

Praxiswissen Sicherheitskonzepte und Security Policy (WSSK)

Network Security ist mehr als die Entwicklung von Sicherheitskonzepten mittels der bekannten Werkzeuge. Für die praktische Umsetzung im Unternehmen ist zusätzlich eine übergreifende Security Policy erforderlich, die klare Prioritäten setzt und das Handeln im konkreten Fall legitimiert.

Doch wie erstellt man ein solches Regelwerk? Welche Möglichkeiten und Alternativen sollte es enthalten?

Zielgruppe

IT-Sicherheitsbeauftragte und IT-Verantwortliche, die für die Erstellung und praktische Umsetzung von Sicherheitskonzepten zuständig sind.

Voraussetzungen

Grundkenntnisse in den Bereichen Netzwerktechnik und Internet sollten vorhanden sein.

Zielsetzung

Die Teilnehmer erlernen in diesem Workshop die Erstellung einer praxisorientierten und umsetzbaren Security Policy unter Berücksichtigung der organisatorischen und rechtlichen Rahmenbedingungen im Unternehmen.

Sie werden in die Lage versetzt, die Bedrohungssituation des Unternehmens in Sachen IT-Sicherheit einzuschätzen und – entsprechend dem jeweiligen Wert der betroffenen Informationen – geeignete Handlungsempfehlungen aus der definierten Security Policy abzuleiten.

Inhalt des Seminars

Standardkonforme Vorgehensweise

- IT-Strukturanalyse
- IT-Sicherheits-Check
- Schutzbedarfsfeststellung
- IT-Sicherheitskonzept
- Bewertung der Systematiken
- BSI-Grundschutzhandbuch und ISO/IEC 17799 im Vergleich

Schwachstellenanalyse als praxisorientierte Grundlage

- Social Engineering
- Internes Vulnerability Assessment
- Externes Vulnerability Assessment
- Auswertung und Einordnung der Informationen
- Datenaufbereitung für das Management

Schutzbedarfsfeststellung

- Wert der zu schützenden Informationen, Gefährdungslage, Schutzbedarf
- Risikobewertung und Operationalisierung der Daten
- Bewertung konkreter Schutzverletzungen

IT-Sicherheitskonzept

- Identifizierung defizitärer Sicherheitsbereiche
- Interpretation der Ergebnisse
- Definition der Maßnahmen
- Kosten- und Aufwandsschätzung
- Risikobewertung
- Umsetzung der Maßnahmen
- Verantwortlichkeiten
- Notfall-Handbuch

Vorgehensweisen zur Erstellung einer Security Policy

- Einordnung der Security Policy in das Sicherheitskonzept als Ganzes
- Inhalte einer Security Policy
- Abgrenzung: Security Policy vs. Sicherheitskonzept
- Schwachstellenanalyse als Grundlage
- Standardkonforme Vorgehensweisen als Grundlage
- Verträglichkeit zu Betriebsvereinbarungen und Richtlinien
- Umsetzung der Security Policy
- Systemorientierte Erstellung
- Strukturorientierte Erstellung

Aufbereitung der Informationen für das Management

- Sinn und Unsinn einer „Return on Security Investment“-Rechnung
- Kosten-Nutzen-Analyse
- Risikobewertung alternativer Bedrohungen
- Praktische Hilfen für die Umsetzung der Security Policy
- Bedeutung von KonTraG und Basel II

Sprachversionen:

WSSKd deutsch

Dauer:

2 Tage
je 9.00 – 16.30 Uhr

Preis:

1.100 € zzgl. MwSt.

Termine / Ort:

siehe beiliegende Übersicht oder
www.hicomcenter.com

