# Social Engineering

## Das Wichtigste in Kürze

Social Engineering ist eine Methode der Informationsbeschaffung, deren Ziel es ist, Menschen so zu manipulieren, dass sie Zugriffe erlauben, vertrauliche und sensible Daten preisgeben, Informationen teilen oder Geldsummen bewegen. Beim Social Engineering werden keine Systeme gehackt oder Firewalls (System, das ein Netzwerk oder einen Computer vor unerwünschtem Zugriff über das Internet schützt) durchbrochen, denn es ist der Mensch selbst, der «aus eigenem Willen» Informationen preisgibt oder eine Handlung ausführt. Social Engineering geschieht sowohl in der analogen, realen Welt, also in der direkten Begegnung mit Personen, wie auch in der digitalen Welt, wenn man online kommuniziert (E-Mails).

Manipulative Methoden der Informationsbeschaffung gibt es schon seit Anbeginn der menschlichen Zivilisation, heute wird der Begriff «Social Engineering» jedoch meistens im Kontext von digitalem Betrug im Internet verwendet. Wir sind über das Internet und soziale Medien stark vernetzt und es kommt vor, dass uns unbekannte Personen auf diesen Kommunikationskanälen kontaktieren.

## Social Engineering im Finanzsektor

Die Digitalisierung macht die meisten Prozesse innerhalb des Finanzsektors komplexer. Kundinnen und Kunden sind sich der einzelnen Prozessschritte nicht unbedingt bewusst und können so leicht Opfer von Social Engineering werden. Für Social Engineers ist es besonders verlockend, ihr Manipulationsglück bei Kundinnen und Kunden von Finanzinstituten (Banken, Versicherungen) zu versuchen, da dort ggf. Geldsummen bewegt werden.

## Wie funktioniert Social Engineering?

Social Engineers bauen sich eine falsche Identität anhand der gesammelten Informationen über das Opfer auf, sodass sie legitim genug wirken. Je nach dem, was sie von der Person berauben wollen, spielen sie eine andere Rolle. Dies kann von einem Bekannten oder Bankangestellten, bis hin zum Handwerker variieren. Ohne einen direkten Kontakt herzustellen, benutzen sie oft Kommunikationsmittel wie Telefon, E-Mail oder SMS. Um das Vertrauen der Menschen für sich zu gewinnen, achten die Engineers auf mehrere Aspekte, um typische menschliche Verhaltensmuster nachzuahmen: Sie geben sich als besonders nett und freundlich aus oder treten auf Autoritätsperson auf, deren Anweisungen zu folgen gilt. Sie sagen, dass sie ein dringendes Anliegen haben oder fordern, dass etwas unbedingt und rasch erledigt werden sollte.

## Einige Beispiele:

**Phishing (von engl. «to phish», Deutsch: etw. abfischen):**
Mit sogenannten Phishing-E-Mails versuchen Social Engineers, an Passwörter zu gelangen oder Viren / Malware (Schadprogramme) zu verbreiten. Die E-Mail könnte bspw. ein verlockendes Angebot, eine gefälschte Rechnung oder eine Update-Aufforderung enthalten. Damit wollen die Social Engineers eine

sofortige Handlung erzielen, bspw. dass du Informationen preisgibst, einen Link anklickst oder einen gefährlichen Mail-Anhang öffnest.

Phishing kann auch per SMS oder per Anruf geschehen. Bei SMS spricht man von «Smishing», bei Anrufen von «Vishing».

**Baiting (von engl. «to bait», Deutsch: ködern):**
Der Köderangriff: Hier versucht der Angreifende, das Opfer mit einem Köder zu locken und hofft auf die Neugierde oder auch Gier des Opfers. Der Angreifende setzt einen physischen oder digitalen Köder ein, hinter dem sich in der Regel Malware (Schadprogramm) verbirgt. Es kann sich dabei bspw. um einen USB-Stick mit scheinbar interessanten Inhalten oder um einen Download-Link handeln, der zu einer coolen Software führen soll.

**Pretexting (von engl. «pretext», Deutsch: Vorwand):**
Der Angreifende zielt darauf ab, Zugang zu sensiblen Daten oder geschützten Systemen zu erlangen. Er beginnt damit, Vertrauen aufzubauen, indem er sich als vertrauenswürdige Person darstellt und sich eine ausgefeilte Geschichte überlegt. Die angreifende Person gibt sich bspw. als Mitarbeiter, Mitarbeiterin eines Grossunternehmens, als Polizist, Polizistin oder als Bankangestellter, Bankangestellte aus. Er mag Fragen stellen, die angeblich notwendig sin, um die Identität des Opfers zu bestätigen, doch eigentlich geht es ihm nur darum, möglichst viele Daten und Informationen über das Opfer zu sammeln (bspw. unternehmensinterne Informationen, persönliche Angaben, Bankunterlagen oder Sicherheitsinformationen). Achtung: Dies kann auch im direkten Kontakt mit einer Person passieren, nicht nur online, via E-Mail oder Telefonanruf.

**CEO-Betrug:**
Du erhältst eine scheinbar legitime E-Mail von deinem Chef (CEO, von engl. «Chief Executive Officer»), in welcher du aufgefordert wirst, einen Auftrag für ihn auszuführen oder ihm einen Gefallen zu tun. In der E-Mail gibt sich die Person extra als Autoritätsperson (eben als Firmenchef/CEO) aus. Menschen tendieren dazu, einen Auftrag, der von einer Autoritäts-/Respektperson kommt, eher auszuführen, auch wenn sie dabei gegen Regeln verstossen oder gegen ihren eigenen Willen handeln. Wenn der Zeitdruck hoch ist und die Dringlichkeit klar gemacht wird, wird das rationale Denken noch mehr vernachlässigt. Dies vorweg: Antworte niemals auf eine solche E-Mail, klicke nicht auf den darin enthaltenen Link und öffne den Mail-Anhang nicht!

## Schutzmassnahmen vor Social Engineering

Social Engineers nutzen menschliche Eigenschaften, nicht technische Schwachstellen aus. Ein Unternehmen kann also eine vollständig und optimal gesicherte IT-Infrastruktur (Netzwerk, Server) haben und trotzdem schaffen es Betrügerinnen und Betrüger, an Daten von Kundinnen und Kunden zu gelangen. Wie kannst du dich also vor Social Engineering schützen?

- Prüfe alle Kontaktaufnahmen und Nachrichten kritisch (E-Mail, Anrufe, SMS)! Gut möglich, dass du den Namen des Absenders, der Absenderin kennst. Überprüfe in diesem Fall die E-Mail-Adresse und Telefonnummer genau! Ist die E-Mail wirklich von der Person, die du glaubst, zu kennen? Oder versteckt sich eine merkwürdige E-Mail-Adresse im Absender-Feld?
- Gib deine Zugangsdaten (Passwörter, Vertragsnummern, Sicherheitscode) nie weiter und achte darauf, dass dir beim Eintippen eines Passwortes niemand zuschaut!
- Klicke nie auf Links in E-Mails oder SMS, die dir verdächtig vorkommen! Öffne keine Anhänge!

- Falls du per E-Mail oder SMS zu einer Zahlung aufgefordert wirst, prüfe die Anfrage sorgfältig mit dem Empfänger, der Empfängerin und kontaktiere ihn, sie über die offizielle Telefonnummer!
- Achte darauf, dass deine Geräte und deine Software immer auf dem neuesten Stand sind!
- Wähle sichere Passwörter!
- Mache Sicherheitskopien / Back-ups von wichtigen Dateien!
- Besuche nur vertrauenswürdige Webseiten! Wenn «https://» vor der Webadresse (URL) steht, handelt es sich um eine eher sichere Webseite.
- Bei diesen und ähnlichen Betreffzeilen in E-Mails solltest du vorsichtig sein: «Passwort-Überprüfung sofort erforderlich», «Problem mit Ihrem Bankkonto», «Letzte Erinnerung: Bitte antworten Sie sofort», «Ihre Bestellung bei Amazon.com». Gut möglich, dass diese E-Mails in englischer Sprache bei dir eintreffen. Sei umso vorsichtiger bei Betreffzeilen wie «Urgent request» etc.

## Quellen

Etzemüller, Thomas (2017): Social engineering, Version: 2.0, in: Docupedia-Zeitgeschichte, http://docupedia.de/zg/Etzemueller_social_engineering_v2_de_2017 DOI: https://doi.org/10.14765/zzf.dok.2.1112.v2, [22.11.22].

Fox, Dirk (2014): Social Engineering im Online-Banking und E-Commerce, in: Datenschutz und Datensicherheit – DuD 38, 325–328, https://link.springer.com/article/10.1007/s11623-014-0119-4, [22.11.22].

Meinert, Monica (2016): Social engineering: the art of human hacking, in: ABA Banking Journal, 108(3), 49–49.

Raiffeisen (2022): Sicherheit im E-Banking. So schützen Sie sich vor Betrügern, online zugänglich: https://www.raiffeisen.ch/rch/de/privatkunden/e-banking/sicherheit-im-e-banking/verhaltenstipps.html, [22.11.22].

Tetri, Pekka und Vuorinen, Jukka (2013): Dissecting Social Engineering, in: Behaviour & information technology 32.10, 1014–1023, DOI:10.1080/0144929X.2013.763860, [22.11.22].