LU03d - Angriff auf lokal VS Zentral IT-Systeme

Lernziele

1. Sie können können typische Angriffsvektoren lokaler IT-Systeme (z. B. USB-Malware, LAN-Angriffe) und zentraler IT-Systeme (z. B. Webangriffe, DDoS) benennen und deren Unterschiede erläutern.
2. Sie sind in der Lage, lokale und zentrale IT-Systeme hinsichtlich ihrer Angriffsflächen, Reichweite und typischer Schutzmassnahmen systematisch zu vergleichen.
3. Sie können geeignete technische und organisatorische Schutzmassnahmen spezifischen Bedrohungsszenarien in lokalen und zentralen Systemen zuordnen.

Einleitung

Moderne IT-Infrastrukturen bestehen in der Praxis meist aus einer **Mischung aus lokalen und zentralen Systemen** – etwa Arbeitsplatzrechnern, lokalen Netzwerken, aber auch Cloud-Diensten, Rechenzentren oder zentralen Servern. Beide Architekturen haben ihre **eigenen Schwachstellen und Angriffspunkte**, die es zu kennen gilt.

Lokale IT-Systeme – Angriffsfläche vor Ort

Lokale Systeme umfassen alles, was physisch oder logisch vor Ort betrieben wird: PCs, Notebooks, Netzlaufwerke, lokale Server oder IoT-Geräte.

Typische Angriffsvektoren

- **Direkter physischer Zugriff**

→ USB-Malware, BIOS-Zugriffe, Boot-Viren

- **Netzwerkangriffe im LAN**

→ ARP-Spoofing, Man-in-the-Middle, unverschlüsselte Übertragungen

- **Malware & Ransomware**

→ Verbreitung durch infizierte USB-Sticks oder lokale Dateifreigaben

- **Veraltete Systeme ohne Updates**

→ Häufig bei abgeschotteten Maschinen (z. B. in der Produktion)

Besonderheit

Angriffe auf lokale Systeme erfordern häufig **physischen Zugriff** oder ein **Netzwerk von innen** – was sie nicht weniger gefährlich, aber lokal begrenzt macht.

Zentrale IT-Systeme – Angriff aus der Ferne

Zentrale Systeme wie Cloud-Plattformen, zentrale Datenbanken oder Webserver sind in der Regel **rund um die Uhr erreichbar** – und damit jederzeit potenziell angreifbar.

Typische Angriffsvektoren

- **Web-basierte Angriffe**

→ SQL-Injection, Cross-Site Scripting (XSS), Directory Traversal

- **Credential Stuffing & Brute Force**

→ Automatisierte Angriffe auf Login-Formulare

- **DDoS-Angriffe**

→ Überlastung des zentralen Systems durch massenhafte Anfragen

- **Sicherheitslücken in Cloud-Konfigurationen**

→ Offene S3-Buckets, falsch konfigurierte Zugriffspolicies

Besonderheit

Zentrale Systeme bieten oft **höhere Angriffsreichweite** – ein erfolgreicher Angriff kann gleich **tausende Nutzer betreffen**. Dafür sind sie meist besser geschützt (z. B. durch CDN, WAFs, Redundanz).

Vergleich – lokale vs. zentrale Systeme

Merkmal	Lokale Systeme	Zentrale Systeme
Zugriffsart	Lokal / intern	Über das Internet
Typische Angriffe	Physischen Zugriff, LAN-Hacks	Webangriffe, Remote Exploits
Skalierung des Schadens	Begrenzt auf Standort	Potenziell global
Schutzmassnahmen	Physische Sicherheit, Netzwerksegmentierung	Cloud-Hardening, API-Schutz