narrowIN

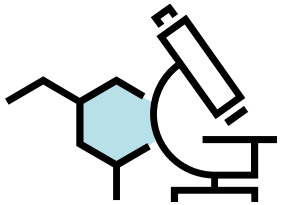
# Netzwerke sind inhärent unsicher – und jetzt?

Mischa Diehm, Co-Founder narrowin

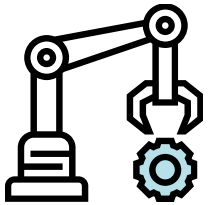
narrowin.ch


# «Alles wird vernetzt»

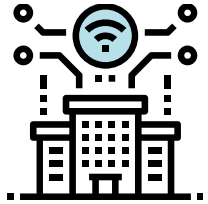
# Die Kehrseite der Medaille



Research &
Clinical



Operational Technology



IoT & Smart
Buildings

Workplace (BYOD)
& Home Office

# Easy to hack, hard to patch.

# 300%

mehr Ransomwareangriffe

>50% der Betroffenen sind kleine Unternehmen.

# 60%

Der betroffenen kleinen Unternehmen gehen offline

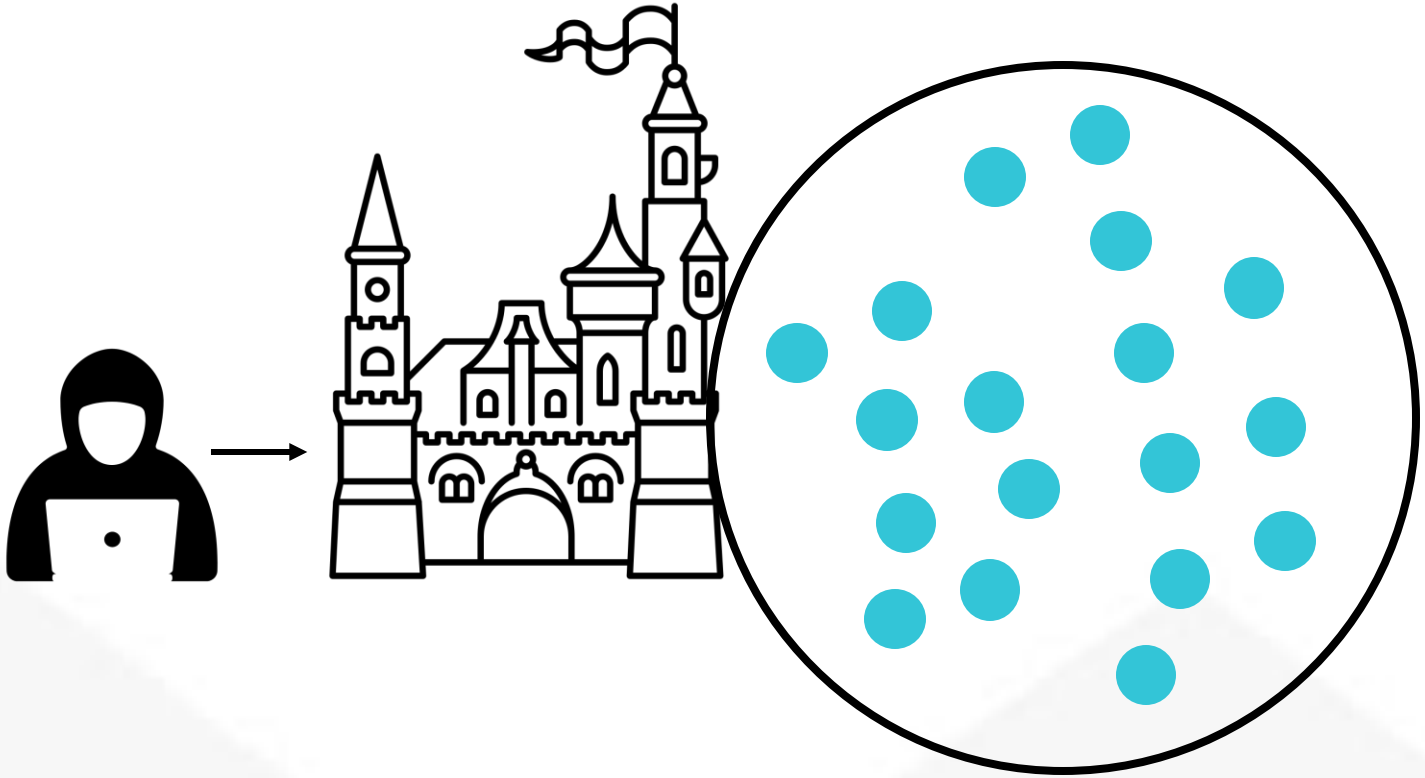
d.h. sie können den Geschäftsbetrieb nicht aufrechterhalten

# >100’000$

durchschnittlicher wirtschaftlicher Schaden

Quelle: Microsoft

# Wie Security historisch gebaut wurde



Ausserhalb = unsicher

Innerhalb = sicher.



Irgendwie kommt aber sowieso jemand ins Netzwerk – bzw. ist schon drin.
Egal ob via Phishing, Log4j, Ripple 20 oder USB-Stick.

» Es gibt zwei Arten von Unternehmen: diejenigen, die gehackt werden, und diejenigen, die gehackt werden, aber es noch nicht wissen. „Das wird uns nicht passieren“, ist nicht die richtige Vorsichtsmaßnahme. «

- BSI-Präsident Arne Schönbohm

# Beispiel Ripple 20, log4j etc.

heise online heise+

IT Wissen Mobiles Security Developer Entertainment Netzpolitik

TOPTHEMEN: UKRAINE-KRIEG WINDOWS 11 KRYPTOWÄHRUNGEN REPARATUR PODCAST

Security 〉7-Tage-News 〉06/2020 〉**Ripple20 erschüttert das Internet der Dinge**

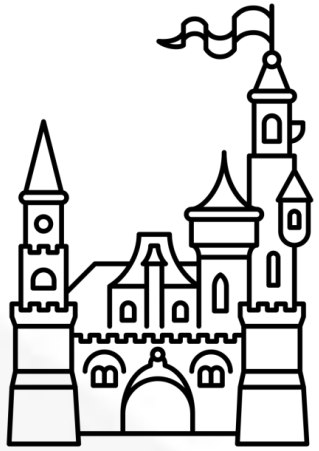
Alert!

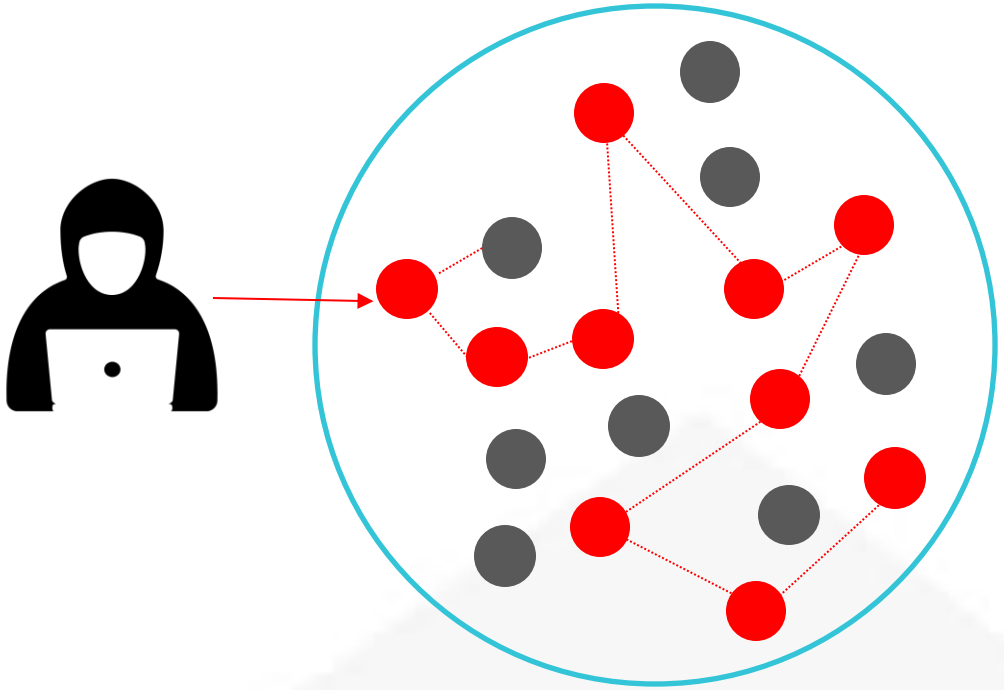
## Ripple20 erschüttert das Internet der Dinge

Eine Reihe von teils kritischen Sicherheitslücken in einer TCP/IP-Implementierung gefährdet Geräte in Haushalten, Krankenhäusern und Industrieanlagen.

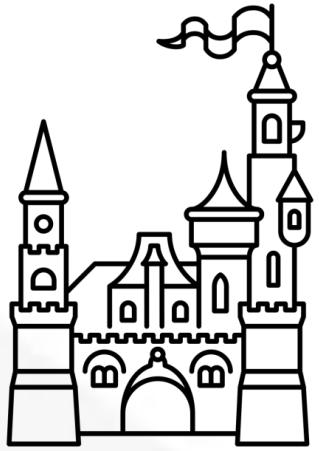

# Wie gehen wir damit um?

# Die Frage ist: Wie weit kommt der/die Angreifer*in im Netzwerk? (egal ob Mensch oder Script)

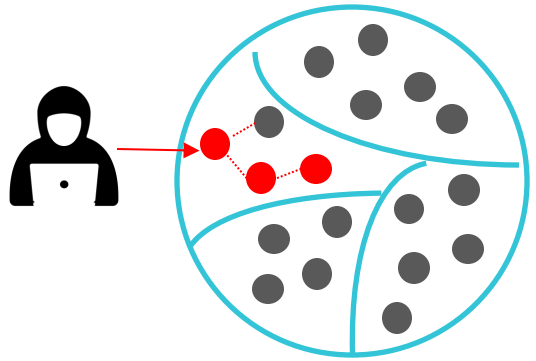




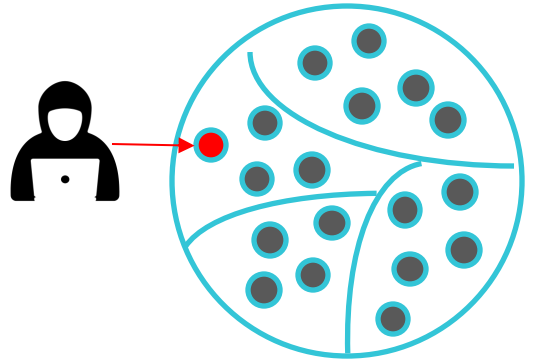
# Hinter der Mauer: Protection nicht nur “um” das Netzwerk bauen, sondern im Netzwerk



Protection



Segmentierung



Endpunktschutz

+ Detection: Monitoring

+ Reaction: Playbooks

# Key Take-aways

- Schutz im Netzwerk denken
- Lieber gleich anfangen und dafür klein: z.B. Liste mit Geräten die a) besonders kritisch oder b) besonders anfällig sind
- Basics umsetzen:
  - Segmentierung und Endpunktschutz als *Protection*
  - Monitoring für *Detection*
  - Playbooks für *Reaction*
- Keine teuren Supertechnologien notwendig, die dann nur von Spezialisten betrieben werden können