3780 IT-Security Professional Komplettausbildung

Warum Sie diesen Kurs besuchen sollen:

- Sie erhalten einen Gesamtüberblick über alle Bereiche der IT-Security.
- Sie lernen Security Policies für Ihr Unternehmen aufzustellen.
- Bei dieser Ausbildung stehen die Praxisgerechten Übungen im Vordergrund.
- Die Ausbildung schließen Sie mit einer theoretischen und praktischen Prüfung ab.
- Anhand eines fiktiven mittelständischen Unternehmens erlernen Sie:
  - gesetzliche IT-Vorschriften im Bereich Sicherheit
  - sicherheitsrelevante IT-Prozesse zu erkennen
  - Maßnahmen zur Risikovermeidung und Risikominimierung
  - Techniken zur laufenden Sicherheitskontrolle

Die Inhalte:

Security Management (48 TE)
In diesem Teil lernen Sie die organisatorischen Grundlagen für einen sicheren IT Betrieb. Dies umfasst die Planung, die Konzeptionierung, eine Übersicht über die Normen und Standards sowie die Übersicht über die geltenden Gesetze

- Compliance – Überblick (Datenschutzgesetz, österreichisches Sicherheitshandbuch)
- IT-Sicherungsprozesse erkennen und optimieren (Business-Continuity)
- Risiko-Management
- Sicherheitsbewusstsein und Schulung
- IT-Dokumentation (Projekthandbuch, Betriebshandbuch, Notfallhandbuch)
- Benchmarks zur laufenden Sicherheitsüberwachung erstellen
- 2700x, Cobit, ITIL
- Recht (Urheberrecht, Signaturgesetze, Telekommunikationsgesetz)

Netzwerksicherheit (16 TE)
In diesem praktischen Teil bauen Sie die jeweiligen Lösungen auf und testen dies mit diversen Tools auf Sicherheit.

- Netzwerkgeräte und deren Sicherheitsfunktionen (Kabel, Firewalls, Router, Switches usw.)
- Sicherheitsrichtlinien für Netzwerkgeräte (VLAN, 802.1x, Loop-Protection, Protokoll-Analysen)
- IPv4 und IPv6 Sicherheit
- Netzwerkprotokolle und Ports (IPSec, SSH, http, HTTPS, SNMP usw.)
- Positionierung von Netzwerkgeräten
- Drahtlose Netzwerke

Anwendungs- und Informationssicherheit (28 TE)

- Betriebssystemsicherheit (Hardening, Patch-Management)
- Anwendungssicherheit (Hardening, Patch-Management, Wiederherstellung nach Ausfall usw.)
- E-Mail-Sicherheit (Spamfilter, Inhaltsfilter, digitale Signaturen)
- VPN-Zugriffe
- Cloud-Services im Unternehmen

- Mobile Geräte (inkl. Bring Your Own Device)
- Datenablage (Verschlüsselung, vermeiden von Datenverlust)
- Authentifizierung und Identifizierung
- Authentifizierungsverfahren (Radius, Kerberos, LDAP, TACACS, Smart-Card, Biometrie usw.)
- Sicherheitskontrollen bei der Durchführung der Benutzerverwaltung (Kennwortrichtlinien, Gruppen-Privilegien)
- Kryptografie (Transportverschlüsselung, Hashing, digitale Signaturen, Unleugbarkeit, PKI, öffentlicher und privater Schlüssel, Trust-Modelle usw.)
-

Bedrohungen und Schwachstellen (16 TE)

- Klassifizierung von Schadsoftware (Virus, Würmer, Trojaner, Rootkits usw.)
- Unterschiedliche Angriffsarten (DDoS, Phishing, Man-in-the-middle usw.)
- Social Engineering Angriffe
- WLAN-Angriffe (Evil Twin, Bluejacking usw.)
- Anwendungsbasierte Angriffe (SQL-Injection, Zero-Day-Exploits, Session-Hijacking usw.)
- Schwachstellenabwehr (physikalische Sicherheit, Hardening, Port-Sicherheit, IDS, IPS)
- Instrumente zur Aufdeckung von Sicherheitsbedrohungen (Protokoll Analyzer, Sniffer, Port-Scanner, Code-Review)

Die Teilnehmer:

IT-Administratoren, IT-Consulter, IT-Leiter, IT-Mitarbeiter bzw. Personen, die im Sicherheitsbereich arbeiten

Voraussetzung:

- Gute Netzwerk- und Betriebssystemkenntnisse

Weitere Ausbildungen:

- 3923 ITIL Foundation v3
- 3925 Management von IT-Projekten
- 3926 Geprüfter Datenschutzbeauftragter
- 3941 Management in Information and Business Technologies, MAS