IT-Sicherheit am Arbeitsplatz

Dr. Holger Beck
IT-Sicherheitsbeauftragter der GWDG
Leiter der Arbeitsgruppe IT-Sicherheit der Georg-August-Universität Göttingen

IT-Sicherheit am Arbeitsplatz

… vernetze Arbeitsplätze am Netz der Universität

Insel der Seligen …

… oder hohe See

Wo sind wir?

IT-Sicherheit am Arbeitsplatz

… Sicherheiten und Gefahren

- Sichere Arbeitsplätze 
  - professionell konfigurierte Rechner
    - sichere Einstellungen in Software
    - Virenscanner
    - Rechteverwaltung
  - Sicherheitssysteme im Netz
    - Viren- und Spamfilter für E-Mail
    - Firewalls
- Gefahren 
  - Freiheit an Universitäten
    - freie Kommunikation mit aller Welt
    - … auch mit beliebigen Fremden
    - Freiheit bei Softwareinstallationen
  - Grenzen von Schutzsystemen
    - Viren werden mit Verzögerung erkannt
    - Unterscheidung Spam oft schwierig

Irgendwo dazwischen sind wir:

Vorsicht: Keine nassen Füße holen (oder Schlimmeres)!

Leben ohne Internet

… geht das heute noch?

- Was ist das Internet?
  - **WWW** – eine riesige Informationsquelle?
  - **E-Mail und Messenger** – immer und überall erreichbar?
  - **E-Business** – einfacher, billiger, bequemer Geschäfte machen?
  - **Unterhaltungsmedium** – flexibler und vielfältiger als Fernsehen und Radio?
  - **Downloads** – eine unerschöpfliche Quelle frei verfügbarer Apps?
  - **Datenspeicher** und **Austauschplattform**
- **ja** – **aber**!

- Noch nie erlebt – noch nie gehört?
  - **Viren**, die Rechner und Netze lahm legen?
  - **Überfüllte Briefkästen**?
  - **Spamwellen** die zur Sperrung von E-Mail-Auslieferung führen?
  - **Geklaute Zugangsdaten** zum Konto?
  - **Einbrüche** in Rechenanlagen?
  - **Software die – böswillig** – etwas ganz anderes tut als versprochen?

Angst vor dem Internet?

- **Angst** – **nein**!
- **Vorsicht** – **ja**!
- **Sicherer Umgang mit dem Internet:**
  - Gefahren kennen,
  - sich auf Gefahren einstellen,
  - Sicherheitsregeln und verfügbare Schutzmaßnahmen anwenden.
- **Ziel des Vortrags:**
  - **Sensibilisierung** für die Gefährdungen,
  - **Grundregeln** vermitteln.
  - Sie sollen nicht alles selbst können, aber wissen, wann Sie Hilfe benötigen.

Grundregeln

… erst einmal ein Blick auf die IT-Sicherheitsrichtlinien der Universität

- Seit 2007
  - Organisationsrichtlinie zur IT-Sicherheit
  - IT-Sicherheitsrahmenrichtlinie
  - s. http://it-sicherheit.uni-goettingen.de
- Inhalte
  - Festlegung der Organisation
  - Maßnahmenkatalog für IT-Anwender
    - 20 Maßnahmen (auch als Faltblatt)
  - Maßnahmenkatalog für IT-Personal
    - 51 Maßnahmen
  - Wer Admin-Rechte auf einem Rechner hat muss die Maßnahmen für IT-Personal kennen und umsetzen!
- Zur Zeit in Überarbeitung (hoffentlich kurz vor Fertigstellung)

Maßnahmen für IT-Anwender

… Überblick

Maßnahmen für IT-Anwender

… Überblick zur Überarbeitung (alt und neu)

- Räumlicher Zugangsschutz
  - Zutritts-, Zugangs- und Zugriffskontrolle
- Sicherung mobiler Computer
  - Sicherung von Notebooks, mobilen Speichermedien, Smartphones
- Keine private Hard- und Software
  - Nutzung privater Hard- und Software
- Sichere Netzwerknutzung
  - Sichere Netzwerknutzung - Allgemeine Anforderungen
  - Sichere Netzwerknutzung - E-Mail
- Datensicherung
  - Datensicherung und Archivierung
- Physisches Löschen von Datenträgern
  - Löschen und Entsorgung von Datenträgern
- Schützenswerte Daten auf dem Arbeitsplatzrechner
  - Datenspeicherung
- Neu:
  - Nutzung externer Dienste

Aktuelle Bedrohungslage

… Ransomware und Kryptotrojaner

- Spezialfälle von Viren, Würmer oder Trojanern
  - Schadsoftware verschlüsselt Dateien,
  - Angreifer bieten Entschlüsselung gegen Bezahlung
  - oder auch nur Vandalismus ohne Erpressung.
- öffentlichkeitswirksame Vorfälle
  - Krankenhäuser, DB, Maersk
  - Locky, WannaCry, NotPetya u.a.
  - in der Universität kaum aufgetreten (und ohne dauerhafte Schäden)
- Infektionswege
  - über Anhänge von E-Mails (z.B. Locky)
  - direkte Angriffe über Netz auf nicht gepatchte Schwachstellen (z.B. WannaCry)
  - über manipulierte Software-Updates eines Herstellers (z.B. NotPetya)

Aktuelle Bedrohungslage

… Phishing, Identitätsdiebstahl, Spionage

- Presseberichte, z.B. Spiegel vom 21.4.18, berichten über Datendiebstahl
  - unter Erwähnung eines Vorfalls vom Januar 2015 an der Universität
- Was ist Phishing
  - Versuch, E-Mails-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 GWDG-Servern ablehnen!

Wie können wir uns schützen?

… aus Sicht eines Anwenders

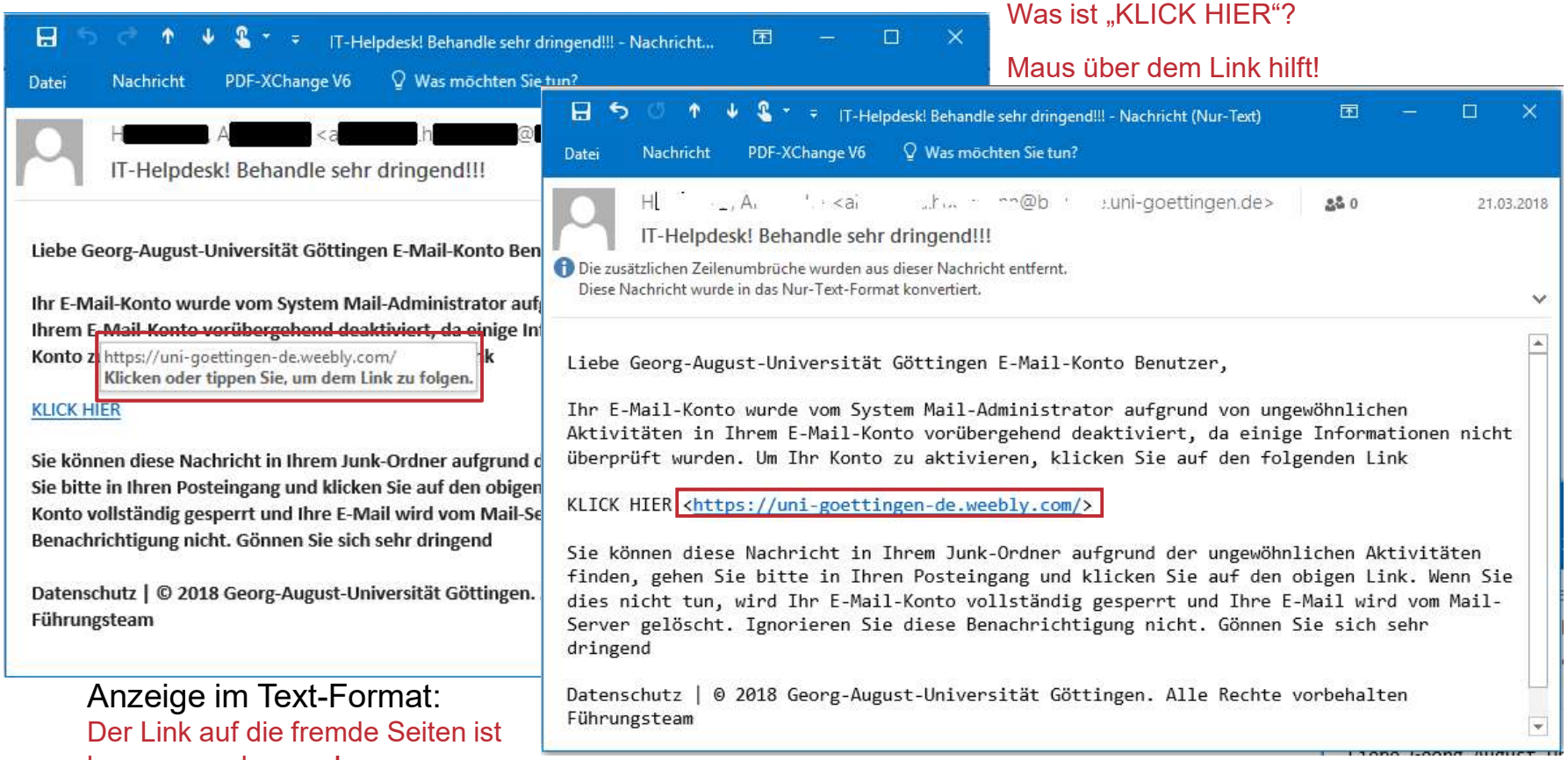
- Patches installieren
  - macht der Admin, nicht der Anwender
- Virenscanner installieren und aktuell halten
  - macht auch der Admin
- Schutz vor manipulierten Updates
  - kann nur der Hersteller sicherstellen
- Schutz vor Angriffen über E-Mails
  - Viren- und Spam-Filter durch Betreiber des E-Mail-Service
    - 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!

Beispiel Phishing

… Drohung

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

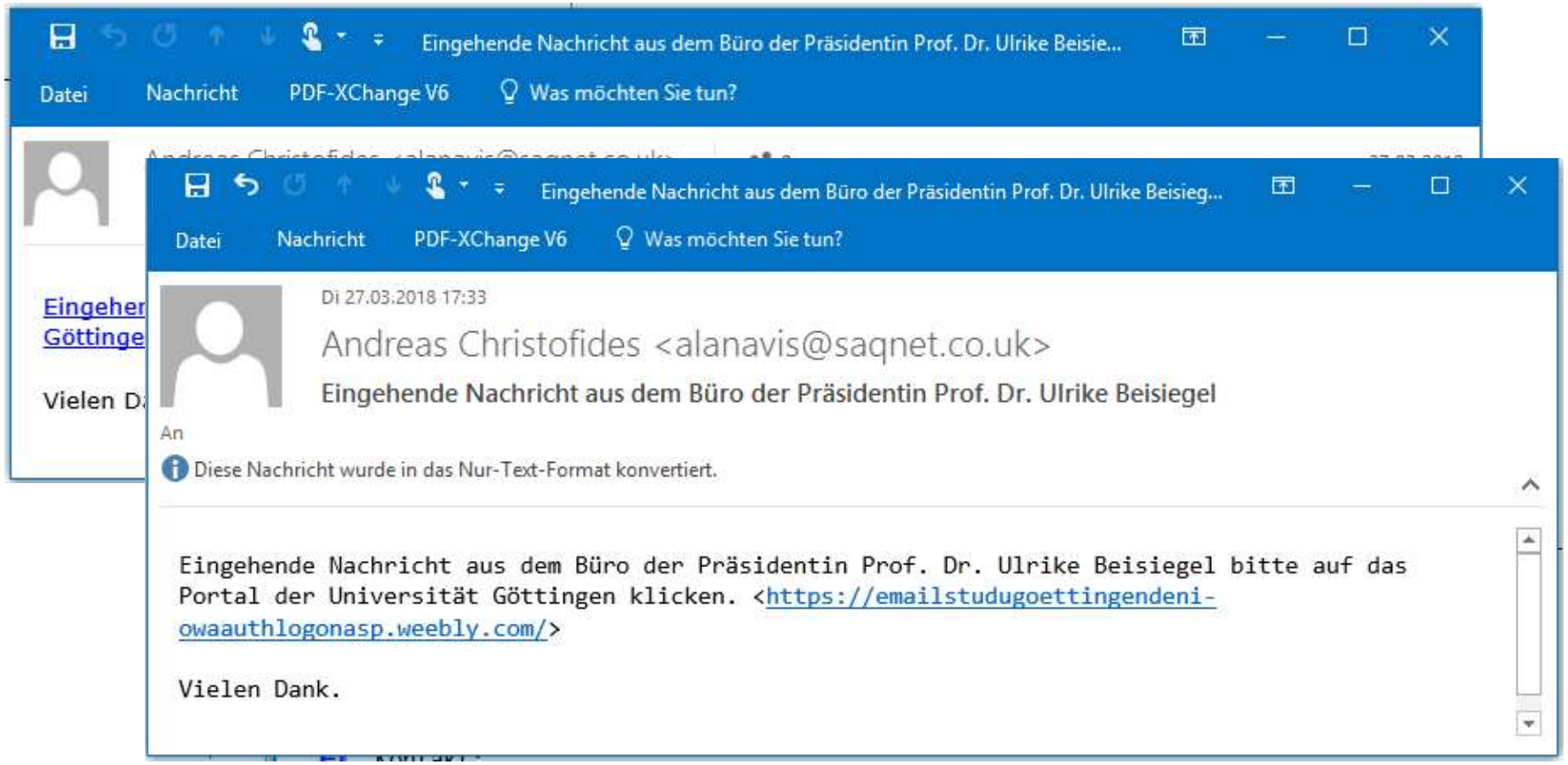
Maus über dem Link hilft!



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

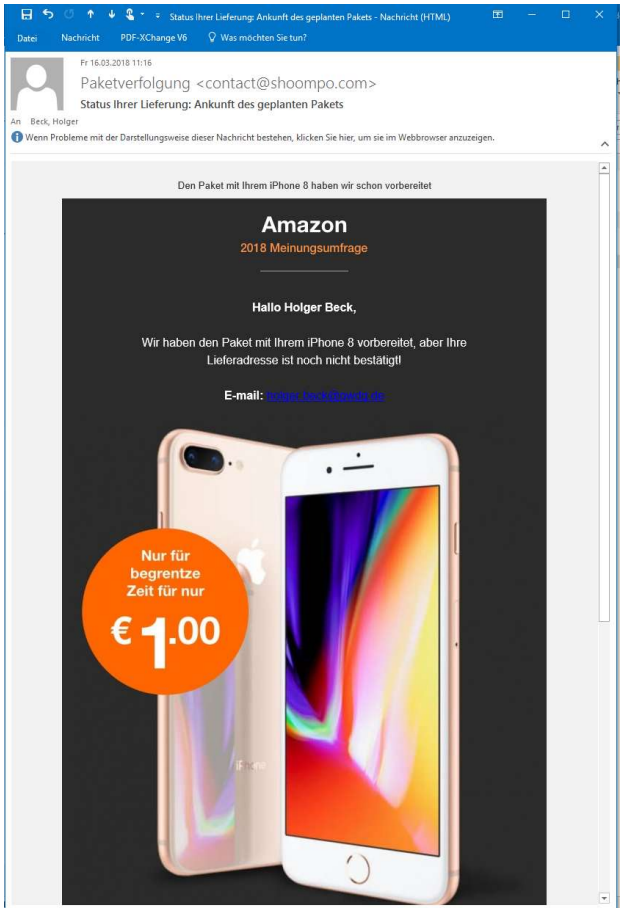
Beispiel Phishing

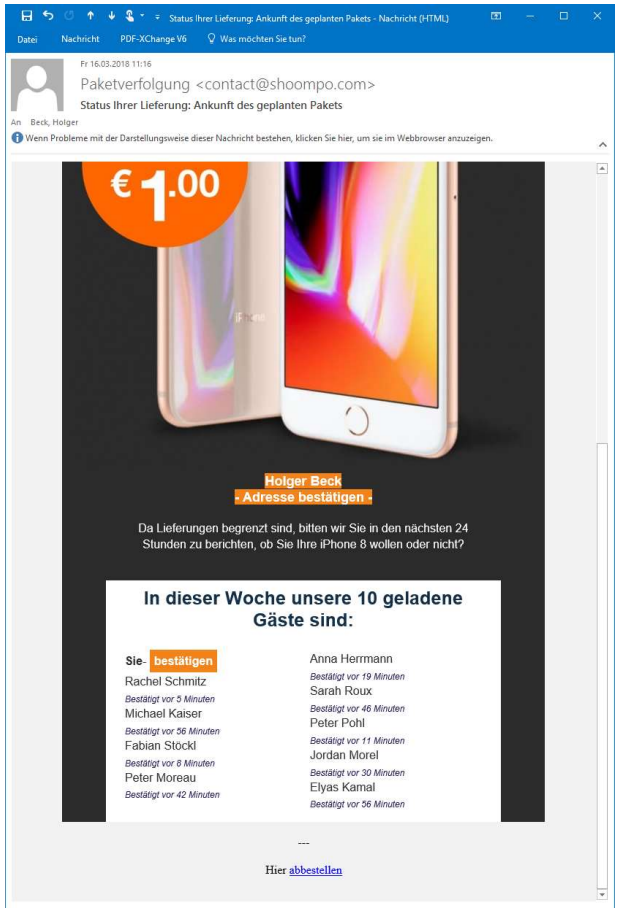
… Interesse wecken



Beispiel Phishing

… Geschenke und Sonderangebote





Betrüger im Internet

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

- Zum Einstieg ein Video von SECUSO, einer Forschergruppe der TU Darmstadt:
  - https://secuso.org oder https://www.secuso.informatik.tu-darmstadt.de
  - Dort sind auch weitere interessante Materialien zu finden

- https://www.secuso.informatik.tu-darmstadt.de/de/secuso/forschung/ergebnisse/security-awareness-und-education/nophish/video/

Kritischer Blick auf E-Mails

… auf was ist zu achten?

- Wer ist der Absender?
  - Ist der Absender bekannt und vertrauenswürdig?
- Ist der angebliche Absender wirklich der Absender?
  - Passt der Inhalt der E-Mail zum Absender?
  - Erwarte ich vom Absender eine E-Mail mit dem aktuellen Inhalt?
- Bei Anhängen
  - Was für Dateitypen sind das wirklich?
- Bei Links
  - Wohin zeigen die Links wirklich?

Sicherheit von E-Mails

… E-Mail ist wie eine Postkarte!

- Wie auf Postkarten oder Briefen kann man einen beliebigen Absender vorgeben!
  - Experten können in den „Mail-Headern“ Indizien für eine Fälschung des Absenders finden (zumindest für falsche Organisation, weniger für falsche Person).
- Inhalt kann einfach so gelesen werden
  - vom Postboten bei Postkarten
  - von allen bei denen eine E-Mail „vorbeikommt“
    - lokale Admins (dürfen das wie der Postbote nicht)
    - von allen, die irgendwo im Internet mitlesen können
      - (wenn die Serverbetreiber keine Verschlüsselung der Transportwege sicherstellen können).

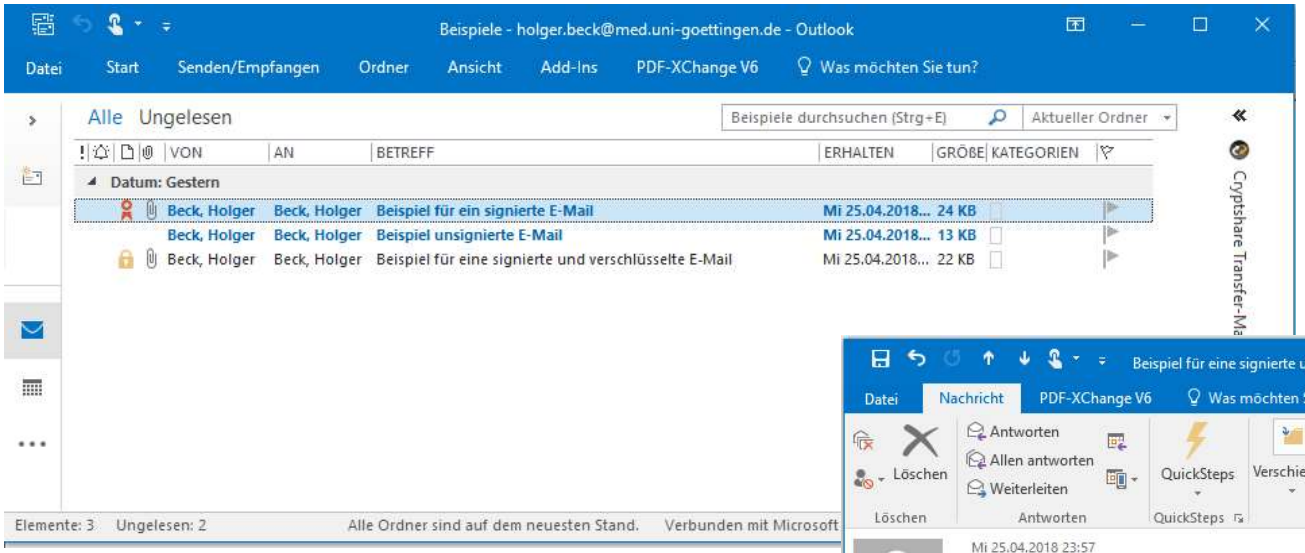
Sicherheit von E-Mails

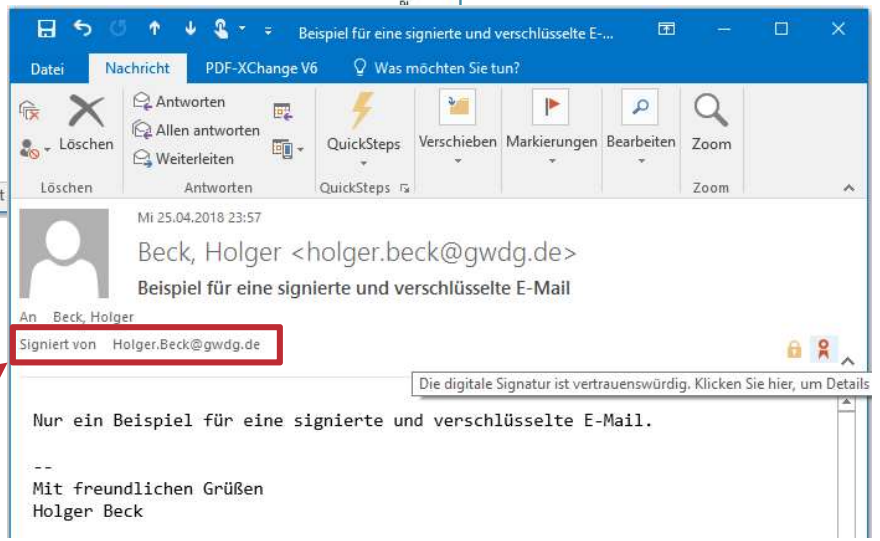
… muss aber keine Postkarte bleiben!

- Signaturen und Verschlüsselung können aus E-Mails gesicherte Kommunikation machen:
  - Garantie über den Absender (= Authentizität der E-Mail-Adresse),
    - Restrisiko: Diebstahl des geheimen Schlüssels, ähnliche E-Mail-Adressen
  - Schutz gegen Mitlesen jeglicher Art
    - Restrisiko: spezielle „Man-in-the-Middle“-Angriffe.
  - Die nötige Infrastruktur besteht in der Universität (und generell für deutsche Forschungseinrichtungen).
  - Sie müssen nur ein „Zertifikat“ beantragen!
    - Sie https://ca.gwdg.de

Signierte und verschlüsselte E-Mails

… wie sieht das aus?





Symbol für signierte E-Mails

Symbol für verschlüsselte E-Mails

Angabe zur geprüfte E-Mail-Adresse

Offizielle E-Mails der GWDG

… sollten IMMER signiert sein!

- … und wenn nicht, beschweren Sie sich!
  - (ok, es gibt aus technischen Gründen vielleicht einzelne Ausnahmen,
    - aber auch dann lieber nachfragen).
- Beispiele für Ausnahmen
  - Automatische Systemmails
    - Probleme mit Aufwand
  - Antworten über Smartphones
    - Soll man den geheimen Schlüssel auf dem Smartphone installieren (wenn das Mail-Programm dort überhaupt sowas unterstützt)?
- Achtung: Absender @gwdg.de könnten auch Nutzer und nicht GWDG-Mitarbeiter sein
  - support@gwdg.de passt, bekannte Ansprechpartner?
  - Gehackte Konten von GWDG-Nutzern stellen ein Restrisiko dar,
    - es gibt aber noch keine bekannten Vorfälle mit signierten E-Mails.

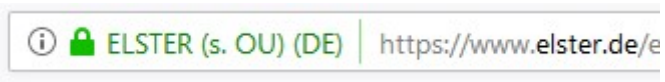
Verschlüsselung und Authentizität von Webseiten

… Webseiten mit und ohne Schloss!

- Browser zeigen ein Schloss-Symbol an, wenn die Seiten verschlüsselt sind:
  - … insbesondere bei Webseiten mit https: statt nur http:
- Muss das sein, wenn man doch nur öffentlich zugängliche Informationen lesen will?
  - Es geht nicht nur um Verschlüsselung, denn
  - das Schloss bestätigt auch die Authentizität des Anbieters!

unverschlüsselt - Betreiber nicht geprüft

verschlüsselt - Betreiber ist Domäneninhaber



verschlüsselt - Betreiber geprüft

  - Daher sollten eigentlich alle Anbieter dafür sorgen, dass ihre Webseiten immer mit https: verwendet werden
    - (dafür kann der Anbieter mittels sogenannter Redirects sorgen)
    - wenn nicht: können Sie versuchen von Hand auf https: zu wechseln

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

Sicherheit im WLAN

… offene Hotspots

- Frei zugängliche Hotspots
  - sind praktisch
  - aber bieten wegen der Freiheit auch keinen Schutz durch Verschlüsselung
  - alles ist in solchen Netzen einfach mitlesbar!
- Sie müssen selbst für Verschlüsselung sorgen
  - https:// statt http://,
  - Einstellung des E-Mail-Programms prüfen (Empfang und Senden nur verschlüsselt),
  - … und, und …
  - oder insgesamt allen Verkehr über eine VPN-Verbindung.
- Nebenbemerkung VPN (Virtual Private Network):
  - Eine verschlüsselte Verbindung in das Netz der Universität ist über https://vpn.gwdg.de möglich.

Sicherheit im WLAN

… Eduroam

- Eduroam ist ein sicheres, verschlüsseltes WLAN
- … wenn die Geräte (Notebooks, Smartphones, …) der Nutzer richtig konfiguriert sind!
- Problem:
  - Betriebssysteme bieten eine bequeme Konfiguration an,
  - … die erst einmal funktioniert,
  - … aber meist Sicherheitsprobleme verursacht!
- Lösung:
  - Konfiguration der Geräte nur mit dem Konfigurations-Tools Eduroam-CAT
  - https://cat.eduroam.de/?idp=55&profile=42 oder
  - obiger QR-Code
  - oder Anleitung unter https://info.gwdg.de unter Netzdienste, Unterpunkt eduroam

Netze: Sicherheitsziel ist auch Verfügbarkeit

… und wir leider gelegentlich durch Eingriffe in die Netzinstallation gestört

- Alle paar Monate funktioniert in einem Gebäude oder gar mehreren das Netz stundenlang nicht
  - Ursache ist häufig nicht ein technischer Defekt (kommt auch vor)
  - sondern Eingriffe von Anwendern im Netz
    - mit Kabel zum Geräteanschluss versehentlich Schleifen / Kurzschlüsse stecken,
    - Installation eigener Switches,
    - Installation eigener WLAN-Router / WLAN-APs
  - Ergebnisse
    - Netze werden bei Schleifen mit Daten geflutet (Daten laufen im Kreis),
    - WLAN-Router stören das Netz, in dem sie wichtige Dienste „ersetzen“
- Keine eigenmächtigen Eingriffe im Netz!
  - Installation nur durch GWDG, GM, G3-7 (UMG)
  - Patchen von Anschlüssen durch lokale Netzwerkbeauftragte

Notebooks, Smartphones und mobile Geräte

… führen zu einem hohen Verlustrisiko

- Das Gerät ist ersetzbar, sind es auch die darauf gespeicherten Daten?
- Zwei Arten Datenverlust:
  - Die Daten sind weg, und niemand hat sie mehr!
  - Lösung:
    - machen Sie Backups oder
    - speichern Sie nur Kopien auf dem mobilen Gerät (z.B. mittels Synchronisationstools).
  - Die Daten sind weg, aber jemand anders hat sie!
  - Lösung:
    - speichern Sie Daten auf mobilen Geräten verschlüsselt!
    - Festplattenverschlüsselung, verschlüsselte Dateien, verschlüsselte Container.
- Für (eigene) USB-Sticks gilt ähnliches,
  - fremde USB-Sticks sollte man möglichst nicht verwenden!

Passwörter

... zum Schluss ein lästiges Thema

- Benutzer + Passwort ist bisher noch die gängige Methode zur Authentifizierung
- Passwörter müssen geheim bleiben!
  - Nicht bewusst weitergeben!
  - Nicht unbewusst weitergeben (z.B. Anmeldung auf der gefälschten Webseite)!
  - Darauf achten, dass niemand die Eingabe beobachtet!
  - Nicht aufschreiben (oder nur an einer sicheren Stelle)!
  - Nicht leicht zu erraten oder auszuprobieren!
- Nie dieselben Passwörter für verschiedene Konten verwenden
- Passwort-Wechsel
  - Wenn der Verdacht besteht, dass das Kennwort nicht mehr geheim ist: Sofort!
  - Sonst: In sinnvollen Abständen (ggf. nach Vorgabe der Anwendung).
- Passwort-Länge
  - mindestens 8 Zeichen, bei sensiblen Zugängen mehr
- Passwort-Komplexität
  - Keine Namen, einfache Wörter, KFZ-Kennzeichen usw.
  - Mischung aus Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen (!§$%&…)
- Achtung: Passwort-Verkauf im Internet ist ein gutgehendes Geschäft!

Danke

Fragen?