zurück

Security – Grundlagen (CIA, Zero Trust, Hardening, Angriffe, Passwörter, Firewalls)

IT-Sicherheit schützt Systeme, Daten und Netzwerkstrukturen vor Angriffen, Fehlbedienung, Verlust und Manipulation.
Sicherheit ist kein Produkt, sondern ein Prozess.

Diese Seite behandelt:

- CIA-Triade
- Zero Trust
- Angriffsarten
- Hardening
- Firewalls
- Passwortrichtlinien
- Updates & Patchmanagement
- Logging & Monitoring
- Zugriffskontrolle (Least Privilege)

---

1. CIA-Triade – die 3 Grundpfeiler der IT-Sicherheit

Die CIA-Triade besteht aus:

- **C – Confidentiality (Vertraulichkeit)**
- **I – Integrity (Integrität)**
- **A – Availability (Verfügbarkeit)**

Confidentiality

Daten dürfen nur von berechtigten Personen eingesehen werden.

Maßnahmen:

- Verschlüsselung (TLS, AES, VPN)
- Zugriffsrechte
- MFA (z. B. FIDO2, App)

Integrity

Daten dürfen nicht unbemerkt verändert werden.

Maßnahmen:

- Signaturen
- Hashes (SHA-256)
- File-Integrity-Monitoring
- Versionskontrolle

Availability

Systeme müssen erreichbar und nutzbar bleiben.

Maßnahmen:

- Monitoring
- Backups
- Load Balancing
- DDoS-Schutz

---

2. Zero Trust Security

Zero Trust = „Traue niemandem, prüfe alles."

Grundprinzipien:

- keine vertrauenswürdige Zone (LAN ≠ sicher)
- jeder Zugriff wird geprüft
- geringste Rechte (Least Privilege)
- dauerhafte Überwachung
- Mikrosegmentierung / VLANs
- Authentifizierung & Autorisierung bei *jeder* Aktion

```
User → Auth → Policies → Zugriff (wenn erlaubt)
```

---

3. Angriffsarten – typische Bedrohungen

Malware

- Viren
- Trojaner
- Ransomware

Netzwerkangriffe

- MITM (Man in the Middle)
- ARP Spoofing
- DNS Spoofing
- Port-Scanning
- DDoS

Webangriffe

- SQL Injection
- XSS (Cross-Site Scripting)
- CSRF
- Directory Traversal

Social Engineering

- Phishing
- Vishing
- Pretexting
- Stimme-KI / Deepfake

Insider Threats

- ehemalige Mitarbeiter
- Missbrauch von Adminrechten

---

4. Hardening – Systeme absichern

System-Hardening bedeutet: „alles entfernen, was nicht gebraucht wird“.

Maßnahmen

- unnötige Dienste deaktivieren
- sichere Passwortrichtlinien
- SSH absichern (kein root login, key auth)
- Firewall aktivieren
- Logs überwachen
- Updates einspielen
- Container als non-root
- Transportverschlüsselung (HTTPS)
- sichere Standardwerte (secure defaults)

Beispiel: Linux Hardening

- /etc/ssh/sshd_config prüfen
- Fail2Ban / CrowdSec
- UFW oder nftables
- Dateirechte korrekt setzen
- root-Login verbieten

Beispiel: Webserver Hardening

- HSTS
- TLS 1.2+
- sichere Ciphers
- keine Directory Listings
- WAF einsetzen

---

5. Zugriffskontrolle (Access Control)

Ein zentrales Prinzip moderner Sicherheit:

Least Privilege
→ Jeder Benutzer bekommt nur die Rechte, die er unbedingt braucht.

Weitere Modelle:

Role-Based Access Control (RBAC)

- Rollen bestimmen Berechtigungen (Admin, User, Support)

Attribute-Based Access Control (ABAC)

- Entscheidungen anhand von Attributen
  (z. B. Standort, Zeit, Gerätetyp)

Multifaktor-Authentifizierung (MFA)

- Passwort + Smartphone
- Passwort + FIDO2-Key

MFA ist Pflicht in modernen Systemen.

---

6. Passwort-Sicherheit

Gute Passwörter

- mindestens 12–16 Zeichen
- zufällig generiert
- Kombination aus Zahl, Groß-, Klein- und Sonderzeichen
- keine Wörter oder Muster

Tools:

- Passwortmanager (z. B. Vaultwarden, Bitwarden)

Schlechte Passwörter

- „Hallo123“
- „Passwort“
- „Lars1983!“
- wiederverwendete Passwörter

Passworthashes

Passwörter werden nie im Klartext gespeichert.

Verfahren:

- bcrypt
- Argon2id (modern, sicher)
- scrypt

7. Updates & Patchmanagement

Viele Sicherheitslücken entstehen durch veraltete Software.

Regeln:

- Betriebssysteme regelmäßig aktualisieren
- Sicherheitsupdates priorisieren
- Firmware aktualisieren (Switches, Router, Controller)
- Container-Images erneuern
- alte Versionen entfernen

---

8. Firewalls

Firewalls überwachen und steuern Netzwerkverkehr.

Arten:

- Paketfilter (Layer 3/4)
- Statefull Inspection
- Next-Gen Firewall (NGFW)
- Web Application Firewall (WAF)

Funktionen:

- Blocken unerwünschter Ports
- Anomalieerkennung
- Benutzerrollen (Identity Firewall)
- IPS/IDS Integration
- Logging

Beispiele:

- iptables / nftables
- OPNsense / pfSense
- FortiGate
- Sophos XG
- Palo Alto

---

9. Logging, IDS & Monitoring

Logs sind essenziell für Sicherheit:

- Auth-Logs
    - Webserver-Logs
      * System-Logs
      * Firewall-Logs
      * IDS-Alarme (z. B. Suricata)
      * CrowdSec Signale

  Moderne Tools:

- Suricata (IDS/IPS)
    - CrowdSec (Erkennung + automatische Gegenmaßnahmen)
      * Loki + Promtail (Log-Analyse)
      * Grafana (Dashboards)

---

10. Netzwerksegmentierung

Netzwerke in VLANs trennen:

- Server
    - Gäste
      * IoT
      * Verwaltung
      * Kamera
      * Kinder-Netz

  Vorteile:

- ein infiziertes Gerät infiziert nicht den Rest
    - Angriffsfläche reduziert
      * Zero Trust leichter umsetzbar

  ASCII:

```
VLAN10 = Server
VLAN20 = Workstations
VLAN30 = Gäste
VLAN40 = IoT
```

---

11. Backups & Datenintegrität

Essentiell:

- 3-2-1 Regel
    - Offsite-Backups
      * Verschlüsselte Backups
      * regelmäßige Restore-Tests

  Sicherheit ≠ nur Firewalls
  → Ohne Backup keine Verfügbarkeit.

Zusammenfassung

- CIA-Triade ist Grundlage der IT-Sicherheit
    - Zero Trust: Nichts ist vertrauenswürdig
      * Hardening = unnötiges entfernen + sicher konfigurieren
      * Firewalls & IDS schützen das Netzwerk
      * Passwörter: lang, zufällig, einzigartig
      * MFA ist Pflicht
      * Logs + Monitoring = Angriffserkennung
      * Netzwerksegmentierung begrenzt Schäden
      * Backups sichern die Verfügbarkeit
      * Sicherheit ist ein kontinuierlicher Prozess