 2004, 590-593
Schmidt-Salzer, Joachim	Produkthaftung, 2. Auflage, Heidelberg –1990
Schmidt-Salzer, Joachim	Entscheidungssammlung Produkthaftung, 5. Ergänzungslieferung 1996
Schmidt-Salzer, Joachim/ Hollmann, Hermann H.	Kommentar EG-Richtlinie Produkthaftung, Bd. 1, 2. Auflage, Heidelberg 1988 zitiert: Schmidt-Salzer/Hollmann-*Bearbeiter*
Schnauder, Franz	„Delikts- und bereicherungsrechtliche Haftung bei gefälschter Giroüberweisung“ in: ZIP 1994, 1069-1078
Schneider, Jochen	„Projektsteuerung – Projektrisiken bei Software“ in: CR 2005, 27-34
Schneider, Jochen	„Softwareerstellung und Softwareanpassung – Wo bleibt der Dienstvertrag?“ in: CR 2003, 317-323
Schneider, Jochen	„Projektsteuerung – Projektrisiken bei Software“

	in: CR 2000, 27-34
Schneider, Jochen	Handbuch des EDV-Rechts, 3. Auflage, Köln 2003
Schneider, Jochen/Günther, Andreas	„Haftung für Computerviren“ in: CR 1997, 389-396
Schneider, Jochen/ Westphalen, Friedrich Graf von	Software-Erstellungsverträge, Köln 2006 Zitiert: *Bearbeiter*, in: Schneider/von Westphalen, Software-Erstellungsverträge
Schöning, Stephan/Weber, Marcus	„Basel II Rahmenwerk: Die Risiken der Projektfinanzierung“ in: Die Bank 2005, 47-51
Schönke, Adolf/Schröder, Horst (Hrsg.)	Strafgesetzbuch, Kommentar, 27. Auflage, München 2006 zitiert: Schönke/Schröder-*Bearbeiter*
Schöttle, Hendrik	Anwaltliche Rechtsberatung via Internet, Stuttgart 2004
Schricker, Gerhard (Hrsg.)	Urheberrecht, Kommentar, 3. Auflage, München 2006 zitiert: Schricker-*Bearbeiter*
Schubert, Thomas/Grießmann, Gundula	„Solveny II = Basel II + X“ in: VW 2004, 1399
Schulte, Martin (Hrsg.)	Handbuch des Technikrechts, Berlin 2003 zitiert: *Bearbeiter*, in: Schulte, Handbuch des Technikrechts
Schulte-Mattler, Hermann/Manns, Thorsten	„Basel II: Falscher Alarm für die Kreditkosten des Mittelstandes“ in: Die Bank 2004, 376-380
Schulte-Mattler, Hermann/von Kenne, Ulrich	“Basel II Framework: Meilenstein der Bankenaufsicht ”

	in: Die Bank 2004, 37-40
Schulze, Reiner/ Ebers, Martin	„Streitfragen im neuen Schuldrecht“ in: JuS 2004, 462-468
Schulze-Melling, Jyn	„IT-Sicherheit in der anwaltlichen Beratung“ in: CR 2005, 73-80
Schumann, Jochen	Grundzüge der mikroökonomischen Theorie, Berlin 1999
Schuster, Fabian (Hrsg.)	Vertragshandbuch Telemedia, München 2001 zitiert: *Bearbeiter*, in: Schuster, Vertragshandbuch Telemedia
Schwab, Hans-Josef	„Zur Mithaftung des Befüllpersonals, das bei vorhandener elektronischer Füllstandsanzeige von einer manuellen Freiraummengenmessung abgesehen hatte, für den beim Überlaufen eines Öltanks verursachten Schaden“ – Anmerkung zu OLG Köln, Urteil v. 24.06.1994 – 19 U 275/93 in: VersR 1995, 1250
Schwalbach, Joachim	„Effizienz des Aufsichtsrats“ in: AG 2004, 186-190
Schwark, Eberhard	Kapitalmarktrechtskommentar, 3. Auflage, München 2004 zitiert: Schwark-*Bearbeiter*
Schwarz, Günter C./Holland, Björn	„Enron, WorldCom… und die Corporate-Governance-Disskussion“ in: ZIP 2002, 1661-1672
Schwarz, Mathias/Peschel-Mehner, Andreas	Recht im Internet, Augsburg 2002
Schwarz, Mathias/Poll, Karolin	„Haftung nach TDG und MDStV“

	in: JurPC Web-Dok. 73/2003, Als. 1-154
Schweinoch, Martin/Roas, Rudolf	„Paradigmenwechsel für Projekte: Vertragstypologie der Neuerstellung von Individualsoftware“ in: CR 2004, 326-331
Schwenzer, Ingeborg	„Rückruf- und Warnpflichten des Warenherstellers“ in: JZ 1987, 1059-1065
Schwintowki, Hans-Peter/Schäfer, Frank A.	Bankrecht, Köln, Berlin, Bonn, München 2004
Schwintowski, Hans-Peter	„Gesellschaftsrechtliche Anforderungen an Vorstandshaftung und Corporate Governance durch das neue System der kartellrechtlichen Legalausnahme“ in: NZG 2005, 200-203
Schwirten, Christian/Zattler, Michaela	„Die Konfliktpunkte“ in: Die Bank 2005, Heft 10, 52-55
Seibert, Ulrich	„Die Entstehung des § 91 Abs. 2 AktG im KonTraG – »Risikomanagement« oder »Frühwarnsystem«?“ in: Westermann, Harm Peter/Mock, Klaus (Hrsg.), Festschrift für Gerold Bezzenberger zum 70. Geburtstag, Berlin, New York 2000, 427-438
Sessinghaus, Karel	„BGH???-Internet-Versteigerung" - ein gemeinschaftsrechtswidriges Ablenkungsmanöver?“ in: WRP 2005, 697-703
Shavell, Steven	Foundations of Economic Analysis of Law, Harvard 2004

Sieber, Stefanie/Nöding, Toralf	„Die Reform der elektronischen Unterschrift“ in: ZUM 2001, 199-210
Siebert, Lars Michael	Das Direktbankgeschäft, Baden-Baden 1998
Siegel, Volker	„Die Auswirkungen von Solvency II auf IT-Projekte“ in: ITRB 2006, 13-15
Siemer, John Philipp	Das Coase-Theorem: Inhalt, Aussagewert und Bedeutung für die ökonomische Analyse des Rechts, Münster 1999
Simitis, Spiros (Hrsg.)	Kommentar zum Bundesdatenschutzgesetz, 6. Auflage, Baden-Baden 2006 zitiert: Simitis-*Bearbeiter*
Simitis, Spiros/ Dammann, Ulrich/ Mallmann, Otto/ Reh, Hans-Joachim (Altauflage)	Kommentar zum Bundesdatenschutzgesetz, 3. Auflage, Baden-Baden 2003 zitiert: Simitis/Dammann/Mallmann/Reh (Altauflage)-*Bearbeiter*
Smith, Graham P./Hamill, Robert M.	“ Neuregelung der Produkthaftpflicht im Vereinigten Königreich - Der Consumer Protection Act 1987“ in: PHi 1988, 82-88
Sodtalbers, Axel	Softwarehaftung im Internet, Frankfurt am Main 2006
Soergel, Hans Theodor	Bürgerliches Gesetzbuch, 13. Auflage, Stuttgart, Berlin, Köln, Mainz 1999 ff. zitiert: Soergel-*Bearbeiter*
Sommerville, Ian	Software Engineering, 7. Auflage, Harlow 2004
Sonntag, Matthias	IT-Sicherheit kritischer Infrastrukturen, München 2005
Spickhoff, Andreas	„Postmortaler Persönlichkeitsschutz und ärztliche

	Schweigepflicht“ in: NJW 2005, 1982-1984
Spindler, Gerald	„Das neue Telemediengesetz – Konvergenz in sachten Schritten“ in: CR 2007, 239-245
Spindler, Gerald	Unternehmensorganisationspflichten, Köln, Berlin, Bonn, München 2001
Spindler, Gerald	„Das Jahr 2000-Problem in der Produkthaftung - Pflichten der Hersteller und der Softwarenutzer“ in: NJW 1999, 3737-3745
Spindler, Gerald (Hrsg.)	Rechtsfragen bei Open Source, Köln 2004 zitiert: *Bearbeiter*, in: Spindler, Rechtsfragen bei Open Source
Spindler, Gerald	Vertragsrecht der Internet-Provider, 2. Auflage, Köln 2004 zitiert: *Bearbeiter*, in: Spindler, Vertragsrecht der Internet-Provider
Spindler, Gerald	Vertragsrecht der Telekommunkations-Anbieter, Köln 2000 zitiert: *Bearbeiter,* in: Spindler, Vertragsrecht der TK-Anbieter
Spindler, Gerald	„IT-Sicherheit und Produkthaftung - Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer“ in: NJW 2004, 3145-3150
Spindler, Gerald	„Der Jahr-2000-Fehler: Vertragsrechtliche Haftungsfragen des Softwareveräußerers“ in: DB 1999, 1991-1998

Spindler, Gerald	„Haftung und Verantwortlichkeit im IT-Recht“ in: CR 2005, 741-747
Spindler, Gerald	„Risiko der heimlichen Installation eines automatischen Einwahlprogramms (Dialer)“ – Anmerkung zu BGH Urteil v. 04.03.2004 - III ZR 96/03 in: JZ 2004, 1128-1132
Spindler, Gerald	„Haftungs- und vertragsrechtliche Probleme von Web-Services“ in: DuD 2005, 139-141
Spindler, Gerald	„Verantwortlichkeit eines Plattformbetreibers für fremde Inhalte“ in: JZ 2005, 37-40
Spindler, Gerald	„Das Gesetz zum elektronischen Geschäftsverkehr - Verantwortlichkeit der Diensteanbieter und Herkunftslandprinzip“ in: NJW 2002, 921-927
Spindler, Gerald	Steuerunbgsfunktionen des Produkthaftungsrecht im IT-Recht und Reformbedarf, in: Hänlein, Andreas/ Roßnagel, Alexander (Hrsg.), Wirtschaftsverfassung in Deutschland und Europa. Festschrift für Bernhard Nagel, Kassel 2007, 21-30 zitiert: *Spindler*, in: FS Nagel
Spindler, Gerald	„Risiko der heimlichen Installation eines automatischen Einwahlprogramms (Dailer)“ in: JZ 2004, 1128-1132
Spindler, Gerald	„Verschuldensunabhängige Produkthaftung im Internet“

	in: MMR 1998, 119-124
Spindler, Gerald/ Börner, Fritjof	E-Commerce-Recht in Europa und den USA, Berlin u.a. 2003 zitiert: *Bearbeiter*, in: Spindler/Börner
Spindler, Gerald/ Ernst, Stefan	„Vertragsgestaltung für den Einsatz von E-Mail-Filtern“ in: CR 2004, 437-445
Spindler, Gerald/ Kasten, A. Kasten	Organisationsverpflichtungen nach der MiFID und ihre Umsetzung in: AG 2006, 785-791
Spindler, Gerald/ Klöhn, Lars	„Neue Qualifikationsprobleme im E-Commerce – Verträge über die Verschaffung digitalisierter Informationen als Kaufvertrag, Werkvertrag, Verbrauchsgüterkauf?“ in: CR 2003, 81-86
Spindler, Gerald/ Klöhn, Lars	„Fehlerhafte Informationen und Software – Die Auswirkungen der Schuld- und Schadensrechtsreform“, Teile 1 und 2 in: VersR 2003, 273-282, 410-414
Spindler, Gerald/ Schmitz, Peter/ Geis, Ivo	Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz : TDG, Kommentar, München 2004 zitiert: Spindler/Schmitz/Geis-*Bearbeiter*
Spindler, Gerald/ Volkmann, Christian	„Die öffentlich-rechtliche Störerhaftung der Access-Provider“ in: K&R 2002, 398-409
Spindler, Gerald/ Wiebe, Andreas (Hrsg.)	Internet-Auktionen und Elektronische Marktplätze, 2. Auflage, Köln 2005 zitiert: *Bearbeiter*, in: Spindler/Wiebe, Internet-

	Auktionen und Elektronische Marktplätze
Stadler, Thomas	Haftung für Informationen im Internet, 2. Auflage, Berlin 2005
Staudinger, Ansgar	„Der Rückgriff des Unternehmers in grenzüberschreitenden Sachverhalten“ in: ZGS 2002, 63-64
Staudinger, Julius von	J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, 13. Bearbeitung, Berlin 1993 ff. zitiert: Staudinger-*Bearbeiter*
Steffen, Erich	„Haftung im Wandel“ in: ZVersWiss 82 (1993), 13-37
Steffen, Erich	„Die haftungsrechtliche Bedeutung der Qualitätssicherung in der Krankenversorgung“ in: Ahrens, Hans-Jürgen/v. Bar, Christian/Fischer, Gerfried/Spickhoff, Andreas/Taupitz, Jochen (Hrsg.), Festschrift für Erwin Deutsch zum 70. Geburtstag, Köln, Berlin, Bonn, München 1999, 799-814
Stein, Friedrich/ Jonas, Martin	Kommentar zur Zivilprozessordnung, 22. Auflage, Tübingen 2002 - zitiert: Stein/Jonas-*Bearbeiter*
Shavell, Steven	„Strict Liability versus Negligence“ in: The Journal of Legal Studies, Vol. 9, No. 1 1980, 1-25
Stichtenoth, Jonas	„Softwareüberlassungsverträge nach dem Schuldrechtsmodernisierungsgesetz“ in: K&R 2003, 105-110.

Stober, Rolf	„Customer Relationship Management, Risikomanagement und Wirtschaftsverwaltungsmanagement“ in: DÖV 2005, 333-338
Stockhausen, Lothar	„Die Einführung des HBCI-Standards aus bankrechtlicher Sicht“ in: WM 2001, 605-619
Stodolkowitz, Heinz Dieter	„Beweislast und Beweiserleichterung bei der Schadensursächlichkeit von Aufklärungspflichtverletzungen“ in: VersR 1994, 11-15
Stoll, Hans	„Anmerkung zu BGH Urteil v. 18.1.1983 – VI ZR 310/79“ in: JZ 1983, 499-504
Stollberger, Thomas	Marktreport: IT-Störfälle in Unternehmen nehmen zu – Risikomanagement beeinflusst auch Kreditwürdigkeit, http://www.verivox.de/news/ArticleDetails.asp?PM=1&aid=2542
Stone, Robert	CenterTrack: An IP Overlay Network for Tracking DoS Floods, http://www.arbornetworks.com/downloads/research51/stone00centertrack_new.pdf
Streinz, Rudolf	Europarecht, 7. Auflage, Heidelberg 2005
Streinz, Rudolf (Hrsg.)	EUV/EGV: Vertrag über die europäische Union und Vertrag zur Gründung der Europäischen Gemeinschaft, München 2003 zitiert: EUV/EGV-*Bearbeiter*
Streitz, Siegfried	„Sicherheit und Datenkommunikation“ in: NJW-CoR 2000, 208-214
Strömer, Tobias H.	Online-Recht, Heidelberg 1997
Taeger, Jürgen	Außervertragliche Haftung für fehlerhafte Computerprogramme, Tübingen 1995

Taeger, Jürgen	„Produkt- und Produzentenhaftung bei Schäden durch fehlerhafte Computerprogramme“ in: CR 1996, 257-271
Tanenbaum, Andrew S.	Computer Networks, Fourth Edition, Upper Saddle River 2003
Tappert, Rainer	EDV-System-Prüfung - bankbetriebliche Revisionsinformatik, Köln 1994
Taschner, Hans Claudius/ Frietsch Edwin	Produkthaftungsgesetz und EG-Produkthaftungslinie, Kommentar, 2. Auflage, München 1990
Taupitz, Jochen	Haftung für Energieleiterstörungen durch Dritte, Berlin 1981
Taupitz, Jochen	Ökonomische Analyse und Haftungsrecht – Eine Zwischenbilanz, AcP 196 (1996), 114-167
Terlau, Matthias	„Das Jahr-2000-Problem und das Risikomanagement im Unternehmen“ in: CR 1999, 284-292
Thaller, Georg Erwin	ISO 9001: Software-Entwicklung in der Praxis, 3. Auflage, Hannover 2001
Thomas, Heinz/ Putzo, Hans	ZPO Kommentar, 27. Auflage, München 2005 zitiert: Thomas/Putzo-*Bearbeiter*
Tiedemann, Stefan	„Kollidierende AGB-Rechtswahlklauseln im österreichischen und deutschen IPR“ in: IPRax 1991, 424-427
Tiedtke, Klaus	„Die Haftung des Produzenten für die Verletzung von Warnpflichten“ in: Lange, Hermann/Nörr, Knut Wolfgang/Westermann, Harm Peter (Hrsg.), Festschrift für Joachim Gernhuber, Tübingen 1993, 471-487

Tiedtke, Klaus	„Produkthaftung des Herstellers und des Zulieferers für Schäden an dem Endprodukt seit dem 1. Januar 1990“ in: NJW 1990, 2961-2963
Tietzel, Manfred	„Die Rationalitätsannahme in den Wirtschaftswissenschaften oder Der homo oeconomicus und seine Verwandten“ in: Jahrbuch für Sozialwissenschaft, Bd. 32, 1981, Heft 2, 115-139
Tilborg, Henk C. A. van	Enyclopedia of Cryptography and Security, berlin u.a. 2005.
Tinnefeld, Marie-Therese/ Ehmann, Eugen/ Gerling, Rainer W.	Einführung in das Datenschutzrecht, 4. Auflage Oldenbourg 2005
Tita, Rolf-Thomas	„Umfang und Grenzen der Softwareversicherung nach Kl. 028 zu den ABE Teil (I) und Teil (II)“ in: VW 2001, 1696, 1781-1785
Trapp, Andreas	„Zivilrechtliche Sicherheitsanforderungen an eCommerce“ in: WM 2001, 1192-1202
Trute, Hans-Heinrich/ Spoerr, Wolfgang/ Bosch, Wolfgang	Telekommunikationsgesetz mit FTEG, Kommentar, Berlin New York 2001 zitiert: Trute/Spoerr/Bosch-*Bearbeiter*
Ulmer, Peter	„Produktbeobachtungs-, Prüfungs- und Warnpflichten eines Warenherstellers in Bezug auf Fremdprodukte?“ in: ZHR 152, 564-599
Ultsch, Michael	„Zugangsprobleme bei elektronischen Willenserklärungen - Dargestellt am Beispiel der

	Electronic Mail“ in: NJW 1997, 3007-3009
Unbekannt	„Italien: Höhere Haftung für Boote“ in: VW 1995, 580
v. Bar, Christian	Produktverantwortung und Risikoakzeptanz, München 1998 zitiert: *Bearbeiter*, in: Produktverantwortung und Risikoakzeptanz
v. Bar, Christian	Vorbeugender Rechtsschutz vor Verkehrspflichtverletzungen“ in: 25 Jahre Karlsruher Forum, Jubiläumsausgabe 1983, S. 80-85
v. Bar, Christian	Verkehrspflichten, Köln, Berlin, Bonn, München 1980
v. Gamm, Otto-Friedrich	„Datenschutz und Wettbewerbsrecht“ in: GRUR 1996, 574-579
v. Lewinski, Kai	„Anwaltliche Schweigepflicht und E-Mail“ in: BRAK-Mitt 2004, 12-17
v. Westphalen, Friedrich	„ Die allgemeine Verkehrssicherungspflicht und die Beleuchtungspflicht auf öffentlichen Straßen“ in: DB 1987, Beilage Nr. 11, 1-15
v. Westphalen, Friedrich	„Warn- oder Rückrufaktion bei nicht sicheren Produkten: §§ 8, 9 ProdSG als Schutzgesetz i.S. von § 823 Abs.–2 BGB - Rechtliche und versicherungsrechtliche Konsequenzen“ in: DB 1999, 1369-1374
v. Westphalen, Friedrich	„Jahr-2000-Fehler und deliktische Haftung“

	in: DStR 1998, 1722-1724
v. Westphalen, Friedrich	„Die Millennium-Garantie und ihre Rechtsfolgen“ in: PHi 1998, 222-227
v. Westphalen, Friedrich (Hrsg.)	Vertragsrecht und AGB-Klauselwerke, Loseblatt, Stand Oktober 2006 zitiert: *Bearbeiter,* in: v. Westphalen, Vertragsrecht und AGB-Klauselwerke
v. Westphalen, Friedrich	Produkthaftungshandbuch, Band I, München 1997 zitiert: *Bearbeiter,* in: v. Westphalen, ProdHaftHdb
v. Westphalen, Friedrich/ Langheid, Theo/ Streitz, Siegfried	Der Jahr-2000-Fehler: Haftung und Versicherung, Köln 2001 zitiert: *Bearbeiter*, in: v.Westphalen/Langheid/ Streitz, Der Jahr-2000-Fehler
v. Wulffen, Matthias	SGB X, Kommentar, 5. Auflage, München 2005 zitiert: v. Wulffen-*Bearbeiter*
Voßbein, Reinhard	„Datenschutzauditierung“ in: DuD 2003, 92-97
Wagner, Christoph/ Lerch, Janusz-Alexander	„Mandatsgeheimnis im Internet?“ in: NJW-CoR 1996, 380-385
Wagner, Gerd Rainer/ Janzen, Henrik	„Umwelt-Auditing als Teil des betrieblichen Umwelt- und Risikomanagements“ in: BFuP 1994, 573-604
Wagner, Gerhard	„Das neue Produktsicherheitsgesetz – Öffentlich-rechtliche Produktverantwortung und zivilrechtliche Folgen (Teil II)“ in: BB 1997, 2541-2546
Wagner, Gerhard	Öffentlich-rechtliche Genehmigung und zilirechtliche Rechtswidrigkeit, Köln 1989

Waldenberger, Arthur	„Grenzen des Verbraucherschutzes beim Abschluß von Verträgen im Internet“ in: BB 1996, 2365-2371
Wandt, Manfred	Internationale Produkthaftung, Heidelberg 1995
Weber, Rolf	Informatik und das Jahr 2000. Risiken und Vorsorgemöglichkeiten aus rechtlicher Sicht, Zürich 1998
Wendehorst, Christiane	„Das Vertragsrecht der Dienstleistungen im deutschen und künftigen europäischen Recht“ in: AcP 206 (2006), 205-299
Wente, Jürgen K.	Das Recht der journalistischen Recherche, UFITA Band 71, Jur. Diss. Universität Göttingen, Baden-Baden 1987
Werner, Stefan	„Elektronischer Zahlungsverkehr“ in: MMR 1998, 338-342
Westermann, Harm Peter (Hrsg.)	Erman, Bürgerliches Gesetzbuch, Handkommentar, Bd. 1 und 2, 11. Auflage, Münster, Köln 2004 zitiert: Erman-*Bearbeiter*
Weyers, Hans-Leo	Unfallschäden, 1971
Wiebe, Andreas	„Wettbewerbs- und zivilrechtliche Rahmenbedingungen der Vergabe und Verwendung von Gütezeichen“ in: WRP 1993, 74-90
Wiebe, Andreas	„Identität eines Teilnehmer an einer Internetauktion“ in: MMR 2002, 257-258
Wiesgickl, Margareta	„Rechtliche Aspekte des Online-Banking“

	in: WM 2000, 1039-1050
Wilhelm, Rudolf	„Qualitätsmanagement-Systeme nach den Normen DIN ISO 9.000 ff in Software-Unternehmen“ in: DuD 1995, 330-337
Wilrich, Thomas	Geräte- und Produktsicherheitsgesetz, Kommentar, Berlin 2004
Wimmer, Konrad	„MaRisk: Überblick und Konsequenzen für die Geschäftsleitung“ in: BKR 2006, 146-153
Winter, Ralf	„Darlegungs- und Beweislast bei Onlineauktion“ in: MMR 2002, 836-837
Witte, Jürgen/ Hrubesch, Boris	„Die persönliche Haftung von Mitgliedern des Aufsichtsrats einer AG - unter besonderer Berücksichtigung der Haftung bei Kreditvergaben“ in: BB 2004, 725-732
Wohlgemuth, Hans H./Gerloff, Jürgen	Datenschutzrecht: eine Einführung mit praktischen Fällen, Neuwied, 2005
Wohlgemuth, Michael	„Das Jahr 2000-Problem – Vertragliche und vertragsähnliche Haftung“ in: MMR 1999, 59-67
Wuermeling, Ulrich	„Einsatz von Programmsperren“ in: CR 1994, 585-595
Zahrnt, Christoph	„Abschlußzwang und Laufzeit beim Softwarepflegevertrag“ in: CR 2000, 205-207
Zerbe, Richard O.	Economic efficiency in law and economics, Chel-

	tenham, UK 2001
Zeuner, Albrecht	„Störungungen des Verhältnisses zwischen Sache und Umwelt als Eigentumsverletzung – Gedanken über Inhalt und Grenzen von Eigentum und Eigentumsschutz“ in: Jakobs, Horst Heinrich/Knobbe-Keuk, Brigitte/Picker, Eduard/Wilhelm, Jan (Hrsg.), Festschrift für Werner Flume zum 70. Geburtstag, Köln 1978, 775-787
Zeuner, Albrecht	„Zum Verhältnis zwischen Fremd- und Eigenverantwortlichkeit im Haftungsrecht“ in: Beuthien, Volker/Fuchs, Maximilian/Roth, Herbert/Schiemann, Gottfried/Wacke, Andreas (Hrsg), Festschrift für Dieter Medicus zum 70. Geburtstag, Köln, Berlin, Bonn, München 1999, 693-706
Zimmermann, Steffen	„Die MaRisk als regulatorischer Imperativ“ in: BKR 2005, 208-217
Zöller, Richard	Zivilprozessordnung, Kommentar (ZPO), 25. Auflage, Köln 2005 zitiert: Zöller-*Bearbeiter*
Zscherpe, Kerstin A./Lutz, Holger	„Geräte- und Produktsicherheitsgesetz: Anwendbarkeit auf Hard- und Software“ in: K&R 2005, 499-502