SC300 Social Engineering Basics

Kurzbeschreibung:

Teilnehmende 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 physische Angriffsmethoden wie Tailgating, Lock-Picking oder RFID-Spoofing zur Stärkung der Sicherheitsawareness.

Zielgruppe:

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

Voraussetzungen:

IT-Erfahrene mit wenig bis mittlerem Social Engineering Know-How

Sonstiges:

Dauer: 2 Tage

Preis: 1590 Euro plus Mwst.

Ziele:

Der Schwerpunkt liegt neben dem Vermitteln der grundsätzlichen ethischen und rechtlichen Rahmenbedingungen auf dem **Aufbau eines Verständnisses von Angriffstechniken**. Dadurch gewinnen Sie einen neuen Blick auf Ihre Angriffsoberfläche und sind in der Lage, Sensibilisierungsprogramme für Ihren Bedarf zu optimieren und Abwehrmaßnahmen durchzuführen.

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:**
  - ♦ ◊ Schaffung falscher Identitäten
    ◊ Recherchen im WWW via Deep Web Search, OSINT-Tools und Social Media
    ◊ Überwinden von Zutrittskontrollen und -barrieren
    ◊ Schwachstellenidentifizierung und Angriffstaktiken
    ◊ WLAN-Hacking mit verschiedenen Tools
    ◊ Hacker-USB- und LAN-Tools
    ◊ Spear-Phishing
    ◊ Vishing und Rollenspiel
- ♦ **Analyse der eigenen Angreifbarkeit und Abwehroptionen**