Risikobeurteilung

Appreciation de risques

Ph. Oechslin, 24.01.20

Outline

- Terminologie nach ISO 27005
- Bedrohungsbäume
- Risikoidentifizierung
- Risikobewertung

Terminologie nach ISO 27005

- Kontext erstellen (context establishment)
- Risikobeurteilung (risk assessment)

  1. Risikoidentifizierung (risk identification)
  was kann schief gehen?
  - Werte: Korrektheit, Stimmgeheimnis, keine frühzeitigen Resultate
  - Massnahmen: Verifizierbarkeit, Verschlüsselung, Patching
  - Bedrohungen: interner/externer liest/manipuliert/löscht ..

  2. Risikoanalyse (risk analysis)
  wie schlimm, häufig ist es?
  - Schadenausmass, Eintrittswahrscheinlichkeit

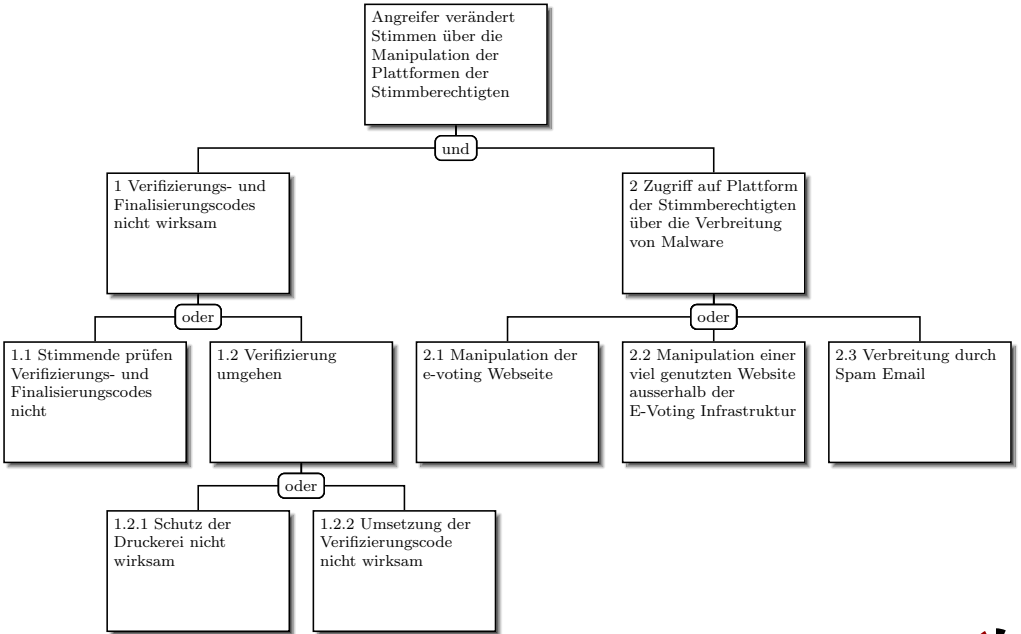
  3. Risikobewertung (risk evaluation) : *kann man es akzeptieren?*
  - Akzeptanzkriterien

- Risikobehandlung (risk treatment)
- Manchmal wird für R-beurteilung und -behandlung auch R-analyse gesagt

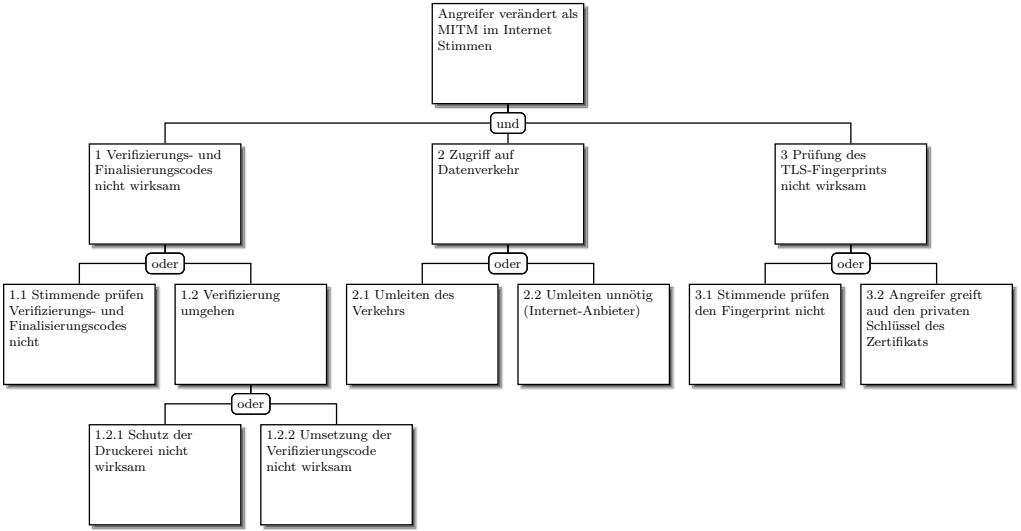
Bedrohungsbäume

- Risikoidientifizierung und -analyse mit Bedrohungsbäumen:
- Für ein Angriffsziel stellt man sich verschiedene Szenarien vor, die alle zum selben Ziel führen
- Die Szenarien werden als Baum dargestellt
  - Das Ziel steht an der Wurzel
  - Die Äste sind Szenarien, die zum Ziel führen

Bedrohungsbäume



Bedrohungsbäume

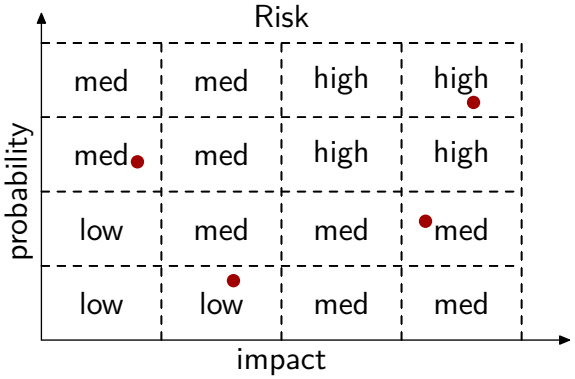


Risikoidentifizierung

- Für jeden Baum
  - Was ist das Schadensausmass der Bedrohung
  - Was ist der einfachste Weg zum Schaden

Risikobewertung

- Zwei Skalen: Ausmass, Wahrscheinlichkeit



- Akzeptierungs-Kriterium ist z.B: nur mittlere und tiefe Risiken