NT300 Design & Implementierung von sicheren Unternehmensnetzen

Kurzbeschreibung:

Fortschrittliche Entwicklungen wie künstliche Intelligenz, Machine Learning und Analytics rücken neue Anforderungen an Netzwerke in den Vordergrund. Netzwerke müssen in der heutigen Zeit einfach, automatisiert und cloudfähig sein. Sie brauchen eine neue Intelligenz, die die komplette Kommunikation im Unternehmen steuert, vernetzt, auswertet und vor unbefugtem Zugriff schützt. Die steigende Anzahl von Endgeräten und mobil arbeitenden Mitarbeitern ist sicher zu integrieren und zu verwalten. Für die IT-Security von Unternehmen spielt Netzwerksicherheit eine entscheidende Rolle, weil sie wertvolle Daten und sensible Informationen vor Cyberangriffen schützt und dafür sorgt, dass das Netzwerk funktionsfähig und vertrauenswürdig ist.

Der Workshop **NT300 Design & Implementierung von sicheren Unternehmensnetzen** ist ein praxisorientierter Einstieg in das Thema IT-Security. Neben der Wiederholung von Netzwerkgrundlagen lernen Sie Gefährdungspotenziale von Netzwerken und Grundelemente für sichere Netze kennen. Es werden Architektur und Topologien von Netzwerken behandelt und Sie erhalten eine kurze Einführung in das Thema Sicherheitsmanagement.

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.

Zu empfehlen ist 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.

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

- ♦ **Grundelemente für sichere Netze**
  - ◊ Paketfilter / Stateful Firewalls
  - ◊ Bridging Firewalls
  - ◊ Proxydienste
  - ◊ Virtual Private Networks (VPN)
  - ◊ Intrusion Detection
  - ◊ Systemdiagnosetools
  - ◊ Exfiltration

- ♦ **Architektur und Netzwerktopologien**
  - ◊ Kaskadierte Firewallsysteme
  - ◊ Demilitarisierte Zonen (DMZ)
  - ◊ Honeypots
  - ◊ Multicloud / Hybrid Cloud / API

- ♦ **Kurzeinführung Sicherheitsmanagement**
  - ◊ Patch- und Vulnerability Management
  - ◊ Pentesting und Red Teaming
  - ◊ Grundlagen ISMS und BCMS
  - ◊ Incident Response

- ♦ ◊