Fragestellung

Wie lässt sich eine Zero Trust Sicherheitsarchitektur in einer kontrollierten Testumgebung auf Basis der Bausteine Identität und Zugriffskontrolle, Netzwerksegmentierung, Gerätesicherheit und richtlinienbasiertem Zugriff praktisch umsetzen und evaluieren?

Am Ende soll:

**Wissenschaftliche Recherche durchgeführt**

* Aktueller Stand der Forschung zu Zero Trust (ZTN)
* Vergleich mit traditionellen Sicherheitsarchitekturen (Perimeter-Modell)
* Identifikation etablierter Konzepte & Best Practices

**Geeignete Umsetzungsmethoden für ZTN-Bausteine ausgewählt**

* Basierend auf Literatur & technischen Anforderungen
* Entscheidungsbegründung für Tools / Methoden (z. B. Fortinet ZTNA, VLANs, Authentifizierungsmechanismen)

**Testumgebung konzipiert und implementiert**

* Realistische, kontrollierte Umgebung für Experimente
* Alle ZTN-Bausteine umgesetzt:
  + Identität & Zugriff
  + Netzwerksegmentierung
  + Gerätesicherheit
  + Richtlinienbasierter Zugriff

**Durchführung gezielter Sicherheitstests**

* Prüfung der Sicherheitsmechanismen durch definierte Bedrohungsszenarien
* Analyse des Systemverhaltens unter verschiedenen Bedingungen (z. B. falsche Rolle, unbekanntes Gerät)

**Vergleich mit klassischem Perimeter-Modell**

* Gegenüberstellung von Vorteilen, Nachteilen & Sicherheitsniveau
* Diskussion: Wo funktioniert ZT besser? Wo sind Grenzen?

**Dokumentation der Umsetzung**

* Schritt-für-Schritt-Dokumentation der technischen Umsetzung
* Screenshots, Konfigurationen, Testprotokolle etc.

**Kritische Reflexion**

* Was war schwieriger als gedacht?
* Was hat besonders gut funktioniert?
* Was würdest du beim nächsten Mal anders machen?