SC210 ISC2 CISSP Vorbereitung

Kurzbeschreibung:

In dem CISSP-Kurs erhalten die Teilnehmer umfassende Kenntnisse und Fähigkeiten, die für die strategische und technische Umsetzung der Informationssicherheit notwendig sind. Gleichzeitig werden sie auf die Prüfung zur ISC2 Zertifizierung des CISSP vorbereitet. In unserem intensiven 5-tägigen Kurs werden die Inhalte der acht Domains des „Common Body of Knowledge“ (CBK) vermittelt. Der CBK stellt ein Kompendium dar, welches bewährte Sicherheitsmethoden (Best Practices), Technologien, Theorien, Modelle und Konzepte bündelt.

Der CISSP ist die erste Zertifizierung die durch ANSI als ISO-Standard 17024:2003 im Bereich Information Security akkreditiert wurde und bietet nicht nur eine objektive Bewertung der Kompetenz, sondern auch einen global anerkannten Leistungsstandard. Der Lehrstoff wird praxisnah, konkret und verständlich anhand von Beispielen an Whiteboard und Flipchart präsentiert.

Begleitend zum Kurs werden die Bücher “ISC2 CISSP Official Study Guide“ und "CISSP Official Practice Tests" kostenfrei bereitgestellt.

Zielgruppe:

An diesem Workshop kann jeder teilnehmen, der sich auf das Examen zum CISSP vorbereiten möchte. Die CISSP-Zertifizierung richtet sich jedoch vornehmlich an technisch versierte und erfahrene Spezialisten, die ihr in Studium, Ausbildung und Job erworbenes Wissen um IT-Sicherheit festigen und erweitern wollen.
Ein solides Verständnis der üblichen Sicherheits-Mechanismen und mehrjährige Erfahrung mit generellen Prinzipien der IT in mindestens zwei Bereichen der folgenden Domains ist empfehlenswert.

Der Workshop richtet sich an folgende Zielgruppen:

- Sicherheitsberater
- Information Security Manager
- Sicherheitsbeauftragte
- Security Engineers
- Netzwerkarchitekten
- Erfahrene IT-Mitarbeiter

Voraussetzungen:

Grundlegend kann jeder an IT-Sicherheit, Informationstechnik und IT-Prozessen interessierte die CISSP-Zertifizierung anstreben, um seine Kenntnisse auf international anerkannter Ebene zu validieren. Um jedoch den großen Umfang des CBK sinnvoll binnen einer Woche zu vermitteln, sind Kenntnisse in mehreren Bereichen der IT von Vorteil. Die Bereitschaft, sich über den Kurs hinaus mit den Inhalten – etwa in Form von vertiefenden Online- Fragebögen zu befassen – ist unbedingt erforderlich.

Obwohl die Teilnahme an der Prüfung keine Schulung oder kein Studium voraussetzt, ist nach erfolgreicher Prüfung für die Erlangung des Zertifikates der Nachweis von mindestens fünf Jahren relevanter Berufserfahrung in mindestens zwei der CBK-Themenbereiche zwingend erforderlich (oder 4 Jahre Erfahrung plus relevanter Hochschulabschluss). Der Nachweis der o.g. einschlägigen Berufserfahrung ist durch ein „Endorsement“ durch einen CISSP (z.B. durch den Trainer) notwendig, um anschließend das Zertifikat beim ISC2 zu beantragen.

Sonstiges:

Dauer: 5 Tage

Preis: 3450 Euro plus Mwst.

Ziele:

Die acht Domains des Common Body of Knowledge (CBK) werden als „a mile wide and an inch thick“ bezeichnet. Eine intensive Vorbereitung auf die Inhalte und den Ablauf der Prüfung zum CISSP (Certified Information Systems Security Professional) incl. der Durchsprache aller relevanter Themenbereiche bedeutet, dass den Teilnehmern in schneller Folge eine große Bandbreite an technischem Knowhow, Prozesswissen und Architekturen vermittelt werden.
Besonderes Augenmerk wird auf die neu hinzugekommenen Themen „BYOD“, Software Defined Networks und Cloud Identity Services gelegt.

Inhalte/Agenda:

- **Domain 1 - Security and Risk Management**
  - ◊ Sicherheitsanforderungen
  - ◊ Compliance, Recht, Regulierung und Richtlinien
  - ◊ Standards und Frameworks
  - ◊ Risiko Management
  - ◊ Business Continuity

- **Domain 2 - Asset Security**
  - ◊ Sicherheitsmodelle und Frameworks
  - ◊ Schutz der Vermögenswerte
  - ◊ Klassifikation

- **Domain 3 - Security Architecture and Engineering**
  - ◊ Verständnis der Sicherheitsmodelle
  - ◊ Design und Schutzmaßnahmen
  - ◊ Kryptographie
  - ◊ Physische Sicherheit

- **Domain 4 - Communication and Network Security**
  - ◊ Topologien
  - ◊ Technologien
  - ◊ Protokolle
  - ◊ Angriffe
  - ◊ Sicherheitsmaßnahmen

- **Domain 5 - Identity and Access Management (IAM)**
  - ◊ Identitätskontrolle
  - ◊ Zugriffskontrollmodelle

- **Domain 6 - Security Assessment and Testing**
  - ◊ Planung und Durchführung von Sicherheitstests
  - ◊ Vulnerability Assessments
  - ◊ Pentests

- **Domain 7 - Security Operations**
  - ◊ Sicherer Betrieb und Wartung
  - ◊ Incidence Response
  - ◊ Disaster Recovery Planning

- **Domain 8 - Software Development Security**
  - ◊ Entwicklung sicherer Software-Anwendungen
  - ◊ Web-Anwendungen und mobile Anwendungen
  - ◊ Malware und Angriffe auf Anwendungen
  - ◊ IoT und ICS

- **Hinzu kommen ein Review und Q&A Sessions, und es werden Tipps und Lernmethoden aufgezeigt.**