SC305 Full Scope Social Engineering - Basiswissen & Awareness

Kurzbeschreibung:

Erfahren Sie in diesem eintägigen Training, welche Möglichkeiten sich Kriminellen abseits von klassischen IT-Sicherheitslücken bieten.
Denn: Kein Patch hilft gegen ein fehlerhaftes „menschliches Betriebssystem“. Daher gilt es, das Bewusstsein der Mitarbeiter durch Training zu schärfen und Opfer von Social-Engineering-Angriffen nicht zu brandmarken.

Wir bieten diese Schulung ausschließlich Inhouse beim Kunden vor Ort oder als "geschlossenen" Kurs bei qSkills in Nürnberg an.

Zielgruppe:

Führungskräfte, IT-Management, ISMS- und BCM Verantwortliche, Datenschutz-, Compliance-Beauftragte, Betriebsrat.

Voraussetzungen:

Grundverständnis von organisationsinternen Sicherheitsstrukturen

Sonstiges:

Dauer: 1 Tage

Preis: Euro plus Mwst.

Ziele:

Social Engineering nutzt Schwachstellen des Menschen aus und stellt eine der größten Bedrohungen für Unternehmen dar, da sie in der Lage sind, Personen durch Täuschung zu manipulieren, um vertrauliche oder persönliche Informationen preiszugeben, die für betrügerische Zwecke verwendet werden können.

Inhalte/Agenda:

- ♦ ◊ Was ist „Full Scope Social Engineering“ im Kontext von Hacking eines Unternehmens?

  ◊ Welche Methoden benutzt der „Social Engineer“? Sensibilisierung für die Wahrnehmung der eigenen, unbewussten Manipulation.

  ◊ Welche Ziele verfolgt der Angreifer? Erstellung einer Angriffs-Methologie zur Durchführung von Self-Assestments.

  ◊ Was sind schützenswerte Informationen im Unternehmen?

  ◊ Vorstellung von Google-Hacking und technischen Werkzeugen eines Hackers (Informationsbeschaffung, Zutritt, LAN/USB-Tools, WLAN-Hacking)

  ◊ Unterschiede der Strategie von Angriff und Verteidigung und Best Practices zur Minimierung der Angriffsoberfläche

  ◊ Bewusstseinsveränderung beim Umgang/Weitergabe von Informationen und Daten

  ◊ Welchen realen Bedrohungen bin ich täglich im Arbeitsumfeld ausgesetzt?

  ◊ Wie anfällig bin ich für Angriffe dieser Art?

  ◊ Wie schütze ich mich und andere davor?

♦ Hinweis zum Training:

♦ ◊ Um die Trainingsinhalte nachhaltig zu vermitteln und in den Köpfen zu verankern, werden die perfiden Methoden des „Social Engineering“ nicht nur in der Theorie, sondern auch in der Praxis den Teilnehmern vorgeführt.

◊ Wir machen ausdrücklich darauf aufmerksam, dass bei der Schulung durch den Referenten teilweise illegale, straftbewertete Vorgehensweisen demonstriert werden, um so die verschiedenen Angriffsszenarien realistisch live zu demonstrieren.

♦ ◊