Zero Trust

Inhaltsverzeichnis

Zero Trust ist ein Sicherheitsmodell, das keinem Benutzer, Gerät oder Netz standardmäßig vertraut. Jeder Zugriff wird kontinuierlich verifiziert – unabhängig davon, ob er aus dem internen Netz oder von außen kommt.

1 Funktionsweise

Statt eines harten Innen/Außen-Grenzzauns gilt: Identität, Gerät und Kontext werden bei jedem Zugriff geprüft. Rechte sind minimal und zeitlich bzw. situativ begrenzt.

- **Verifizieren:** starke Authentifizierung und Geräteprüfung
- **Least Privilege:** nur die wirklich benötigten Rechte
- **Annehmen von Kompromittierung:** Segmentierung und Monitoring als Normalzustand

2 Typische Bausteine

- MFA / Passkeys und zentrales Identity-Management
- Mikrosegmentierung und bedingte Zugriffsrichtlinien
- Geräte-Compliance (Patch-Stand, Verschlüsselung)
- Logging, Erkennung und schnelle Reaktion

3 Wichtige Hinweise

- Zero Trust ist eine Strategie, kein einzelnes Produkt.
- Umsetzung erfolgt schrittweise – oft zuerst bei Remote-Zugriff und kritischen Apps.
- Ohne saubere Identitäten und Inventar greifen Richtlinien schlecht.

4 Fazit

Zero Trust ersetzt blindes Netzvertrauen durch kontinuierliche Prüfung. Gerade bei Hybrid-Arbeit, Cloud und wachsenden Angriffsflächen ist das ein robuster Leitrahmen für moderne IT-Sicherheit.