SC300 Social Engineering Basics

Kurzbeschreibung:

Teilnehmer erhalten eine praxisnahe Einführung in Social Engineering und lernen, wie gängige Angriffswerkzeuge und Manipulationstechniken eingesetzt werden. Vermittelt wird der Umgang mit OSINT, psychologischer Beeinflussung sowie WLAN- und LAN-Angriffswerkzeugen. Behandelt werden zudem Angriffe über Telefon, SMS oder Social Media sowie physische Methoden wie Tailgating, Lock-Picking oder RFID-Spoofing zur Stärkung der Awareness.

Zielgruppe:

Der Kurs **SC300 Social Engineering Basics** richtet sich an:

- IT-Sec-Management
- Pentester
- Red- und Blueteamer
- CISOs

Voraussetzungen:

Um dem Lerntempo und den Inhalten des Workshops **SC300 Social Engineering Basics** gut folgen zu können, sind grundlegende bis fortgeschrittene Kenntnisse im Bereich Social Engineering empfehlenswert.

Sonstiges:

Dauer: 2 Tage

Preis: 1590 Euro plus Mwst.

Ziele:

- Vermittlung eines fundierten Überblicks über klassische und moderne Social-Engineering-Techniken
- Aufzeigen, wie psychologische Entscheidungsmechanismen die Anfälligkeit für Manipulationen beeinflussen
- Erläuterung grundlegender Prinzipien der Überzeugungs- und Einflussnahme, damit Teilnehmende Manipulationsmuster erkennen und Gegenstrategien entwickeln können
- Vorstellung nonverbaler Indikatoren (Micro-/Macroexpressions) zur besseren Einschätzung von Gesprächssituationen
- Einführung in Befragungstechniken zur Wahrheitsfindung und deren praktische Anwendung in Interviews und Incident-Untersuchungen
- Praktische Einordnung von OSINT-Methoden, Spoofing-Techniken und Deepfakes mit Fokus auf Erkennung, Prävention und rechtliche Rahmenbedingungen
- Erarbeitung von Awareness- und Incident-Playbooks zur Minimierung sozialer Angriffsflächen

Inhalte/Agenda:

- ♦ **Woher kommen die Gefahren, wer ist betroffen? Erstellung eines individuellen Lagebildes**
- ♦ **Rechtliche und ethische Aspekte beim Einsatz von Social Engineering**
- ♦ **Lernpakete zu folgenden Themen (jeweils als Übersicht und Einführung):**
  - ♦ ◊ Schaffung falscher Identitäten
  - ◊ Recherchen im WWW via Deep Web Search, OSINT-Tools, KI-basierte Dienste und Social Media
  - ◊ Überwinden von Zutrittskontrollen und -barrieren
  - ◊ Schwachstellenidentifizierung und Angriffstaktiken
  - ◊ WLAN-Hacking mit verschiedenen Tools
  - ◊ Hacker-USB- und LAN-Tools
  - ◊ Spear-Phishing
  - ◊ Vishing, Smishing, Call-Spoofing und Rollenspielübungen
  - ◊ Einsatz von Deepfakes (Stimme & Gesicht) mit den dazugehörigen Tools und Erkennungsmethoden
  - ◊ Einführung in Daniel Kahnemans Konzept „Thinking, Fast and Slow“ — System 1 / System 2 als Erklärung kognitiver Entscheidungsprozesse und ihre Relevanz für Manipulationen und Fehleranfälligkeit
  - ◊ Einführung in Robert Cialdinis Prinzipien der Beeinflussung — Übersicht der wichtigsten Prinzipien und ihre Anwendung in Social-Engineering-Szenarien
  - ◊ Einführung in Paul Ekmans Micro- und Macroexpressions — Grundzüge der nonverbalen Kommunikation und praktische Hinweise zur Erkennung emotionaler Signale
  - ◊ Befragungstechniken zur Wahrheitsfindung — Übersicht gängiger Fragetechniken, strukturierter Interviewführung und plausibilitätsorientierter Nachfragen zur besseren Einschätzung von Aussagen
- ♦ **Analyse der eigenen Angreifbarkeit und Abwehroptionen — Priorisierung von Maßnahmen und Quick-Wins**
  - ♦