Leitblatt

Social Engineering

Anti Fraud Management

Bundesverband

Social Engineering = Manipulation oder „Die Kunst der Täuschung"

Unter Social Engineering versteht man das gezielte Ausnutzen menschlicher Schwächen oder Verhaltensmuster wie zum Beispiel Unachtsamkeit oder Neugier. Das Opfer soll dabei zu einem vom Angreifer gewünschten Verhalten bewegt werden.

Vorgehen der Angreifer

Der Social Engineer geht oftmals mehrstufig vor:

1. Zunächst sammelt der Angreifer z. B. in sozialen Netzwerken Informationen über das Opfer.
2. Bei den ersten Kontaktaufnahmen geht es noch ausschließlich um den Aufbau von Vertrauen.
3. Bei späteren Kontaktaufnahmen versucht der Social Engineer, an die geheimen Informationen zu kommen. Bekannte Schwächen des Opfers werden nun ausgenutzt. Je nach Schwachstelle setzt der Angreifer auf Gutgläubigkeit, Hilfsbereitschaft oder Autoritätshörigkeit, Druck und/oder Angst.

Rollen des Social Engineers

Gerne tarnt sich der Social Engineer z.B. als

- Geschäftsführer, der Sie autorisiert eine geheime Finanztransaktion durchzuführen.
- IT Support, der wegen einer Systemumstellung Ihren Usernamen und Passwort benötigt.
- Kunde, der dringend sensible Daten von Ihnen benötigt.
- Dienstleister, der Sie auffordert, sofort eine Transaktion auszulösen, um ein Scheitern zu verhindern.
- Journalist, der angelblich die Freigabe erhalten hat, von Ihnen sensible Informationen zu erhalten oder ein Interview mit Ihnen als wichtige Person führen will.
- Kunde, der Sie unter Wahrung einer falschen Legende auf einer Messe zum Plaudern verleitet.
- Kollege, der sich schnell eine Datei, eine E-Mail oder ein Fax zusenden lassen muss.
- Mitarbeiter eines Service-Unternehmens, das Details der Nutzung braucht, um die Kunden-zufriedenheit zu testen.
- Mitarbeiter eines angeblichen Umfrage-Instituts, der nicht zurückgerufen werden kann, weil er im Call-Center arbeitet.
- Job-Bewerber, der sich seinen zukünftigen Aufgabenbereich erklären lässt oder Headhunter, der Mitarbeitern des Unternehmens gute Job-Angebote macht, um ihnen Firmen-internas zu entlocken.

Mitarbeiter stärken durch Informationen

Ein Problem entsteht immer dann, wenn die Mitarbeiter nicht wissen,

- was vertrauliche Informationen an ihrem jeweiligen Arbeitsplatz sind. Schützenswerte Unternehmensdaten müssen abteilungsbezogen klar definiert und verständlich für die Mitarbeiter sein.
- welcher Grad an Flexibilität und Kunden-Entgegenkommen ohne Gefährdung der Vertraulichkeit möglich ist.
- welche Möglichkeiten sie haben, einen Anrufer zu legitimieren.
- wen sie außerhalb der Arbeitszeiten zu Rate ziehen können, wenn eine Bitte am äußersten Rand der Regeln liegt.
- wie sie die anderen Kollegen warnen können, dass eine eigenartige Anfrage stattgefunden hat, die ihnen suspekt erschien.
- ob ihr Chef auch bei Drohungen von wichtigen Kunden hinter ihnen steht.

Für Sie als Mitarbeiter gilt:

- Seien Sie niemals arglos oder gutgläubig!
- Lassen Sie sich nicht einwickeln, denn Hilfsbereitschaft wird gerne ausgenutzt und hinter Schmeicheleien steckt mehr!
- Jemandem der Ängste schürt oder Druck aufbaut, ist nicht zu trauen!
- Seien Sie kritisch bei unbekannten Anrufern!
- Hinterfragen Sie selbstbewusst unverständliche Anfragen!
- Geben Sie keine Informationen zu Organisation oder sogar betriebskritische Daten am Telefon heraus!
- Im Fall eines E-Mail-Kontaktes verifizieren Sie die E-Mail-Adresse anhand des betrieblichen Telefonbuchs!

Faustregeln

- Alles, was nicht auf der Website des Unternehmens veröffentlicht ist, gilt als vertraulich und ist daher nicht für Dritte bestimmt!
- Die Einhaltung der bestehenden Compliance-Richtlinien ist ein effektiver Schutz!

ASW Bundesverband

Herausgeber: ASW Bundesverband – Allianz für Sicherheit in der Wirtschaft e. V.
Stand: Juli 2017 | **Kontakt:** info@asw-bundesverband.de