SECUTAIN Schulungen

Social Engineering-Workshop

Wohl kein anderes Thema der Informationssicherheit verdeutlicht so stark wie Social Engineering, dass der Schutz von Informationen kein reines IT-Thema ist. Angriffe erfolgen am Telefon oder ganz ohne Technik. Es geht um psychologische Manipulation von Opfern, um an Informationen zu gelangen, Systeme zu kompromittieren oder Geld zu erschleichen.

> *Ich habe selten eine Schulung erlebt, die so ein ernstes Thema zu kurzweilig und unterhaltsam dargestellt hat.*

Die Methoden sind zum Teil mit minimalem Kostenaufwand verbunden, geschickt und perfide. Opfer melden häufig aus Scham erfolgreiche Angriffe nicht, so dass Situationen nicht oder zu spät bekämpft werden und Organisationen nicht lernen können. Das beste Mittel gegen diese Art von Angriffen sind wissende, aufmerksame und selbstbewusste Mitarbeiter, die diese Art von Angriffen erkennen, abwehren und melden.

> *Die höhere Achtsamkeit in unseren Haus war sofort ab dem Tag 1 nach der Schulung geradezu spürbar.*

Ziel der Schulung ist das Vermitteln des Vorgehens von Social Engineering-Angriffen, um achtsamer für diese Art von Situationen zu werden. Je nach gewünschter Dauer der Schulung erhalten die Teilnehmenden ein Gefühl dafür, für welche Art von Angriffen sie auf Grund ihrer Persönlichkeitsstruktur anfällig sein könnten. Im ganztägigen Termin wird in einem Workshop-Charakter am konkreten Schutz Ihrer Organisation vor Social Engineering-Attacken gearbeitet.

Social Engineering - Wie nähert man sich diesem Thema?

Obwohl vielen Organisationen bereits bewusst ist, dass Social Engineering keine abstrakte oder ferne Bedrohung mehr ist, fällt die Annäherung an das Thema häufig schwer. Unser Workshop ist ein niederschwelliges Angebot, sich mit dem Thema auseinanderzusetzen, das drei Punkte erreicht:

1. Die Mechanismen von Social Engineering-Angriffen werden den Teilnehmern vermittelt. Entsprechende Situationen werden zukünftig besser erkannt.

2. Die Teilnehmer erhalten Ansatzpunkte, welche ihrer persönlichen Eigenschaften durch Angreifer ausgenutzt werden könnten. Das Schutzniveau Ihrer Organisation wird unmittelbar erhöht.

3. Es werden gemeinsam ganz konkrete Ansatzpunkte erarbeitet, welche Schutzmechanismen in Ihrer Organisation verbessert werden können und welche Werte besonders schützenswert sind. Sinnvolle Folgemaßnahmen werden so transparent.

ANZAHL DER TEILNEHMER
10-30 Teilnehmer

DAUER
8 Stunden

VORKENNTNISSE
kein Vorwissen notwendig

SECUTAIN. Gutes Lernen. Gute Unterhaltung.

SECUTAIN

SECUTAIN Schulungen

Social Engineering-Workshop

Ihre Trainer

David Scribane

David Scribane hat über 15 Jahre Erfahrung im Betrieb komplexer IT-Infrastrukturen in verantwortlicher Position. Bestandteil dieser Aufgabe war unter anderem die Wahrung der IT-Sicherheit und die Konzeption und Aufrechterhaltung des Informationssicherheitmanagements. Im Rahmen dieser Tätigkeit gewann er die Erkenntnis, dass die Nutzer ein wichtiges Puzzleteil zur Wahrung der Informationssicherheit sind.

Im Jahr 2016 war er daher Mitbegründer der Marke SECUTAIN, die Organisationen hilft, Sensibilität für dieses Thema zu steigern.

Michael Willer

Michael Willer war über 10 Jahre im militärischen Nachrichtenwesen in der Informationsgewinnung durch menschliche Quellen eingesetzt. Als Intelligence Analyst und Ausbilder für militärische Befragungs-/ Vernehmungstechniken sowie Verhalten in Kriegsgefangenschaft/ Geiselnahmen hat er sich intensiv mit der menschlichen Psychologie auseinandergesetzt.

Seit 2014 ist er selbstständig als Sicherheitsberater und hat sich mit der Gründung der Human Risk Consulting GmbH in 2015 auf das Thema Social Engineering konzentriert.

> *Beide Trainer ergänzen sich durch ihre unterschiedlichen Hintergründe sehr gut, was die Schulung abwechslungsreich macht.*

Die Inhalte

Schulungsteil:

- Was ist Social Engineering?
- Welche Schutzziele können verletzt werden?
- Welche menschlichen Eigenschaften werden ausgenutzt?
- Wie können Angriffe erkannt und abgewehrt werden?
- Wieso spielt Wahrnehmung eine wichtige Rolle?
- Was ist der kognitive Reflex?

Workshopteil:

- Bestimmung Ihrer informationellen Kronjuwelen
- Bewertung bestehender Sicherheitsregelungen
- Schwachstellenerkennung durch Perspektivwechsel (Angreifersicht)
- konkrete Arbeit an der Erhöhung des Schutzes für Ihre Organisation
- Aufbereitung der erarbeiteten Inhalte für nächste Schritte in Ihrer Organisation

> *Im Workshopteil haben wir wichtige Ansatzpunkte für unsere Firma gewinnen können, ohne viele Beratungstage investieren zu müssen.*

Mehr Infos unter info@secutain.com oder auf secutain.com.

SECUTAIN. Gutes Lernen. Gute Unterhaltung.

SECUTAIN