Social Engineering

Mirjam Loewe-Baur

Psychologische Aspekte und Prävention

Herr Glaubegut sitzt am Freitagabend an seinem Arbeitsplatz im Sekretariat einer Grossbank. Bald ist Wochenende. Es scheint ruhig, bis das wichtige E-Mail des Vorgesetzten von Herrn Glaubegut reinflattert. DRINGEND, bitte die Zahlung an einen externen Partner über CHF 23'000.00 noch heute freigeben. Wird gemacht und dann ab ins Wochenende! Am kommenden Montag stellt sich leider heraus, dass der Vorgesetzte von Herrn Glaubegut nichts von seinem Auftrag weiss – sowohl das E-Mail als auch die darin vorhandenen Kontoangaben wurden von einem Social Engineer manipuliert und gesteuert. Herr Glaubegut wurde Opfer[1] eines CEO-Betruges. Nie hätte er gedacht, dass ihm dies passieren könnte! Bei genauer Betrachtung des E-Mails hätte man die Fälschung erkennen können. Herr Glaubegut schämt sich zutiefst für sein Versehen und wird sich hüten, anderen Mitarbeitenden vom Erlebten zu erzählen.

Das kurze Einstiegsbeispiel soll verschiedene Facetten des Phänomens Social Engineering aufzeigen, die für die Prävention relevant sind und in diesem Beitrag thematisiert werden. Neben der Beschäftigung mit der Begrifflichkeit «Social Engineering» wird insbesondere auf die psychologischen Aspekte eingegangen, ohne deren Verständnis, so die These, Prävention nicht greift.

I. Was ist Social Engineering?

Social Engineering ist weder ein Straftatbestand noch existiert eine allgemeingültige Definition des Phänomens. Die Melde- und Analysestelle MELANI beschreibt Social Engineering Angriffe dahingehend, dass die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen ausgenutzt wird, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Aktionen, wie beispielsweise zum Kauf eines Produktes oder, wie in unserem Einstiegsbeispiel zur Freigabe von Finanzmitteln, zu bewegen (Social Engineering, Stand 28.10.2016, siehe: https://www.melani.admin.ch/melani/de/home/themen/socialengineering.html).

Gehackt wird demnach nicht wie einst das technische System, sondern die menschliche Psyche. Diese Verschiebung ist unter anderem auf den technologischen Fortschritt der IT-Systeme zurückzuführen. Während die Systeme immer sicherer werden, bleibt der Mensch mit seinen grundlegenden Eigenschaften wie Vertrauen, Autoritätsgläubigkeit oder Angst weiterhin für gezielte Manipulationen angreifbar. Dies gelingt der Täterschaft insbesondere, jedoch nicht nur, im Cyberspace, da dieser die

1 Im vorliegenden Beitrag wird der kriminologische Opfer-Begriff verwendet, welcher weiter gefasst ist als der Opfer-Begriff im juristischen Sinn.

grösstmögliche Anonymität bietet.[2] Um die Vielschichtigkeit von Cyber-Phänomenen mit Bezug zu Social Engineering aufzuzeigen, werden nachfolgend jene Cybercrime-Phänomene aufgelistet, bei welchen Social Engineering gemäss Einschätzung der Autorin eine besonders grosse Rolle spielt.

	Kurzbeschrieb
Phishing	Unbefugtes Erhältlichmachen von persönlichen Daten mit dem Ziel unbefugter finanzieller Bereicherung.
Romance Scam	Vortäuschen einer Liebesbeziehung um Geld zu erhalten, «Heiratsschwindel» der Neuzeit.
Sextortion	Erpressen von Geld mittels vorhandener oder angeblich vorhandener Nacktaufnahmen.
CEO-Betrug	Als angeblicher Vertreter einer Firma zur Geldüberweisung auf ein ausländisches Konto verleiten.
Money-Mule	Weiterleiten von Geld oder Ware durch Dritte (Geldwäscherei).
Betrügerischer technischer Support	Betrug, bei dem die Täter die potenziellen Opfer anrufen und sich als technische Supporter (z.B. Microsoft-Techniker) ausgeben. Übernehmen der Kontrolle über den Computer und finanzielle Bereicherung durch kriminelle Handlungen am Computer.
Falsche Immobilienanzeigen	Publikation falscher Immobilienanzeigen, Verlangen von Vorauszahlungen für fiktive Immobilien.

2 Beispiele für Social Engineering im analogen Bereich sind der Telefonbetrug (besser bekannt als Enkeltrickbetrug) oder der Heiratsschwindel.

Problematisch ist, dass betroffene Personen unzulässig agieren, indem sie durch ihr Handeln einen Schaden verursachen. Wird bekannt, dass eine Person manipuliert und dadurch ein Schaden generiert wurde, wird in der Praxis leider häufig die getäuschte Person und nicht etwa der dahinterstehende Social Engineer verantwortlich gemacht. Zumindest wird dem Getäuschten eine Mitverantwortung zugeschrieben. Dies mag damit zusammenhängen, dass der Social Engineer in praktisch allen Fällen unbekannt bleibt – die Strafverfolgung stösst in diesem Bereich rasch an ihre Grenzen. Umso wichtiger ist Prävention. Das Verständnis dafür, weshalb wir Menschen anfällig für Social Engineering Angriffe sind und wie sich Opfer nach einem Angriff fühlen, ist Voraussetzung für eine effektive Prävention.

II. Psychologische Mechanismen des Social Engineerings

A. Weshalb werden wir Opfer?

Im Bereich der IT-Security wird bereits seit Jahren intensiv Prävention betrieben. Die meisten Personen wissen beispielsweise, dass es Phishing-Mails gibt und reagieren richtig, wenn sie ein entsprechendes E-Mail erhalten. Selbst immer professioneller werdende Phishing-Mails vermögen uns in den meisten Fällen nicht zu täuschen. Die ständige Wiederholung von Awareness-Programmen ist eine wichtige Grundlage dafür, dass wir sensibilisiert sind und richtig handeln. Und trotzdem gibt es sie: Personen, die trotz Wissen um Angriffe in die Falle von Social Engineers tappen. Aus einer psychologischen Sicht kann dies damit zusammenhängen, dass wir Menschen Informationen auf zwei unterschiedliche Arten verarbeiten: Entweder unbewusst oder bewusst. Dieser Ansatz wurde durch den Psychologen und Nobelpreisträger Daniel Kahneman begründet. In seinem berühmten Buch «Schnelles Denken, langsames Denken» legt er dar, welche Charakteristika für welches Denksystem gelten.

Kognitives System 1	Kognitives System 2
• Unbewusst • Automatisch • Schnell • Mühelos • Ohne willentliche Steuerung	• Bewusst • Kontrolliert • Langsam • Anstrengend • Willentliche Steuerung

Kahneman (2014) geht davon aus, dass der Mensch, wenn immer möglich, die unbewusste automatische Strategie nutzt, da die bewusste Verarbeitung von Informationen sehr anstrengend ist. Gerade wenn mehrere Informationen gleichzeitig auf ihn einwirken, ist eine parallele Verarbeitung kaum möglich. Anhand eines einfachen Beispiels wird dies deutlich: Man versuche *gleichzeitig* die Rechenaufgabe 14x72 zu lösen und eine E-Mail zu lesen (und sich deren Inhalt zu merken!). Praktisch unmöglich, da beide Aufgaben über das bewusste kognitive System laufen. Wie sieht es aus, gleichzeitig dieselbe Rechenaufgabe zu lösen und dabei einen Stapel Papier nach Farben zu sortieren? Das klappt ganz mühelos, da das Papier Sortieren unbewusst ablaufen kann. Je mehr Informationen auf uns einprallen, desto schwieriger wird die bewusste Verarbeitung von Informationen. Die Social Engineers zählen auf den unbewussten schnellen Verarbeitungsweg: So sollen beispielsweise (Phishing-)Mails noch kurz vor dem Wochenende oder neben einer anderen Bürotätigkeit bearbeitet werden. Wäre Herr Glaubegut auch Opfer geworden, wenn das E-Mail am Montagmorgen angekommen und der Vorgesetzte im Büro nebenan gewesen wäre? Die Wahrscheinlichkeit, dass Herr Glaubegut das E-Mail auf dem bewussten Informationsweg verarbeitet hätte und misstrauisch geworden wäre, wäre sicherlich grösser. Der Fakt, dass unsere Gesellschaft einer zunehmenden Informationsflut über unterschiedliche digitale Kanäle ausgesetzt ist, mag zudem dazu beitragen, dass Informationen vermehrt automatisch und unbewusst verarbeitet werden und somit eine grössere Anfälligkeit für Social Engineering Angriffe besteht. Social Engineers leiten ihre Opfer zudem bewusst auf den schnellen Verarbeitungsweg, indem sie eine Dringlichkeit vorgeben. So enthalten die meisten Phishing-Mails eine Art Deadline (beispielsweise soll eine Zahlung noch am selben Tag ausgeführt werden, damit ein Schaden verhindert werden kann). Auch recherchieren Social Engineers teilweise Informationen über ihre potentiellen Opfer, um die eigene Glaubwürdigkeit zu erhöhen. Dies können Informationen über ein Unternehmen, recherchiert über die Webseite des Unternehmens, oder auch einzelne Personen, recherchiert über soziale Netzwerke, sein. An dieser Stelle soll darauf hingewiesen werden, dass neben dem dualen Erklärungsansatz mittels des Modells von Kahneman selbstverständlich andere Erklärungen für eine Opferwerdung denkbar sind. So scheint es beispielsweise naheliegend, dass Personen mit einem hohen Ausmass an Hilfsbereitschaft und Vertrauen besonders vulnerabel sind.

B. Was wird bei den Betroffenen ausgelöst und was sind die Konsequenzen daraus?

Betroffene von Social Engineering sehen sich selber eher als Täter denn als Opfer. Schliesslich hat man selbst einen Fehler begangen, allenfalls gegen die Sicherheits-Policy des eigenen Unternehmens verstossen, vertrauliche Informationen preisgegeben oder einen hohen Schaden verursacht.

Diese Reaktion ist verständlich, jedoch aus Präventionssicht fatal: Ohne die Offenheit der Betroffenen können sich die Unternehmen nicht gegen Social Engineering immunisieren. Was steckt hinter dem Verhalten? Die Betroffenheit von Social Engineering löst bei den meisten

Als betroffene Person ist man Täter und Opfer zugleich.

Personen Scham aus – ein Gefühl der starken Verletzlichkeit, der Überzeugung, etwas falsch gemacht zu haben und infolgedessen negativen oder zumindest unangenehmen Konsequenzen ausgesetzt zu werden. Negative Konsequenzen können beispielsweise die Stellungnahme gegenüber den Vorgesetzten, die verständnislosen Blicke der Arbeitskollegen oder schlimmstenfalls die Angst vor einer Kündigung sein. Auch bei Angriffen auf den privaten Bereich einer Person (beispielsweise dem Phänomen Sextortion: Der Erpressung mittels vom Opfer überlieferter Nacktbilder) steht die Scham und Angst, vor Bekannten das Gesicht zu verlieren, im Zentrum. Als Konsequenz schweigen die Opfer. Die fehlende Auseinandersetzung mit der Opferwerdung führt zeitweise zu erheblichen psychischen Belastungen und insbesondere zur fehlerhaften Meinung, das einzige Opfer zu sein.

III. Betroffenheit von Social Engineering und Cyber-Angriffen

Wie sieht die Lage jedoch tatsächlich aus? Da Social Engineering Angriffe selten angezeigt werden, stellen die Hellfeld Daten keine verlässlichen Quellen dar. Eine im Auftrag unterschiedlicher nationaler Akteure im Bereich der IT-Sicherheit und durch das Markt- und Sozialforschungsinstitut GFS (2019) durchgeführte Befragung der Deutsch- und Westschweizer Bevölkerung zum Thema Sicherheit im Internet zeigt auf, dass rund jede siebte Person bereits einmal von Cyberangriffen betroffen war. Aus den Angriffen resultierten finanzielle Schäden, relevante Aufwände für die Schadensbereinigung oder emotionale Belastungen. Paradoxerweise geben aber mehr als die Hälfte der von einem Angriff betroffenen Personen an, ausreichend hinsichtlich präventiver Massnahmen sensibilisiert zu sein. Dieser Widerspruch zur Schadenrealität könnte darauf hinweisen, dass sich Betroffene zu wenig mit den Gründen ihrer Opferwerdung auseinandersetzen bzw. sich nicht überlegen, *weshalb* sie in der Situation unachtsam waren.

Im Rahmen der Befragung wurde zudem das Sicherheitsgefühl bzgl. Verhalten im Internet erfragt und in Relation zum Informationsgrad gesetzt. Auch hier ergibt sich eine Diskrepanz: Gut zwei Drittel der Personen mit tiefem Informationsgrad fühlen sich trotzdem sicher, während sich gut jede zehnte Person mit hohem Informationsgrad unsicher fühlt. Informationsgrad und Sicherheitsgefühl verlaufen demnach nicht, wie man annehmen könnte, gleichförmig.

Gerade was Verhaltensregeln betrifft, deckt die Befragung grosses Verbesserungspotential auf: So verwendet die Hälfte der Internetnutzerinnen und -nutzer überall oder mehrfach das gleiche Passwort. Auch wird als bekannteste und am häufigsten angewendete Schutzmassnahme eine technische Lösung, nämlich die Benutzung eines Antivirenprogrammes, genannt. Aus Präventionssicht eine besondere Herausforderung ist das Desinteresse der Befragten bzgl. Informationen: Nicht einmal die Hälfte der Befragten wünscht sich, besser über die Sicherheit im Internet informiert zu werden.

> Das Problem ist: IT-Sicherheit interessiert den Bürger nicht.

IV. Learnings für die Präventionsarbeit

Wie kann die Bevölkerung vor dem Hintergrund dieser herausfordernden Ausgangslage geschützt werden? Vielversprechend scheint ein dreistufiger Ansatz: Der *Primärprävention*, das heisst der flächendeckenden Sensibilisierung, kommt eine zentrale Rolle zu. Dabei bilden technische Präventionsmassnahmen wie der Einsatz eines Antivirenprogrammes wohl eine notwendige, jedoch keineswegs hinreichende Voraussetzung. Prävention muss auf das Verhalten der Personen Einfluss nehmen können.

Freilich handelt es sich hier um einen sehr herausfordernden Ansatz, dessen konkrete Massnahmen erprobt und evaluiert werden müssen. Zentral scheint es, im Rahmen von wiederkehrenden Awareness-Programmen wenige, jedoch wirksame Präventionsbotschaften zu platzieren, welche einen Grundschutz gewährleisten. Der Security Spickzettel der globalen Initiative *Stop Think Connect* nennt beispielsweise die folgenden fünf Punkte:

1. *Datensicherung:* Eine Kopie aller Daten erstellen und diese auf einer externen Festplatte speichern.
2. *Updates installieren*: Auf allen Geräten die aktuellsten Sicherheitsupdates installieren.
3. *Starke Passwörter*: Unterschiedliche Passwörter mit mindestens 10 Zeichen wählen.
4. *Realitätscheck*: Misstrauisch bei verführerischen Angeboten und dringenden Anfragen sein.
5. *Hilfe*: Bei Verdacht auf einen Angriff oder eine Infizierung professionelle Hilfe holen.

Wer diese fünf Tipps befolgt, ist bereits gegen eine Vielzahl von Angriffen geschützt. Hätte Herr Glaubegut beispielsweise Punkt 4 beachtet, nämlich misstrauisch bei dringenden Anfragen zu sein, hätte er das E-Mail womöglich genauer überprüft oder sich bei seinem Vorgesetzten rückversichert, bevor er die Zahlung ausgelöst hätte. Damit das Interesse an Präventionsbotschaften geweckt werden kann, ist es neben ihrer wiederholten Darstellung wichtig, Betroffenheit zu schaffen. Es soll beispielsweise aufgezeigt werden, dass Personen jeden Alters und jeden Bildungsstandes betroffen sind. Ziel soll es sein, Personen dahingehend zu sensibilisieren, dass sie relevante Informationen über das bewusste kognitive System verarbeiten, das heisst, dass eine tatsächliche Auseinandersetzung mit der Thematik stattfindet. Bei der Ausarbeitung von Awareness-Programmen ist es zwingend, werbe- und motivationspsychologische Erkenntnisse einzubeziehen.

Auf einer zweiten Stufe sollen Angebote für besonders vulnerable Personengruppen geschaffen werden (*Sekundärprävention*). Während Jugendliche in Schulen und arbeitstätige Erwachsene in Unternehmen zumindest relativ flächendeckend sensibilisiert werden können, ist der Zugang zu älteren Personen sehr eingeschränkt. In der Praxis zeigt sich, dass sich gerade diese Personengruppe sehr wenig mit IT-Sicherheit auseinandersetzt und gleichzeitig immer aktiver im Internet wird. Diese Personengruppe ist demnach besonders gefährdet, Opfer von Social Engineering zu werden. Es braucht somit auf ältere Personen zugeschnittene präventive Angebote seitens unterschiedlicher privater und behördlicher Organisationen.

Eine besondere Bedeutung kommt der dritten Stufe, der *Tertiärprävention*, zu. Dabei geht es darum, Angebote für betroffene Personen zu schaffen. Was den spezifischen Bereich der Unternehmen betrifft, so scheint die Einflussnahme auf die Unternehmens-Sicherheitskultur besonders relevant. Betroffene müssen im Rahmen eines Incident Managements die Gelegenheit erhalten, Vorkommnisse ohne negative Konsequenzen zu melden und Unterstützung bei der Verarbeitung zu erhalten. In anderen Bereichen wie beispielsweise der Aviatik ist es üblich, real begangene Pilotenfehler zu Trainingszwecken zu nutzen, ohne dabei das Verhalten der betroffenen Personen zu verurteilen. Nur so kann das Problembewusstsein bei den Mitarbeitenden geschärft und somit die Bereitschaft, das eigene Verhalten kritisch zu hinterfragen und zu ändern, geschaffen werden.

Ebenfalls braucht es Angebote für betroffene Privatpersonen. Ziel soll es in erster Linie sein, eine weitere Opferwerdung zu verhindern. Dies ist teilweise gar nicht so einfach: Gerade wenn es um Phänomene wie Romance Scam geht, fehlt das Problembewusstsein teilweise gänzlich und die Gefahr ist gross, dass die betroffene Person immer wieder Geld übermittelt. In solchen Fällen braucht es intensive Einzelgespräche mit den Betroffenen, in welchen das Problem in einem ersten Schritt aufgezeigt wird und in einem zweiten Schritt eine Betreuung

bzw. Beratung in psychologischer und/oder finanzieller Hinsicht stattfinden soll.

Die Prävention hat im Bereich der Cyber-Kriminalität einen langen Weg vor sich. Eine der Hauptherausforderungen besteht darin, die präventiven Angebote sowohl für Unternehmen als auch Privatpersonen schweizweit zu bündeln. Dabei darf nicht vergessen werden, die psychologischen Wirkmechanismen von Social Engineering einzubeziehen. Es braucht demnach in der Präventionsarbeit neben IT-Experten vermehrt auch psychologisch und sozialwissenschaftlich geschulte und auf den Cyberbereich spezialisierte Personen, welche die Präventionsarbeit auf allen drei Stufen, der Primär-, Sekundär- und Tertiärprävention mit ihrem Fachwissen unterstützen können.