

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

Praxisorientierte Überprüfung von WLAN-Umgebungen und Bluetooth mit Fokus auf Unternehmensrisiken: Konfiguration, Client-Verhalten, Rogue-AP-Szenarien und Hardening

### Voraussetzungen

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

### Preis pro Teilnehmer

EUR 950,- exklusive der gesetzlichen MwSt.

### Hinweise

### Seminardauer

1 Tag(e)/Day(s)

Version: N/A

### Seminarinhalte

- \* WLAN-Sicherheitsniveau objektiv bewerten
  - WPA2/3
  - Enterprise/802.1X
  
- \* Rogue-/Evil-Twin-Risiken verstehen und Detection/Prevention ableiten
  
- \* Hardening-Plan erstellen
  - RADIUS
  - Zertifikate
  - Client Policies
  - Monitoring
  
- \* Labs
  - WLAN-Baseline-Assessment im isolierten Lab
  - Rogue-AP-Szenario als Risiko-Demonstration + Erkennungs-/Abwehrmaßnahmen
  - Hardening + Re-Test
  
- \* Tools
  - aircrack-ng Suite
  - Wireshark
  - ergänzende WLAN-Audit-Tools
  
- \* Output
  - WLAN-Hardening-Backlog
  - Prüfcheckliste für wiederholbare Audits

