SC500 Informations-Sicherheitsbeauftragter (ITSIBE/CISO) mit Zertifizierung

Kurzbeschreibung:

Dieses Seminar vermittelt fundierte Kenntnisse über die Aufgaben, die mit den Rollen eines Information Security Officers / Informationssicherheitsbeauftragten (ISBs) und Chief Information Security Officers (CISOs) verbunden sind.

Ein routinierter CISO-Praktiker präsentiert viele Praxisbeispiele und Berichte aus dem Unternehmensalltag mit umfangreichem Erfahrungsaustausch.

Die Hauptaufgabe des Informationssicherheitsbeauftragten ist die Unterstützung der Geschäftsführung bei der Wahrnehmung ihrer Pflichten zur Umsetzung von Maßnahmen zur Sicherstellung eines avisierten Informationssicherheitsniveaus bei der Risikofrüherkennung von Bedrohungen aus dem IT-Betrieb.

Neben den rein organisatorischen und strategischen Fragestellungen werden dem (angehenden) ISB/CISO die grundlegenden technischen Betriebsgegenstände und Prozesse vermittelt. Damit ist er in seiner Schnittstellenfunktion Management - Technik gut gerüstet.

Auch die Koordination von Sicherheitszielen, die Aufarbeitung des Berichtswesens und die regelmäßige Überwachung von Chancen und Risiken sind nur einige Aufgaben des Informationssicherheitsbeauftragten.

Weiterhin sollte er rechtliche Änderungen im Blick und auch den Datenschutz im Auge behalten ebenso wie die Sicherstellung der Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität.

Im Mittelpunkt des Trainings steht die Vorgehensweise nach ISO/IEC 27001, ISO/IEC 22301, erweitert um ein Grundverständnis des BSI-Grundschutzes und weiteren branchenspezifischen Standards und Regelungen.

Es wird rege über typische Fragestellungen aus der Praxis diskutiert werden, wie beispielsweise mögliche Probleme im ISMS-Prozess.

Die Inhalte werden in überschaubarer Runde in Form von Präsentationen, praktischen Übungen und Gruppendiskussionen interaktiv erarbeitet.

Das Seminar schließt am letzten Schulungstag mit einer Prüfung sowie einem Zertifikat ab.

Für die Prüfung, die am Nachmittag stattfindet, haben die Teilnehmer 90 Minuten Zeit. Es handelt sich um 45 Multiple Choice-Fragen. Um die Prüfung erfolgreich zu bestehen müssen 70 % davon richtig beantwortet werden.

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