



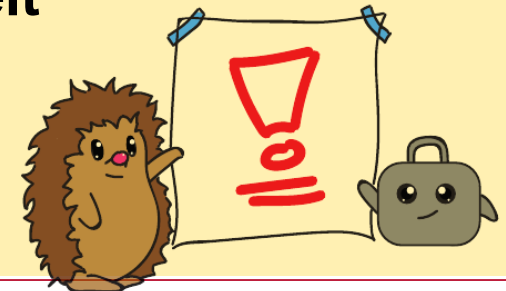
Technische
Universität
Braunschweig

Gauß-IT-Zentrum



Goldene Regeln der Informationssicherheit

Dr. Christian Böttger, 27.10.2019



Technische
Universität
Braunschweig

Agenda

- Einführung
- Goldene Regeln 1 – 11
- Bonus-Regeln
- Links





Einführung

- Informationssicherheit kann man nicht aus dem Regal kaufen. Alle Nutzer/innen müssen sich aktiv beteiligen.
- Informationssicherheit ist ein dauernder Prozess, keine einmalige Installation oder Einrichtung einer Software.
- Angriffe erfolgen zunehmend über den Menschen, nicht mehr nur über die Technik.
 - Welche Folgen hätte es, wenn die Daten von diesem Gerät in fremde Hände gelangen würden und welche Maßnahmen kann ich treffen, um dies zu verhindern?
 - Welche Konsequenzen hätte es, wenn wichtige Daten auf diesem Gerät verändert würden, sei es durch böse Absicht oder auch durch technische Fehler und was kann ich dagegen tun?
 - Was würde geschehen, wenn dieses Gerät plötzlich ausfiele und wie kann ich dem vorbeugen bzw. die Folgen vermindern?



Regel 1: *Update! Update! Update!*

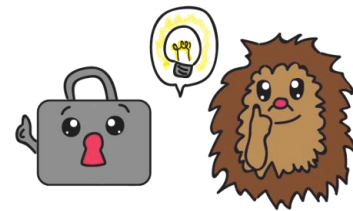
- Halten Sie
 - ihre Software,
 - ihr Betriebssystem und insbesondere
 - Ihren Virens Scanner (Habe einen Virens Scanner!)
 - auf allen Ihren Geräten
- **immer** aktuell.

- PC, Smartphone, Smartwatch, Router (Fritz!Box...), SmartHome Geräte,



Regel 2: *Verschiedene Adressen für verschiedene Zwecke*

- Besonders für E-Mails wichtig:
 - Ein Konto für Foren und Shops, auf der auch mal Spam ankommen darf
 - Ein Konto für Kommunikation mit Freunden und Bekannten, die nicht unbedingt den realen Namen enthalten muss
 - Ein Konto für Nachrichtenaustausch mit wichtigen privaten bzw. offiziellen Kontakten wie Banken und Behörden
 - Ein Konto für die Arbeit und dortige Kontakte („die im Urlaub ignoriert werden kann) – wird im Allgemeinen durch den Arbeitgeber gestellt



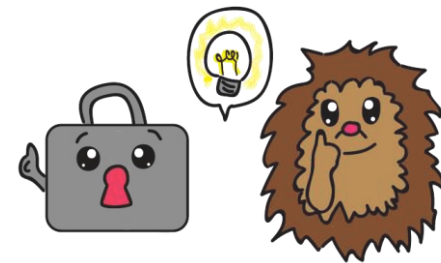
Regel 3: für jedes Konto ein anderes Passwort

- Nutzen Sie für jeden Zugang (Konto, E-Mail, ...) jeweils ein verschiedenes, sicheres Passwort! Mit unserem Passwort-generator ist es ganz einfach sich eins erzeugen zu lassen.
- Stressig, aber würden wir unsere Haustür mit dem selben Schlüssel wie die Gartenpforte und die Bürotür abschließen?
- Erlaubt unterschiedliche Sicherheitsstufen
- Wenn ein Passwort geknackt wird ist nur dieses Konto betroffen
- Verwaltung mit Passwort-Safe Programmen möglich
- Siehe Vortrag „(un)sichere Passwörter“



Regel 4: *klicke nicht einfach auf OK*

- Immer die eigentliche Frage vorher lesen
 - Keine unabsichtlichen Verträge abschließen
 - Keine unnötige Software installieren
 - Nicht ungewollt die letzten Urlaubsbilder löschen
 - ...
-
- Klicken Sie nie auf "OK", "Weiter", "Ja", "Einverstanden" oder "Akzeptieren" etc., ohne vorher gelesen und nachgedacht zu haben.



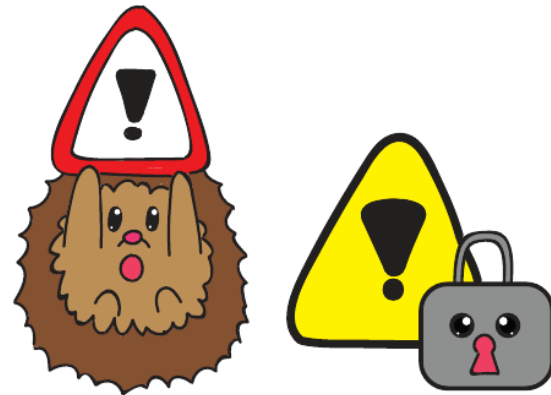
Regel 5: „kostenlos“ ist oft (zu) teuer!

- Sie bezahlen mit Ihren Daten!
- Daher verbreiten Sie Ihre Daten mit Bedacht: Nicht immer muss jedes Online-Formularfeld befüllt werden.
- Nicht einfach in jedes Fenster, das nach einem Passwort oder einer anderen wichtigen Information fragt, sollte man diese eingeben.
- Gerade zusätzliche Popups und Fragen an ungewohnten Stellen sind gefährlich
- Kein Dienst wird über E-Mail darum bitten, ein Konto durch Anmeldung zu verifizieren!
- Trau, schau, wem!



Regel 6: *E-Mail ist wie eine Postkarte!*

- Normale E-Mails ähneln einer Postkarte
 - ... und nicht einem Brief!
- Normale E-Mails können an einigen Stellen gelesen werden
- Nur verschlüsselte E-Mails können nicht so einfach gelesen werden.



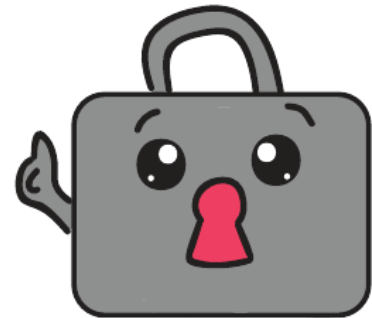
Regel 7: *Nicht überall klicken und nicht alles öffnen!*

- Achten Sie bei jeder E-Mail und bei jeder Webseite auf die Links und die Anhänge:
 - nicht einfach klicken, erst schauen! –
 - Phishing und Erpressungs-Trojaner sind ganz groß in Mode!
- Je wachsender wir sind, desto raffinierter aber auch die Tricks – jederzeit können neue Betrugsmaschen auftauchen!



Regel 8: *Immer an die Bildschirmsperre denken!*

- Vorsicht vor „Schultersurfern“ und ähnlichen Gestalten!
 - Aktivieren Sie immer eine Bildschirmsperre (Bildschirmschoner mit Passwortschutz) (z.B. bei Windows: "**Windows**"-Taste+ "**L**"),
 - wenn Sie den Rechner verlassen,
 - und sei es noch so kurz!
-
- Insbesondere in den PC-Pools, in Großraumbüros und anderen öffentlichen Orten



Regel 9: "Automatisch" ist nicht automatisch gut!

- Stellen Sie das automatische Verbinden mit "bekanntem" WLANs ab!
- WLAN-Namen können frei vergeben werden!
- Denkanstoß:
 - Was passiert, wenn ein Angreifer mitten in der Stadt ein WLAN namens „ICE“ oder T-Mobile Hotspot“ oder ... aufmacht?
 - Also einen Namen, der von den entsprechenden Anbietern verwendet wird...
 - Richtig: die Smartphones verbinden sich ohne Warnung damit – und BINGO für den Angreifer!



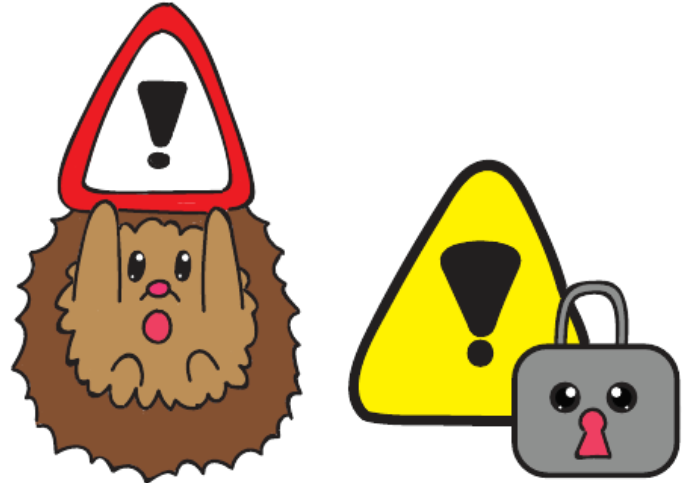
Regel 10: *NIE als Administrator arbeiten!*

- arbeiten Sie nicht als "Administrator" bzw. „root“
 - nur wenn Sie wirklich administrieren
 - Surfen Sie nicht im Web mit Admin-Rechten
- ... sondern als normaler Anwender
- deaktivieren oder löschen Sie alle Anwendungen und Dienste, die Sie nicht brauchen
 - Was nicht da ist, kann nicht angegriffen werden!
 - Nutzen Sie lokale Firewall (Application-Firewall)



Regel 11: *Kein Backup – kein Mitleid!*

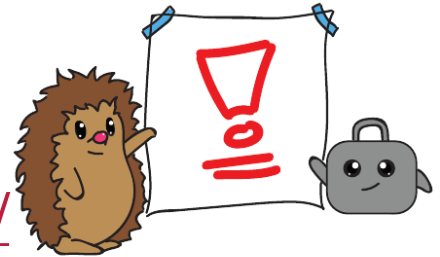
- Sichern Sie
 - oft und regelmäßig
 - Ihre Daten
 - an einem sicheren Ort
 - (offline!!).
- Es ist Ihre
 - einzige Versicherung gegen
 - Erpressungstrojaner –
 - und gegen Hardware-Ausfälle.





Bonus-Regeln:

- Achte auf die Daten deines Nächsten wie auf deine eigenen!
- Gebe nichts ein, was Du auch nicht von Dir selbst eingeben würdest.
- Wisse um den Wert deiner Daten!
- „kostenlos“ und nicht umsonst (persönliche Daten sind Geld (wert)!)!
- Begrenze was du über dich preisgibst!
- Das Internet vergisst nichts! <https://archive.org/>
- Schütze deinen Rechner!
- Virens Scanner, Firewall, Downloads, USB-Sticks, ...



Links

- <https://www.tu-braunschweig.de/it-sicherheit>
- <https://www.tu-braunschweig.de/it-sicherheit/kurztipps>
- <https://www.tu-braunschweig.de/it-sicherheit/pwsec>
- <https://doku.rz.tu-bs.de/doku.php?id=it-sec:it-sec>
- <https://www.heise.de/newsticker/meldung/WannaCry-Co-So-schuetzen-Sie-sich-3714596.html>
- <https://www.bsi-fuer-buerger.de/>
- <https://zac-niedersachsen.de/inhalte.php>
- <https://www.polizei-praevention.de/aktuelles.html>





Weitere Infos:

<https://doku.rz.tu-bs.de/doku.php?id=it-sec:it-sec> und
<http://it-sicherheit.tu-braunschweig.de/>

und beim IT-Service-Desk des Gauß-IT-Zentrums
Tel. +49.531.391.5555

it-service-desk@tu-braunschweig.de

<https://www.tu-braunschweig.de/it/service-desk>

Vielen Dank für Ihre Aufmerksamkeit!



<https://pixabay.com/de/baby-lernen-laptop-frage-2709666/>
CC0 Lizenz

