

SC320 Informationssicherheit vs Full Scope Social Engineering

Kurzbeschreibung:

Unser Class-Room-Training ermöglicht das Kennenlernen grundsätzlicher Social-Engineering-Skills und Wege, wie man Hacker, die sich derartiger Tools bedienen, abwehren kann. Dabei profitieren Sie von praktischen Erfahrungen aus echten Attacken.

Enthalten sind: Kursunterlagen, USB-Hackertool

Zielgruppe:

IT-Sec-Management, IT-Sicherheits-, Datenschutz-, Compliance-Beauftragte, Betriebsrat

Voraussetzungen:

Niveau: geübte IT-Anwender als Beginner im Social Engineering

Sonstiges:

Dauer: 2 Tage

Preis: 1700 Euro plus Mwst.

Ziele:

Ziel des Kurses ist es, Sie in die Lage zu versetzen, Ihren Informationsverbund aus der Sicht von Angreifern betrachten zu können, zugleich aber auch rechtliche Aspekte und gesetzliche Anforderungen zu identifizieren und daraus Strategien zur Verbesserung Ihrer präventiven, detektiven, reaktiven und auch prädiktiven Fähigkeiten zu entwickeln.

Inhalte/Agenda:

- ◆ Woher kommen die Gefahren, wer ist betroffen? Erstellung eines individuellen Lagebildes.
- ◆ Datenschutzrechtliche und ethische Aspekte beim Einsatz von Social Engineering
- ◆ Vorstellung von Sozialen Skills und psychologischen Tricks zur Manipulation von Verhalten
- ◆ Kennenlernen von Technologie (Phishing, Spoofing, LAN, WLAN, USB, RFID)
- ◆ Methoden zur Schwachstellenidentifizierung und zum Entwickeln von Angriffstaktiken
- ◆ Entwickeln eines individuellen Angriffsplans inkl. Training verschiedener Vorgehensweisen
- ◆ Auswertung der Übungen, Analyse der eigenen Angreifbarkeit und Abwehroptionen