Plötzlich digital - Die Sprechstunde

Session 6 - Informationssicherheit

Agenda

1. Grundlagen / Allgemeines
2. Passwortmanagement
3. Empfehlungen für Passwortmanager
4. Zwei-Faktor-Authentisierung (2FA)
5. Weiterführende Informationen
6. IT-Security Stories von Non-Profits

1. Grundlagen

Die Informationssicherheit hat drei Schutzziele:

1. **Vertraulichkeit**: Vertrauliche Informationen vor unbefugter Preisgabe schützen
2. **Integrität**: Korrektheit, Manipulationsfreiheit und Unversehrtheit von IT-Systemen und Informationen → Authentizität berücksichtigen (Echtheit, Zurechenbarkeit von Informationen)
3. **Verfügbarkeit**: Funktionen des IT-Systems oder Informationen stehen zum geforderten Zeitpunkt zur Verfügung

1. Grundlagen

- Lasse sensitive Daten nicht auf dem Tisch liegen
  (Passwort auf dem Post-It, etc.)
- Sperre den Bildschirm/Computer, wenn du ihn verlässt (auch nur kurz)

  → Tipp: Screensaver, Auto-Lock, Hot-Corners

- Verschlüssele die Geräte
- Mache regelmäßig Backups (verschlüsselt) und teste die Recovery-Funktion

1. Grundlagen

- Benutze VPN in öffentlichen WLANs
- Stecke keine unbekannten Geräte (z.B. USB-Sticks) an den Computer
- Öffne keine Links, die du nicht haben wolltest
- Öffne keine unbekannten Mailanhänge

1. Grundlagen

- Gewähre nur den Zugang zu Systemen & Informationen, wenn die Person dazu auch berechtigt ist
- Was ist das schwächste Glied in der Kette?

  → Betreibe soviel Aufwand wie nötig / möglich

  → ungutes Bauchgefühl?

  Nicht klicken bzw. einfach nichts tun & eine Person deines Vertrauens fragen bzw. jemand, der/die sich damit auskennt

2. Passwortmanagement

Passwörter:

- Schützen den Zugang zu persönlichen Internetdiensten (E-Mail-Accounts, Online-Banking, Social-Media-Accounts, Foren, etc.) vor dem unberechtigten Zugriff anderer Nutzer*innen
- die wichtigste Eigenschaft eines Passworts ist, dass es "sicher" ist - und nicht etwa, dass es leicht zu merken ist ;)
- als sicher gelten möglichst lange und zufällig gewählte Kombinationen aus Buchstaben, Zahlen und Sonderzeichen (gegen "Wörterbuchangriffe" und "Brute-Force-Angriffe")

2. Passwortmanagement

Passwortgeneratoren:

- erstellen nach zuvor bestimmten Kriterien eine zufällige Zeichenkette
- erzeugen die sichersten Passwörter!

2. Passwortmanagement

Merkmale sicherer Passwörter (vgl. Digitalcourage):

- bestehen **nicht** aus: Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars oder deren Geburtsdaten und so weiter
- kommen **nicht** in Wörterbüchern oder im Internet vor und sollten **nicht** die Anfängssätze von Büchern sein oder abkürzen

2. Passwortmanagement

Merkmale sicherer Passwörter (vgl. Digitalcourage):

- sollten **nicht** bestehen aus: gängigen Varianten und Wiederholungs- oder Tastaturmustern (also nicht qwertz oder 1234abcd und so weiter)
- sollten **nicht** einfache Ziffern und Zeichen angehängt bekommen

  → Ein simples Passwort mit Zeichen am Anfang oder Ende zu ergänzen (beliebt sind: $, !, ?, #), ist ebenfalls nicht empfehlenswert!

2. Passwortmanagement

Passphrasen:

- werden als Alternative zu Passwörtern empfohlen
- bestehen aus sechs oder mehr **beliebigen** Wörtern, die über Worttrenner (Leerzeichen/Bindestriche/Unterstriche, etc.) zu einem zusammenhängenden Zeichenstrang verbunden werden

2. Passwortmanagement

Passphrasen:

- sie sind statistisch gesehen sogar sicherer und einfacher zu merken (vgl. http://diceware.blogspot.com/2014/03/time-to-add-word.html)
- sie lassen sich ebenfalls über Zufallsgeneratoren erzeugen, aber auch analog über das Würfeln eines Würfels erstellen

  → siehe hierzu: https://de.wikipedia.org/wiki/Diceware

- sollten mindestens 17 Zeichen enthalten!

2. Passwortmanagement

Warum einen Passwortmanager?

- damit Passwörter auch ihren Zweck erfüllen, sollte bei jeder Vergabe ein **bisher noch nicht verwendetes** Passwort gesetzt werden, **das nur ihr selber kennt** bzw. **auf das nur ihr selber Zugriff** habt!
- in der Regel übersteigt die Menge der von einer Person verwendeten Passwörter die Kapazität eines gewöhnlichen menschlichen Gedächtnisses ;-)

2. Passwortmanagement

Warum einen Passwortmanager?

- es ist aber **keine** Lösung, deshalb Passwörter zu "recyclen" (auch nicht in verschiedenen Variationen) und schon gar nicht, gängige Passwörter wie "123456" zu verwenden
- Passwörter sollten sowieso regelmäßig erneuert werden!

2. Passwortmanagement

Welche Vorteile bieten Passwortmanager?

- alle eigenen Passwörter können in einer Datenbank abgelegt werden, die wiederum mit einem Masterpasswort verschlüsselt wird
- es reicht also, sich ein einziges Passwort zu merken (das sollte dann aber auch den oben genannten Standards entsprechen!)

2. Passwortmanagement

Welche Vorteile bieten Passwortmanager?

- für alle zukünftigen Registrierungen lassen sich dann im Passwortmanager Zufalls-Passwörter generieren
- es lassen sich aber auch bereits gebrauchte Passwörter händisch ablegen
- es können sogar "Ablaufdaten" für Passwörter generiert werden, um daran erinnert zu werden, die Passwörter zu erneuern

3. Empfehlungen: KeepassXC

KeepassXC → Download: https://keepassxc.org/

- kostenlos
- offener Quellcode
- aktive Community
- regelmäßige Updates
- Reboot des früheren KeepassX

3. Empfehlungen: KeepassXC

- Betriebssystem-übergreifend einsetzbar (Linux, Windows, Mac)
- Die gesamte Datenbank wird immer mit dem Industriestandard AES verschlüsselt
- Enthält einen Zufallsgenerator sowohl für Passwörter als auch für Passphrasen
- es gibt auch Keepass-Apps für Smartphones (Android,iOS)

3. Empfehlungen: 1Password

1Password: https://1password.com/sign-up/eu/

- Kostenpflichtig (personal, family-team, business) - 2,99 $/Mnt.
- Betriebssystem-übergreifend einsetzbar (Linux, Windows, Mac)
- Synchronisiert über verschiedene Varianten (z.B. als Datei, 1password, iCloud)

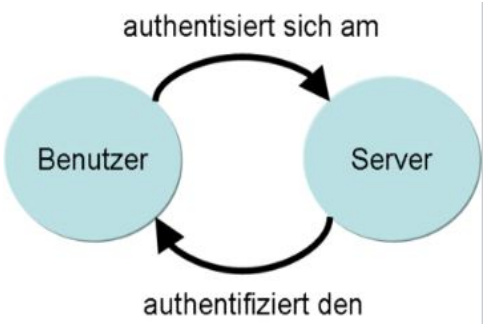
3. Empfehlungen: 1Password

- hohe Benutzerfreundlichkeit
- Viele zusätzliche Features: Passwortgenerator, Kategorien / Tags, 2FA/Token Integration, Team Accounts & Rollenbasierte Zugriffskontrolle, Travel Mode, Watchtower / Breach Warning, etc.

Es gibt noch viele weitere Passwortmanager wie z.B. LastPass, Dashblane, Bitwarden, etc.

4. Zwei-Faktor-Authentisierung (2FA)

- Oft als “Zwei-Faktor-Authenti*fizierung*” bezeichnet



Christoph Probst at de.wikipedia

4. Zwei-Faktor-Authentisierung (2FA)

- Identitätsnachweis einer/s Nutzer:in mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren)
- Typische Beispiele:
  - Bankkarte plus PIN beim Geldautomaten,
  - Passphrase und Transaktionsnummer (TAN) beim Online-Banking
  - Passwort und PIN-Nummer via Smartphone (zB bei Facebook)
  - Fingerabdruck plus Zugangscode in Gebäuden

4. Multi-Faktor-Authentisierung (MFA)

- Die Zwei-Faktor-Authentisierung ist ein Spezialfall der Multi-Faktor-Authentisierung
- Hierbei wird die Zugangsberechtigung durch mehrere unabhängige Merkmale (Faktoren) überprüft
- Beispiel: BSI empfiehlt Cloudanbietern, die Multi-Faktor-Authentisierung einzusetzen

5. Weiterführende Informationen

- BSI für Bürger (Bundesamt für Sicherheit in der Informationstechnik): Basisschutz für Computer, Hilfe bei Infektionen etc.: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Infektionsbeseitigung/Infektionsbeseitigung_node.html
- Digitalcourage e.V.: Digitale Selbstverteidigung für den PC: https://digitalcourage.de/digitale-selbstverteidigung/pc

6. IT-Security Stories von Non-Profits

- Nonprofits on Facebook Get Hacked—Then They Really Need Help
- nex on Twitter: "Looking at the phishing campaigns @AmnestyTech Security Lab responded to and investigated in the last year, there hasn't been one which wasn't provided with at least some capability to bypass non-U2F multi-factor authentication."
- Operation Kingphish: Uncovering a Campaign of Cyber Attacks against Civil Society in Qatar and...
- Cyber Threat Assessment: UK Charity Sector
- Evolving Phishing Attacks Targeting Journalists and Human Rights Defenders from the Middle-East and North Africa