SOCIAL ENGINEERING

Fünf strategische Hebel für mehr Sicherheit im Unternehmen

Worum geht es?

Social Engineering ist kein technisches Problem, es ist ein menschliches. Angreifer nutzen nicht Schwachstellen in Firewalls, sondern Lücken im Verhalten: fehlende Prozesse, Zeitdruck, unklare Zuständigkeiten oder den Reflex, hilfsbereit zu sein. Ein glaubhafter Anruf, eine dringlich klingende Mail, ein „Kollege“ mit Clipboard an der Tür und schon steht der Zugriff offen. Nicht, weil Systeme versagt haben, sondern weil niemand gefragt hat.

Genau hier liegt die Herausforderung für Unternehmen: Wie schafft man eine Sicherheitskultur, in der Menschen sich trauen, zu hinterfragen? In der Fachbereiche erkennen, was riskant wirkt? In der Sicherheit nicht „die Aufgabe der IT“ ist, sondern Teil des Arbeitsalltags?

Was hilft in der Praxis wirklich?

Awareness ist keine reine IT-Aufgabe

Die IT kennt Phishing-Mails. Aber wie sieht es in HR, Finance oder am Empfang aus? Genau dort finden viele Angriffsversuche statt, mit harmlos wirkenden Fragen, gefälschten Mails oder autoritär klingenden Anrufen. Wer nur die IT sensibilisiert,
lässt die Hauptangriffsfläche offen.

📌 **Praxistipp:** Hängt im Eingangsbereich oder der Teeküche einen Hinweis aus „Unbekannte Anfragen? Erst fragen, dann helfen.

Zuständigkeiten bei Verdachtsfällen klären

Was passiert, wenn jemand etwas Seltsames beobachtet oder unsicher ist? Wer nimmt sich Zeit, wenn eine Mail komisch klingt oder jemand am Telefon drängt? Ohne klare Anlaufstelle bleibt der Vorfall im Kopf oder wird intern bagatellisiert. Das schafft Unsicherheit.

📌 **Praxistipp:** Einen festen Kontaktweg einrichten, z. B. ein internes „Security-Postfach“ oder einen Ansprechpartner in der IT.

Psychologie ins Training holen

Klassische Phishing-Schulungen reichen nicht. Social Engineering spielt mit Druck, Hilfsbereitschaft und Unsicherheit. Was passiert, wenn jemand sagt: „Ich hab das mit der Geschäftsleitung abgesprochen. Geben Sie mir bitte direkt Zugang“?

📌 **Praxistipp:** Rollenspiele im Team: Eine Person spielt Angreifer:in, andere reagieren spontan. Danach offen analysieren: Was hat gewirkt? Was war auffällig?

Testen – aber fair

Phishing-Tests, Fake-Anrufe oder Social-Tests an der Tür sind hilfreich, wenn sie gut gemacht sind. Wichtig ist: Es geht nicht um Blaming. Wer reingefallen ist, hat gezeigt, wo das System noch Lücken hat. Das ist ein Gewinn.

📌 **Praxistipp:** Nach einem Test immer Nachbesprechung: Was war der Trick? Was hat funktioniert? Welche Reaktion wäre sinnvoll gewesen?

Fehlerkultur stärken

Social Engineering funktioniert nur dann dauerhaft, wenn niemand sich traut, etwas zu sagen. Wer glaubt, für Unsicherheit oder Rückfragen ausgelacht zu werden, schweigt lieber. Das ist gefährlicher als jede Lücke im Code.

📌 **Praxistipp:** Regelmäßig Teamrunden durchführen, bei denen auch Unsicherheiten besprochen werden dürfen, ohne Bewertung. Das senkt die Hemmschwelle.

Schulungsblatt: Social Engineering erkennen und verhindern

Für alle Mitarbeitenden – Schutz beginnt beim Menschen

Was ist Social Engineering?

Social Engineering ist **menschliche Manipulation** im Kontext der IT- und Unternehmenssicherheit. Statt Firewalls zu knacken, zielt der Angreifer darauf ab, **Mitarbeiter oder Führungskräfte zu täuschen**, um Passwörter, Zugangsdaten, Geldüberweisungen oder sonstige kritische Informationen zu erhalten.

> *Es geht nicht um Technik – sondern darum, wie man dich dazu bringt, einem Angreifer zu vertrauen.*

Typische Angriffsarten:

Angriffsmethode	Beschreibung	Beispiel
Phishing	Gefälschte E-Mails mit Links oder Dateianhängen	"Ihr Passwort läuft ab – bitte hier klicken"
Vishing	Telefonanrufe mit falscher Identität	"Ich bin vom IT-Support – wie lautet Ihr Zugangscode?"
Pretexting	Täuschung durch erfundene Rollen	"Ich bin die neue Buchhalterin vom Steuerberater"
Baiting	Köder wie USB-Sticks, Fake-Webseiten	"Gratis Geschenke – einfach downloaden!"
CEO-Fraud	Falsche E-Mail vom Chef mit Zahlungsaufforderung	"Überweisen Sie 12.000 € noch heute – vertraulich!"

Konkretes Beispiel aus dem Unternehmensalltag:

> *Ein Angreifer ruft im Unternehmen an und gibt sich als IT-Techniker aus. Er behauptet, er müsse ein Sicherheitsupdate aufspielen – und bittet um das aktuelle Passwort oder Remote-Zugriff. Ein gutgläubiger Mitarbeiter folgt der Anweisung – und der Angreifer hat Zugang zum System.*

Warum ist Social Engineering gefährlich für Unternehmer?

- **Technik allein reicht nicht:** Selbst mit bester IT-Security kann ein einzelner Klick auf einen Link oder ein falsch geführtes Gespräch großen Schaden anrichten.
- **Vertrauen wird ausgenutzt:** Menschen handeln oft im Sinne von Hilfe, Respekt oder Autorität – genau das nutzt der Angreifer aus.
- **Schäden sind oft immens:** Datendiebstahl, Rufschädigung, Geldverlust, Betriebsstillstand, Rechtsfolgen.

Was Unternehmer tun können:

1. **Mitarbeiterschulung**: Regelmäßige Awareness-Trainings zu Erkennungsmerkmalen von Social Engineering.
2. **Sicherheitsprozesse**: Klare Regeln für Datenweitergabe, Passwortvergabe, Zahlungsfreigaben.
3. **Technische Unterstützung**: Zwei-Faktor-Authentifizierung, eingeschränkte Berechtigungen.
4. **Kultur der Vorsicht**: Keine Angst vor „dummen Fragen“ – lieber ein Kollege zu viel gefragt, als einmal vertrauliche Daten preisgegeben.

> *Es geht nicht um Technik – sondern darum, wie man dich dazu bringt, einem Angreifer zu vertrauen.*

Checkliste

Beim Umgang mit E-Mails:

- ☐ Absenderadresse genau prüfen (nicht nur den Namen!)
- ☐ Keine Anhänge oder Links aus unbekannten Quellen öffnen
- ☐ Bei Druck („dringend“, „vertraulich“) besonders wachsam sein
- ☐ Niemals Passwörter oder PINs per E-Mail weitergeben

Beim Telefon:

- ☐ Niemals sensible Infos am Telefon weitergeben – auch nicht an „IT“, „Chef“ oder „Kollege“
- ☐ Rufnummer unbekannt? Rückruf über bekannte Firmenzentrale veranlassen
- ☐ Gespräch notieren und verdächtige Fälle sofort melden

Vor Ort:

- ☐ Fremde Personen niemals unbeaufsichtigt lassen
- ☐ Keine fremden USB-Sticks oder Geräte anschließen
- ☐ Zutritt nur mit Ausweis oder Absprache

> *"Vertrauen ist gut – Absichern ist besser."*
> *"Wenn du unsicher bist, frag nach!"*
> *"Lieber einmal zu viel melden als einmal zu wenig!"*

Meldestelle im Unternehmen

Verdacht auf Social Engineering? Melde dich sofort bei:

IT-Sicherheit / Datenschutzbeauftragte:r _____

Telefon _____

Mail _____