>> IT Security

Hacking: Mobile Endpoint & MDM Security

EGOS! the education company

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

Dieses Modul zeigt, wie mobile Risiken in Unternehmen geprüft und reduziert werden können. Der Fokus liegt auf MDM-Baselines, Identitäts-/Zugriffspfade, VPN/WiFi Policies und API-/Traffic-Transparenz.

Voraussetzungen

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

Preis pro Teilnehmer

EUR 950,- exklusive der gesetzlichen MwSt.

Seminardauer

1 Tag(e)/Day(s)

Hinweise

Version: N/A

Seminarinhalte

* MDM-/Compliance-Baselines definieren und bewerten
- Verschlüsselung
- Passcode
- OS-Level
- Jailbreak/Root
- App Policies

* Mobile-to-Internal Access Paths prüfen
- VPN
- Zertifikate
- Conditional Access
- Split-Tunnel-Risiken

* App-/Endpoint-Traffic nachvollziehen
- Shadow-APIs
- unsichere Endpoints
- Fehlkonfigurationen sichtbar machen

* Mobile Hardening & Verification Runbook erstellen

* Labs
- MDM Baseline Review: Beispiel-Policy gegen Checkliste
- Access Path Validation: VPN/Zertifikate/Conditional Access
- Traffic Observation & API Inventory (proxy-gestützt)
- Hardening + Re-Test
- Mini-Report

* Tools
- Burp Suite Community oder OWASP ZAP
- Wireshark
- Emulator/Testgerät (z.B. Android Emulator + adb)
- Dokumentations-Templates

* Output
- MDM Baseline Checklist + priorisiertes Policy-Gap-Backlog
- Mobile Access Path Testkatalog (VPN/WiFi/Cert/Conditional Access)
- API/Endpoint Exposure Inventory
- Mini-Report + Re-Test-Runbook