Applied IT Security

explained for non-IT-people

Disclaimer zu Beginn…

- Sicherheit ist immer Abwägungssache!
  - ➢ Sehr oft verlangt „höhere Sicherheit” Einschränkungen an anderer Stelle, z.B. schlechtere Usability oder mehr Ressourcen
  - ➢ Durchaus möglich, dass verschiedene Leute berechtigterweise verschiedene Meinungen haben
- Ich versuche, im Vortrag alles sinnvoll zu begründen – trotzdem sind Diskussionen ausdrücklich erwünscht ;)

IT Security – was bedeutet das überhaupt?

- Ziel: Sicherstellen, dass IT-Systeme und Prozesse so ablaufen, wie rechtmäßige Anwender:innen es vorsehen
- In der Regel 3 grundlegende *Sicherheitsziele*
  - Vertraulichkeit (Confidentiality)
  - Integrität (Integrity)
  - Verfügbarkeit (Availability)
- Manchmal je nach Kontext weitere Ziele formuliert

Und was wird dafür gemacht?

- Mögliche Schadensszenarien überlegen und Risiko einschätzen
- Ggf. entsprechende Maßnahmen zur Risikoreduktion treffen
  - Wahrscheinlichkeit des Schadensfalls verringern (z.B. Eingangskontrollen)
  - Schadenshöhe begrenzen (z.B. Geld auf Konto statt im privaten Safe lagern)
  - „Perfekte" Sicherheit i.d.R. unmöglich oder unwirtschaftlich, daher in der Praxis gute Kompromisse nötig
- Entspricht oft Schutz vor absichtlich böswilligen Angriffen
  - Aber auch z.B. technischer Ausfall von Komponenten oder Fehler von Mitarbeitenden können *Sicherheitsvorfälle* darstellen

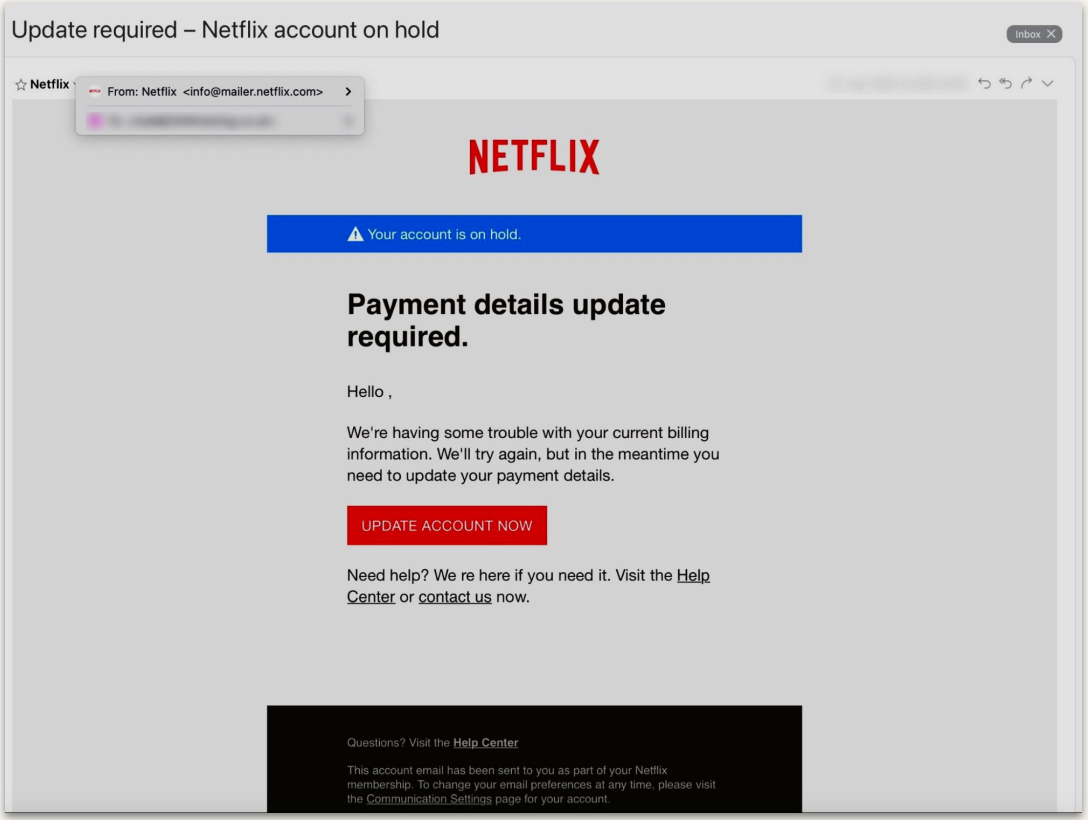
Warum betrifft mich das konkret?

- Letztendlich natürlich immer individuelle Abwägung
- Für Unternehmen in aller Regel wesentlicher als für Privatpersonen
  - ➢ Wirtschaftlicher Schaden durch Cyberattacken nach wie vor stark wachsend
- Nichtsdestotrotz auch für Privatleute relevant, da meist auch einfacher angreifbar
  - ➢ Üblicherweise erst realisiert, wenn Schaden bereits eingetreten ist
- Meine Message: **Ein gutes Schutzniveau ist nicht schwer zu erreichen – es müssen nur ein paar Grundregeln verstanden und konsequent eingehalten werden!**

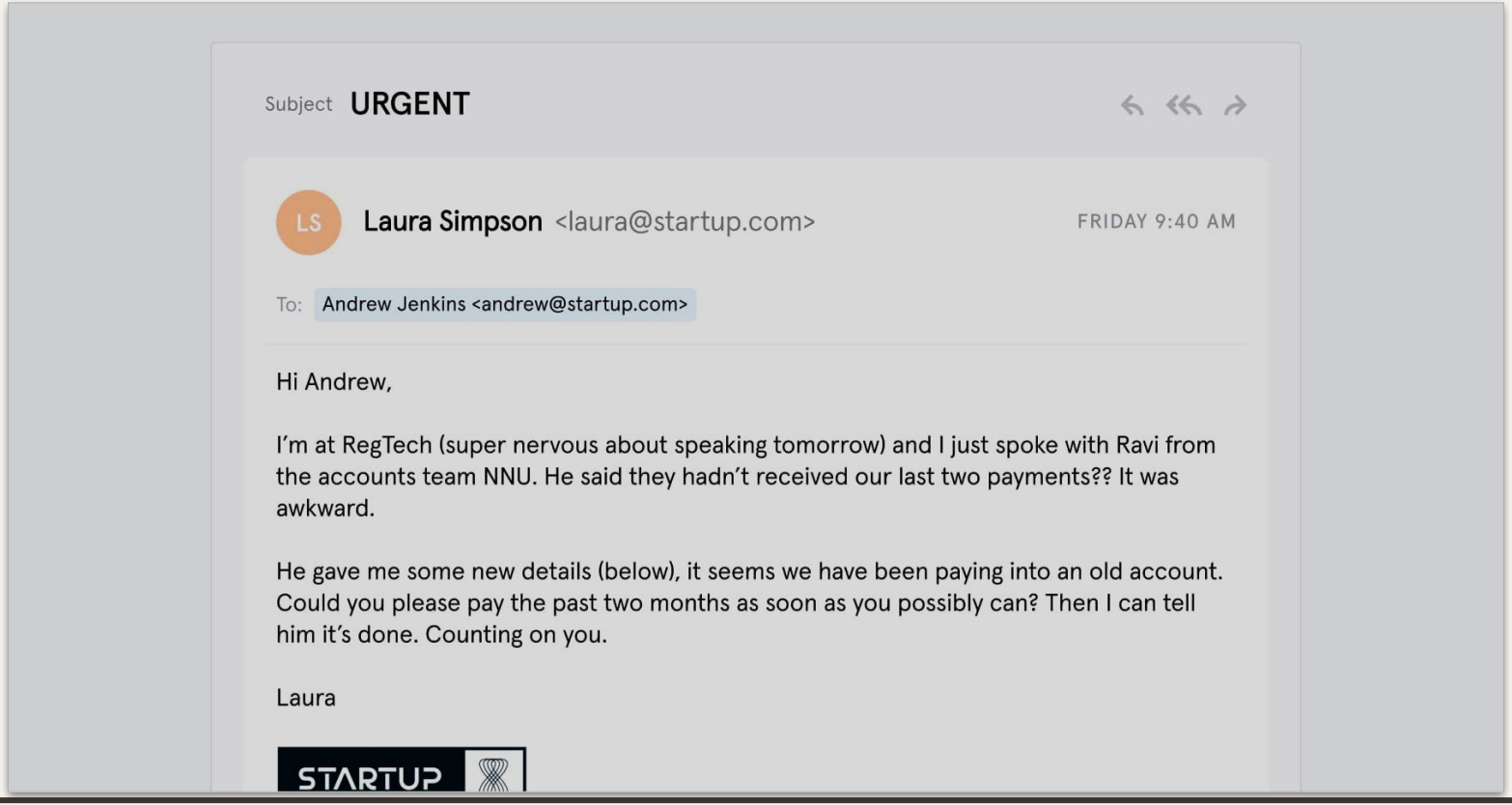
Allseits bekannt: *Phishing*

- Bezeichnet Senden von Nachrichten (E-Mails, SMS, …) mit ausgedachten „Forderungen” an sehr viele Leute
- Gewünschtes Ziel: Irgendwelche Menschen durch falschen Glauben und vorgespielte Eile dazu bringen, bestimmte Aktionen zu tätigen
  - Geld überweisen
  - Daten wie z.B. Passwörter übergeben (Identitätsdiebstahl)
  - Anderweitige „Hilfe” annehmen (z.B. Remote-Desktop-Verbindung zum eigenen Computer einrichten)
- Zwar oft sehr auffällig, aber eben nicht immer!
  - Z.B. mit sehr guter Imitation einer vertrauenswürdigen Website
  - *Spearfishing*: Auf bestimmte Person durch Recherche gezielt angepasst

Typisches Phishing



Typisches Spearfishing



Subject **URGENT**

LS **Laura Simpson** <laura@startup.com> FRIDAY 9:40 AM

To: Andrew Jenkins <andrew@startup.com>

Hi Andrew,

I'm at RegTech (super nervous about speaking tomorrow) and I just spoke with Ravi from the accounts team NNU. He said they hadn't received our last two payments?? It was awkward.

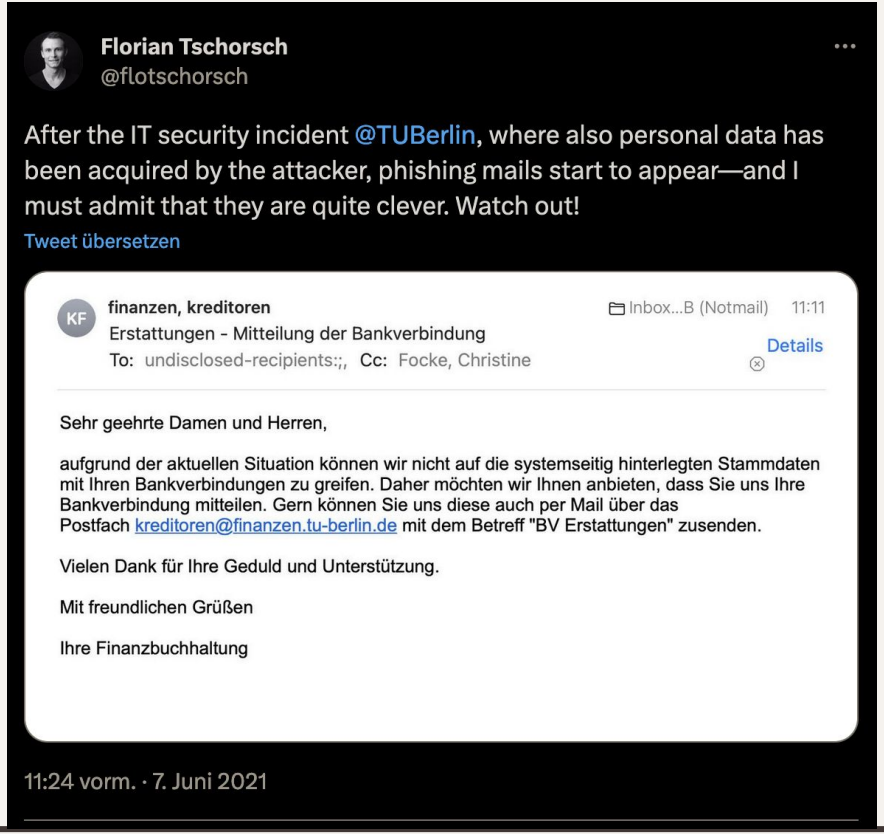
He gave me some new details (below), it seems we have been paying into an old account. Could you please pay the past two months as soon as you possibly can? Then I can tell him it's done. Counting on you.

Laura

STARTUP

Beide Bilder aus https://www.tessian.com/blog/phishing-vs-spear-phishing/

Phishing at TU Berlin?!?



Florian Tschorsch
@flotschorsch

After the IT security incident @TUBerlin, where also personal data has been acquired by the attacker, phishing mails start to appear—and I must admit that they are quite clever. Watch out!

Tweet übersetzen

KF **finanzen, kreditoren** Inbox...B (Notmail) 11:11
Erstattungen - Mitteilung der Bankverbindung
To: undisclosed-recipients:;, Cc: Focke, Christine Details

Sehr geehrte Damen und Herren,

aufgrund der aktuellen Situation können wir nicht auf die systemseitig hinterlegten Stammdaten mit Ihren Bankverbindungen zu greifen. Daher möchten wir Ihnen anbieten, dass Sie uns Ihre Bankverbindung mitteilen. Gern können Sie uns diese auch per Mail über das Postfach kreditoren@finanzen.tu-berlin.de mit dem Betreff "BV Erstattungen" zusenden.

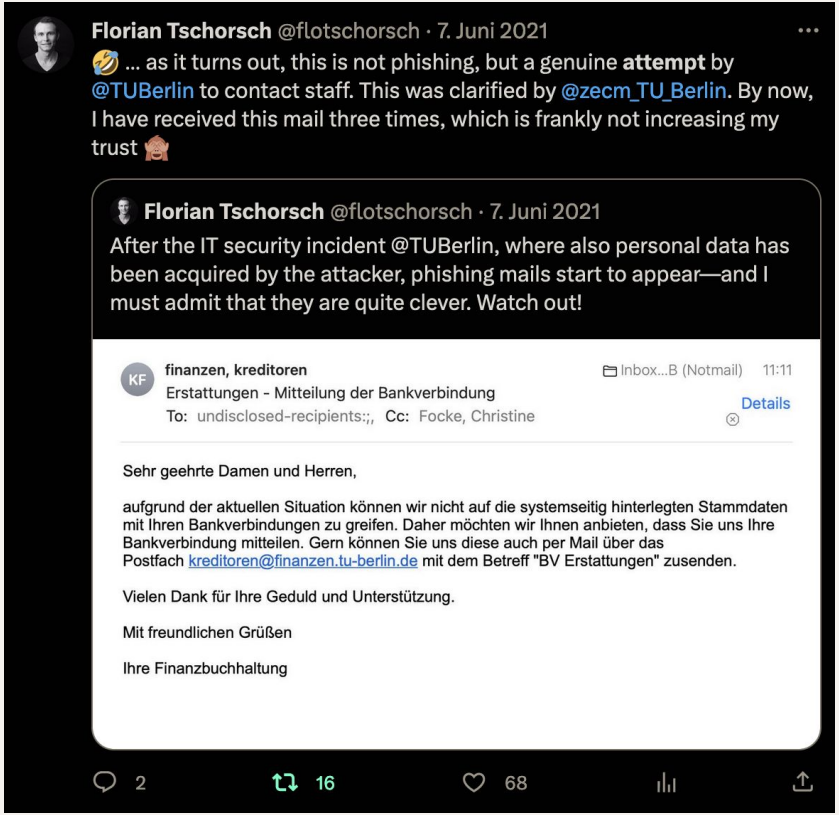
Vielen Dank für Ihre Geduld und Unterstützung.

Mit freundlichen Grüßen

Ihre Finanzbuchhaltung

11:24 vorm. · 7. Juni 2021

Well, it's more like "How not to write Mails"…



Florian Tschorsch @flotschorsch · 7. Juni 2021

🤣 … as it turns out, this is not phishing, but a genuine **attempt** by @TUBerlin to contact staff. This was clarified by @zecm_TU_Berlin. By now, I have received this mail three times, which is frankly not increasing my trust 🙈

> **Florian Tschorsch** @flotschorsch · 7. Juni 2021
>
> After the IT security incident @TUBerlin, where also personal data has been acquired by the attacker, phishing mails start to appear—and I must admit that they are quite clever. Watch out!

KF **finanzen, kreditoren** Inbox…B (Notmail) 11:11

Erstattungen - Mitteilung der Bankverbindung

To: undisclosed-recipients::, Cc: Focke, Christine Details

Sehr geehrte Damen und Herren,

aufgrund der aktuellen Situation können wir nicht auf die systemseitig hinterlegten Stammdaten mit Ihren Bankverbindungen zu greifen. Daher möchten wir Ihnen anbieten, dass Sie uns Ihre Bankverbindung mitteilen. Gern können Sie uns diese auch per Mail über das Postfach kreditoren@finanzen.tu-berlin.de mit dem Betreff "BV Erstattungen" zusenden.

Vielen Dank für Ihre Geduld und Unterstützung.

Mit freundlichen Grüßen

Ihre Finanzbuchhaltung

2 16 68

Wie aus den Screenshots ersichtlich, gehen die Credits an Florian Tschorsch :)

Detail: Links in fragwürdigen E-Mails

- ❖ Oft höre ich Aussagen der Form „Klicke niemals auf Links in E-Mails!”
  - Was sagt ihr dazu? (Gerade, wenn man sich wirklich mal unsicher ist…)
- ❖ Realistische Einschätzung hängt davon ab, was schiefgehen kann:
  - Der Browser oder die besuchten Webseiten haben schwere ungepatchte Sicherheitslücken
    - Entsprechend problematisch, aber zum Glück sehr unwahrscheinlich
    - Vertrauenswürdige Browser haben gute Sicherheitsmechanismen
  - Man vertraut der verlinkten Website und gibt Daten (Passwörter, Telefonnummer, …) weiter
  - Man lädt irgendwelche Dateien herunter und/oder führt Malware wie Plugins aus
- ➢ Links klicken also *meistens* sicher – ihnen vertrauen aber nicht!

Weiteres zu E-Mails bzw. Textnachrichten

- Absender:innen können gefälscht werden, also kein Vertrauen durch angezeigte Namen möglich
- E-Mails können vollen HTML-Code (wie Webseiten) beinhalten, je nach Mailprogramm wird mehr oder weniger angezeigt
  - So aber zum Beispiel möglich, klickbare Links „harmloser” aussehen zu lassen, als sie eigentlich sind
- Im Zweifel auch die Webseite im Browser überprüfen
  - Auf „sicher verschlüsselte Verbindung” achten
  - Per Suchmaschine checken, ob Webseite authentisch
  - Und/oder separaten Kommunikationskanal zur Verifizierung nutzen

Apropos Passwörter klauen…

- Was macht überhaupt ein „gutes Passwort” aus?
  - Beinhalten von Sonderzeichen?
    - Grundsätzlich ok, aber tendenziell relativ schwer merkbar
  - Alle 3 Monate wechseln?
    - Gefahr von Passwort-Schemata wie „**#Juli2023!**“
    - Im Allgemeinen daher keine gute Idee
  - Rein zufällige Zeichen?
    - Oft schwer zu merken: Gefahr, als Zettel am Bildschirm zu kleben…
- **Am wichtigsten ist die Länge des Passworts!**

Gute Passwörter ideell

- Ein Passwort sollte nur mit sehr vielen Versuchen erratbar sein
  - Zum „Raten” kann elementar jede Kombination aus Zeichen und/oder Wörtern aus einem Wörterbuch getestet werden
- Genauer definiertes Ziel: Selbst Supercomputer brauchen Jahre an Ratezeit, bis sie das Passwort finden
  - Kombinatorik also essenziell
- Password Reuse bedeutet leider, Services komplett zu vertrauen :(
  - Hier kann z.B. ein Passwort-Manager helfen

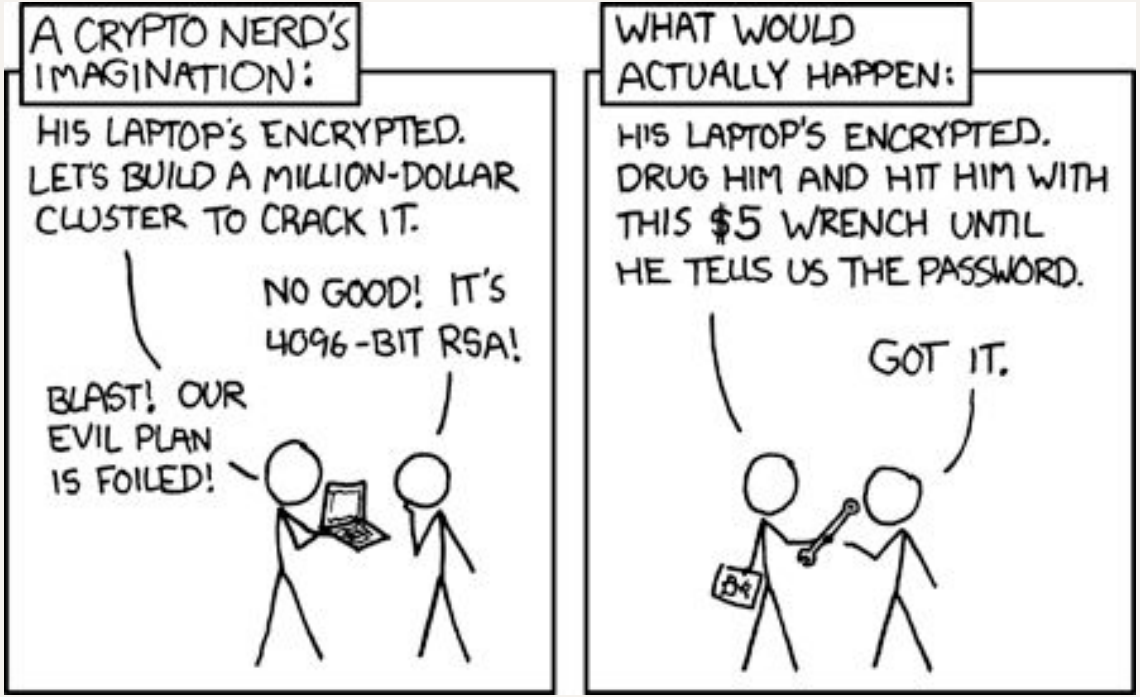
Konkrete Methoden für bessere Passwörter

- Einen ganzen Satz merken, davon nur die Anfangsbuchstaben & Sonderzeichen verwenden
  - „Jedes Semester mache ich 30 ECTS an der Uni für meinen Bachelor.” → „JSmi30ECTSadUfmB.”
- 4 bis 5 Wörter aus dem Wörterbuch echt-zufällig auswählen, zusammen mit irgendeiner Eselsbrücke merken
  - „Kredit-Blockade-Epidemie-Wein”
- 15 oder mehr echt-zufällige Zeichen mithilfe eines Passwort-Managers
  - Z.B. im Format „15 zufällige Buchstaben plus ein Punkt”

2-Faktor-Authentifizierung

- Kombination von Identifikationsmerkmalen verschiedener Kategorien
- Vorteil: Kompromittieren eines Accounts viel schwieriger, weil dafür 2 (möglichst unabhängige) Faktoren unter Kontrolle sein müssen
- Typischer Fallstrick: Verwendung schwacher Passwörter, weil es ja einen zweiten Faktor gibt
  - ➢ Dann ist es nur noch 1-Faktor-Authentifizierung ;)

Authentifizierung: Theorie vs. Realität?



Weitere nützliche Maßnahmen

- **Software Updates**, möglichst sobald sie verfügbar sind
  - Eigentlich die wichtigste Maßnahme überhaupt, da universell bekannte Software-Sicherheitslücken so in der Regel auch schnell behoben werden
  - Wenn ein verwendetes System keine Updates mehr bekommt, dann sollte zumindest überlegt werden, es zu ersetzen (muss aber nicht immer sein, u.a. auch weil nicht unbedingt nachhaltig)
- **Elementarmaßnahmen**
  - Z.B. Rechner sperren, nicht über die Schulter gucken lassen, keine sensiblen Daten offen liegen lassen
  - „Gelegenheit macht Diebe” gilt auch im Bereich der IT :)

Kein Backup, kein Mitleid…

- Geräte wie Festplatten können ausfallen, geschweige denn gestohlen oder kompromittiert werden
- Gutes privates Backup sollte schnell erreichbar und einspielbar sein
  - Verschiedene Zeitpunkte der Vergangenheit wiederherstellbar
  - Präferenz ist oft eine Cloud, aber auch z.B. private NAS sind beliebt
  - Offsite-Backup auch gut, aber für private Zwecke nicht unbedingt nötig
- Meist reicht es, selektiv wichtige Daten zu sichern
  - Frage immer: Was brauche ich noch, wenn der Laptop bzw. PC morgen spontan nicht mehr läuft?
- Für die Tekkies: RAID ist kein Backup ;)

Festplattenverschlüsselung?

- Grundsätzlich sehr sinnvoll, trotzdem oft überschätzt
  - Schützt wirklich nur die Vertraulichkeit der Daten vor Diebstahl
  - Schützt nicht den Laptop selbst und schützt vor allem auch nicht vor Identitätsdiebstahl, Malware, etc.
  - Streng genommen auch nur ganz sicher, wenn der Computer aus ist (allerdings Hardware-Angriffe sehr kompliziert und meist unpraktikabel)
- Oft ein paar Usability-Drawbacks
  - Z.B. Passwort doppelt eingeben oder nur erschwerter Zugriff auf die Platte von außen
  - Daher letztendlich wieder individuelle Abwägung
  - Insbesondere für Dienst-Laptops aber klar empfohlen

Virenscanner?

- Pro: Kann manchmal aus Versehen installierte Malware stoppen
- Cons:
  - Frisst Rechenressourcen des Computers, weil immer aktiv
  - Findet meist nur bereits gemeldete Malware
  - Kann durch Fehlalarme und weitere Meldungen nerven
  - Wirklich „gute” AV-Lösungen sind nicht kostenlos
- Mein Fazit: Für Privatpersonen meist überflüssig
  - Besser generelle Tipps befolgen und Standard-Schutz des OS nutzen
  - Insbesondere nicht einfach so fremde Software ausführen

Zusammenfassung

- Was wirklich wichtig ist:
  - Gute Passwörter
  - Software Updates
  - Backups
- Seid immer skeptisch! Vertrauen ist gut, aber zu viel Vertrauen führt zu Problemen.
- Die besten Sicherheitsmaßnahmen haben sehr großen Impact mit nur relativ kleinen Einschränkungen.

Endcard

Folien von Carsten Schubert,
Kontakt gerne via
carsten@freitagsrunde.org