
Schulung

HISOLUTIONS

# Social Engineering

Der Mitarbeiter Peter Müller gibt dem netten Anrufer aus dem IT-Support sein Passwort heraus. Frau Meier überweist auf Anweisung ihres Chefs 5 Millionen Euro auf ein bestimmtes Konto. Und die Elektrikerfirma hilft bei technischen Störungen sofort, auch ohne Beauftragung.

Diese Szenarien erscheinen nicht zwingend ungewöhnlich, werden aber von Hackern mit Social Engineering-Kenntnissen immer wieder gnadenlos ausgenutzt und führen zu Millionenschäden in Unternehmen.

Diese Schulung versetzt Sie in die Sichtweise solcher Täter und möchte die funktionierenden Angriffstechniken intensiver beleuchten. Zudem werden Sie während der Schulung selbst zu Angreifern, um zu verstehen, warum der Mensch sich schwer gegen Manipulationstechniken und clevere Täter schützen kann. Nur wer die Denkweise der Täter versteht, kann sich auch dagegen wehren. In einer interaktiven Schulung lernen Sie sich selbst von einer ganz anderen Seite kennen und erfahren, wie Sie besser und effektiver schützen können.

## ZIELGRUPPE

Alle Mitarbeitenden mit Sicherheitsaufgaben, Zentralfunktionen und Führungskräfte, grundsätzlich aber alle Mitarbeitenden im Unternehmen.

## AUSFÜHRLICHE INHALTE NACH MODULEN

1. **Wahrnehmung:** Verschiedene Wahrnehmungsübungen und Rollenspiele.
2. **Was ist Social Engineering (kurz SE):** Kurze Einführung und Erklärung, was SE im Grundsatz ist.
3. **Analyse eines Social-Engineering-Angriffs:** Analyse anhand von gedrehten Videos.
4. **Persönlichkeitsanalyse:** Selbsterkenntnis und Kommunikationstraining.
5. **E-Mail und Vishing:** Erläuterung dieser häufig erfolgreichen Angriffsvektoren anhand eigens durchgeführter Tests.
6. **Erkenntnisse des eigenen Kommunikationsstils:** Wie kommuniziere ich selbst? Wie kommunizieren andere?
7. **Umgang mit unterschiedlichen Kommunikationsstilen:** Analyse der Stile und kommunikative Abwehrmöglichkeiten.
8. **Wie Angreifer unsere Gedanken catchen:** Vorstellung der Manipulationstechniken von Angreifern und Erarbeitung von Gegenmaßnahmen.
9. **„Bodyreading" – der Körper spricht Bände:** Erkennen von Mikromimik und Ganzkörperverhalten.
10. **SE-Angriff in einem kompletten Ablauf von A-Z:** Von OSINT, über Aufklärung bis zum Angriff werden alle Schritte aus einem erfolgreichen Social-Engineering-Test vorgestellt.
11. **Jetzt wird angegriffen:** Schulungsteilnehmende schlüpfen in die Angreiferrolle und lernen das Observieren und Beobachten von Angriffen. Die Ergebnisse der Praxisübung werden im Nachgang ausgewertet.

## IHR TRAINER

Alexander Fischer ist ehemaliger Beamter einer Spezialeinheit für verdeckte Ermittlungen gegen das Organsierte Verbrechen. Durch unzählige Undercover-Einsätze im schwerkriminellen Milieu gewann er tiefe Einblicke in die Gedankenwelt und Vorgehensweisen von Schwerverbrechern.

## PREIS

Preis: 599,- Euro

## ORT

Die Schulung findet in den Räumen von HiSolutions in Berlin statt.

**HiSolutions AG** | Schloßstraße 1 | 12163 Berlin | Fon: +49 30 533 289-0 | info@hisolutions.com | www.hisolutions.com