Social Engineering: Psychologie der Täuschung

Die „Schwachstelle Mensch“ zu knacken, ist meist einfacher als gut gesicherte Netzwerke zu hacken: Um an Information oder Geld zu gelangen, setzen Betrüger auf psychologische Tricks, die nicht nur naive Gemüter manipulieren.

Spiel mit Emotionen
Wer den Begriff zum ersten Mal hört, denkt bei Social Engineering oder angewandter Sozialwissenschaft vermutlich an positive Gestaltung des Zusammenlebens. Dem Philosophen Karl Popper schwebte tatsächlich vor, gesellschaftliche Strukturen zu verbessern, als er den Ausdruck 1945 prägte. Heute ist „Social Engineering“ ein Instrument der „Verführung“, das Eigenschaften wie Neugierde, Stolz, Hilfsbereitschaft oder Unerfahrenheit, aber auch die Angst vor Konflikten oder angedrohten Konsequenzen geschickt nutzt und gekonnt Köder auslegt. **Mit viel Raffinesse werden Menschen dazu gebracht, etwas zu tun, was sie normalerweise nicht tun würden.** Die Methoden sind vielseitig und keineswegs auf technische Netzwerke beschränkt. Im Überblick über die wichtigsten „Betätigungsfelder“ erfahren Sie, wie Social Engineering funktioniert und wie Sie sich schützen.

⇒ **Druckmittel Telefon**
Gratulation, Sie haben gewonnen! Eine sympathische Stimme teilt Ihnen mit, dass Sie das große Los gezogen haben. Leider fehlen noch einige Angaben, um den Betrag auszuzahlen bzw. den Betrug perfekt zu machen.

Auch in Unternehmen „bewährt“ sich das Telefon: Ein angeblicher Support-Mitarbeiter will ein Problem rasch beheben und benötigt dazu die Routerkonfiguration … Ein Journalist benötigt dringend Informationen zur Fertigstellung eines für die Firma wichtigen Beitrags … Ein Bekannter des Chefs bittet um Auskunft und beruft sich auf höhere Stellen … Oder eine gestresste Mutter ruft an, um sich für den Account ihres Mannes zu registrieren, während im Hintergrund ein Baby vom Band weint … In solchen Notsituationen will man doch schnell helfen!

Die Überrumpelung am Telefon basiert auf psychologischer Schulung: Falsche Tatsachen und Identitäten werden vorgetäuscht, Autoritäten und enormer Zeitdruck vorgeschoben, zudem wird an Verständnis und Mitgefühl appelliert – oder an die Angst, etwas falsch zu machen, sollte man Aufforderungen nicht Folge leisten.

⇒ **E-Mail im Visier**
Beim Versand von Spam-Mails mit „rührenden“ Spendenaufrufen oder Phishing-Absichten können Trickbetrüger mit genügend Opfern rechnen, die „ins Netz“ gehen. Auch ganz gezielt wird gefischt: Die attraktive Russin, die in den Westen reisen möchte, ist nur ein Fake, doch in Erwartung einer Liebesbeziehung lassen sich Männer verleiten, Geld zu schicken oder weiterzuleiten, verlieren ihr gesamtes Vermögen oder beteiligen sich unwissentlich an Geldwäscherei…

Vorsicht auch bei Botschaften, die **neugierig machen**: Der vorschnelle Klick auf E-Mail-Anhänge aktiviert eine Schadsoftware, die Zugriff auf das System gewährt. Oft führen angefügte Links auf gefälschte Websites, die Passwörter oder Kundennummern abfragen.

⇒ **Tatort Internet**
Schadprogramme fordern von verängstigen Internet-Nutzern die Einzahlung von Geldbeträgen zur Behebung von Störungen, doch wie geraten sie auf den Computer? Beispielsweise durch den Hinweis, dass er gehackt wurde: Solche – täuschend echte – Warnungen auf Websites, in Pop-up-Fenstern oder als Browsermeldung erzeugen Panik; doch erst die **empfohlenen Abwehrmaßnahmen** führen zum Download eines Trojaners und zum tatsächlichen Hackerangriff. Häufig werden Logos oder Namen verwendet, die leicht mit seriösen Partnern oder Produkten zu verwechseln sind: Hat man im Vertrauen auf die zuverlässige Quelle eine „Scareware“ installiert, hat man auch die Probleme! Wenn auf Ihrem Gerät ein kostenloses Antivirenprogramm läuft, animieren fiktive Virenwarnungen mitunter zum Kauf der Vollversion.

⇒ **Risiko Umfeld**
Social Engineering macht auch vor Ihrer Umgebung nicht Halt. Liegen im Büro Ausdrucke oder Ordner offen herum, können Besucher, Kunden, Sicherheits- oder Reinigungspersonal darauf zugreifen. Diskutieren Kollegen im Wirtshaus lautstark Geschäftsentwicklungen oder Arbeitsprozesse, sitzen am Nebentisch vielleicht Lauscher, oder sie verfolgen in der U-Bahn Handygespräche mit. Haben Sie in Netzwerken arglos Informationen gepostet? Sie erlauben Betrügern das **Vortäuschen von Insider-Wissen** oder helfen, Manipulationen in eine glaubwürdige Geschichte zu verpacken. Die oft aufwändige Recherche von Social Engineering „Experten" erstreckt sich mitunter sogar auf den Müll, der durchwühlt wird, um Rückschlüsse auf Verhalten und Interessen ihrer Opfer zu ziehen. Manche Betrüger setzen auf Zeit, **erschleichen sich allmählich das Vertrauen** von Wissensträgern und erhalten schließlich jene Informationen, auf die sie es abgesehen haben.

Vorsichtsmaßnahmen
Gesunde Skepsis und gesunder Menschenverstand sind die wichtigsten Abwehrmechanismen gegen Social Engineering:

- Geben Sie weder am Telefon noch per Mail Daten oder scheinbar harmlose Informationen preis bzw. überprüfen Sie unbekannte Absender oder Anrufer – die Nummer für einen Rückruf sollte aus einer unabhängigen Quelle stammen.
- Sperren Sie den Bildschirm beim Verlassen Ihres Arbeitsplatzes und lassen Sie keine Dokumente auf Ihrem Schreibtisch liegen.
- Verwenden Sie sichere Passwörter, die nur Sie kennen, wechseln Sie Codes häufig und notieren Sie Ihre Zugangsberechtigung nicht unter der Tastatur!
- Befolgen Sie keine unüblichen Aufforderungen ohne Rückfrage, machen Sie keine Eingaben in E-Mail-Links, öffnen Sie keine suspekten Anlagen.
- Teilen Sie private Inhalte nicht mit jedermann in sozialen Medien und bleiben Sie mit Ihren Auskünften vorsichtig gegenüber Betriebsfremden.

Mit anderen Worten: **Bleiben Sie wachsam!**