Die Kunst der Manipulation:

Social Engineering als wachsende Bedrohung

Social Engineering zählt heute zu den gefährlichsten Methoden im Bereich der Informationssicherheit. Anstatt technische Schwachstellen auszunutzen, zielen Angreifer direkt auf die Schwachstelle Mensch – mit grossem Erfolg. Denn allzu oft wird diese Schwachstelle sträflich unterschätzt. Höchste Zeit, etwas dagegen zu unternehmen.

Ardiana Krasniqi

Der Mensch als Einfallstor

Social Engineering bezeichnet psychologisch geschickte Manipulationsversuche, durch die Angreifer Mitarbeitende dazu bringen, sensible Informationen preiszugeben oder Zugänge zu gewähren. Während Unternehmen viel in Firewalls, Verschlüsselung und Authentifizierung investieren, wird der Faktor Mensch oft vernachlässigt. Genau hier setzen Social Engineers an – indem sie menschliche Eigenschaften wie Hilfsbereitschaft, Respekt vor Autorität oder das Bedürfnis, Probleme schnell zu lösen, gezielt ausnützen.

Erfolg durch Täuschung

Im Vergleich zu technischen Angriffen sind Social Engineering-Manipulationen nicht nur einfacher, sondern oft auch deutlich effektiver. Statt sich durch Firewalls zu kämpfen, reicht oft ein überzeugend formulierter Anruf oder eine harmlose Frage an der Rezeption. Die Erfolgsquote ist hoch, denn viele Mitarbeitende erkennen die Gefahr nicht – oder erst, wenn es zu spät ist.

Häufige Angriffsmethoden

Während das gefühlt allgegenwärtige Phishing (Beschaffung von Informationen mittels gefälschter Emails, SMS- oder Nachrichten) im Bewusstsein der Öffentlichkeit und in Unternehmen angekommen ist, werden andere, sehr effektive Angriffsmöglichkeiten noch zu häufig übersehen. Zum Vorteil der Angreifer notabene.

Weitere gängige Methoden sind:

- **Tailgating:** Unbefugtes Betreten gesicherter Bereiche, oft durch Ausnutzen von Höflichkeit («Türe aufhalten»).
- **Pretexting:** Vortäuschen einer Identität, etwa als Techniker oder Lieferantin, um Zugang oder Informationen zu erhalten.
- **Impersonation:** Auftreten als neue Mitarbeiterin, als externer Dienstleister oder IT-Support, um Vertrauen zu erschleichen – oft verbunden mit einem erfundenen Problem (Reverse Social Engineering).
- **Baiting/USB Drop:** Platzieren infizierter USB-Sticks in der Nähe von Mitarbeitenden mit dem Ziel, sie zum Gebrauch und damit zum Einschleusen von Schadsoftware zu verleiten.

Der typische Ablauf eines Angriffs

Social Engineering-Angriffe folgen oft einem wiederkehrenden Muster in vier Phasen:

1. **Informationsbeschaffung:** Sammeln öffentlicher Informationen über das Unternehmen (Website, Social Media, Presseberichte).
2. **Externe Zugriffsversuche:** Kontaktaufnahme über E-Mail, Telefon oder gefälschte Online-Kommunikation (z. B. Phishing). Oftmals ist der Angriff bereits nach Phase zwei erfolgreich.
3. **Physischer Zugang:** Falls Phase 2 nicht von Erfolg gekrönt ist, wird versucht, sich Zutritt zum Gebäude oder zu spezifischen Räumen zu verschaffen (Tailgating, Pretexting).
4. **Angriffsausführung:** Mit den gewonnenen Informationen wird ein gezielter externer Zugriff durchgeführt – die Falle schnappt zu.

Prävention beginnt im Unternehmen

Um Social Engineering-Angriffe wirksam abzuwehren, sind technische Massnahmen allein unzureichend. Unternehmen müssen strukturiert vorgehen und sowohl Informationen als auch physische Zugänge schützen.

Zentrale Schritte sind:

- **Identifikation schützenswerter Informationen und Einheiten:** Welche Daten oder Bereiche wären für Angreifer besonders wertvoll?
- **Klassifizierung und Zugriffsregelung:** Wer darf worauf zugreifen? Wer hat Zutritt zu welchen Bereichen?
- **Formulierung klarer Sicherheitsrichtlinien:** Etwa zur Nutzung von Geräten, zur Aufbewahrung vertraulicher Unterlagen oder zum Verhalten im Homeoffice.
- **Verankerung im Alltag:** Weisungen müssen gelebt werden – durch einfache, wiederkehrende Botschaften und konkrete Handlungsempfehlungen.
- **Berücksichtigung aller Hierarchiestufen:** Social Engineering zielt nicht nur auf Führungskräfte, sondern auf alle Mitarbeitenden (-> Schulung).

Die wichtigsten Massnahmen gegen Social Engineering kurz zusammengefasst:

1. Informationssicherheit strategisch verankern, Sicherheitskultur etablieren und leben
2. Schutzbedarf und Risiken identifizieren
3. Sicherheitsmassnahmen definieren und umsetzen
4. Konsequente Mitarbeitersensibilisierung mittels Schulungen, eLearning etc.
5. Wirksamkeit der Sicherheitsmassnahmen regelmässig überprüfen (Social Engineering-Simulationen) und weiterentwickeln

Sensibilisierung als Schlüssel

Die nachhaltigste Massnahme gegen Social Engineering ist eine starke Sicherheitskultur. Wie beim Sporttraining gilt: Nur regelmässiges Üben zeigt Wirkung. Sensibilisierung muss kontinuierlich erfolgen – über eLearning, interne Schulungen, Infomaterial oder die Diskussion realer Fälle aus der Branche. Wichtig: Die Massnahmen müssen an die Heterogenität der Belegschaft angepasst werden.

Regelmässige Überprüfung und Anpassung

Technologien entwickeln sich – und mit ihnen die Angreifer. Unternehmen müssen deshalb ihre Sicherheitskonzepte laufend überprüfen und anpassen. Social Engineering-Tests – also kontrollierte Manipulationsversuche – zeigen Schwachstellen auf und helfen, Schulungsbedarf zu erkennen. Die Erkenntnisse fliessen zurück in die Schutzmassnahmen.

Informationssicherheit beginnt im Kopf

Wer die Mechanismen des Social Engineering kennt und versteht, kann Manipulationsversuche erkennen und abwehren. Die Schulung und Sensibilisierung der Mitarbeitenden ist dabei das wichtigste Werkzeug – und sollte konsequent angegangen werden. Lieber heute als morgen.

Ardiana Krasniqi ist Projektleiterin und Consultant bei der Swiss Infosec AG, einem unabhängigen Beratungs- und Ausbildungsunternehmen in den Bereichen Informationssicherheit, Datenschutz und IT-Sicherheit. Mit ihrer umfassenden Erfahrung in Informationssicherheit und Krisenmanagement leitet sie u. a. gezielte Security-Awareness-Projekte und schafft dadurch Sensibilisierung und sicheres Verhalten bei Social Engineering-Angriffen.
www.infosec.ch

Publikation in Zusammenarbeit mit:
VIW – Wirtschaftsinformatik Schweiz | www.viw.ch

VIW Wirtschaftsinformatik Schweiz