Social Engineering

Faktor Mensch: Angriffsvektor soziale Manipulation

Seminar	2 Termine verfügbar	Teilnahmebescheinigung
Präsenz / Virtual Classroom	8 Unterrichtseinheiten	Online durchführbar

Seminarnummer: 32260

Stand: 19.04.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/32260

Bei Cybersicherheit wird oft an Technik wie Virenschutz und Firewalls gedacht, doch das größte Sicherheitsrisiko dürfte weiterhin der Mensch sein: Social Engineering (SE) eröffnet zahlreiche erfolgversprechende Angriffsmöglichkeiten, von Phishing über CEO-Fraud bis zu KI-Angriffen. Das Seminar bietet Lösungsansätze für Awarenessmaßnahmen sowie ein erstes Schulungskonzept gegen SE-Attacken.

Nutzen

- Aufklärung über den wahrscheinlich wichtigsten Risikofaktor in der Cybersicherheit
- Hilfe bei der Entwicklung von Abwehrstrategien und Schulungsmaßnahmen
- Lückenschluss in der Cyberabwehr: hier werden nicht die technischen oder rechtlichen, sondern die sozialen Risiken behandelt und damit ein wichtiger Baustein für ganzheitliche Sicherheit geliefert

Darstellung der Entwicklungsmöglichkeiten eigener SE-Rahmenkonzepte für langfristige Abwehrgestaltung

Zielgruppe

- Berufsgeheimnisträger und Anwender mit Zugang zu sensiblen digitalen wie analogen Daten
- IT- und OT-Sicherheitsexperten in Firmen, Behörden, NGOs, etc.
- Am Themenkomplex „Soziale Manipulation“ Interessierte

Voraussetzungen

Empfohlen:

- Grundlegendes Interesse an Social Engineering, d.h. sowohl an der Diskussion der theoretischen Grundlagen (Methodik, Forschungsfragen, etc.) als auch an der konkreten Anwendung im sozio-technischen Bereich in Form von Gruppenarbeit im Seminar
- Interesse an technischen, kulturellen, ethischen und rechtlichen Grundlagen des Social Engineerings
- Interesse an der Entwicklung von ersten eigenen Schulungskonzepten zur Awarenessentwicklung für Risikopersonen und -gruppen im eigenen Unternehmen

Optional:

- Erste Kenntnisse relevanter IT-Sicherheits-Trends und -Entwicklungen (z.B. Phishing)

Inhalte des Seminars

1. Angriff

Der erste Teil des Seminars klärt über Geschichte, Entwicklung und aktuelle Angriffe sowie den Stand von Forschung und Anwendung auf, damit deutlich wird, was SE ist und – mindestens genauso wichtig – was nicht. Es werden sowohl analoge als auch digitale SE-Angriffe und die dahinterstehenden psychologischen und soziologischen Grundlagen (Heuristiken) besprochen. Die Rolle der Digitalisierung der Gesellschaft sowie der Aspekt der digitalen Kultur werden dabei besonders betont. Ethische und rechtliche Aspekte kommen hinzu.

1. Abwehr

Es werden historische und aktuelle Fälle und Beispiele aus der Praxis besprochen, die die Abwehr von SE-Angriffen demonstrieren. Diese dienen als Grundlage für eigene Szenarien, die durch die TeilnehmerInnen entwickelt werden. So wird das Wissen aus Teil 1 des Seminars direkt angewandt. Hiermit werden die inhaltlichen Grundlagen für eigene Up-to-date-Lösungen und Schulungskonzepte generiert.

1. Awareness

Angriff und Abwehr werden in ein erstes exemplarisches Schulungsrahmenkonzept überführt, welches eine dauerhafte Awareness im Unternehmen schaffen soll (3A-Ansatz). Das Rahmenkonzept wird ganzheitlich dargestellt, d.h. es behandelt auch Themen wie Verantwortlichkeiten, Umgang mit neuen technischen Entwicklungen (z.B. KI, IoT), Kosten-Nutzen-Rechnungen für Abwehrmaßnahmen und Schulungen, Innovation und Kultur im Unternehmen.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/32260 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.