>> IT Security

Hacking: IoT/OT Security Assessment

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

IoT/OT Security Assessment – Exposure & Hardening
Dieses Modul vermittelt eine praxistaugliche Vorgehensweise, um IoT-/OT-nahe Umgebungen zu inventarisieren, Exposures zu erkennen, Segmentierung zu validieren und daraus einen Hardening- und Monitoring-Plan abzuleiten. Fokus liegt auf passiven/low-impact Methoden, reproduzierbaren Testfällen und „Fix & Verify“-Nachweisen.

Preis pro Teilnehmer

EUR 950,- exklusive der gesetzlichen MwSt.

Seminardauer

1 Tag(e)/Day(s)

Seminarinhalte

* IoT/OT-Assets inventarisieren und ein Exposure-/Kritikalitätsprofil erstellen
- Owner
- Zweck
- Risiko
- Lifecycle

* Segmentierung/Zonen (IT?OT?Vendor) validieren
- allowed/blocked paths

* Typische Risiken identifizieren
- offene Management-Interfaces
- unsichere Remote-Zugänge
- schwache/Shared Credentials
- fehlende Auth/TLS
- Legacy-Protokolle

* Sichere Testmethodik anwenden
- passiv vor aktiv
- safe scanning
- Change Windows
- Do no harm
- Maßnahmen so formulieren, dass Betrieb/OT sie umsetzen kann (Priorität, Aufwand, Verify Step)
- Monitoring-/Detection-Anforderungen definieren (was muss sichtbar sein?)

* Labs
- Passive Baseline: Traffic/Flows erfassen, Kommunikationsmatrix erstellen
- Safe Discovery & Service-Mapping (aktive Discovery, Management-Interfaces, Exposures)
- Protokoll-/Service-Exposure Check (read-only): Auth/TLS/Role-Konzept bewerten
- Segmentierung & Remote Access: Zonen/Conduits, Jump-Host-/Vendor-Access-Validierung
- Hardening Sprint + Re-Test
- Monitoring-Minimum: Logging-/Sensorik-Anforderungen ableiten
- Mini-Report: 3–5 Findings inkl. Impact (Availability/Safety), Root Cause, Fix, Verify Step

* Tools
- Kali Linux: nmap (safe Profile)
- Zeek oder Suricata (als Sensor)

Voraussetzungen

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

Hinweise

Version: N/A

* Output
- IoT/OT Asset-Inventory Template
- Zonen-/Segmentierungs-Matrix + Testfallkatalog
- priorisiertes Hardening-Backlog inkl. Verify Steps
- Monitoring-Minimum-Standard
- Mini-Report als Vorlage für interne OT/IoT-Assessments