CybSec Hygiene

- [ ] Passwort-Manager: Bitwarden
- [ ] 2FA mit Security Key: Yubikey
- [ ] Alles auf dem neuesten Stand halten
- [ ] Keine Mail Anhänge direkt öffnen
- [ ] Angeklickte Links doppelt prüfen
- [ ] Alle Daten off-site im Backup
- [ ] Keine unbekannten Geräte nutzen
- [ ] So wenig Daten wie möglich teilen

Bleibt achtsam!

Passwort-Manager: Bitwarden

Ein Passwortmanager verwaltet deine Passwörter. Es ist also keine Aufgabe mehr, sich jedes Passwort zu merken. Dank dessen kannst du damit auch Passwörter wählen, die deutlich komplexer sind - ich empfehle min. 20 Stellen und alle Sonderzeichen

2FA mit Security Key: Yubikey

2FA - also ein zweiter Faktor - wird zusätzlich beim Login von einer Website verlangt. Passwörter können gestohlen werden. 2FA Tokens ändern sich alle 30 Sekunden oder im Fall vom Yubikey sind sie sogar kryptographisch. Die kann ein Hacker nicht stehlen - außer er bricht ein!

Alles auf dem neuesten Stand halten

Software kann Sicherheitslücken haben - das sind Bugs und die kann man kaum vermeiden. Aber es ist selten (und teuer) für einen Hacker, diese Lücken VOR der Firma selbst zu kennen. Die allermeisten Lücken, die angegriffen werden, sind auf veralteter Software. Also Updates installieren!

Keine Mail Anhänge direkt öffnen

Eigentlich betrifft das nicht nur Mail, sondern alle Dateien, die ihr bekommt. Wird euer Gegenüber gehackt oder ihr kennt denjenigen nicht, könnte das natürlich immer ein Hacker sein. Vertraut den Dateien nicht, sondern öffnet sie in einer Sandbox wie Google Drive oder am besten gar nicht!

Angeklickte Links doppelt prüfen

Ein Link kann eine Sache sagen (“Link”) und eine andere sein. Ich kann euch auf PayPal leiten, aber in Wahrheit landet ihr auf meiner Website! Das Design kann man klauen. Prüft deshalb immer in der Adresszeile eures Browsers genau nach, wo ihr seid!

Alle Daten off-site im Backup

Sollten eure Dateien mal weg sein - Hacker, Brand oder sogar einfach Festplattenfehler - habt ein Backup! Es gibt viele Möglichkeiten dazu, NAS, Cloud, Backblaze, sogar Festplatten. Aber macht es automatisch! Denn wenn es 3 Monate alt ist, sind das die neuesten Dateien, die euch fehlen!

Keine unbekannten Geräte nutzen

“Fallengelassene” USBs sind laut Studien immer noch die häufigsten Gründe, wie Geräte gehackt werden. Aber Malware kann auch in USB-Kabeln, Controllern, Stationen und sogar HDMI-Kabeln kommen. Seid vorsichtig auch mit unbekannten Händlern!

So wenig Daten wie möglich teilen

Daten, die ihr nicht online stellt, können nicht gestohlen werden. Und wenn eine Website nichts weiß, macht’s auch nichts, wenn sie gehackt werden und ihr dort registriert wart. Haben die aber alle Infos über euch, könnt ihr mit Phishing, Identitätsdiebstahl und mehr rechnen.