

# meetUP

SMART WORKPLACE 

Reinach, 25.11.2025

# Zero Trust

Der Arbeitsplatz als Sicherheitsrisiko  
von Perry Müller-Bauer



- Was ist Zero Trust?
- Die Kernprinzipien
- Warum Zero Trust?
- Welche Vorteile bringt ZTA?
- Architekturansätze und Bausteine
- Beispiel Access Flow
- Wie implementiert man Zero Trust?
- Eine Lösungsarchitektur
- Herausforderungen
- Fazit

- Zero Trust ist kein Produkt und keine einzelne Technologie
- Zero Trust ist viel mehr:
  - Ein Sicherheitskonzept
  - Eine Strategie
  - Ein Rahmenwerk
  - Ein Paradigma
  - Eine Architektur

Eine Zero Trust Architektur umzusetzen bedeutet wesentliches dem Motto „never trust, always verify“ zu folgen – Ein End-to-End Ansatz.



- **neue Bedrohungslagen:** Der perimeterbasierte Schutz bzw. Sicherheit ist outdated und im Verhältnis leicht zu kompromittieren
- **Prinzipielle Sicherheit:** Zero Trust folgt dem Grundsatz „nie vertrauen, immer verifizieren“ // Nichts und niemand ist grundsätzlich als sicher zu bewerten; weder der Admin Client noch das Device der Geschäftsführung
- **Geeignet für Remote-Arbeit:** Homeoffice, Cloud-Dienste und externe Partner machen ein perimeterbasiertes Modell obsolet; Zero Trust funktioniert in hybriden Umgebungen besser

# Welche Vorteile bringt die ZTA?

---



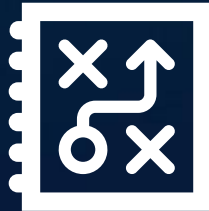
- **Schutz kritischer Daten:** Zugriffskontrolle auf Basis von Identität, Gerät und Kontext
- **Reduktion von Ransomware-Risiko:** Mikrosegmentierung begrenzt seitliche Bewegungen eines Angreifers innerhalb der Umgebung
- **Compliance und Vertrauen:** Bessere Nachvollziehbarkeit von Zugriffseignissen hilft bei Datenschutzerfordernungen und stärkt Kundenvertrauen

- **Identität**sbasierende Architektur:
  - Identity and Access Management (IAM)
  - Multi-Factor Authentication (MFA)
- **Geräte**basierende Architektur:
  - Endpoint Detection and Response
  - Mobile Device Management
  - Compliance Check
- **Netzwerk**basierende Architektur:
  - Mikrosegmentierung
  - ZTNA (Zero Trust Network Access) / Network Access Proxy / Network Access Control
- **Daten**basierende Architektur:
  - Verschlüsselung
  - DLP (Data Loss Prevention)
  - RBAC (Role Based Access Control)
- **Applikation**sbasierende Architektur
  - Least Privilege
  - RBAC
  - Conditional Access

# Beispiel Access-Flow

- Benutzer/Identität

- Authentifizierung via MFA (Multi-Faktor-Authentifizierung)
- Identitätsprüfung (z. B. über Identity Provider wie Azure AD)



- Datei-Server / Cloud-Speicher

- Zugriff erfolgt über verschlüsselte Verbindung (TLS)
- Autorisierung auf Basis von Least Privilege

- Policy Engine

- Richtlinien prüfen: Rolle, Standort, Zeit, Risiko-Level
- Zugriff wird nur gewährt, wenn alle Bedingungen erfüllt sind



- Geräte-Compliance

- Gerät wird auf Sicherheitsstatus geprüft (z. B. aktuelles OS, Antivirus aktiv)

- Monitoring & Logging

- Jeder Zugriff wird protokolliert
- Anomalie-Erkennung aktiv

- Skalierbare Investition: Zero-Trust-Prinzipien lassen sich stufenweise einführen; KMU können Prioritäten setzen und mit überschaubaren Maßnahmen beginnen

Schritt 1: Ist-Analyse: Assets, Nutzer, Datenflüsse, Risiken (Asset-Inventory)

Schritt 2: **Identity** und Account Security (MFA, zentrales IAM)

Schritt 3: **Device** Security (Compliance Check, Patchmanagement, EDR)

Schritt 4: **Access** Control (RBAC, Conditional Access, Just-In-Time Access)

Schritt 5: **Network** Security (Microsegmentation, ZT Network Access)

Schritt 6: **Data** and **Application** Security (Least Privilege, RBAC, DLP, Encryption)

Schritt 7: Kontinuierliche Verbesserung, Monitoring, Logging (SIEM, Threat Detection)

- Identität: Entra ID mit MFA, Passwortless-Optionen, Conditional Access
- Geräte: Intune zur Verwaltung mobiler und stationärer Geräte, Compliance-Richtlinien
- Endpunktschutz: Defender for Endpoint für EDR/EDR-Response und automatisches Containment
- Daten & Apps: Purview (DLP, Klassifizierung) + Sicherheitsrichtlinien für Microsoft 365 Apps
- Observability & Response: Microsoft Sentinel (SIEM) + automatisierte Playbooks (SOAR) zusammen mit Defender-Logs.

- Mensch und Kultur - Awareness und Akzeptanz
- Fachkräfte und Know-How - Fachkräftemangel
- Bestehende IT-Landschaft und Komplexität - Heterogene Alt-Systeme
- Kosten und Lizenzierung - Lizenz- und Betriebskosten
- Prozesse, Governance und Verantwortlichkeiten - Fehlende Prozesse
- Datenschutz und rechtliche Anforderungen - Compliance
- Betrieb, Monitoring und Reaktionsfähigkeit - Kontinuierliches Monitoring

- Zero Trust Architektur als GOAL
- Low-Hanging Fruits identifizieren
- Lifecycle sinnvoll nutzen
- ZTA Komponenten mit grossem Hebel identifizieren (Beispiel MFA)
- Stakeholder überzeugen
- Techn. als auch partnerschaftliche Synergien nutzen und ausbauen