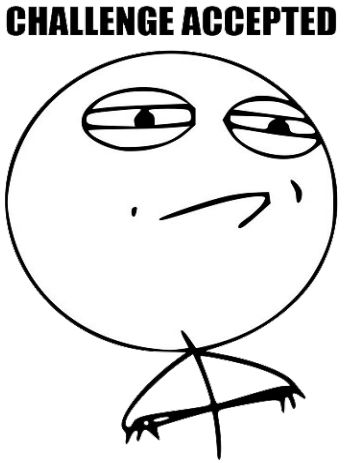
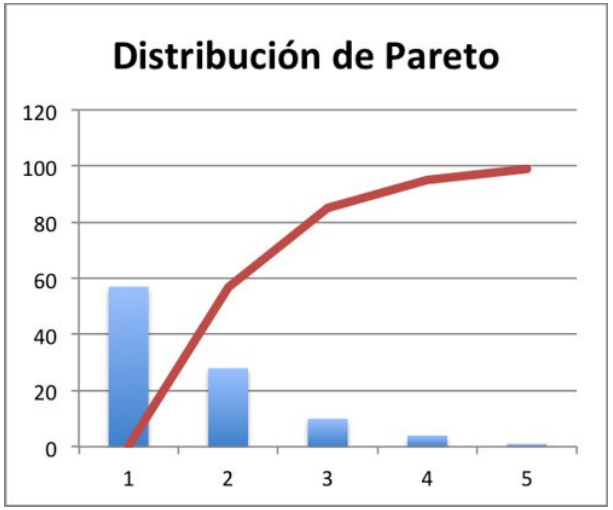
Gefahren im Netz

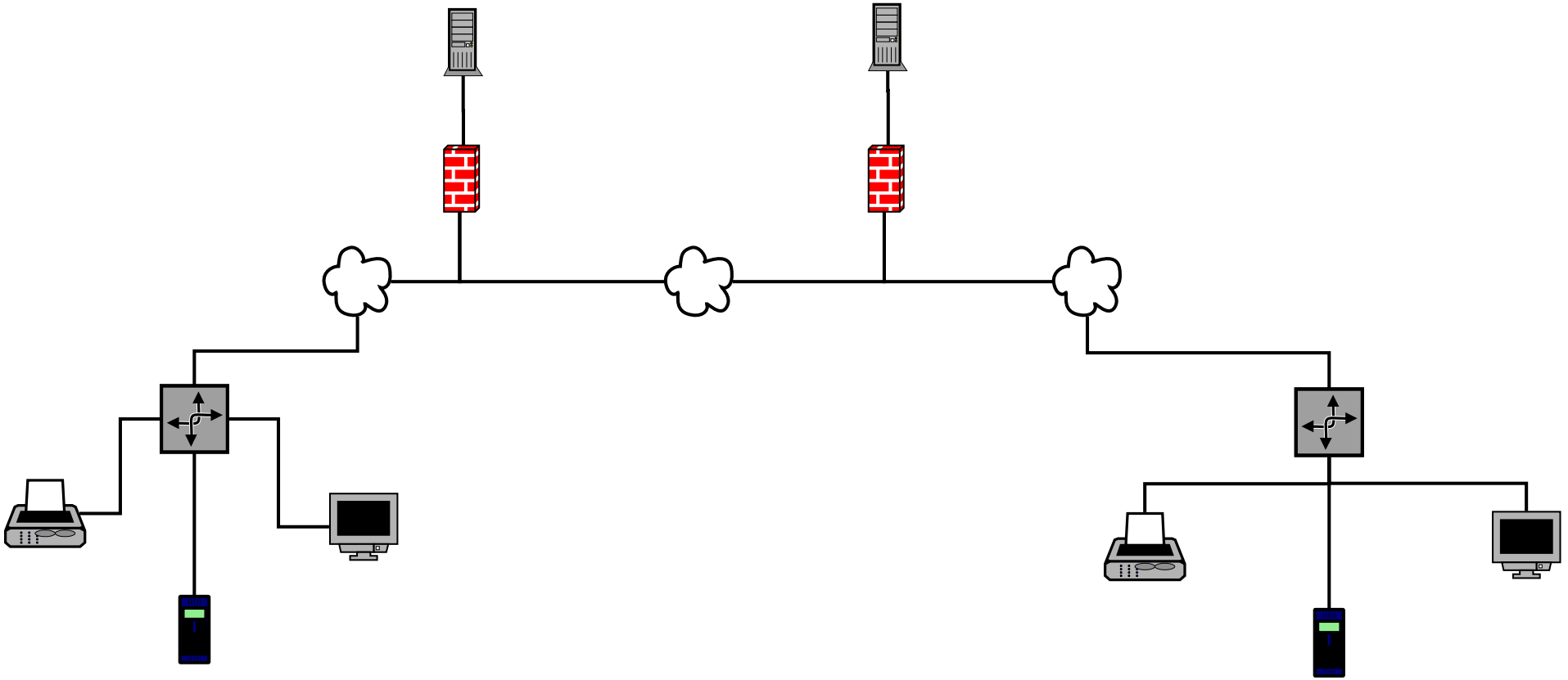


Es gibt keine absolute Sicherheit.



Gefahrenmodell

- Wovor will ich mich schützen?
- Was will ich investieren?
- Wem will, wem muss ich vertrauen?



Von welcher Gefahr reden wir?

- Kriminelle (greifen direkt an)
- Ermittlungsbehörden (überwachen)
- Wirtschaft (will Werbung schalten)

Gewöhnliche Kriminelle

- Betreiben Phishing
- Installieren Trojanische Pferde
- Verschlüsseln Daten und verlangen Lösegeld
- Greifen Server an und saugen Nutzerdatenbanken ab
- Kaufen Passwortlisten und probieren sie aus
- Suchen Sicherheitslücken und verkaufen sie

- The 18 biggest data breaches of the 21st century
- Warum eine komplette Arztpraxis offen im Netz stand
- Daten-Leak bei Autovermietung Buchbinder: 3 Millionen Kundendaten offen im Netz
- Deine Daten sind im Netz! | ct uplink 31.3

Ermittlungsbehörden

- Greifen Daten an Knotenpunkten (DE-CIX) ab
- Werten Metadaten aus (Vorratsdatenspeicherung)
- Installieren Trojanische Pferde (Quellen-TKÜ)
- Installieren Trojanische Pferde (Onlinedurchsuchung)
- Kaufen Sicherheitslücken auf dem Schwarzmarkt

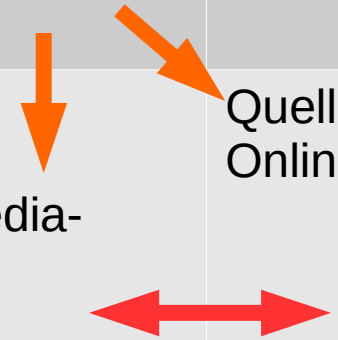
Privatwirtschaft

- Installiert Apps
- Wertet Metadaten aus
- Die Nutzer liefern die Daten freiwillig (unter anderem Metadaten) und meist ohne sich dessen bewusst zu sein

Allgemein oder gezielt?

- Allgemein
  - Man nimmt, was man bekommt
  - Geringe Trefferquote, Erfolg durch Masse
  - Abwehr relativ leicht
- Gezielt
  - Genaues Wissen über das Ziel
  - Hoher Aufwand
  - Abwehr schwer bis unmöglich

	Kriminelle	Staat	Wirtschaft
allgemein	Phishing Scam Verseuchte Mailanhänge Drive-By-Downloads Passwortlisten Trojanische Pferde Viren Fake-Hotspots	Vorratsdatenspeicherung	Big-Data-Analysen
spezifisch	Social Engineering Belauschen von WLANs Auswerten von Social-Media-Profilen	Quellen-TKÜ Online-Durchsuchung	Apps Nutzerprofile



Klassische kriminelle Angriffe

- Schwache oder mehrfach verwendete Passworte
  - https://haveibeenpwned.com/
  - https://sec.hpi.de/ilc/search?lang=de
- Phishing
- Drive-by-Downloads
- Leichtfertig installierte Software

Apps und Werbenetzwerke

- Schnüffel-Apps durch Analyse und Monitoring aufdecken
- A WSJ Investigation finds that iPhone and Android apps are breaching the privacy of smartphone users
- How One App Sees Location Without Asking
-

Was geht?

- Kommunikationsanbieter (Internet, Telefon) wissen, wann wir wo mit wem wie lange reden.
- Gratis-Apps liefern in der Summe ein Komplettprofil
- Payback liefert Kundenprofile
- Gesundheits-Apps liefern Patientenprofile

Was geht nicht?

- Instagram und Facebook können zwar heimlich auf das Mikrofon zugreifen, aber es gibt keine belastbare Untersuchung, dass dies auch wirklich geschieht – im Gegenteil.
- Der auf einigen Smartphone-Akkus verbaute NFC-Chip ist kein verstecktes Mikrofon.
- Nicht existierende Kameras können mich nicht filmen, egal wobei.

Was tun?

- Gute Passworte verwenden
- Festplatte verschlüsseln
- Backups
- Vorsicht bei
  - unbekannter Software. Macros in Office-Dokumenten deaktivieren.
  - Mails mit Links und Anhängen. Kryptografische Signaturen verwenden.
- Software aktuell halten, auch auf Routern und Druckern
- Vorsicht in offenen WLANs
- Weg von den großen Datensammlern (Google, Facebook, Whatsapp), hin zu Unternehmen mit anderem Geschäftsmodell (z.B. Duckduckgo, Posteo, Mastodon Signal)
- Vor allem aber: politischen Einfluss ausüben, z.B. für
  - Herstellergarantie auf Firmware
  - Kein staatliches Hacken

Zum Weiterlesen

- Malte Spitz: Was macht ihr mit meinen Daten?
- Katharina Nocun: Die Daten, die ich rief
- Daten als Ware – Spaß und Kurzweil im Überwachungsstaat
- Cryptoparty Köln-Bonn
- Cryptoparty international
- Linkliste zur DSGVO
- Verschiedene Messenger im Vergleich
- c’t-Raspion: Datenpetzen finden und bändigen
- Desinfec't 2019
-

Software

- Personal Software Inspector (PSI)
- FileHippo App Manager
- Desinfec‘t zum kostenpflichtigen Download