UNIVERSITÄTSMEDIZIN GÖTTINGEN UMG

Informationssicherheit

Einführungsveranstaltung für neue Mitarbeiter der UMG

Dr. Holger Beck, Informationssicherheitsbeauftragter

Informationssicherheit

… oder eher Unsicherheit?

Shutdown der IT-Infrastruktur: Malware befällt Katholische Hochschule Freiburg

Der Lehrbetrieb an der Katholischen Hochschule Freiburg (KH) läuft derzeit nur eingeschränkt, Verwaltungsmitarbeiter wurden früher in den Urlaub geschickt.

Universität Maastricht ist Opfer einer

122

Malware-Be … Frankfurt a …

Emotet hat Frankfur … den Aufräumarbeite …

Lesezeit: 1 Min.

(Bild: @Stadt_FFM / Twitt…

Uni Gießen offline und lahmgelegt – Cyber-Ermittler eingeschaltet

Nichts geht mehr an der Universität Gießen, alle Server stehen still. Die Ursachensuche läuft auf Hochtouren, ein Hackerangriff ist nicht auszuschließen.

Lesezeit: 1 Min. In Pocket speichern 215

Universität Gießen aus Sicherheitsgründen offline

Wegen Verdachts auf Cyber-Angriff wird Strafanzeige gestellt

Die Justus-Liebig-Universität Gießen hat nach einem schwerwiegenden IT-Sicherheitsvorfall ihre Server aus Sicherheitsgründen heruntergefahren. Seit Sonntagmittag ist … Internet, E-Mail-Systeme und interne Netzwerke sind nicht nutzbar. Wegen des Verdachts auf einen Cyber-Angriff wird die JLU Strafanzeige stellen. Zur genauen Ursache können - auch mit Blick auf die laufenden Ermittlungen - derzeit keine Angaben gemacht werden.

Die JLU hat einen Krisenstab unter der Leitung des Präsidenten eingerichtet und wird fortlaufend informieren, wann welche Komponenten wieder in Betrieb genommen we… in Kontakt mit den zuständigen Landesbehörden wie dem Wissenschafts- und dem Innenministerium. Aktuell sind keine Informationen zur Dauer des Serverausfalls mögli… externer IT-Experten - unter anderem des Darmstädter Forschungszentrums für Cybersicherheit Athene - wird die JLU in den nächsten Tagen das Ausmaß des Schadens …

Unter der Webadresse www.uni-giessen.de ist seit dem Nachmittag des 9. Dezember 2019 diese temporäre Ersatz-Webseite mit aktuellen Informationen geschaltet. Für …

(Bild: Universität Gießen)

…ürth offline und …eb

…such

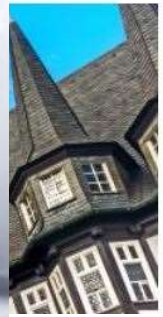
Trojaner sein Unwesen. Das gemeldet.

…r

…n und ist …t noch

405

81



IT im Wandel – Chancen und Risiken

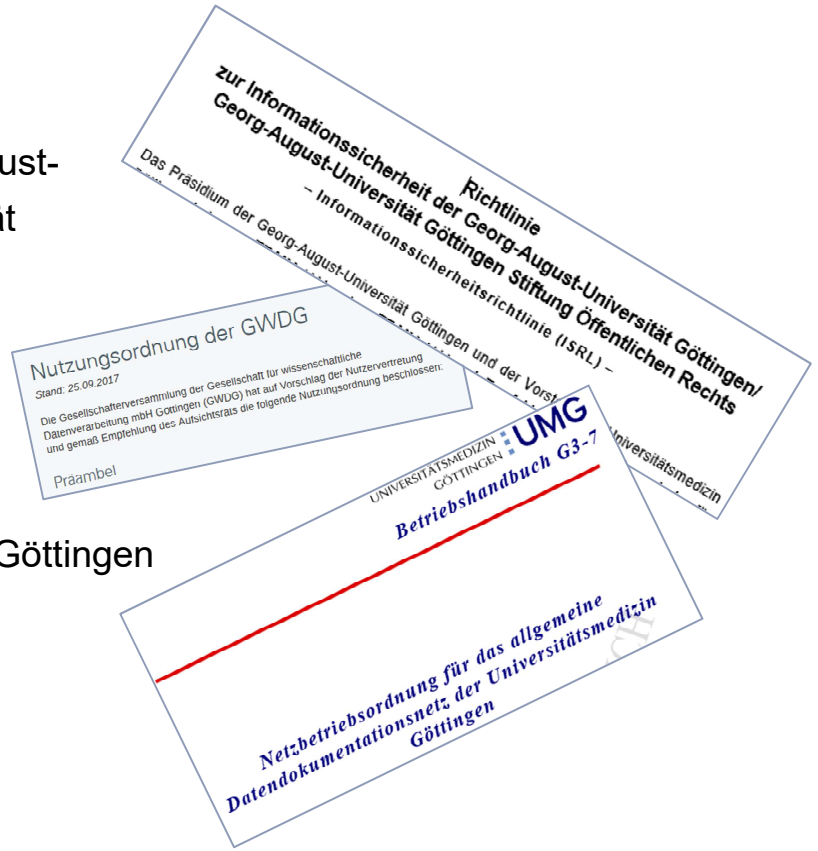
Informationstechnologie in der UMG

- Vorteile und Chancen
  - Mehr Effizienz, freie Information, neue Kommunikationsmöglichkeiten, ganz neue Techniken, auch in der Medizin
- Risiken
  - Abhängigkeit von IT
  - bis zu Zusammenbruch wichtiger, gesellschaftsrelevanter Dienste
- Was tun?
  - Verzicht auf moderne Technologie?
  - Sicherer Umgang mit IT!
- Reaktion des Gesetzgebers: IT-Sicherheitsgesetz von 2015
  - Definition von Kritischen Infrastrukturen
  - Auflagen zur IT-Sicherheit für Betreiber Kritischer Infrastrukturen
  - Auch die UMG ist Betreiber einer solchen Kritischen Infrastruktur

Richtlinien u.ä.

für Mitarbeiter der Universität und Universitätsmedizin

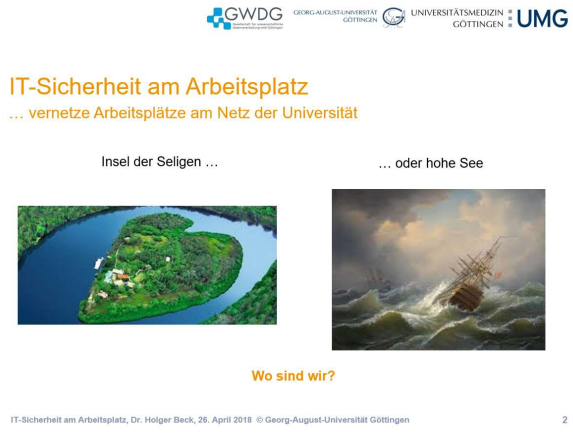
- Übergeordnet
  - Richtlinie zur Informationssicherheit der Georg-August-Universität Göttingen / der Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts
  - s. http://it-sicherheit.uni-goettingen.de
- Richtlinien für Teilbereiche
  - Netzbetriebsordnung für das allgemeine Datendokumentationsnetz der Universitätsmedizin Göttingen
  - Nutzungsordnung der GWDG
- …



Umgang mit Informationssicherheit

… Thema für Alle (dienstlich und privat)

- Themenflut und Verunsicherung
- Reaktion: Probleme ignorieren?
- Fokus auf Grundregeln
- Informations- und Schulungsangebote



Maßnahmen für IT-Anwender

… Überblick

A.1 Anwenderqualifizierung
A.2 Meldung von IT-Problemen
A.3 Konsequenzen und Sanktionen bei Sicherheitsverstößen
A.4 Kontrollierter Softwareeinsatz
A.5 Schutz vor Viren und anderer Schadsoftware
A.6 Zutritts-, Zugangs- und Zugriffskontrolle
A.7 Sperren und ausschalten
A.8 Sicherung von Notebooks, mobilen Speichermedien, Smartphones
A.9 Personenbezogene Nutzerkonten
A.10 Gebrauch von Passwörtern
A.11 Zugriffsrechte
A.12 Netzzugänge
A.13 Telearbeit
A.14 Sichere Netzwerknutzung - Allgemeine Anforderungen
A.15 Sichere Netzwerknutzung - E-Mail
A.16 Datenspeicherung
A.17 Nutzung externer Dienste
A.18 Nutzung privater Hard- und Software
A.19 Datensicherung und Archivierung
A.20 Umgang mit Datenträgern
A.21 Löschen und Entsorgung von Datenträgern
A.22 Sichere Entsorgung vertraulicher Papiere

Wie können wir uns schützen?

… und die Sicht eines Anwenders

- (Fehlerhafte) Software aktualisieren
  - macht der Admin, nicht der Anwender
- Virenscanner installieren und aktuell halten
  - macht auch der Admin
- Schutz vor manipulierter Software / Updates
  - kann nur der Hersteller sicherstellen
- Schutz vor Angriffen über E-Mails
  - Viren- und Spam-Filter durch Betreiber des E-Mail-Service
    - aber: Zeitfenster zwischen erstem Auftreten eines Virus und Erkennung bleibt
    - Spam und Phishing ist immer schwerer von „echten“ Mails zu unterscheiden.
  - kritischer Blick auf E-Mails durch den Anwender nötig!
- Nicht mit Admin-Rechten arbeiten!

Passwörter

… die wichtigsten Regeln

- Geben Sie Passwörter nie weiter, halten Sie Ihr Passwort geheim!
  - Geben Sie Passwörter nur unbeobachtet ein!
- Geben Sie Passwörter nur in den „richtigen“ Programmen und Internetseiten ein!
- Verwenden Sie für verschiedene Dienste verschieden Passwörter
  - Insbesondere verwenden Sie das dienstliche Passwort nie an anderen Stellen (privat, …)
  - Verschieden sollte auch wirklich ganz verschieden sein.
- Verwenden Sie gute, nicht zu erratende Passwörter
- Ändern Sie ihr Passwort
  - Sofort, wenn Sie den Verdacht haben, dass es nicht mehr geheim ist!
  - Regelmäßig, z.B. alle 90 Tage, jährlich (in UMG vorgeschrieben)
- Passwörter nicht in Browsern und anderen Programmen hinterlegen
  - Ausnahmen?

Passwörter

… gute Passwörter

- Schlecht sind
  - Namen, Ort, Tiere, …,
  - überhaupt alle Wörter die in Wörterbüchern zu finden sind,
- Vorgaben / Vorschläge für gute Kennworte
  - Mischung aus Groß- und Kleinbuchstaben, Ziffern, Satzzeichen u.ä.
  - Mindestlänge 10 Zeichen
- Wie komme ich zu einem guten Passwort
  - Anfangsbuchstaben eines Satzes (ergänzt durch Ziffern, Satzzeichen u.ä.)
  - Aus einem Passwort-Manager, der sichere Passwörter erzeugt
    - Insbesondere bei selten genutzten Passwörtern sinnvoll
    - z.B. KeePass (freie Software, auch für private Verwendung)

Phishing

… Einstieg zum Identitätsdiebstahl

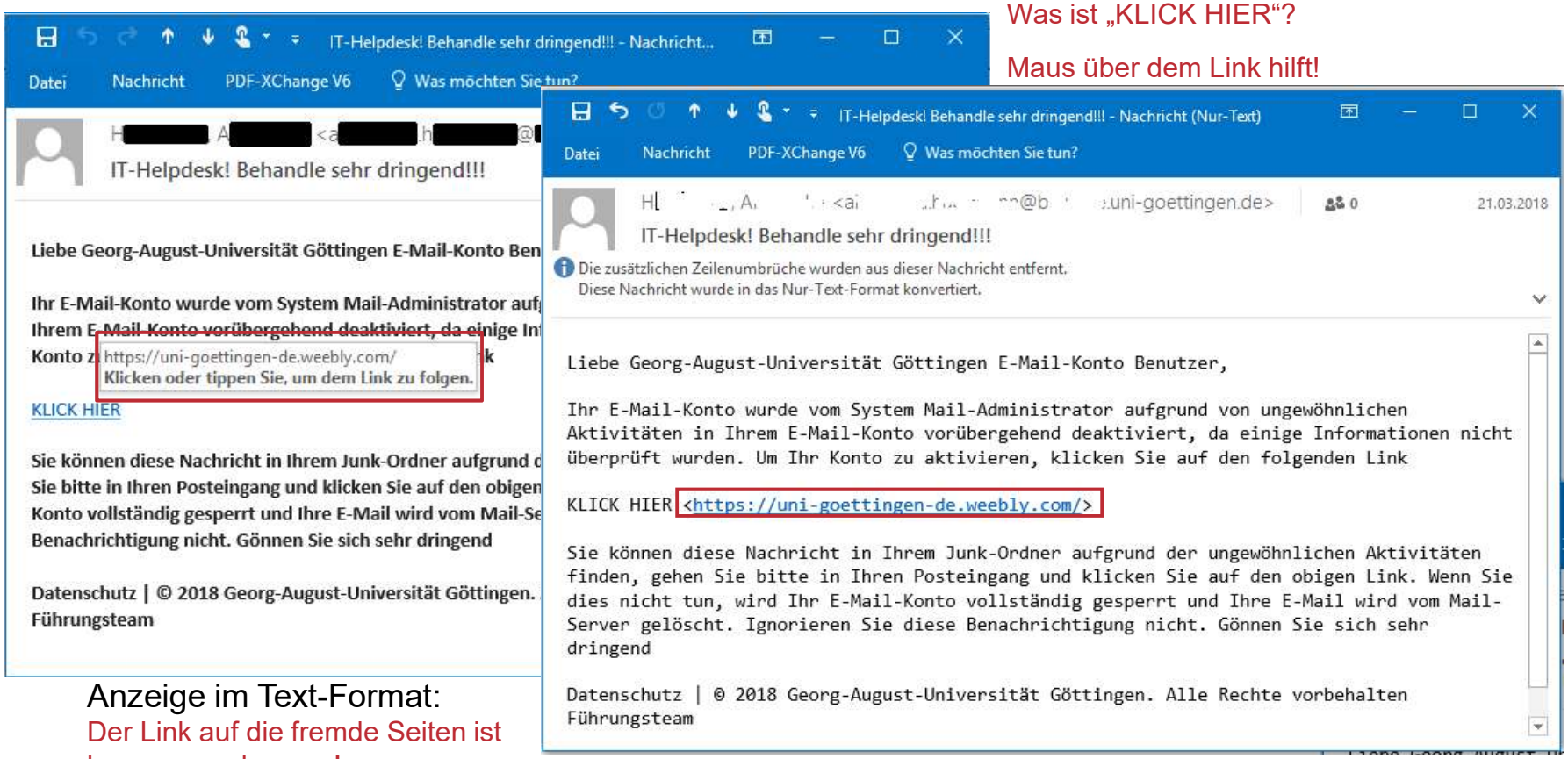
- Was ist Phishing
  - Versuch, E-Mail-Empfänger zu verleiten, sich an gefälschten Webseiten mit ihren Zugangsdaten anzumelden
- Folgen
  - Zugangsdaten werden missbraucht
    - Zugriff auf geheime Informationen
    - Missbrauch von Zugängen (z.B. Zugriff auf E-Journals),
    - Versand weitere Spam- und Phishing-E-Mails
  - Störung von E-Mail-Diensten bei Missbrauch zum Spam-Versand,
    - weil interne E-Mail-Server auf „Blacklists“ gesetzt werden und
    - externe E-Mail-Server E-Mails von UMG-Servern ablehnen!

Beispiel Phishing

… Drohung

E-Mail im HTML-Format:
Was ist „KLICK HIER“?

Maus über dem Link hilft!



Anzeige im Text-Format:
Der Link auf die fremde Seiten ist besser zu erkennen!

Betrüger im Internet

… wenn vieles ins Internet verlegt wird, tun das auch die Betrüger

- Zum Einstieg helfen zwei Videos von SECUSO, einer Forschergruppe des Karlsruher Institut für Technologie (früher TU Darmstadt):
  - https://secuso.org oder https://secuso.aifb.kit.edu
  - Dort sind auch weitere interessante Materialien zu finden

https://wiki.secuso.org/videos/nophish/video-1-anhaenge-2020-deutsch-precredits-001_recode.mp4

https://wiki.secuso.org/videos/nophish/Phishing-Links-2020-Deutsch-005_recode.mp4

Ein Blick auf Domänennamen

… oder: „Wer ist das überhaupt?“

- uni-goettingen.de ist die Universität Göttingen, also
  - ein Universitätsangehöriger als E-Mail-Absender (…@uni-goettingen.de)
  - eine Webseite der Universität (URLs http://...uni-goettingen.de).
- Variationen und komplexe URLs erschweren das Erkennen, z.B.
  - karl-theodor-von-und-zu.Mustermann@noch-ne-institutsdomaene.uni-goettingen.de
  - https://windturbinen.maschinenbau.uni-goettingen.de/turbine-einsatz/selbst-bei-tornados/php?id=34i2tbfu2iiu+name=suedlich-des-nordpols
- Wer guckt da genau hin und erkennt noch Fälschungen
  - karl-theodor-von-und-zu.Mustermann@noch-ne-institutsdomaene.uni-goetingen.de
  - https://windturbinen.maschinenbau.uni-goettingen.de-i.in/turbine-einsatz/selbst-bei-tornados/php?id=34i2tbfu2iiu+name=suedlich-des-nordpols
  - Beides sind Fälschungen! Aber wo ist der Fehler?

Domänennamen prüfen

… Fehlerarten und Erkennung

- Tippfehler-Domänen und Namensähnlichkeit:
  - uni-geottingen.de, uni-goettiingen.de, uni-goettingen.dk, …
- Täuschung mit Subdomänen, die den richtigen Domänennamen enthalten:
  - was-auch-immer.uni-goettingen.de.hier.kommt.der.fake
- Wie prüft man die Domäne / Organisation?
  - Anfangen nach dem „@“ bei E-Mails oder nach dem „://“ bei Web-Adressen,
  - bis zum Ende der Adresse oder dem nächsten „/“ (bei Web-Adressen) gehen,
  - von da zwei „.“ zurückgehen.
  - Nur was zwischen diesem „.“ und dem Ende oder dem „/“ steht ist die Domäne der Organisation!

https://ach.so.schoen.uni-goettingen.de-i.in/tolles-projekt/noch/besser/jetzt.html

Informationssicherheitsbeauftragter

… und Mitarbeiter

- Personen
  - Dr. Holger Beck (ISB)
  - Florian Gottschalk (Vertreter ISB)
  - Ilia Koźmińska
- Kontakt
  - Tel.: 0551 39 65670
  - Fax: 0551 39 130 65670
  - E-Mail: isb@med.uni-goettingen.de

Danke

Fragen?