

Angriffe auf Netzwerke stellen eine ernstzunehmende Bedrohung für IT Netzwerke und damit das ganze Unternehmen dar. Systemadministratoren können ein Netzwerk nur mit fundierten Kenntnissen des "Hacking" sinnvoll schützen.

### Ihr Nutzen

Kryptografie & PKI in der Praxis – TLS/SSH/Cert-Hygiene:  
Typischen TLS-/PKI-Probleme und Security Findings: Zertifikatsketten, Trust Stores, mTLS, sichere Defaults, SSH-Härtung und professionelles Zertifikats-Lifecycle-Management. Baseline ? Hardening ? Re-Test, inklusive Incident-Runbooks

### Preis pro Teilnehmer

EUR 950,- exklusive der gesetzlichen MwSt.

### Seminardauer

1 Tag(e)/Day(s)

### Seminarinhalte

- \* TLS-Konfigurationen objektiv bewerten
  - Protokolle
  - Ciphers
  - Key Exchange
  - Chain
  - HSTS/Headers
- \* Zertifikatsketten- und Trust-Probleme debuggen
  - Intermediate
  - SAN
  - EKU/KeyUsage
  - OCSP/CRL
- \* mTLS-Grundkonzepte implementieren und SSH-Server härten
  - Key-only
  - KEX/MAC-Standards
  - Logging/Brute-Force-Schutz
- \* SSH-Server auditieren und härten
  - Key-only, KEX/MAC-Standards, Logging/Brute-Force-Schutz als Betriebskonzept
- \* Zertifikats-Lifecycle professionell betreiben
  - Issuance
  - Renewal
  - Rotation
  - Revocation
  - Monitoring
  - Notfallablauf
- \* Labs
  - TLS Baseline Scan: misconfigured Targets bewerten
  - TLS Hardening Sprint + Re-Test
  - Chain & Trust Debugging
  - mTLS Mini-Lab: Client-Cert-Auth aktivieren
  - SSH Audit & Hardening
  - Incident Drill ,Cert läuft aus
  - Mini-Report: 3–5 Findings + Hardening-Backlog + Verify Steps

\* Tools

### Voraussetzungen

TCP/IP-Basics, Windows-/Linux-Admin-Grundlagen

### Hinweise

Version: N/A

- TLS: testssl.sh, sslyze, openssl s\_client, curl, optional: nmap ssl-enum-ciphers
- PKI-Lab: OpenSSL-basierte CA oder interne Lab-CA (für Renewal/Rotation)
- ssh-audit, ssh/ssh-keygen
- Dokumentation: Evidence-/Report-Templates
- \* Output
  - TLS Hardening Checklist (Web/API/Reverse Proxy)
  - PKI Mini-Policy Template
  - Certificate Inventory & Renewal/Rotation Runbook inkl. Verify Steps + Monitoring-Minimum
  - SSH Hardening Standard inkl. Audit-/Re-Test-Profil
  - Mini-Report + priorisiertes Backlog

