Informationsdienst Datenschutz & Datensicherheit

Schwerpunktthema: Social Engineering

Liebe Kolleginnen und Kollegen,

in dieser Ausgabe unseres Informationsdienstes widmen wir uns einem Thema, das jeden von uns betrifft: Social Engineering - oder einfacher ausgedrückt, die Kunst der Manipulation.

In der Praxis erleben wir leider immer wieder, dass selbst die beste technische Sicherheitsinfrastruktur durch einen unbedachten Klick umgangen werden kann. Denken Sie daran: Cyberkriminelle setzen nicht immer auf komplizierte Hackerangriffe - oft ist es einfacher, einen gutgläubigen Mitarbeitenden zu täuschen.

Die gute Nachricht: Mit dem richtigen Wissen können Sie sich und unser Unternehmen effektiv schützen. Diese Ausgabe gibt Ihnen praktische Tipps, wie Sie Manipulationsversuche erkennen und richtig reagieren.

Wir wünschen Ihnen eine aufschlussreiche Lektüre.

Mit besten Grüßen

Ihr Team vom

Informationsdienst Datenschutz & Datensicherheit

Das Wichtigste in Kürze:

- *Social Engineering nutzt menschliche Schwächen statt technischer Lücken*
- *91% aller erfolgreichen Cyberangriffe beginnen mit Social Engineering*
- *Wichtigste Warnsignale: Zeitdruck, ungewöhnliche Anfragen, Vertraulichkeit*
- *Bei Verdacht: Stoppen, nachfragen, IT-Support informieren*

Social Engineering: Was ist das?

Social Engineering ist eine der erfolgreichsten Angriffsmethoden auf Unternehmen. Dabei nutzen Kriminelle nicht technische Schwachstellen, sondern manipulieren Menschen durch psychologische Tricks. Laut aktueller BSI-Statistik beginnen 91% aller erfolgreichen Cyberangriffe mit Social Engineering. Für Unternehmen ist es daher essentiell, dass alle Mitarbeitenden die typischen Angriffsszenarien kennen und wissen, wie sie diese erkennen und abwehren können.

Aktueller Trend: KI „klont“ Stimmen

Seit 2024 nutzen Angreifer verstärkt KI-generierte Stimmen für telefonische Social Engineering Angriffe. Dabei werden öffentlich verfügbare Aufnahmen von Führungskräften genutzt, um täuschend echte Sprachnachrichten oder Telefonanrufe zu erstellen.

Fallbeispiel: Der „falsche“ Chef

Ein Mitarbeiter der Buchhaltung erhielt eine dringende E-Mail, vermeintlich vom Geschäftsführer. Dieser bat um die sofortige Überweisung von 45.000 EUR für einen wichtigen Geschäftsabschluss.

Die E-Mail-Adresse sah auf den ersten Blick echt aus, enthielt aber einen kleinen Tippfehler. Der Absender drängte auf absolute Vertraulichkeit und schnelles Handeln. Glücklicherweise hatte der Mitarbeiter kürzlich eine Security-Awareness-Schulung besucht und erkannte die typischen Warnsignale der Cyberattacke, die allgemein als „Chef-Masche oder „CEO-Fraud“ bekannt ist.

Warnbeispiele im Fallbeispiel:

- *Ungewöhnlich dringende Anfrage*
- *Forderung nach Vertraulichkeit*
- *Kleine Abweichung in der E-Mail-Adresse*
- *Umgehen üblicher Prozesse*

Social Engineering: „Erfolgs“-Faktoren

Social Engineering basiert auf grundlegenden menschlichen Verhaltensweisen und Emotionen:

- Häufig genutzte psychologische Hebel:
- Autorität (z.B. Vorgesetzter, IT-Support)
- Zeitdruck ("Muss sofort erledigt werden!")
- Hilfsbereitschaft ("Könnten Sie mir kurz helfen?")
- Angst ("Ihr Account wird gesperrt, wenn...")
- Neugier ("Schauen Sie sich diese Fotos an!")

Typische Angriffsszenarien liegen in der Regel im Online-Bereich:

- Phishing-E-Mails
- CEO-Fraud (Chef-Masche)
- Fake-Profile in sozialen Medien

Es gibt allerdings auch eine Reihe von Angriffsszenarien, die offline durchgeführt werden, z.B. durch

- Telefonanrufe (Vishing = **V**oice Ph**ishing**)
- Manipulation vor Ort (Tailgating)

Bei der letztgenannten Social Engineering-Form gelingt es dem Angreifer, sich Zutritt zu sensiblen Bereichen im Unternehmen (Serverraum, Buchhaltung, etc.) zu verschaffen. So verkleidet sich der Angreifer beispielsweise als Pizza- oder Paketbote bzw. Handwerker und lässt such unter einem Vorwand die Tür aufhalten oder bittet um Zugang, z.B. weil er die Heizung/Klimaanlage kontrollieren soll.

Checkliste für den Arbeitsalltag

Trotz vieler anderer „ToDos" sollten Sie sich im beruflichen Alltag stets der Risiken und Gefahren von Social Engineering bewusst sein. Am Ende sind es in der Regel Kleinigkeiten und Flüchtigkeitsfehler, die sich am Ende zu einem Datenschutz- oder Datensicherheitsfiasko für das ganze Unternehmen ausweiten können. Aus diesem Grund gilt unser dringender Rat: Beachten Sie stets die nachfolgenden Grundregeln:

Die wichtigsten Grundregeln:

1. Misstrauisch sein ist erlaubt und erwünscht
2. Im Zweifelsfall beim vermeintlichen Absender über bekannte Kontaktdaten nachfragen
3. Etablierte Prozesse nicht aufgrund von Dringlichkeit umgehen
4. Ungewöhnliche Vorfälle sofort dem IT-Support und dem Datenschutzbeauftragten melden

Bei unerwarteten Anfragen immer prüfen:

[ ] Kenne ich den Absender persönlich?

[ ] Ist die Anfrage plausibel und entspricht üblichen Prozessen?

[ ] Werde ich unter Zeitdruck gesetzt?

[ ] Wird nach vertraulichen Informationen gefragt?

[ ] Stimmen die Kontaktdaten exakt mit den bekannten überein?

Hinweis

Ein gesundes Misstrauen ist kein Zeichen von Unhöflichkeit, sondern von Professionalität!

Wissens-Check

Na? Bisher alles verstanden? Dann sollte unser kurzer Wissens-Check eigentlich kein Problem sein:

Frage1: Sie erhalten eine E-Mail vom IT-Support mit der Aufforderung, Ihr Passwort über einen Link zu ändern. Was tun Sie?

a) Dem Link folgen und Passwort ändern, IT-Sicherheit ist wichtig

b) Die Absenderadresse genau prüfen und beim IT-Support telefonisch nachfragen

c) Die E-Mail an Kollegen weiterleiten und fragen, ob sie auch solch eine Mail bekommen haben

Frage 2: Ein Kollege aus einer anderen Abteilung ruft an und bittet dringend um Zusendung von Kundendaten per E-Mail, da er keinen Zugriff auf das System hat. Wie reagieren Sie?

a) Die Daten sofort schicken, Kollegialität ist wichtig

b) Die Daten nur an seine offizielle Firmen-E-Mail-Adresse senden

c) Den Vorgesetzten kontaktieren und den korrekten Prozess für Datenzugriffe einhalten.

Auflösung:

Frage 1: Richtige Antwort: b)

Erklärung: Der IT-Support wird Sie nie per E-Mail auffordern, auf einen Link zu klicken und Ihr Passwort zu ändern. Im Zweifelsfall immer über die bekannte Telefonnummer beim Support nachfragen.

Frage 2: Richtige Antwort: c)

Erklärung: Auch bei internen Anfragen müssen die festgelegten Prozesse für den Datenzugriff eingehalten werden. Dringlichkeit ist kein Grund, von Sicherheitsrichtlinien