consilia

Wirtschaftsprüfung
Steuerberatung
Rechtsberatung
Unternehmensberatung

Social Engineering – Sicherheitslücke Mensch

- Phishing, Pretexting etc. verständlich erklärt
- Psychologische Manipulation als Sicherheitsrisiko
- Handlungsempfehlungen für Mitarbeitende

Social Engineering - Sicherheitslücke Mensch

Inhalt

1. Einleitung: Warum Social Engineering für jeden relevant ist

Vertrauen ist in modernen Geschäftsbeziehungen ein wichtiger Anker – Kunden und Geschäftspartner[1] übergeben hochsensible Daten und setzen auf absolute Diskretion. Doch was, wenn Angreifer nicht die Technik angreifen, sondern den Menschen? Social Engineering ist eine subtile, aber gefährliche Manipulation, die genau hier ansetzt. In dieser Broschüre zeigen wir Ihnen, wie Sie sich und Ihr Unternehmen gegen solche Angriffe wappnen.

Wichtiger Hinweis

Social Engineering betrifft sowohl Privatpersonen als auch Unternehmen und deren Mitarbeitende.

2. Definition: Was ist Social Engineering?

Social Engineering bedeutet, dass Angreifer gezielt menschliche Eigenschaften wie Vertrauen, Hilfsbereitschaft oder Neugier ausnutzen, um an vertrauliche Informationen zu gelangen. Dabei agieren sie nicht wie Hacker im klassischen Sinne, sondern manipulieren Personen, um Zugang zu sensiblen Daten oder Systemen zu erhalten. In Unternehmen könnte das z. B. bedeuten, dass sensible Daten durch geschickte Täuschung preisgegeben werden.

[1] In dieser Publikation wird aus Gründen der besseren Lesbarkeit in der Regel das generische Maskulinum verwendet. Die verwendete Sprachform bezieht sich auf alle Menschen, hat ausschließlich redaktionelle Gründe und ist wertneutral.

3. Typische Social-Engineering-Szenarien für Unternehmen

3.1 Der angebliche Kunde am Telefon

Ein Anrufer gibt sich als Kunde aus und behauptet, dringend Unterlagen oder steuerliche Informationen zu benötigen. Durch Zeitdruck („Ich sitze gerade beim Notar") oder Unsicherheit versucht er Mitarbeitende dazu zu bewegen, sensible Daten telefonisch herauszugeben.

Risiko: Preisgabe personenbezogener Daten, Steuerunterlagen oder interner Informationen.

3.2 Der angebliche Personalvermittler am Telefon

Auch ein Anruf eines angeblichen Personalvermittlers zur Abwerbung von Mitarbeitenden kann Teil eines Betrugsversuchs sein.

Ein unbekannter Anrufer fragt nach der aktuellen Tätigkeit des Mitarbeitenden, über welche Erfahrungen er verfügt, ob eine Bereitschaft zum Arbeitsplatzwechsel vorliegt und welche Gehaltsvorstellungen bestehen.

Risiko: Preisgabe personenbezogener Daten oder interner Informationen, z. B. zur Mitarbeitenden- und Gehaltsstruktur innerhalb des Unternehmens.

3.3 Gefälschte E-Mails mit Zahlungsänderungen oder fingierten Rechnungen

Eine E-Mail scheint von einem bekannten Kunden oder Geschäftspartner zu stammen. Darin wird darum gebeten, eine neue Bankverbindung zu hinterlegen oder kurzfristig Zahlungen umzuleiten. Möglich ist auch eine komplett neue, fingierte Rechnung.

Risiko: Manipulierte Überweisungen und finanzieller Schaden.

3.4 CEO- oder Chef-Masche

Mitarbeitende erhalten eine scheinbar interne Nachricht von der Unternehmensleitung mit einer dringenden Anweisung. Oft wird Autorität genutzt:

„Bitte sofort erledigen und vertraulich behandeln."

Risiko: Umgehung interner Kontrollmechanismen.

3.5 Gefälschte Behördenanfragen

Angreifer geben sich als Finanzamt, Datenschutzbehörde oder IT-Dienstleister aus und verlangen Zugangsdaten, Unterlagen oder schnelle Rückmeldungen.

Risiko: Offenlegung sensibler Unternehmens- und Kundendaten.

3.6 Schadsoftware über Bewerbungen oder Dokumente

Ein Unternehmen erhält scheinbar legitime Bewerbungsunterlagen oder Kundendokumente mit infizierten Anhängen.

Risiko: Schadsoftware, Ransomware oder Datendiebstahl.

3.7 Der „vergessene“ Besucher vor Ort

Eine Person erscheint freundlich und glaubwürdig im Unternehmen, etwa als Techniker, Paketdienst oder Bewerber. Durch Höflichkeit oder Ablenkung versucht sie, unbegleitet Zugang zu Räumen oder Informationen zu erhalten.

Risiko: Physischer Zugriff auf Akten, Bildschirme oder IT-Systeme.

3.8 Social Media & öffentliche Informationen

Angreifer sammeln Informationen über Mitarbeitende, Kunden, Zuständigkeiten oder Urlaubszeiten über soziale Netzwerke oder Webseiten.

Risiko: Gezielte Vorbereitung weiterer Angriffe („Spear Phishing“).

3.9 Passwort-Reset durch Manipulation

Ein Angreifer kontaktiert die IT oder Mitarbeitende und behauptet dringend, keinen Zugriff mehr auf ein Konto zu haben.

Risiko: Übernahme interner Accounts.

4. Konkrete Social Engineering Fallbeispiele für Unternehmen

4.1 Der angebliche Kunde am Telefon

Das Telefon klingelt. Ein freundlicher Anrufer meldet sich mit Namen und behauptet, Kunde des Unternehmens zu sein. Er wirkt glaubwürdig, kennt möglicherweise sogar den Namen einer Führungskraft oder einige allgemeine Informationen über das Unternehmen.

Der Anrufer schildert eine dringende Situation:

„Ich sitze gerade bei einem Termin und benötige sofort die letzte Auswertung."

Oder:

„Ich habe keinen Zugriff auf meine Unterlagen und brauche dringend die hinterlegte Bankverbindung."

Im Gespräch erzeugt der Angreifer gezielt Zeitdruck und versucht gleichzeitig, Vertrauen aufzubauen. Mitarbeitende sollen spontan handeln, ohne die Anfrage ausreichend zu prüfen. Genau hier setzt Social Engineering an: Nicht die Technik wird angegriffen, sondern der Mensch.

Besonders gefährlich ist dabei die Kombination aus Hilfsbereitschaft, Routine und vermeintlicher Dringlichkeit. In vielen Unternehmen ist ein serviceorientierter Umgang mit Kunden selbstverständlich – und genau diese Professionalität kann von Angreifern missbraucht werden.

Mögliche Risiken

- Herausgabe sensibler Informationen zu Kunden und Geschäftspartnern
- Offenlegung interner Abläufe oder Ansprechpartner
- Vorbereitung weiterer gezielter Angriffe
- Vertrauensverlust gegenüber Kunden
- Datenschutzrechtliche Konsequenzen

Wichtiger Hinweis

Sensible Informationen sollten niemals allein aufgrund eines Telefonats herausgegeben werden. Identitäten müssen eindeutig geprüft und definierte Rückruf- oder Freigabeprozesse eingehalten werden. Eine Telefonnummer kann durch einen Angreifer technisch simuliert werden (Caller-ID-Spoofing), somit ist eine eingehende Telefonnummer im eigenen Telefon-Display keine sichere Verifizierung.

4.2 Gefälschte Zahlungsänderungen per E-Mail

Eine E-Mail trifft scheinbar von einem bekannten Kunden, Dienstleister oder Geschäftspartner ein. Inhaltlich wirkt die Nachricht unauffällig und professionell formuliert. Häufig geht es um eine angeblich neue Bankverbindung oder eine kurzfristige Änderung von Zahlungsdaten.

Typische Formulierungen sind beispielsweise:

„Bitte berücksichtigen Sie ab sofort unsere neue Kontoverbindung."

Oder:

„Aufgrund einer Systemumstellung bitten wir um kurzfristige Anpassung."

Oft erzeugen Angreifer bewusst Druck oder verweisen auf dringende Fristen. Gleichzeitig nutzen sie bekannte Namen, Logos oder E-Mail-Signaturen, um Vertrauen aufzubauen. Teilweise unterscheiden sich die verwendeten E-Mail-Adressen nur minimal vom Original.

Im stressigen Arbeitsalltag werden solche Änderungen häufig nicht ausreichend hinterfragt – insbesondere dann, wenn die Anfrage auf den ersten Blick plausibel erscheint. Genau diese Routine nutzen Angreifer gezielt aus.

Mögliche Risiken

- Überweisungen auf betrügerische Konten
- Finanzielle Schäden
- Verlust sensibler Informationen
- Manipulation von Stammdaten
- Vertrauensverlust bei Kunden und Geschäftspartnern

Wichtiger Hinweis

Änderungen von Zahlungsdaten sollten niemals ungeprüft übernommen werden. Eine Rückverifizierung sollte über offiziell bekannte Kontaktdaten der jeweiligen Ansprechpartner erfolgen – niemals ausschließlich über die Angaben der erhaltenen E-Mail.

Zusätzlich kann das Risiko durch definierte Freigabeprozesse erheblich reduziert werden.

4.3 Die angebliche Behördenanfrage

Eine Mitarbeitende erhält einen Anruf oder eine E-Mail von einer vermeintlichen Behörde. Der Absender gibt sich beispielsweise als Finanzamt, Datenschutzbehörde oder Ermittlungsstelle aus. Oft wirken Auftreten und Sprache professionell und überzeugend.

Der Angreifer behauptet, es liege ein dringender Vorgang vor. Häufig wird Druck aufgebaut:

„Wir benötigen die Unterlagen noch heute."

Oder:

„Sollten Sie die Informationen nicht kurzfristig bereitstellen, kann dies Konsequenzen nach sich ziehen."

Durch die vermeintliche Autorität der anfragenden Stelle entsteht schnell Unsicherheit. Mitarbeitende möchten kooperativ handeln und mögliche Fehler vermeiden. Genau diese Situation wird gezielt ausgenutzt, um sensible Informationen, Dokumente oder interne Daten zu erhalten.

Teilweise versuchen Angreifer auch, Zugangsdaten oder technische Informationen abzufragen – beispielsweise unter dem Vorwand einer Prüfung oder Sicherheitskontrolle.

Mögliche Risiken

- Herausgabe vertraulicher Informationen zu Kunden und Geschäftspartnern
- Datenschutzverletzungen
- Offenlegung interner Prozesse und Zuständigkeiten
- Vorbereitung weiterer gezielter Angriffe
- Reputations- und Vertrauensschäden

Wichtiger Hinweis

Behördliche Anfragen sollten stets über definierte interne Prozesse geprüft werden. Im Zweifel empfiehlt sich eine Rückverifizierung über offiziell bekannte Kontaktdaten der jeweiligen Behörde – niemals ausschließlich über die Angaben aus der erhaltenen Nachricht.

4.4 Die Bewerbung mit Schadsoftware

Im Unternehmen geht eine Bewerbung per E-Mail ein. Die Nachricht wirkt professionell und enthält einen Lebenslauf, Zeugnisse oder ein Anschreiben als Anhang. Häufig besteht zunächst kein offensichtlicher Verdacht.

Beim Öffnen der Datei wird jedoch unbemerkt Schadsoftware ausgeführt. Diese kann beispielsweise Passwörter auslesen, Systeme manipulieren oder den Zugriff auf Daten verschlüsseln. Besonders gefährlich ist dabei, dass Bewerbungen in vielen Unternehmen zum normalen Arbeitsalltag gehören und Anhänge daher regelmäßig geöffnet werden.

Angreifer nutzen gezielt die Neugier und Routine der Mitarbeitenden aus. Teilweise werden Dateinamen verwendet wie:

„Bewerbung_Bilanzbuchhalterin.pdf.exe"

oder manipulierte Microsoft-Office-Dokumente mit eingebetteten Schadfunktionen.

Oft reicht bereits ein einzelner unbedachter Klick aus, um erhebliche Auswirkungen auf den gesamten Betrieb zu verursachen.

Mögliche Risiken

- Infektion mit Schadsoftware oder Ransomware
- Ausfall von Systemen und Arbeitsprozessen
- Verlust oder Verschlüsselung sensibler Daten
- Zugriff auf Informationen zu Kunden und Geschäftspartnern
- Hohe finanzielle und organisatorische Schäden

Wichtiger Hinweis

Dateianhänge sollten grundsätzlich mit besonderer Vorsicht behandelt werden. Technische Schutzmaßnahmen, aktuelle Sicherheitslösungen sowie sensibilisierte Mitarbeitende bilden gemeinsam die wichtigste Verteidigung gegen solche Angriffe.

4.5 Der Besucher vor Ort

Eine freundlich auftretende Person betritt das Unternehmen und gibt sich beispielsweise als Techniker, Paketdienstleister, Handwerker oder externer Dienstleister aus. Oft wirkt die Situation alltäglich und unauffällig.

Der Besucher erklärt, kurzfristig einen Auftrag durchführen zu müssen oder einen Termin mit einer bestimmten Person zu haben. Nicht selten wird dabei auf Zeitdruck verwiesen:

„Ich muss nur kurz in den Technikraum."

Oder:

„Der Termin wurde bereits abgestimmt."

Durch ein selbstbewusstes Auftreten, Arbeitskleidung oder scheinbar glaubwürdige Informationen gelingt es Angreifern häufig, Vertrauen aufzubauen. Mitarbeitende möchten höflich und hilfsbereit reagieren – insbesondere im direkten persönlichen Kontakt.

Genau diese menschlichen Eigenschaften werden beim Social Engineering gezielt ausgenutzt. Bereits wenige Minuten unbeobachteter Zugang können ausreichen, um sensible Informationen einzusehen, Geräte anzuschließen oder interne Bereiche auszuspähen.

Mögliche Risiken

- Unbefugter Zutritt zu sensiblen Bereichen
- Einsicht in vertrauliche Unterlagen oder Bildschirme
- Manipulation oder Anschluss technischer Geräte
- Vorbereitung weiterer Angriffe
- Gefährdung von Kunden- und Unternehmensdaten

Wichtiger Hinweis

Externe Personen sollten niemals unbeaufsichtigt Zugang zu sensiblen Bereichen erhalten. Klare Besucherprozesse, sichtbare Legitimationen und eine aktive Sicherheitskultur helfen dabei, solche Risiken frühzeitig zu erkennen.

5. Die psychologischen Tricks dahinter

Social Engineering funktioniert nicht primär durch technische Schwachstellen, sondern durch gezielte Manipulation menschlichen Verhaltens. Angreifer nutzen dabei psychologische Mechanismen aus, die Teil unseres normalen Arbeitsalltags sind.

Angreifer treffen häufig auf Mitarbeitende, die serviceorientiert, hilfsbereit und lösungsorientiert arbeiten. Genau diese Eigenschaften machen viele Angriffe erst möglich.

Vertrauen

Angreifer versuchen gezielt, Vertrauen aufzubauen. Sie geben sich beispielsweise als Kunden, Behörden oder bekannte Dienstleister aus. Häufig wirken Auftreten, Sprache und Verhalten dabei professionell und glaubwürdig.

Menschen neigen dazu, bekannten oder seriös wirkenden Personen schneller zu vertrauen – insbesondere unter Zeitdruck oder im stressigen Arbeitsalltag.

Zeitdruck

„Es muss sofort erledigt werden."

„Die Frist läuft heute ab."

„Ich benötige die Unterlagen dringend."

Zeitdruck gehört zu den häufigsten Werkzeugen im Social Engineering. Mitarbeitende sollen dazu gebracht werden, schneller zu handeln und bestehende Kontrollmechanismen zu umgehen.

Unter Druck sinkt häufig die Aufmerksamkeit für Warnsignale.

Autorität

Menschen reagieren oft besonders kooperativ auf vermeintliche Autoritäten. Angreifer nutzen dies gezielt aus, indem sie sich beispielsweise als:

- Finanzamt
- Datenschutzbehörde
- Rechtsanwalt
- Kanzleileitung

- IT-Dienstleister
- Geschäftspartner

ausgeben.

Die Angst, Fehler zu machen oder Anweisungen nicht korrekt umzusetzen, erhöht die Wahrscheinlichkeit unüberlegter Handlungen.

Hilfsbereitschaft

Freundlichkeit und Serviceorientierung sind wichtige Bestandteile professioneller Kundenbetreuung. Angreifer nutzen genau diese Eigenschaften aus.

Viele Social-Engineering-Angriffe funktionieren deshalb, weil Mitarbeitende helfen möchten, Probleme lösen wollen oder vermeiden möchten, unhöflich zu wirken.

Routine und Gewohnheit

Wiederkehrende Arbeitsabläufe führen dazu, dass Entscheidungen oft automatisch getroffen werden. Genau darauf setzen Angreifer.

Wenn täglich zahlreiche E-Mails, Anrufe oder Dokumente bearbeitet werden, sinkt die Aufmerksamkeit für kleine Auffälligkeiten.

Angst und Unsicherheit

Drohungen, angebliche Konsequenzen oder formelle Sprache erzeugen Unsicherheit. Menschen treffen unter Stress häufig vorschnelle Entscheidungen – insbesondere dann, wenn sie negative Folgen vermeiden möchten.

Wichtig zu verstehen

Social Engineering kann grundsätzlich jede Person betreffen – unabhängig von Erfahrung, Position oder Fachwissen.

Sicherheitsbewusstsein bedeutet daher nicht Misstrauen gegenüber Geschäftspartnern oder Kollegen, sondern einen professionellen und bewussten Umgang mit sensiblen Informationen und ungewöhnlichen Situationen.

6. Die spezifischen Risiken für sensible Daten und Vertraulichkeit

Je nach Geschäftsfeld arbeiten viele Unternehmen täglich mit besonders sensiblen Informationen. Geschäftspartner vertrauen darauf, dass persönliche, finanzielle und unternehmerische Daten vertraulich behandelt und geschützt werden.

Genau dieses hohe Maß an Vertrauen macht diese Unternehmen zu attraktiven Zielen für Social-Engineering-Angriffe. Bereits einzelne Informationen können für Angreifer von großem Wert sein – insbesondere dann, wenn sie für weitere Betrugsversuche oder gezielte Angriffe genutzt werden können.

Besonders schützenswerte Informationen

Zu den sensiblen Daten gehören unter anderem:

- Steuerunterlagen und Jahresabschlüsse
- Einkommens- und Vermögensdaten
- Bankverbindungen
- Zugangsdaten und digitale Zugänge
- Vertragsunterlagen
- Personaldaten
- Unternehmenskennzahlen
- Informationen zu privaten oder geschäftlichen Verhältnissen

Der Verlust oder die unberechtigte Weitergabe solcher Daten kann erhebliche Folgen haben – sowohl für Kunden als auch für das Unternehmen selbst.

Vertrauensverlust gegenüber Kunden und Geschäftspartnern

Vertrauen ist eine der wichtigsten Grundlagen erfolgreicher Geschäftsbeziehungen. Bereits ein einzelner Sicherheitsvorfall kann dieses Vertrauen nachhaltig beschädigen.

Geschäftspartner erwarten nicht nur fachliche Kompetenz, sondern auch einen professionellen Umgang mit sensiblen Informationen. Sicherheitsvorfälle können daher schnell zu Reputationsschäden führen.

Datenschutzrechtliche Folgen

Die Verarbeitung sensibler personenbezogener Daten unterliegt hohen gesetzlichen Anforderungen. Gelangen Daten durch Social Engineering in falsche Hände, können unter anderem:

- Datenschutzverletzungen
- Meldepflichten
- Haftungsfragen
- oder regulatorische Konsequenzen

entstehen.

Finanzielle Schäden

Social-Engineering-Angriffe können direkte finanzielle Schäden verursachen – beispielsweise durch manipulierte Zahlungsanweisungen, Betrugsfälle oder Betriebsunterbrechungen infolge von Schadsoftware.

Hinzu kommen mögliche Kosten für:

- IT-Forensik
- Wiederherstellung von Systemen
- Rechtsberatung
- Kommunikationsmaßnahmen
- Ausfallzeiten

Auswirkungen auf den Unternehmensbetrieb

Bereits ein einzelner erfolgreicher Angriff kann Arbeitsabläufe erheblich beeinträchtigen. Besonders Ransomware-Angriffe oder kompromittierte Systeme können dazu führen, dass:

- Fristen nicht eingehalten werden
- Unterlagen nicht verfügbar sind
- Kommunikation eingeschränkt wird
- oder der Unternehmensbetrieb zeitweise stillsteht.

Sicherheit als Bestandteil professioneller Unternehmensführung

Der Schutz sensibler Informationen ist heute nicht mehr ausschließlich eine technische Aufgabe. Sicherheitsbewusstsein, klare Prozesse und sensibilisierte Mitarbeitende sind ein zentraler Bestandteil moderner Unternehmenssicherheit.

7. Präventive Maßnahmen: technisch, organisatorisch, menschlich

Ein wirksamer Schutz vor Social Engineering entsteht nicht durch einzelne Maßnahmen allein. Entscheidend ist das Zusammenspiel aus technischen Schutzmaßnahmen, organisatorischen Regelungen und dem bewussten Umgang mit dem Faktor Mensch.

Viele Unternehmen investieren bereits in technische Sicherheitslösungen. Gleichzeitig zeigen zahlreiche Sicherheitsvorfälle, dass Angreifer gezielt den Menschen als vermeintlich schwächstes Glied der Sicherheitskette angreifen.

Deshalb gewinnt ein strukturierter Umgang mit dem sogenannten Human Risk zunehmend an Bedeutung.

Organisatorische Maßnahmen

Klare Prozesse und verbindliche Regeln helfen dabei, Risiken im Arbeitsalltag zu reduzieren.

Dazu gehören beispielsweise:

- definierte Freigabeprozesse
- verbindliche Rückrufverfahren
- klare Besucherregelungen
- Vier-Augen-Prinzipien
- geregelte Zuständigkeiten
- standardisierte Sicherheitsprozesse

Besonders wichtig ist dabei, dass Sicherheitsmaßnahmen praktikabel und verständlich in den Unternehmensalltag integriert werden.

Technische Maßnahmen

Technische Schutzmaßnahmen bilden weiterhin eine wichtige Grundlage moderner Informationssicherheit.

Dazu zählen unter anderem:

- aktuelle Sicherheitssoftware
- Multi-Faktor-Authentifizierung
- E-Mail-Sicherheitslösungen
- Zugriffsbeschränkungen
- Netzwerksegmentierung
- regelmäßige Updates und Datensicherungen

Technik allein kann Social Engineering jedoch nicht vollständig verhindern. Angreifer versuchen häufig, technische Schutzmaßnahmen gezielt über den menschlichen Faktor zu umgehen.

Der Mensch als zentraler Sicherheitsfaktor

Traditionelle Awareness-Maßnahmen bestehen häufig aus allgemeinen Schulungen oder standardisierten Lerninhalten. Diese schaffen zwar Aufmerksamkeit, machen tatsächliche Risiken jedoch oft nur schwer messbar.

Ein moderner Ansatz geht deshalb weiter: Human-Risk-Management.

Dabei wird der Faktor Mensch nicht nur sensibilisiert, sondern systematisch bewertet, gemessen und kontinuierlich verbessert.

Human Risk messbar machen

Ziel eines Human-Risk-Managements ist es, konkrete Sicherheitskennzahlen (KPIs) zu erfassen und daraus gezielte Maßnahmen abzuleiten.

Beispiele für messbare Human-Risk-KPIs:

- Klickrate bei Phishing-Simulationen
- Eingabe von Zugangsdaten
- Melderate verdächtiger Vorfälle
- Reaktionszeit bei Sicherheitsmeldungen

- Verhalten bei Telefonangriffen
- Einhaltung definierter Prozesse
- Ergebnisse physischer Sicherheitsüberprüfungen

Dadurch entsteht erstmals ein objektiver Blick auf den tatsächlichen Sicherheitsstatus im Bereich Mensch und Verhalten.

Maßnahmen mit messbarer Wirkung

Awareness-Maßnahmen sollten nicht isoliert durchgeführt werden, sondern gezielt auf definierte Risiken und KPIs einzahlen.

Das bedeutet:

- Risiken identifizieren
- aktuelle Werte messen
- Ziele definieren
- passende Maßnahmen ableiten
- Veränderungen erneut messen

So entsteht ein kontinuierlicher Verbesserungsprozess anstelle einmaliger Schulungen ohne nachvollziehbare Wirkung. Dadurch können Unternehmen Risiken transparenter bewerten, Fortschritte sichtbar machen und Sicherheitsmaßnahmen gezielt steuern.

8. Sofortmaßnahmen bei Verdachtsfällen

Nicht jeder Social-Engineering-Angriff lässt sich vollständig verhindern. Umso wichtiger ist es, verdächtige Situationen frühzeitig zu erkennen und angemessen darauf zu reagieren.

Schnelles und strukturiertes Handeln kann dabei helfen, Schäden zu begrenzen und weitere Risiken zu vermeiden. Entscheidend ist vor allem, dass Mitarbeitende Verdachtsfälle ernst nehmen und ohne Angst vor Fehlern melden können.

Ruhe bewahren

Social-Engineering-Angriffe arbeiten häufig mit Druck, Unsicherheit oder emotionaler Einflussnahme. Gerade deshalb ist es wichtig, in verdächtigen Situationen bewusst Ruhe zu bewahren und nicht vorschnell zu handeln.

Zeitdruck sollte niemals dazu führen, Sicherheitsprozesse zu umgehen.

Keine sensiblen Informationen herausgeben

Bei Unsicherheiten gilt grundsätzlich:

- keine vertraulichen Informationen weitergeben
- keine Zugangsdaten mitteilen
- keine Zahlungsdaten ändern
- keine unbekannten Anhänge öffnen
- keine spontanen Freigaben erteilen

Im Zweifel sollte eine Anfrage zunächst überprüft werden.

Identitäten aktiv überprüfen

Verdächtige Anrufe oder Nachrichten sollten immer unabhängig verifiziert werden.

Beispiele:

- Rückruf über bekannte Telefonnummern
- Rückfrage bei internen Ansprechpartnern
- Prüfung von E-Mail-Adressen
- Legitimation externer Besucher kontrollieren

Wichtig ist dabei, nicht ausschließlich den Informationen aus der verdächtigen Nachricht zu vertrauen.

Vorfall intern melden

Verdächtige Situationen sollten frühzeitig an die zuständigen Stellen innerhalb des Unternehmens gemeldet werden.

Dazu können beispielsweise gehören:

- Unternehmensleitung
- IT-Verantwortliche
- Datenschutzbeauftragte
- Informationssicherheitsbeauftragte

Frühzeitige Meldungen helfen dabei, mögliche Schäden schneller zu erkennen und weitere Angriffe zu verhindern.

Systeme und Zugänge absichern

Wurde bereits auf einen Angriff reagiert oder versehentlich eine Handlung durchgeführt, sollten umgehend Schutzmaßnahmen eingeleitet werden:

- Passwörter ändern
- betroffene Systeme prüfen
- Zugänge sperren
- IT-Verantwortliche informieren
- verdächtige Dateien isolieren

Je schneller reagiert wird, desto besser lassen sich Folgeschäden begrenzen.

Fehlerkultur statt Schuldzuweisung

Social Engineering zielt gezielt auf menschliches Verhalten ab. Deshalb ist eine offene Sicherheits- und Fehlerkultur besonders wichtig.

Mitarbeitende sollten Verdachtsfälle oder Fehler ohne Angst vor persönlichen Konsequenzen melden können. Nur so können Risiken frühzeitig erkannt und Sicherheitsmaßnahmen verbessert werden.

Vorbereitung schafft Sicherheit

Klare Prozesse, definierte Ansprechpartner und regelmäßige Übungen helfen dabei, im Ernstfall sicherer und strukturierter zu reagieren. Gute Vorbereitung reduziert Unsicherheit und stärkt die Handlungsfähigkeit des gesamten Unternehmens.

9. Eine Checkliste und Handlungsempfehlungen

9.1 Checkliste und Handlungsempfehlungen

Social-Engineering-Angriffe nutzen häufig alltägliche Situationen, Zeitdruck und menschliche Gewohnheiten aus. Eine klare Orientierung im Arbeitsalltag hilft dabei, Risiken frühzeitig zu erkennen und angemessen zu reagieren.

Die folgende Checkliste unterstützt Mitarbeitende dabei, verdächtige Situationen bewusster wahrzunehmen und Sicherheitsprozesse konsequent einzuhalten.

9.2 Checkliste: Verdächtige Situationen erkennen

Am Telefon

- Werden ungewöhnlich viele Informationen abgefragt?
- Wird Zeitdruck aufgebaut?
- Soll eine Sicherheitsregel umgangen werden?
- Wird auf Vertraulichkeit gedrängt?
- Ist die Identität des Anrufers eindeutig geprüft?

Bei E-Mails

- Ist die Absenderadresse korrekt geschrieben?
- Enthält die Nachricht ungewöhnliche Anhänge oder Links?
- Werden kurzfristige Zahlungsänderungen gefordert?
- Wirkt die Nachricht ungewöhnlich dringend?
- Passt die Anfrage zum üblichen Ablauf?

Bei Besuchern vor Ort

- Ist der Besucher angemeldet?
- Liegt eine eindeutige Legitimation vor?
- Wird versucht, unbeaufsichtigt Zugang zu erhalten?
- Besteht ein nachvollziehbarer Grund für den Besuch?
- Werden sensible Bereiche geschützt?

9.3 Handlungsempfehlungen für Mitarbeitende

Sicherheitsprozesse klar definieren

Klare und verständliche Prozesse helfen Mitarbeitenden dabei, auch unter Zeitdruck sicher zu handeln. Dazu gehören unter anderem:

- Rückrufverfahren
- Freigabeprozesse
- Besucherregelungen
- Meldewege bei Verdachtsfällen

Den Faktor Mensch aktiv einbeziehen

Sicherheit sollte nicht ausschließlich technisch betrachtet werden. Mitarbeitende sind ein zentraler Bestandteil der Sicherheitsstrategie und sollten aktiv in Schutzmaßnahmen eingebunden werden.

Risiken messbar machen

Human Risk sollte regelmäßig bewertet und anhand konkreter KPIs messbar gemacht werden. Nur so lassen sich tatsächliche Risiken erkennen und gezielte Verbesserungen ableiten.

Maßnahmen regelmäßig überprüfen

Sicherheitsmaßnahmen sollten kontinuierlich überprüft und weiterentwickelt werden. Angriffsstrategien verändern sich ständig – Sicherheitskonzepte müssen sich entsprechend anpassen.

Eine offene Sicherheitskultur fördern

Mitarbeitende sollten verdächtige Situationen oder Fehler ohne Angst vor Schuldzuweisungen melden können. Eine offene Sicherheitskultur stärkt die Sicherheit des gesamten Unternehmens.

Sicherheit als kontinuierlichen Prozess verstehen

Wirksamer Schutz vor Social Engineering entsteht nicht durch Einzelmaßnahmen, sondern durch einen fortlaufenden Prozess aus:

- Bewusstsein
- Messbarkeit
- gezielten Maßnahmen
- und kontinuierlicher Verbesserung

10. Fazit mit Hinweis auf mögliche weiterführende Unterstützungsangebote

Social Engineering gehört heute zu den größten Risiken für Unternehmen und Organisationen – insbesondere dort, wo mit sensiblen Informationen und hohem Vertrauen gearbeitet wird.

Zentrale und strategisch wichtige Unternehmensbereiche stehen dabei besonders im Fokus, da sie täglich mit vertraulichen Kunden- und Unternehmensdaten umgehen.

Angreifer greifen dabei nicht primär technische Systeme an, sondern gezielt menschliches Verhalten. Vertrauen, Hilfsbereitschaft, Routine und Zeitdruck werden bewusst genutzt, um Sicherheitsmechanismen zu umgehen.

Ein wirksamer Schutz entsteht deshalb nicht allein durch technische Lösungen oder einzelne Schulungen. Entscheidend ist ein ganzheitlicher Ansatz, der technische, organisatorische und menschliche Sicherheitsaspekte miteinander verbindet.

Moderne Sicherheitskonzepte gehen dabei einen Schritt weiter: Sie machen Human Risk messbar, definieren klare Sicherheitsziele und setzen gezielte Maßnahmen dort ein, wo tatsächliche Risiken bestehen. Dadurch wird Sicherheit nicht nur theoretisch vermittelt, sondern nachhaltig steuerbar und überprüfbar gemacht.

Sicherheit ist heute kein einmaliges Projekt, sondern ein kontinuierlicher Prozess. Unternehmen, die frühzeitig in Sicherheitsbewusstsein, klare Prozesse und Human-Risk-Management investieren, stärken nicht nur ihren Schutz vor Angriffen, sondern auch das Vertrauen ihrer Kunden und Geschäftspartner.

Impressum

DATEV eG, 90329 Nürnberg (Verlag)

E-Mail: literatur@service.datev.de