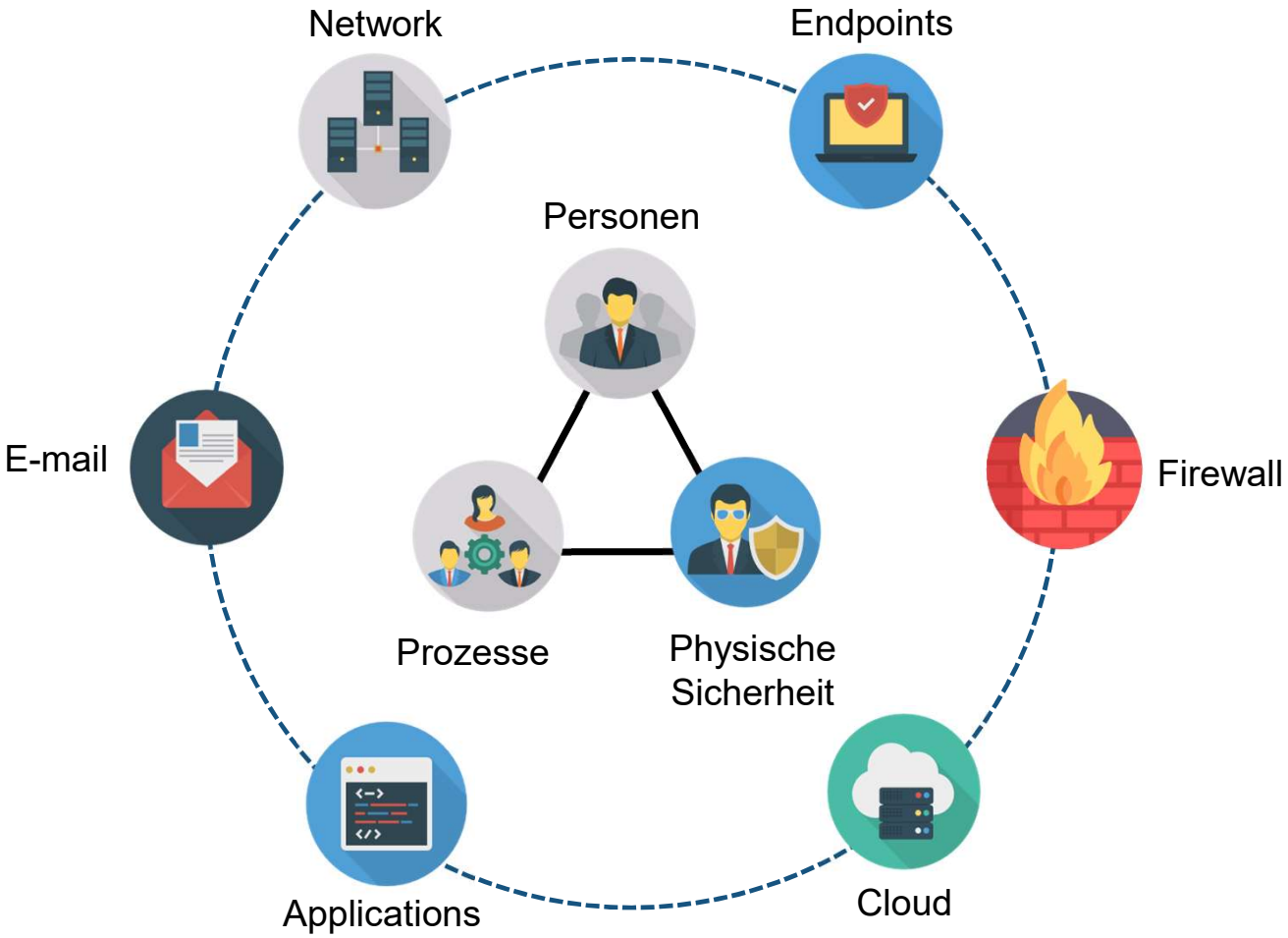
Nach Penetration Testing kommt…

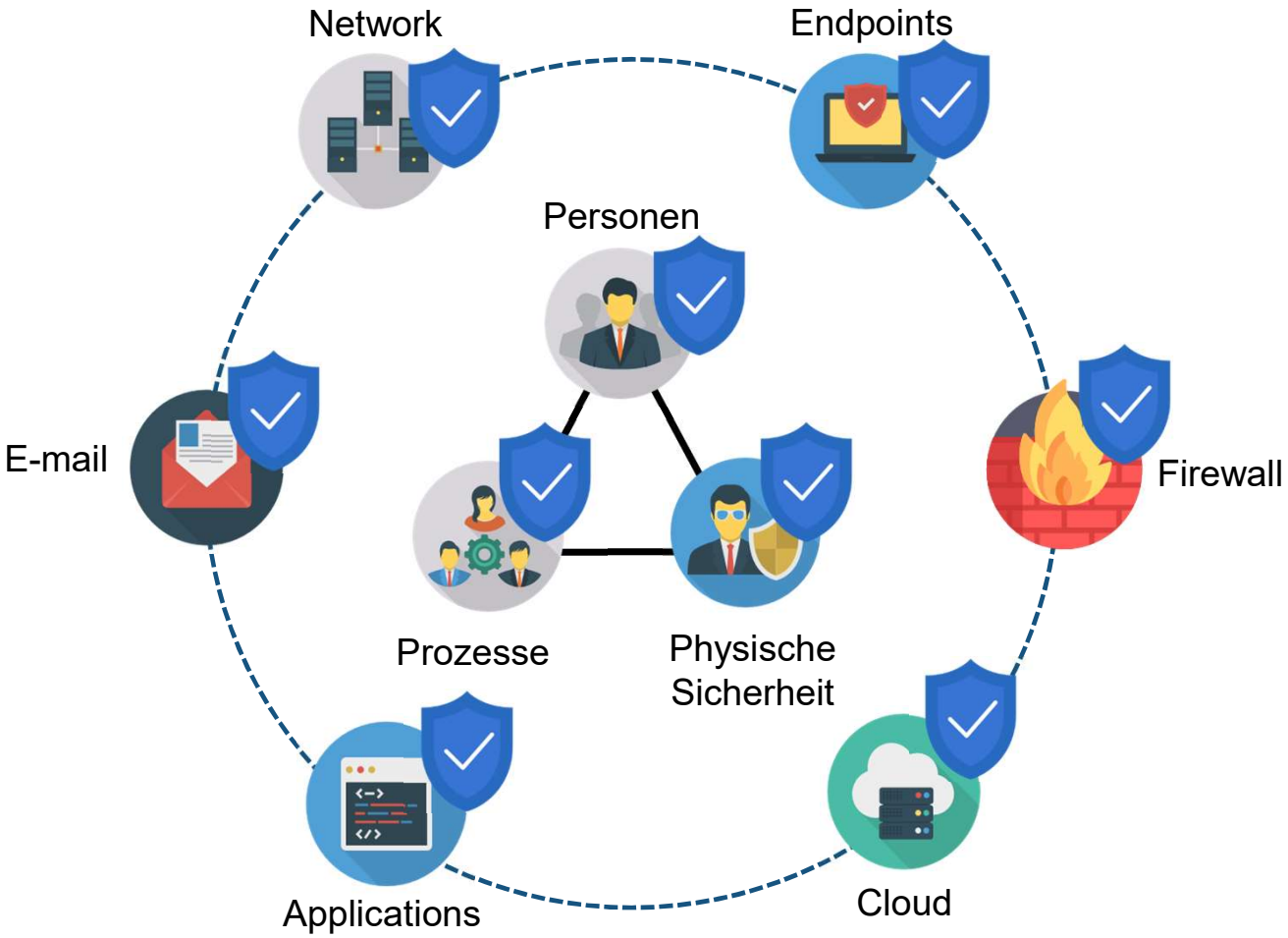
Red Teaming

Patrick Vananti

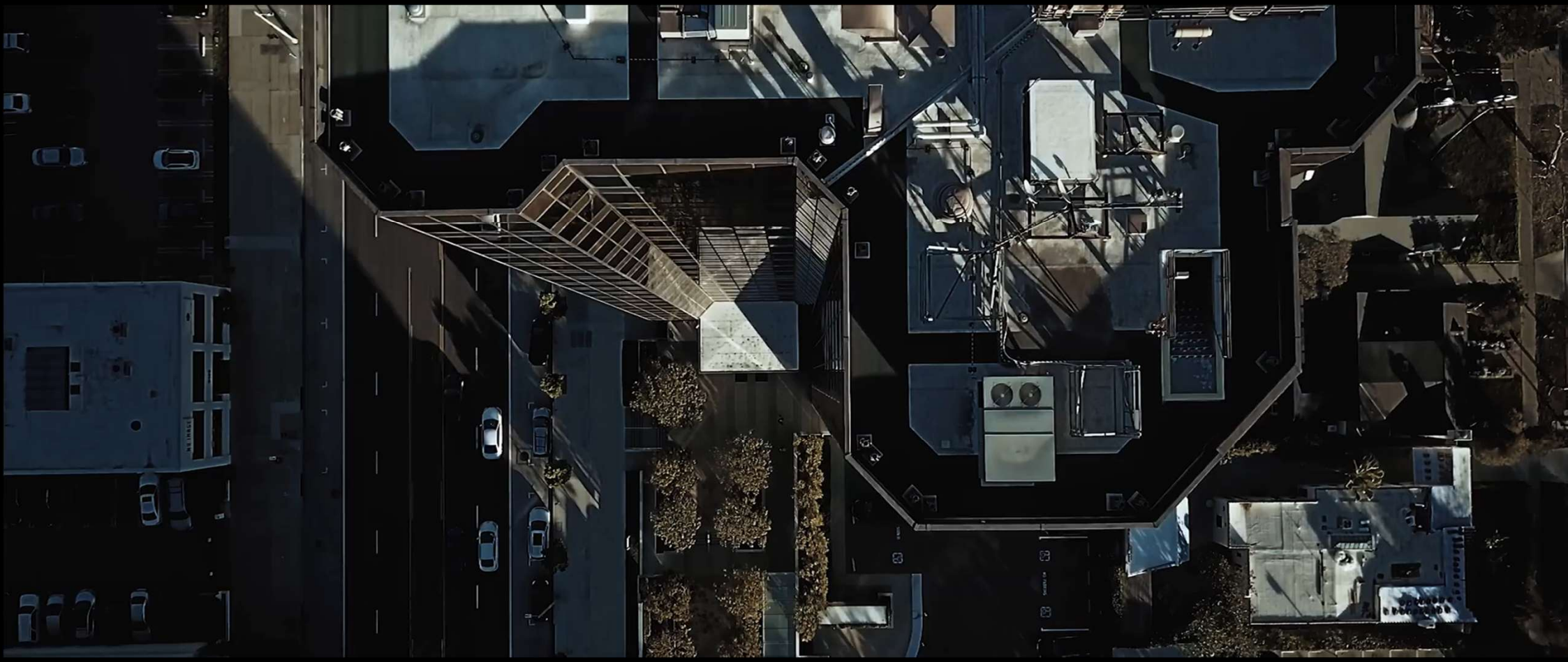
Die IT-Sicherheit ist…



Seit 20 Jahren…



Was ist Red Teaming?



[Source: www.f-secure.com]

Zusammenfassung

Red Teaming ist eine vollumfängliche, mehrstufige Simulation eines Angriffs auf ein Unternehmen

Training

Compass Security (Angreifer)

Kunde, Provider (Verteidiger)

Wie macht das Compass Security?

Red Teaming Phasen bei Compass Security

Heute zeige ich euch…

… einen Red Teaming Fall

Kunde:

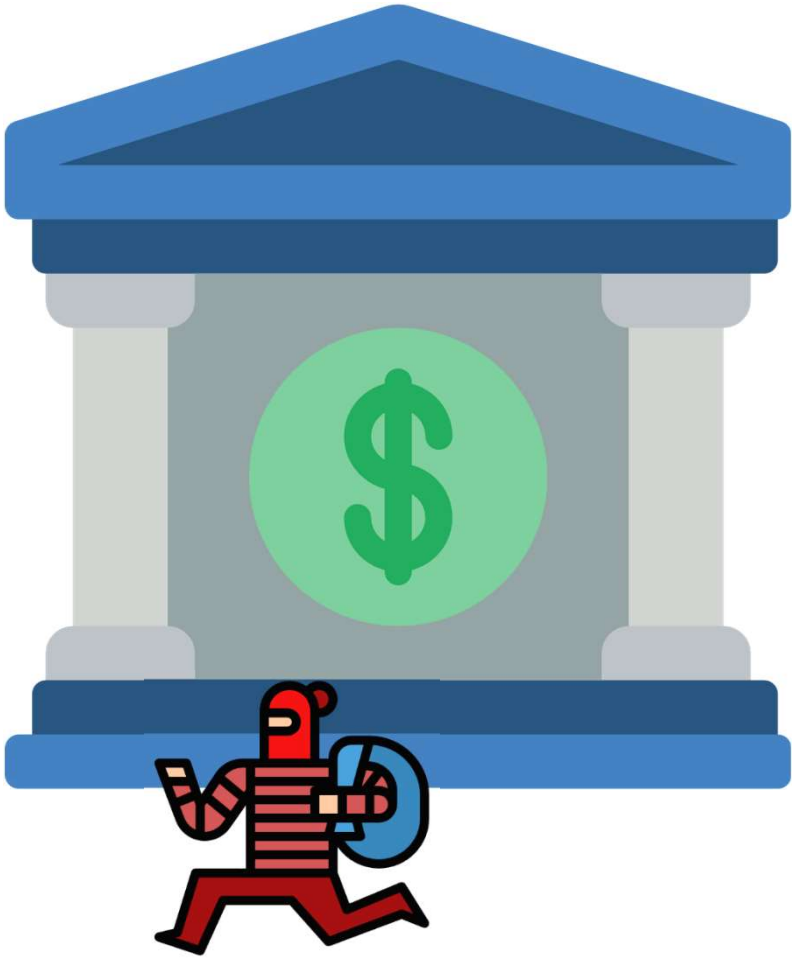
- Bank

Missionen:

- Defacement der öffentlichen Website
- Zugriff auf die Finanzdaten der Bank-Kunden
- Finanzdaten exfiltrieren

Ausgangslage:

- Keine Information



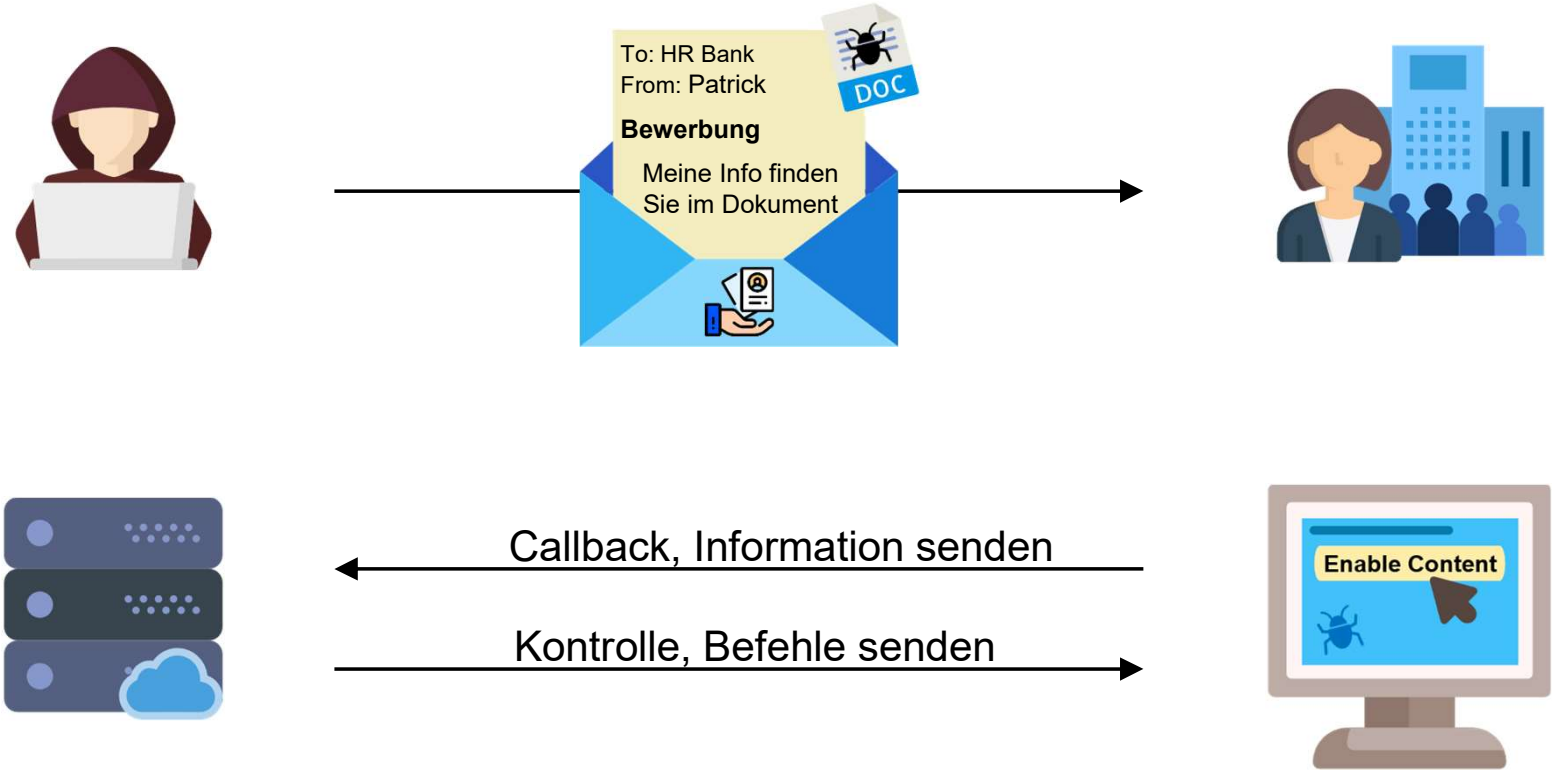
Informationen beschaffen

Informationen gesammelt

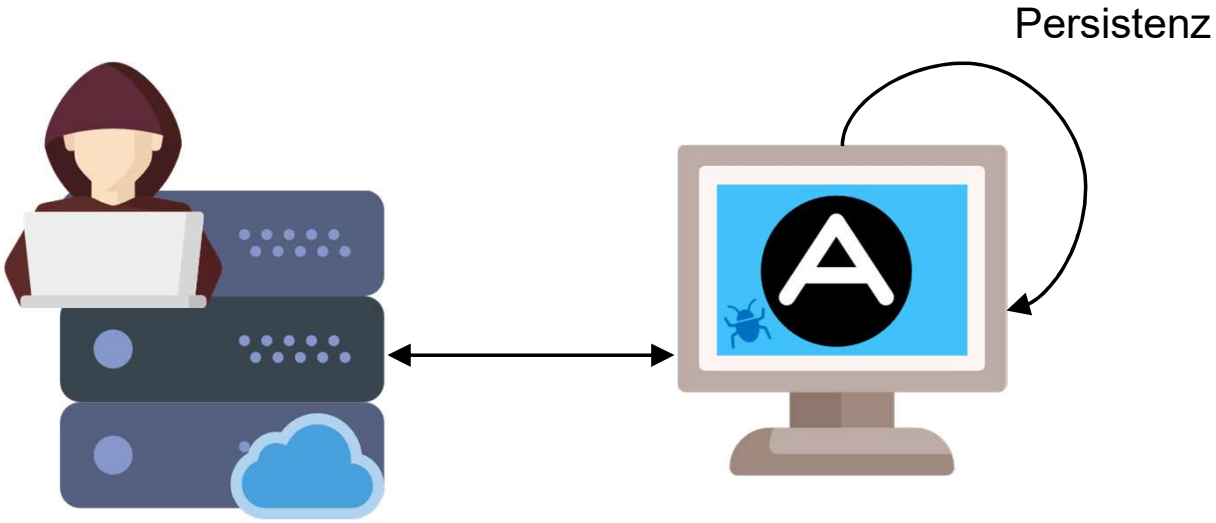
- Mittelgrosse Privatbank
- Hoher physischer Schutz der Gebäude
- Remote Virtual Desktop mit 2FA
- 200 MA Informationen
  - E-Mail Adressen
  - Funktion

Initialer Zugang

Die Idee…

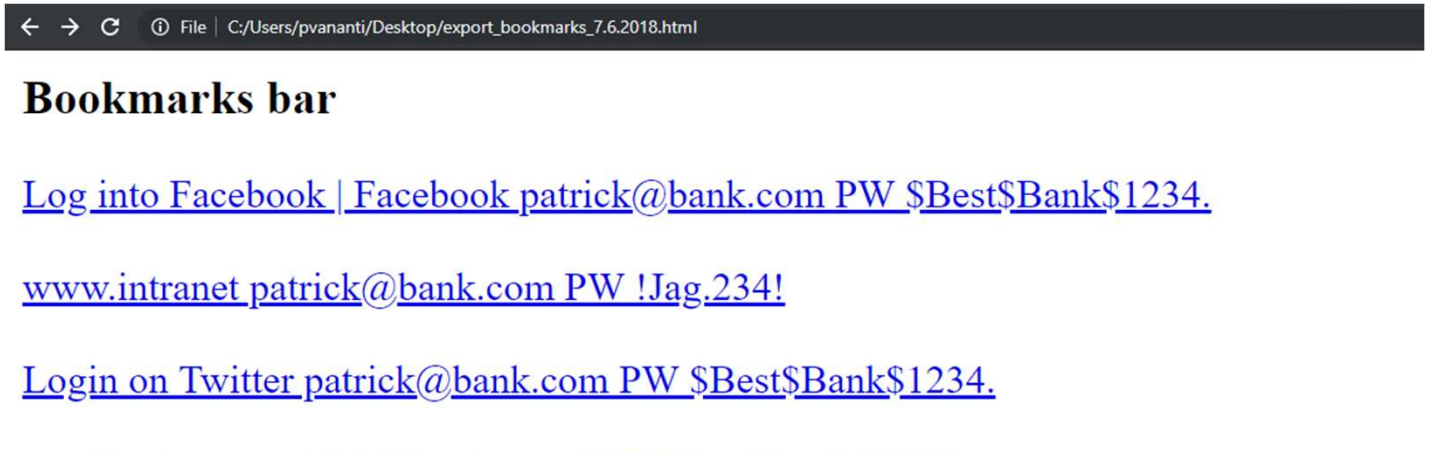


Persistenz Sicherstellen



Rechte Erweitern

Schauen wir uns noch genauer die gefundenen Dateien an:



Und …

Rechte Erweitern

… das Passwort $Best$Bank$1234 wird mehrmals verwendet

Ok, probieren will mal dieses Passwort bei allen Accounts…

…30 Accounts der Bank haben das gleiche Passwort…

…3 davon gehören zur Gruppe der Domain Administrators

Missionen Durchführen

Defacement der öffentlichen Webseite ✓

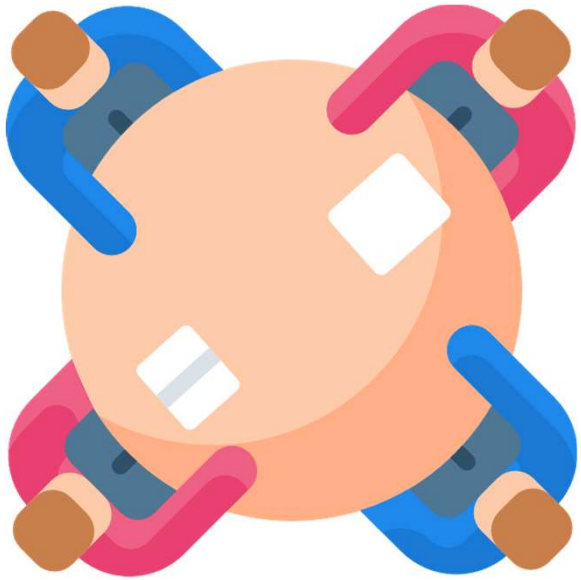
Zugriff auf die Finanzdaten der Bank-Kunden ✓

- Keylogger auf PC eines Backoffice MA installiert
- Zugriff auf Kunden Daten

Finanzdaten exfiltrieren ✓

Debriefing

- Wir haben gezeigt was wir gemacht haben
- Das Blue Team hat uns gezeigt was für Spuren gefunden wurden
- Wir haben zusammen die Massnahmen definiert




Credits: Eugene Onischenko / Alarmy Stock Photo


COMPASS
SECURITY