SC110 CompTIA Security+

Kurzbeschreibung:

In der 5-tägigen Schulung **SC110 CompTIA Security+** lernen Sie die grundlegenden Kenntnisse im Bereich der IT-Sicherheit und erhalten eine herstellerneutrale Zertifizierung von CompTIA. Der inhaltliche Schwerpunkt liegt auf generellen Sicherheitskonzepten für Zugangskontrolle, Authentifizierung und Abwehr externer Angriffe. Sie werden in diesem Workshop auch Sicherheitsaspekte für Kommunikation und Infrastruktur kennenlernen sowie die Grundlagen der Verschlüsselung, die für die erfolgreiche Absolvierung des Exams erforderlich sind. Diese Zertifizierung richtet sich an IT-Profis, die ihre Fähigkeiten offiziell bestätigen lassen möchten oder grundlegende Kenntnisse im Bereich IT-Sicherheit erwerben wollen.

Kurssprache: Wahlweise Deutsch oder Englisch
Kursunterlagen: Englisch
Prüfungssprache: Englisch

Zielgruppe:

Die Schulung **SC110 CompTIA Security+** richtet sich sowohl an System- und Netzwerkadministratoren, als auch an IT-Sicherheitsverantwortliche in einem Unternehmen.

Voraussetzungen:

Es werden folgende Vorkenntnisse empfohlen:

- zwei Jahre Erfahrung in der IT Administration mit Schwerpunkt Security
- Verständnis von Betriebssystemen und Kenntnisse von Windows-basierten Systemen wie Windows 7 oder Windows 8.1
- Fähigkeit, grundlegende Netzwerkkomponenten und ihre Rollen zu identifizieren, einschließlich Routern, Switches, Firewalls und Serverrollen. Erfahrungen in der Konfiguration von Firewalls sind vorteilhaft.
- Grundverständnis von drahtlosen Netzwerken
- Grundverständnis des OSI Modells und TCP/IP einschließlich IPv4 Subnetting

Sonstiges:

Dauer: 5 Tage

Preis: 3050 Euro plus Mwst.

Ziele:

- Bewerten Sie den Sicherheitsstatus einer Unternehmensumgebung und empfehlen und implementieren Sie geeignete Sicherheitslösungen
- Überwachen und sichern Sie hybride Umgebungen, einschließlich Cloud, Mobile und IoT
- Arbeiten Sie mit einem Bewusstsein für geltende Gesetze und Richtlinien, einschließlich der Grundsätze der Governance, des Risikos und der Compliance
- Identifizieren, Analysieren und Reagieren auf Sicherheitsereignisse und -vorfälle

Die CompTIA Security+ Zertifizierungsprüfung besteht aus maximal 90 Fragen, die in 90 Minuten beantwortet werden müssen. Sie brauchen ein Ergebnis von mindestens 750 Punkten (auf einer Skala von 100-900), um die Prüfung zu bestehen.

Die Prüfung können Sie in einem Pearson VUE Testzentrum oder online ablegen.

Inhalte/Agenda:

- ♦ **Allgemeine Sicherheitskonzepte**
  - ♦ ◊ Verschiedene Arten von Sicherheitskontrollen
    ◊ Grundlegende Sicherheitskonzepte
    ◊ Bedeutung von Change-Management-Prozessen und deren Einfluss auf die Sicherheit
    ◊ Bedeutung des Einsatzes geeigneter kryptografischer Lösungen
- ♦ ◊
- ♦ **Bedrohungen, Schwachstellen und Gegenmaßnahmen**
  - ♦ ◊ Gängige Angreifertypen und deren Motive
    ◊ Gängige Threat Vectors und Attack Surfaces
    ◊ Verschiedene Arten von Schwachstellen
    ◊ Analyse von Indikatoren für bösartige Aktivitäten
    ◊ Zweck von Gegenmaßnahmen zur Absicherung der Unternehmensumgebung
- ♦ ◊
- ♦ **Sicherheitsarchitektur**
  - ♦ ◊ Auswirkungen verschiedener Architekturmodelle auf die Sicherheit
    ◊ Anwendung von Sicherheitsprinzipien zur Absicherung der Unternehmensinfrastruktur
    ◊ Konzepte und Strategien zum Schutz von Daten
    ◊ Bedeutung von Resilienz und Wiederherstellung in der Sicherheitsarchitektur
- ♦ ◊
- ♦ **Operative IT-Sicherheit**
  - ♦ ◊ Einsatz gängiger Sicherheitstechniken für IT-Ressourcen
    ◊ Sicherheitsauswirkungen einer ordnungsgemäßen Verwaltung von Hardware-, Software- und Daten-Assets
    ◊ Verschiedene Aktivitäten im Rahmen des Schwachstellenmanagements
    ◊ Konzepte und Tools für Security-Alerting und -Monitoring
    ◊ Anpassung der Unternehmensumgebung zur Verbesserung der Sicherheit
    ◊ Implementierung und Betrieb von Identity and Access Management (IAM)
    ◊ Bedeutung von Automatisierung und Orchestrierung für einen sicheren IT-Betrieb
    ◊ Angemessene Incident-Response-Maßnahmen
    ◊ Nutzung von Datenquellen zur Unterstützung von Untersuchungen
- ♦ ◊
- ♦ **Management und Überwachung von Sicherheitsprogrammen**
  - ♦ ◊ Elemente einer effektiven Security Governance
    ◊ Elemente des Risikomanagement-Prozesses
    ◊ Prozesse im Zusammenhang mit der Risikobewertung und dem Risikomanagement von Drittanbietern
    ◊ Elemente einer effektiven Security Compliance
    ◊ Arten und Zwecke von Audits und Assessments
    ◊ Implementierung von Security-Awareness-Maßnahmen
  - ♦ ◊