Password(-Manager), LogIns, Auth etc.

19. September 2019 @ ThoughtWorks Event Space

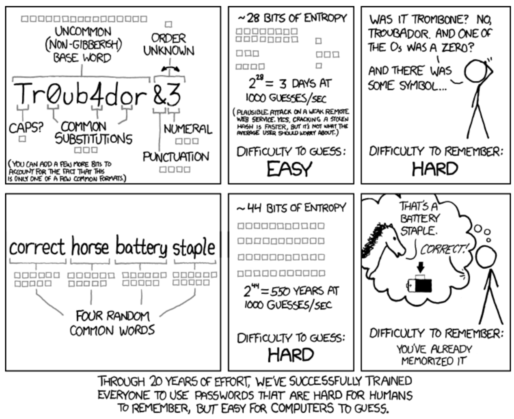
Wozu gute Passwörter und Authentifizierung?

- Jede(r/s) Service, Unternehmen oder Website wird irgenwann gehackt. Oft ist ein schwaches Passwort der Startpunkt des Einbruchs und unsere Daten sind vergleichbar schlecht geschützt
- Wiederverwendete Passwörter können zu Reihen-Attacken führen (z.B. Passwort-Reset durch gehackten E-Mail-Account)
- Ein gutes Passwort ist zufällig aber Menschen sind berechenbar
- Übeltäter sind meistens an leichten Zielen interessiert und nicht an uns persönlich

Wann ist ein(e) Passwort/Passwortphrase gut?

- Es ist laaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaang
- Es ist einzigartig (also nicht von weiteren Accounts genutzt)
- Es ist nur Dir bekannt
- Es ist keine Standardeinstellung (z.B. bei Routern und IoT-Geräten)
- Es folgt keinem simplen Algorithmus (z.B. Variation älterer Passwörter or Tastaturmuster)
- **Dein System ist leicht zu handhaben**

https://xkcd.com/936/



Passwortmanager können helfen!

CONs:

- Single point of failure
- Wem vertraust Du?
- Wertvolles Ziel für Hacker
- Verlust der Bequemlichkeit (?)

PROs:

- Unterschiedliche Lösungen für diverse Anwendungsfälle (z.B. offline vs online)
- Browser-Integration
- Passwortgeneratoren
- Aufbewahrung unterschiedlicher Datentypen

Was ist mit dem 2. Faktor?

- **1. Faktor** ist **etwas, dass Du weißt** (Passwort)
- **2. Faktor** nutzt meist **wer Du bist** (Biometrik) oder **was Du hast** (z.B. Smartphone oder Hardware-Token)
- In aufsteigender Reihenfolge sicher: SMS, E-Mail, Anruf > Authenticator App (z.B. Authy, Google Authenticator) > Hardware-Token (z.B. Yubikey)
- Immer noch anfällig für Social Engineering (Phishing)

Verhaltenskodex:

1. Grundlegende Fragen sind die wichtigsten. Wenn Du Dich unwohl fühlst, eine Frage zu stellen oder die Antwort nicht verstehst, ist das unsere Schuld und Du solltest es uns mitteilen.
2. Wir wollen Dich befähigen, Dich selbst zu schützen. Also arbeiten wir zusammen und beraten. Du bist aber die einzige Person, die Dein Gerät/Keyboard anfasst.
3. Wir tolerieren weder feindseliges noch herablassendes oder ausgrenzendes Verhalten. Jeder ist willkommen ungeachtet der Herkunft, Meinung und Fähigkeiten, des Geschlechts, Aussehens oder Glaubens. Seid einfach nett und hilfsbereit im Umgang miteinander.

Links & Resourcen

- https://haveibeenpwned.com/
- https://checkdeinpasswort.de/
- https://howsecureismypassword.net/
- https://bitwarden.com/
- https://keepassxc.org
- https://www.privacytools.io
- Wie man dieses Booklet faltet und schneidet: