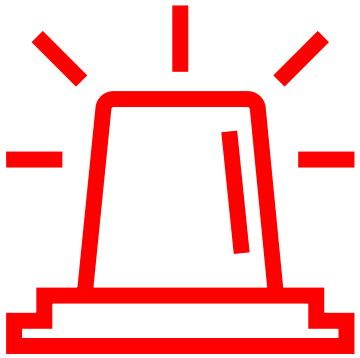
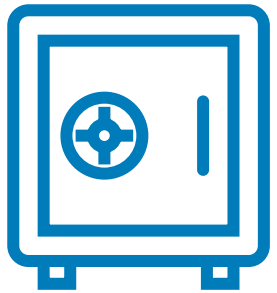
NETSEC.CO
THE NETWORK SECURITY COMPANY

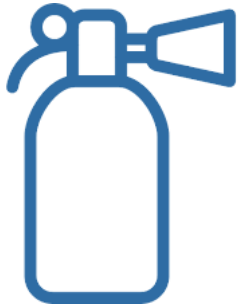
# Cyber-Sicherheitsstrategie für KMU

Wie sich KMU mit den ihnen zur Verfügung stehenden Ressourcen gegen Gefahren aus dem Internet effizient und wirkungsvoll schützen können

# physische Sicherheit







**118**

# typischer Angriff

- Angriff startet in Ihrem Netzwerk → Inside Out Attack
- es wird ein Trojaner platziert
- dieser kommuniziert mit einem Server des Angreifers
- Angreifer hat vollen Zugriff auf ein oder mehrere Systeme
  - lokale Daten
  - Netzlaufwerke
  - Applikationen
  - Bildschirm, Mikrofon, Kamera
- laterale Ausbreitung → Ziel: AD übernehmen

# Womit Sie rechnen müssen

- Benutzerkonten werden gestohlen
- Daten werden gestohlen und veröffentlicht oder verkauft
- Daten werden verschlüsselt
- IT Systeme sind nicht mehr nutzbar (Tage … Wochen)
- Sie sind nicht mehr erreichbar
- Angreifer hat sich in ihre Systeme eingenistet
- Angreifer verwischt seine Spuren

**Sie werden lange nichts davon merken**

# Strategie

**Schützen**

- Hürden für Angreifer so hoch wie möglich machen

**Erkennen**

- laufenden Angriff so schnell wie möglich erkennen

**Notfall planen**

- mit einem Angriff rechnen und sich darauf vorbereiten

# Schützen

- NG Firewall
- sicherer Remotezugang (Home Office)
- mobile Geräte verschlüsseln (Bitlocker mit PIN)
- Mitarbeitende schulen
- Vorgaben für Nutzung IT und Internet
- Least Privilege Prinzip umsetzen
- regelmässige System-Updates
- Datensicherung

# Erkennen

- zentrales Monitoring (Firewall, Endpoint Protection, …)
- Anlaufstelle für Mitarbeitende
- Alarmierung
  → 7 x 24h (Hacker halten sich nicht an Bürozeiten)

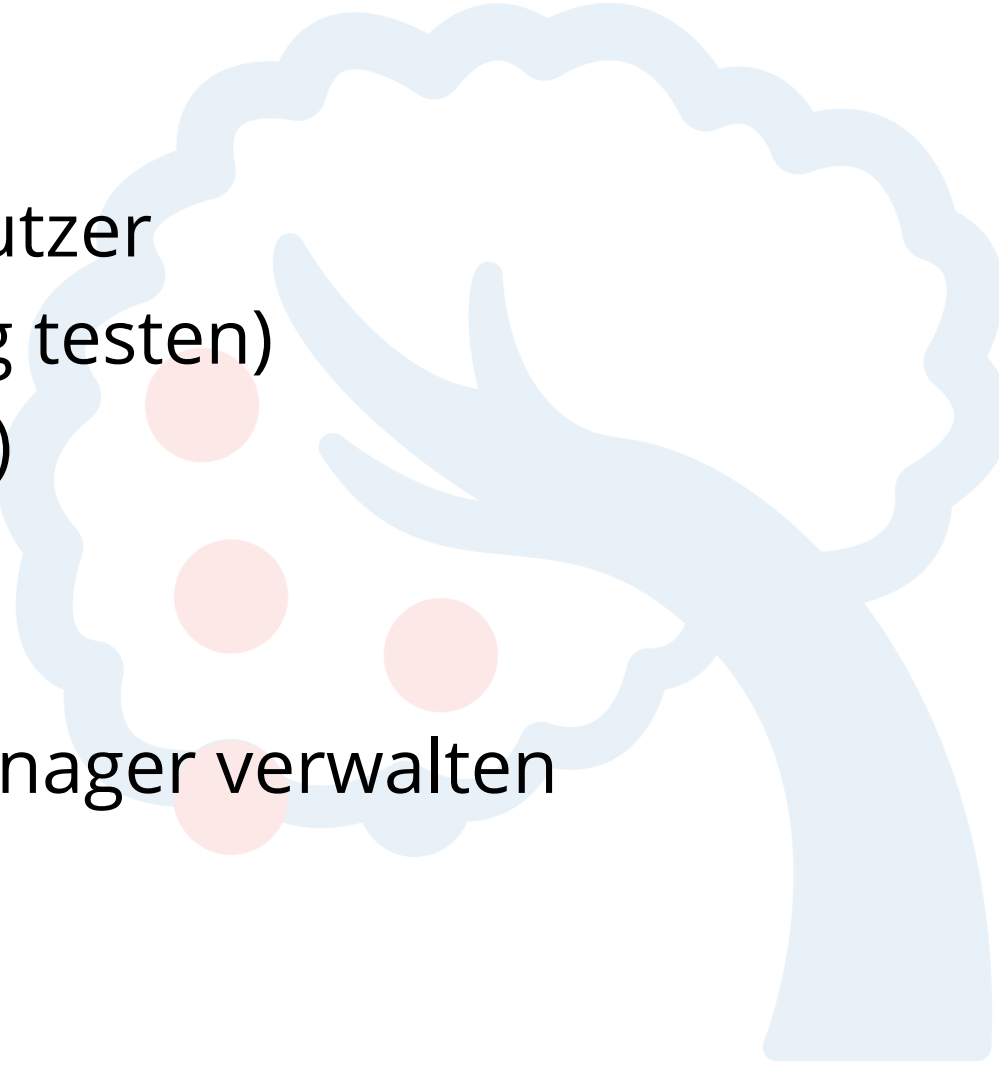
# Notfallplan

- Cyber Risiken in Risikomanagement aufnehmen
- Erstellen Sie einen Notfallplan
  - Wie reagieren wir auf bestimmte Ereignisse
  - Wie stellen wir einen Notbetrieb sicher
  - Wie können wir unsere Systeme wiederherstellen
  - Wo holen wir externe Hilfe
  - Wer trifft Entscheidungen (inkl. Stellvertretungen)
- Proben Sie den Notfall

**Wissen Sie über Ihre IT-Assets Bescheid**

# low hanging Fruits

- keine Admin Rechte für Benutzer
- Datensicherung (regelmässig testen)
- starke Authentisierung (MFA)
- Mitarbeitende schulen
- KEINE privaten Geräte
- Passwörter mit Passwort Manager verwalten



# Ist Cloud Computing die Lösung

# Fazit

- Entwickeln Sie eine passende Cyber-Sicherheitsstrategie
  → schrittweise vorgehen
- Bauen Sie eine sichere Infrastruktur für Homeoffice
  → One Client Strategie
- Prüfen Sie, ob Sie den Schritt in die Cloud wagen wollen
  → falls ja, dann richtig

**Cyber-Security ist Chefsache**

# Fragen