

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**

Ein praxisfokussierter Deep-Dive in die häufigsten Angriffswege auf Webserver, Webanwendungen und APIs. Teilnehmer lernen, Schwachstellen nachzuweisen, technische Ursachen zu verstehen und konkrete Hardening- und Fix-Maßnahmen umzusetzen.

**Preis pro Teilnehmer**

EUR 950,- exklusive der gesetzlichen MwSt.

**Seminardauer**

1 Tag(e)/Day(s)

**Seminarinhalte**

- \* Webserver-Exposure schnell bewerten
  - TLS
  - Headers
  - Admin-Interfaces
  - Patch-Status)
- \* Webapp-/API-Tests strukturiert durchführen
  - AuthN/AuthZ
  - Sessions
  - Input Validation)
- \* Findings dokumentieren
  - Dev/Owner Problembehebung
- \* Labs
  - Webserver-Härtung: Vorher/Nachher-Verify (TLS/Headers/Config
  - Proxy-basierte Analyse eines Auth-Flows + Autorisierungs-Testfälle (IDOR/Role-Checks)
  - Injection-Grundmuster (inkl. SQLi-Konzeptblock) und sichere Verifikation
- \* Tools
  - Burp Suite Community, OWASP ZAP, nuclei/nikto
- \* Output
  - Web Security Checklist und Mini-Report
  - Fix/Verify - Testfälle pro Finding

**Voraussetzungen**

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

**Hinweise**

Version: N/A

