SC440 Cyber Resilience - Incident Response für Manager

Kurzbeschreibung:

Die Bedrohungen durch Cyberkriminalität in Unternehmen nehmen kontinuierlich zu. Es kann nicht mehr nur darum gehen, Angriffe zu verhindern, sondern bestmöglich auf diese vorbereitet zu sein.

In diesem bewusst auf einen Tag konzentrierten Workshop vermitteln wir Entscheidern und Managern genau das Wissen, das sie zur professionellen Führung bei IT-Sicherheitsvorfällen unmittelbar parat haben müssen.

Es wird aufgezeigt, wie Manager IT-Sicherheitsvorfällen richtig und sicher begegnen können, indem sowohl auf präventive Handlungsempfehlungen als auch auf Verhaltensregeln im Ernstfall eingegangen wird.

Zielgruppe:

- Senior/Executive Manager
- Verantwortliche im Bereich Informationssicherheit
- Compliance-Beauftragte

Voraussetzungen:

Es sind keine spezifischen Vorkenntnisse für die Teilnahme an diesem Kurs erforderlich.

Sonstiges:

Dauer: 1 Tage

Preis: 790 Euro plus Mwst.

Ziele:

In diesem bewusst auf einen Tag konzentrierten Workshop vermitteln wir Entscheidern und Managern genau jenes Wissen, das sie bei IT-Sicherheitsvorfällen unmittelbar parat haben müssen.

Durch den Workshop erhalten Sie:

- Die Fähigkeit, Sicherheitsvorfälle besser einschätzen zu können
- Die Kompetenz, die wesentlichen erste Schritte einer Incident Response anzuführen
- Handlungsempfehlungen für den Umgang mit Versicherungen und Ermittlungsbehörden
- Überlebenswichtiges zu Compliance und Haftungsfragen

Inhalte/Agenda:

- **Einführung**
  - Kontext (Informationssicherheit, IT-Sicherheit und Datenschutz)
  - Überblick über die Cyber-Bedrohungslage
  - Grundbegriffe der Informationssicherheit
  - Einführung in Incident Response and Digital Forensics (DFIR)
    - Zielsetzung
    - Definition
    - Prinzipien

- **Ablauf eines Incident-Response-Prozesses**

- **Regulatorischer Rahmen und Haftungsfragen**
  - Anforderungen und Grenzen durch das Datenschutzrecht (DSGVO)
  - Betriebliche Mitbestimmung
  - Zivilrechtliche Meldepflichten und Meldeobliegenheiten (Versicherungen)
  - Kurz-Exkurs in das Strafrecht ("Cyber Crime")
  - KRITIS / BSIG (Kurzüberblick)
  - ISM-Rahmenwerke (Kurzüberblick)

- **Praktische Problemfelder**
  - Erkennung, Analyse und Klassifizierung von Sicherheitsvorfällen
  - Eindämmung
  - Ressourcen
  - Interne und externe Kommunikation
  - Entscheidungsbefugnisse
  - Wiederherstellung

- **Vorbereitungsmaßnahmen (Notfallmanagement und Notfallhandbücher)**