NT300 Design & Implementierung von sicheren Unternehmensnetzen

Kurzbeschreibung:

Teilnehmer erhalten einen praxisorientierten Einstieg in moderne Netzwerksicherheit. Der Workshop vermittelt Architektur und Topologien moderner Netzwerke sowie Basiselemente für sichere Netze im Kontext von Entwicklungen wie Zero-Trust, Next-Generation Firewalling, hybriden Cloud-/Multi-Cloud-Umgebungen, Containern, integrierten SDN, CDN und SIEM-Systemen.

Zielgruppe:

Der Kurs **NT300 Design & Implementierung von sicheren Unternehmensnetzen** richtet sich an:

- Systemadministratoren
- Netzwerkadministratoren
- Internet- bzw. Intranetadministratoren
- Entscheidungsträger der IT-Sicherheit

Voraussetzungen:

Um dem Lerntempo und den Inhalten des Workshops **NT300 Design & Implementierung von sicheren Unternehmensnetzen** gut folgen zu können, sind allgemeine IT-Kenntnisse, sowie Grundlagen zu Netzwerkprotokollen TCP/IP (Transmission Control Protocol/Internet Protocol) nötig.

Empfohlen wird die vorherige Teilnahme am Workshop **SC100 Grundlagen Cyber Security**.

Sonstiges:

Dauer: 5 Tage

Preis: 2490 Euro plus Mwst.

Ziele:

In diesem Kurs bauen Sie sich essenzielles Grundwissen im Bereich Netzwerksicherheit auf, so dass Sie in der Lage sind, eine Sicherheitsstrategie zu definieren, die Ihr Unternehmensnetzwerk schützt und gleichzeitig genügend Leistung und Benutzerfreundlichkeit ermöglicht.
Dabei lernen Sie nicht nur klassische Grundlagen, sondern auch moderne Konzepte wie Zero Trust, Next-Generation Firewalling, Container-Sicherheit, hybride Cloud-Sicherheit, SDN/CDN-Architekturen und den Einsatz von SIEM/Log-Monitoring für Echtzeit-Erkennung kennen.

Inhalte/Agenda:

- ♦ **Wichtige Definitionen und Begriffsklärungen**

- ♦ **Wiederholung Netzwerkgrundlagen**

- ♦ **Gefährdungspotentiale von Netzwerken**
- ♦ ◊ Portscaning, Sniffing, Session Hijacking, Spoofing
  ◊ Standardexploits, Bufferoverflows
  ◊ "Denial of Service" Angriffe
  ◊ Man-in-the-Middle Angriffe
  ◊ Neue Bedrohungsszenarien: Angriffe auf Container-Umgebungen (Docker/Kubernetes), Angriffe via Cloud-APIs, Angriffe auf CDN und SDN-Infrastrukturen

- ♦ **Grundelemente für sichere Netze**
- ♦ ◊ Paketfilter / Stateful Firewalls
  ◊ Bridging Firewalls
  ◊ Proxydienste
  ◊ Virtual Private Networks (VPN)
  ◊ Intrusion Detection
  ◊ Systemdiagnosetools
  ◊ Exfiltration
  ◊ Next-Generation Firewalls (NGFW) mit Application Layer Security und Threat Intelligence
  ◊ Network Behavior Anomaly Detection (NBAD) als Ergänzung zur klassischen IDS/IPS
  ◊ Zero-Trust-Architekturansätze (Microsegmentation, Identity-based Access Control)

- ♦ **Architektur und Netzwerktopologien**
- ♦ ◊ Kaskadierte Firewallsysteme
  ◊ Demilitarisierte Zonen (DMZ)
  ◊ Honeypots
  ◊ Multicloud / Hybrid Cloud / API
  ◊ Compliance und Sicherheit in hybrider Cloud- und Multi-Cloud-Umgebungen (Cloud Security Posture Management, Verschlüsselung, Datenklassifizierung)
  ◊ Software Defined Networking (SDN) und Content Delivery Networks (CDN) – Chancen und Sicherheitsimplikationen

- ♦ **Kurzeinführung Sicherheitsmanagement**
- ♦ ◊ Patch- und Vulnerability Management
  ◊ Pentesting und Red Teaming
  ◊ Grundlagen ISMS und BCMS
  ◊ Incident Response
  ◊ Implementierung von Log-Monitoring und SIEM-Systemen zur Angriffserkennung und Forensik
- ♦ ◊