RC350 Cloud Information Security (ISO 27017/27018)

Kurzbeschreibung:

Die Nutzung von Cloud Services ist heute aus dem unternehmerischen Alltag nicht mehr wegzudenken. Viele Firmen stellen ihren Kunden auch Cloud Services zur entgeltlichen oder unentgeltlichen Nutzung zur Verfügung. Aus Sicht der Informationssicherheit und des Datenschutzes haben beide Seiten - Nutzung und Anbieten von Cloud Service - besondere Aspekte, die berücksichtigt werden müssen.

Zwei Normen in der ISO 27000-Reihe haben sich speziell auf dieses Thema fokussiert:
- ISO/IEC 27017 adressiert sowohl die Nutzung von Cloud Lösungen als auch das Anbieten von Cloud Services
- ISO/IEC 27018 bezieht sich auf den Schutz personenbezogener Daten in öffentlichen Cloud-Lösungen

Im Kurs wird das Know-how-Fundament zum Thema Cloud Security aus der Sichtweise der Strategie (ISB, CISO, Unternehmensführung) und Taktik bzw. Betrieb (Operative Sicherheitsteams und Infrastruktur bzw. Betrieb) dargestellt. Weiterhin wird die Verantwortung im Rahmen der Cloud Security (Datenschutz, Betriebsthemen) von Kunde und Betreiber aufgezeigt.

Ein pragmatischer Überblick über mögliche Lösungsansätze bei verschiedenen Herstellern (Azure, Google Cloud, Amazon Web Services) wird exemplarisch erarbeitet.

Zielgruppe:

Informationssicherheitsbeauftragte, Geschäftsführer, Compliance-Beauftragte, Datenschutzbeauftragte.

Voraussetzungen:

Kenntnis der Funktion und des Aufbaus eines Informationssicherheits-Managementsystems nach ISO/IEC 27001, z.B. Implementierung und Foundation ISO/IEC 27001 oder Lead Auditor ISO/IEC 27001

Sonstiges:

Dauer: 3 Tage

Preis: 2100 Euro plus Mwst.

Ziele:

Die Teilnehmer erhalten einen soliden Überblick über die Möglichkeiten Cloud Services in einem ISMS zu behandeln. Sie lernen dabei den Aufbau eines sogenannten Sektor-spezifischen ISMS kennen und können dieses Wissen in ihrem Unternehmen sicher anwenden.

Die Leitfragen, die in diesem Seminar bearbeitet werden, sind:
1. Wie kann im Rahmen eines ISMS der Schutz personenbezogener Daten in einer Cloud-Lösung mit ISO/IEC 27018 behandelt werden? Welche Rolle spielen dabei Datenschutzprinzipien und die EU-Datenschutzgrundverordnung?

2. Welche Möglichkeiten bietet ISO/IEC 27017 sowohl für Unternehmen die Cloud Services nutzen wollen, als auch für Unternehmen die Cloud Services anbieten? Welche Möglichkeiten gibt es für die Vereinbarung von

Verträgen und die Steuerung von Lieferanten?

3. Gibt es Möglichkeiten der Zertifizierung? Wie kann die Zertifizierung angestrebt werden und welchen Aussagewert hat sie?

Wir vermitteln Ihnen das umfassende Wissen für die Planung, Implementierung, Überwachung und Verbesserung von Cloud Information Security. In diesem Intensivtraining erwerben die Teilnehmer fundiertes Wissen über die notwendigen Schritte bis hin zur erfolgreichen Zertifizierung.

Inhalte/Agenda:

- Motivation und Grundlagen
  - ♦ Grundbegriffe des Cloud Computing
    - ◊ Konzepte
    - ◊ Referenzarchitektur
  - ♦ Cloud Security
    - ◊ Bedrohungen und Angriffsvektoren
    - ◊ Sicherheitskonzepte
  - ♦ Cloud Dienste und Services
    - ◊ Azure
    - ◊ Google Cloud Platform (GCP)
    - ◊ AWS

- Wichtige Normen/Standards, Zertifikate und Best-Practices
  - ♦ Normen und Standards
    - ◊ ISO/IEC 27017/18
    - ◊ ISO/IEC 20000-9
    - ◊ BSI C5
    - ◊ NIST 800-144
  - ♦ Personenzertifikate
    - ◊ CSA CCSK
    - ◊ ISC2 CCSP
  - ♦ Zertifikate zu Produkten
    - ◊ Azure Security Engineer
    - ◊ Google Cloud Security Engineer
    - ◊ AWS Certified Security

- Organisatorische Anforderungen und Empfehlungen der Cloud Security
  - ♦ Management (ISMS, Security Controls, DR, BCM)
    - ◊ Planung der Implementierung
    - ◊ Ausrollen der Implementierung
    - ◊ Überprüfen und Anpassung der Implementierung
  - ♦ Management und Analyse der Risken
  - ♦ Entscheidungsfindung für Projekte und Produkte
  - ♦ Datenschutz, Vertragsgestaltung und Einkaufsprozess
  - ♦ Reporting und Berichtserstattung
  - ♦ Auditierung und Compliance
  - ♦ Nutzung von Tools aus strategischer Sicht
    - ◊ Azure: Compliance Manager
    - ◊ Google Cloud: Security Command Center
    - ◊ AWS: AWS Security Hub

- Technische Anforderungen und operationeller Betrieb der Cloud Security
  - ♦ Infrastruktur und Virtualisierung am Beispiel von Openstack, VMware, Multi-Cloud
  - ♦ Datensicherheit und -architektur
  - ♦ Betrieb und Aufbau von sicheren Cloud-Anwendungen
  - ♦ Identity and Access Management
  - ♦ Überwachen der Cloud Security (Monitoring, Vorfälle, Forensik)
  - ♦ Nutzung von Tools aus taktischer und operativer Sicht

- Diskussion und Zusammenfassung