SC500 Informationssicherheitsbeauftragter (ISB/CISO) mit Zertifizierung

Kurzbeschreibung:

Teilnehmer erhalten eine fundierte Einführung in die Aufgaben eines Informationssicherheitsbeauftragten (ISB) und Chief Information Security Officer (CISO). Vermittelt werden Vorgehensweisen nach ISO/IEC 27001, ISO/IEC 22301 sowie Grundlagen des BSI-Grundschutzes. Behandelt werden praxisnahe Fragestellungen im ISMS-Prozess, ergänzt durch Übungen, Diskussionen und eine Abschlussprüfung mit Zertifikat.

Zielgruppe:

- Angehende Informationssicherheitsbeauftragte
- CISO
- Verantwortliche im Bereich Informationssicherheit
- IT-Sicherheitsmanager

Voraussetzungen:

Es werden keine besonderen Vorkenntnisse verlangt.

Sonstiges:

Dauer: 5 Tage

Preis: 2950 Euro plus Mwst.

Ziele:

Der Schwerpunkt des Seminars liegt auf der praxisorientierten Vermittlung des notwendigen Wissens für den Aufbau, Betrieb und Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) sowie der Ausgestaltung der Schnittstelle zwischen Unternehmensführung und Technik.

Inhalte/Agenda:

- ♦ **Vorstellen und Kennenlernen**

♦ **Motivation, Grundlagen und Rollenanforderung**
♦ ◊ Aktuelle Beispiele
◊ Grundbegriffe der Informationssicherheit
◊ Grundbegriffe der Unternehmensführung
◊ Anforderung und Ziele an die Rolle des CISOs/ISBs

♦ **Übersicht über Normen/Standards, Zertifikate, Regulierungen und Best-Practices**
♦ ◊ Normen und Standards
◊ Personenzertifikate
◊ Praktisches Arbeiten mit den Standards

♦ **Strategische Arbeit des CISOs und ISBs**
♦ ◊ Managementsystem
(Aufbau, Implementierung, Prüfen)
◊ Unternehmensziele und Strategieabstimmung
(Lagebildes, Roadmap, Reifegraderhöhungen, Budget und Benchmarking)
◊ Kommunikation und Berichtswesen
(Stakeholder, Kennzahlen, Zusammenarbeit)
◊ Wichtige Instrumente des CISOs
(Programme, Projekte, Risiken, Entscheidungen, Sicherheitsanalysen, Awareness)

♦ **Taktische Arbeit und operativer Betrieb für den CISO und ISB**
♦ ◊ Angriffsvektoren mit grundlegender Einführung in die Forensik
◊ Wichtige Sicherheitsprotokolle
◊ Operativer IT-Sicherheitsbetrieb: Prozesse und Organisation
(Incident-Response-Prozess, Patchen, SIEM, SOC)
◊ Operativer IT-Sicherheitsbetrieb: Betriebsgegenstände und Technik

♦ **Notfallmanagement und BCM**
♦ ◊ Motive für die Einführung eines BCM-Systems
◊ BCM als Führungsaufgabe
◊ Ein BCMS einrichten, warten und pflegen
(Prozesse, BIA, Risikoanalyse, BCM-Strategien, Tests, Berichtswesen)

♦ **Regulierungen und Datenschutzarbeit des CISOs und ISBs**
♦ ◊ Sorgfaltspflicht in wichtigen Gesetzen
(KRITIS, Sicherheitsgesetz, IT-Compliance, Cloud, BYOD)
◊ Aufbau einer effizienten Zusammenarbeit mit dem Datenschutz
(Grundlagen, DSGVO, Pragmatismus)

♦ **Diskussion und Zusammenfassung**
♦ ◊ Fallstudie
◊ Vorbereitung auf die Zertifikationsprüfung

♦ ◊