

# □ Typische Fragestellungen aus der Praxis

Die dargestellten Beispiele stehen stellvertretend für eine Vielzahl ähnlicher Situationen, in denen bestehende Systeme analysiert, strukturiert und weiterentwickelt werden.

## □ PRAXISBEISPIEL 1

### PKI in gewachsener Active Directory Umgebung

#### Ausgangssituation

In einer bestehenden Microsoft Active Directory Umgebung sollte eine Public Key Infrastructure (PKI) eingeführt werden, um Zertifikats-basierte Authentifizierung und Verschlüsselung unternehmensweit zu etablieren.

Die Herausforderung bestand in:

- historisch gewachsenen Strukturen
  - uneinheitlichen Sicherheitsrichtlinien
  - fehlender Übersicht über bestehende Abhängigkeiten
-

## Fragestellung

Wie lässt sich eine PKI so integrieren, dass sie:

- bestehende Systeme nicht destabilisiert
  - zukünftige Anforderungen (z. B. MFA, Geräteauthentifizierung) unterstützt
  - langfristig wartbar bleibt
- 

## Vorgehen

- Analyse der bestehenden AD- und Sicherheitsstruktur
  - Definition einer mehrstufigen PKI-Architektur (Offline Root / Issuing CA)
  - Abstimmung von Zertifikatstemplates und GPOs
  - Berücksichtigung von Backup-, Recovery- und Lifecycle-Prozessen
- 

## Ergebnis

- stabile und nachvollziehbare PKI-Struktur
  - Integration in bestehende Authentifizierungsprozesse
  - Grundlage für zukünftige Security- und Identity-Themen
- 

## □ PRAXISBEISPIEL 2

# Kerberos / SPN Konflikte in komplexer Web-Infrastruktur

## Ausgangssituation

Mehrere geschäftskritische Webanwendungen konnten plötzlich keine Kerberos-basierte Authentifizierung mehr durchführen.

Betroffen waren insbesondere:

- Anwendungen mit Delegation
  - Services mit eigenen Service Principal Names (SPN)
  - mehrere parallel betriebene Systeme auf identischen Servern
- 

## Fragestellung

Wie lassen sich Authentifizierungsprobleme analysieren und beheben, ohne den laufenden Betrieb zu gefährden?

---

## Vorgehen

- Analyse der bestehenden SPN-Struktur
- Identifikation von Konflikten und Überschreibungen
- Bewertung der Auswirkungen auf Delegation und Authentifizierung
- gezielte Bereinigung und Neustrukturierung der SPNs

---

## Ergebnis

- sofortige Wiederherstellung der Authentifizierungsfunktion
  - saubere und nachvollziehbare SPN-Struktur
  - reduzierte Fehleranfälligkeit bei zukünftigen Änderungen
- 

## □ PRAXISBEISPIEL 3

# RADIUS / NPS Architektur für zentrale Authentifizierung

## Ausgangssituation

Ein Unternehmen benötigte eine zentrale Lösung für die Authentifizierung von:

- WLAN-Zugängen
- VPN-Verbindungen
- Netzwerkkomponenten

Die bestehende Infrastruktur war fragmentiert und schwer wartbar.

---

## Fragestellung

Wie kann eine skalierbare und sichere Authentifizierungsarchitektur aufgebaut werden, die:

- zentral verwaltet werden kann
  - Active Directory integriert
  - zukünftige Anforderungen (z. B. MFA) unterstützt
- 

## Vorgehen

- Design einer zentralen RADIUS-Architektur (FreeRADIUS / NPS)
  - Integration in Active Directory
  - Definition von Policies und Zugriffskonzepten
  - Berücksichtigung von Redundanz und Skalierung
- 

## Ergebnis

- zentrale und konsistente Authentifizierungsstruktur
  - deutlich vereinfachte Administration
  - Grundlage für Erweiterungen wie MFA und Zero Trust
-

## □ OPTIONALER ABSCHLUSS

### Typische Fragestellungen aus der Praxis

Die dargestellten Beispiele stehen stellvertretend für eine Vielzahl ähnlicher Situationen, in denen bestehende Systeme analysiert, strukturiert und weiterentwickelt werden.