SC110 CompTIA Security+

Kurzbeschreibung:

Teilnehmende erhalten eine praxisnahe Einführung in die Grundlagen der Informationssicherheit nach international anerkanntem Standard. Vermittelt werden Methoden zur Absicherung von Netzwerken, Anwendungen und Endgeräten mit Fokus auf Vertraulichkeit, Integrität und Verfügbarkeit. Behandelt werden Bedrohungserkennung, Authentifizierung, Zugriffskontrolle sowie Reaktion und Verschlüsselungstechniken.

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: 2590 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 (12%)**
  - ♦ ◊ **Sicherheitskontrollen:** Vergleich von technischen, präventiven, administrativen, abschreckenden, operativen, detektiven, physischen, korrektiven, kompensierenden und direktiven Kontrollen.
  - ◊ **Grundlegende Konzepte:** Zusammenfassung von Vertraulichkeit, Integrität und Verfügbarkeit (CIA); Nichtabstreitbarkeit; Authentifizierung, Autorisierung und Abrechnung (AAA); Zero Trust; sowie Täuschungs- und Disruptionstechnologien.
  - ◊ **Änderungsmanagement**: Erläuterung von Geschäftsprozessen, technischen Auswirkungen, Dokumentation und Versionskontrolle.
  - ◊ **Kryptografische Lösungen:** Einsatz von Public Key Infrastructure (PKI), Verschlüsselung, Verschleierung, Hashing, digitalen Signaturen und Blockchain.
- ♦ ◊
- ♦ **Bedrohungen, Schwachstellen und Gegenmaßnahmen (22%)**
  - ♦ ◊ **Bedrohungsakteure und Motivationen:** Vergleich von Nationalstaaten, unqualifizierten Angreifern, Hacktivisten, internen Bedrohungen, organisierter Kriminalität, Shadow IT und Motivationen wie Datenexfiltration, Spionage und finanzieller Gewinn.
  - ◊ **Bedrohungsvektoren und Angriffsflächen:** Erläuterung von nachrichtenbasierten, unsicheren Netzwerken, Social Engineering, dateibasierten, Sprachanruf-, Lieferketten- und softwarebezogenen Schwachstellenvektoren.
  - ◊ **Schwachstellen:** Erläuterung von Schwachstellen in Anwendungen, Hardware, mobilen Geräten, Virtualisierung, Betriebssystemen (OS), Cloud-spezifischen Umgebungen, webbasierten Anwendungen und in der Lieferkette.
  - ◊ **Bösartige Aktivitäten:** Analyse von Malware-Angriffen, Passwortangriffen, Anwendungsangriffen, physischen Angriffen, Netzwerkangriffen und kryptografischen Angriffen.
  - ◊ **Abwehrtechniken:** Einsatz von Segmentierung, Zugriffskontrolle, Konfigurationsdurchsetzung, Härtung, Isolierung und Patch-Management.
- ♦ ◊
- ♦ **Sicherheitsarchitektur (18%)**
  - ♦ ◊ **Architekturmodelle:** Vergleich von On-Premises, Cloud, Virtualisierung, Internet of Things (IoT), Industrial Control Systems (ICS) und Infrastructure as Code (IaC).
  - ◊ **Unternehmensinfrastruktur:** Anwendung von Sicherheitsprinzipien auf Infrastrukturaspekte, Kontrollauswahl und sichere Kommunikation/Zugriffe.
  - ◊ **Datenschutz:** Vergleich von Datentypen, Schutzmethoden, allgemeinen Überlegungen und Klassifizierungen.
  - ◊ **Resilienz und Wiederherstellung:** Erläuterung von Hochverfügbarkeit, Standortüberlegungen, Tests, Stromversorgung, Plattformdiversität, Backups und Aufrechterhaltung des Geschäftsbetriebs.
- ♦ ◊
- ♦ **Sicherheitsbetrieb (28 %)**
  - ♦ ◊ **Rechenressourcen:** Anwendung von sicheren Baselines, mobilen Lösungen, Härtung, WLAN-Sicherheit, Anwendungssicherheit, Sandboxing und Monitoring.
  - ◊ **Asset-Management:** Erläuterung von Beschaffung, Entsorgung, Zuweisung sowie Überwachung/Verfolgung von Hardware-, Software- und Daten-Assets.
  - ◊ **Schwachstellenmanagement:** Identifikation, Analyse, Behebung, Validierung und Berichterstattung von Schwachstellen.
  - ◊ **Alarmierung und Monitoring:** Erläuterung von Überwachungstools und Aktivitäten von Rechenressourcen.
  - ◊ **Unternehmenssicherheit:** Anpassung von Firewalls, IDS/IPS, DNS-Filterung, DLP (Data Loss Prevention), NAC (Network Access Control) und EDR/XDR (Endpoint/Extended Detection and Response).
  - ◊ **Identity and Access Management:** Implementierung von Provisioning, SSO (Single Sign-On), MFA (Multifactor Authentication) und Tools für privilegierte Zugriffe.
  - ◊ **Automatisierung und Orchestrierung:** Erläuterung von Automatisierungsanwendungsfällen, Vorteilen von Skripten und Überlegungen.
  - ◊ **Incident Response:** Umsetzung von Prozessen, Schulung, Tests, Ursachenanalyse, Threat Hunting und digitaler Forensik.
  - ◊ **Datenquellen:** Nutzung von Protokolldaten und anderen Quellen zur Unterstützung von Untersuchungen.
- ♦ ◊
- ♦ **Management und Überwachung von Sicherheitsprogrammen (20%)**
  - ♦ ◊ **Security Governance:** Zusammenfassung von Richtlinien, Policies, Standards, Verfahren, externen Einflüssen, Monitoring, Governance-Strukturen sowie Rollen und Verantwortlichkeiten.
  - ◊ **Risikomanagement:** Erläuterung von Risikoidentifikation, -bewertung, -analyse, Risikoregister, Toleranz, Risikoappetit, Strategien, Reporting und Business Impact Analysis (BIA).
  - ◊ **Drittparteirisiken:** Verwaltung von Anbieterbewertung, -auswahl, -vereinbarungen, Monitoring, Fragebögen und Rules of Engagement.
  - ◊

◊ **Security Compliance:** Zusammenfassung von Compliance-Reporting, Konsequenzen bei Nichteinhaltung, Monitoring und Datenschutz.
◊ **Audits und Assessments:** Erläuterung von Attestierung, internen/externen Audits und Penetrationstests.
◊ **Security Awareness:** Umsetzung von Phishing-Trainings, Erkennung anomalen Verhaltens, Benutzeranleitungen, Meldung und Überwachung.

◊