SC300 Social Engineering Basics

Kurzbeschreibung:

Lernen Sie, wie moderne Social-Engineering-Angriffswerkzeuge eingesetzt werden und entwickeln Sie dadurch ein besseres Verständnis für Ihre eigenen Angriffsvektoren. Im Kurs geht es darum, ein **Verständnis für die Möglichkeiten und Gefahren des Social Engineering** herzustellen und so die **Sicherheitsawareness im Unternehmen** im Ganzen zu stärken.

Der praktische Teil des Seminars zeigt Einsatzwege von Open Source-Intelligenz (**OSINT**, **Google Dorking**, **Risikobewertung von Menschen**), Technologien der **psychologischen Beeinflussung**, manipulative **WLAN- und LAN-Werkzeuge**, sowie die Durchführung von physischen Computerangriffen mit **Keygrabbern** und dem **Hak5 Bash Bunny**.

Erweitern Sie darüber hinaus Ihr Wissen über Techniken vom Tailgating über klassisches Lock-Picking bis zum RFID-Spoofing mittels Flipper Zero und welche gängigen Methoden für die Überwindung von physischen Zutrittsbeschränkungen häufig eingesetzt werden.

Erweitern Sie Ihr Wissen um Fähigkeiten zur praktischen Anwendung im Aufbaukurs SC305 Social Engineering Practitioner.

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**