

## ***SC300 - WS Webseminar: Social Engineering - Täuschen, Tarnen und Tricksen***

### **Kurzbeschreibung:**

Social Engineering gilt seit Längerem als eine der größten Bedrohungen für Assets und Informationen. Immer öfter richten sich die Attacken von Hackern gegen das vermeintlich schwächste Glied in der Sicherheitskette - den Menschen.

Auch wenn es kein Standard-Gegenmittel gibt, es ist entscheidend, die Methoden der Angreifer zu verstehen. Nur dann hat man eine reelle Chance, solche Cyber-Attacken abzuwehren.

Im Online Training **Social Engineering - Täuschen, Tarnen und Tricksen** vermitteln wir einen generellen Überblick über mögliche Gefahren, Vorgehensweisen der Angreifer und Tipps zum besseren Schutz

### **Zielgruppe:**

Upper Management, IT-Management, CISOs, IT-Security Spezialisten, Pentester, Red- und Blueteamer, DSBs, Betriebsrat

### **Voraussetzungen:**

Für das Online Training **Social Engineering - Täuschen, Tarnen und Tricksen** gibt es keine Voraussetzung, außer generelles Interesse am Schutz vor Cyberangriffen

### **Sonstiges:**

**Dauer:** Tage

**Preis:** 0 Euro plus Mwst.

### **Ziele:**

Erkennen Sie die Methoden und Tricks eines Social Engineers. Nur so können Sie gezielt auf Angriffe und Attacken reagieren.

**Inhalte/Agenda:**

- - ◆ Die digitale und emotionale Täuschung
  - ◆ Werkzeuge, Webseiten und Services, die Social Engineers bei ihrem Vorgehen benutzen
  - ◆ Aufbau und Wirkungsweise von Social Engineering-Kampagnen
  - ◆ Tipps & Tricks, die mit einfachen Maßnahmen ihren Schutz verbessern
  - ◆ Diskussion und Fragen
  - ◆