



# Social Engineering

**Social Engineering** (engl. eigentlich „angewandte Sozialwissenschaft“, auch „soziale Manipulation“) nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Daten oder Dinge zu gelangen. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen falsche Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um Dinge wie geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Meist dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von Social Hacking (vgl. Hacker).

## Geschichte

Ein frühe Form des Social Engineering wurde in den 1980er Jahren mit Phreaking praktiziert. Phreaker riefen unter anderem bei Telefongesellschaften an, gaben sich als Systemadministrator aus und baten um neue Passwörter, mit denen sie schließlich kostenlose Modemverbindungen herstellten.

## Grundmuster

Das Grundmuster des Social Engineering zeigt sich bei fingierten Telefonanrufen: Der Social Engineer ruft Mitarbeiter eines Unternehmens an und gibt sich als Techniker aus, der vertrauliche Zugangsdaten benötigt, um wichtige Arbeiten abzuschließen. Bereits im Vorfeld hat er aus öffentlich zugänglichen Quellen oder vorangegangenen gescheiterten Telefonaten kleine Informationsfetzen über Verfahrensweisen, tägliches Bürogerede und Unternehmenshierarchie zusammengetragen, die ihm bei der zwischenmenschlichen Manipulation helfen. Der Angreifer verwirrt sein technisch ungebildetes Opfer mit Fachjargon, baut mit Smalltalk über scheinbar gemeinsame Kollegen Sympathie auf und nutzt Autoritätsrespekt aus, indem er droht, den Vorgesetzten stören zu müssen. Unter Umständen hat der Mitarbeiter sogar

tatsächlich technische Hilfe angefordert und erwartet bereits einen derartigen Anruf.

Eine bekannte und unpersönliche Variante des Social Engineering ist das Phishing: Fingierte E-Mails mit vertrauenswürdiger Aufmachung fordern den Empfänger auf, auf einer präparierten Webseite geheime Zugangsdaten wie Passwörter für Online-Banking preis zu geben. Das Grundmuster ist ähnlich dem fingierten Telefonanruf, denn auch hier gibt sich der Social Engineer in der Regel als technischer Mitarbeiter aus, der zur Datenüberprüfung oder -wiederherstellung die Geheiminformation benötigt. Anders als dort verfügt der Angreifer hier über nicht viel mehr als die E-Mail-Adresse des Empfängers, was die Attacke weniger persönlich und damit auch weniger wirkungsvoll macht.

*Quelle: wikipedia*

Die Veröffentlichung der folgenden Artikel erfolgt mit ausdrücklicher Genehmigung durch die Konradin IT-Verlag GmbH, Ernst-Mey-Straße 8, 70771 Leinfelden-Echterdingen

## Das Angriffsprinzip - und die Neugier als Beispiel

Dass Computer angreifbar sind, wissen Sie längst. Haben Sie auch schon mal daran gedacht, dass sie als Mensch genau so große Angriffsflächen bieten? Wenn sie Herr über vertrauliche Informationen sind, wird ein unberechtigter Interessent heute genau nicht nur die Firewall Ihres Unternehmensnetzwerks bearbeiten. Er wird genau so viel Energie darauf verwenden, Sie selbst über den Tisch zu ziehen und Ihnen entweder die Daten selbst zu entlocken oder Informationen abzugreifen, die ihn den Quellen etwas näher bringen.

"So dumm bin ich nicht", werden Sie sich jetzt sagen, "ich merke doch, wenn einer etwas von mir will." Leider liegen Sie falsch. Wenn ein Social Engineer Sie zu einer Handlung verleiten will, setzt er bei seinem Beeinflussungsversuch nie auf Ihre Dummheit - die Gefahr, dass sie gar nicht dumm sind, ist viel zu groß. Es versucht stattdessen, Sie bei angeborenen oder im Alltag anerkannten und bewährten Verhaltensweisen zu packen - etwa damit, dass er mit einem Geschenk oder mit Sympathie Ihr Wohlwollen gewinnt, mit Autorität, mit dem Appell an bewährte Entscheidungen oder an Ihren unüberwindlichen Wunsch, zu Ihrem Wort zu stehen. In den nächsten Folgen werden wir die erfolgreichsten Tricks dieser Art durchgehen und Ihnen Abwehrmaßnahmen an die Hand geben, mit denen Sie sich ohne unangenehme Nebenwirkungen helfen können.

Heute sind die wichtigsten Punkte, die Sie sich merken sollten:

- 1.) Menschen, die Sie ungerechtfertigt beeinflussen wollen, werden nur in Ausnahmefällen unangenehm auftreten. Meist werden Sie Ihnen gefallen, und Ihre Wünsche werden auf den ersten Blick logisch erscheinen. Achten Sie deshalb immer auf Ihr Bauchgefühl, wenn Sie etwas heikles für jemanden tun sollen. Ist Ihnen die Erfüllung eines Wunsches unangenehm, vor allem wenn es um die Herausgabe von Informationen geht, dann prüfen Sie den Wunsch und den Antragsteller lieber einmal mehr.

*Gehälter Vorstand  
Mitarbeitergespräche 2006*

- 2.) Wenn Sie Informationen herausgeben, fragen Sie sich auch, was diese Infos einem

Fremden nützen könnten. So ermitteln Sie das Risiko, dem Sie ausgesetzt sind.

Darüber hinaus sollten Sie daran denken, dass technische und menschliche Angriffe oft Hand in Hand gehen. Erinnern Sie sich noch an den Trick aus Tipp Nr. 2? Da hatte jemand USB-Sticks auf einem Parkplatz verteilt. Weil die Finder neugierig waren, schlossen sie die Speicher fast allesamt an ihre Büro-PCs an, um zu sehen, was sich darauf befand - und schon hatte der Angreifer ein Spionageprogramm auf ihre Computer geschleust. Werner Degenhardt empfiehlt für derartige Aktionen übrigens eher CDs, will man da mehr draufschreiben kann: "Gehälter Vorstand" etwa oder "Mitarbeitergespräche 2006". Sind sie sicher, dass Sie widerstehen könnten? Neugier ist gut, denn sie stellt sicher, dass Sie permanent lernen und sich in ihrem Umfeld bewähren können. In diesem Fall aber wird sie schamlos ausgenutzt.

## Beeinflussung per Sympathie

"Hallo, guten Morgen!"

"Guten Morgen!"

"Sagen Sie - die Stiefel, die Sie da an haben - waren Sie etwa schon reiten heute morgen?"

"Ja, allerdings, dass Sie das sehen - ich ziehe mich gleich um im Büro!"

"Das ist ja toll. Mein Pferd steht draußen in Moosberg, ich komme aber immer erst abends hin - wir müssen uns mal unterhalten!"

"Ja, gerne doch, ich wusste gar nicht, dass hier noch jemand Spaß am Reiten hat."

"Ich bin ja auch noch ganz neu hier, vielleicht können Sie mir noch ein paar Tipps geben für Tierärzte und Läden und was man so braucht - ach, Sie steigen hier aus, in der Personalabteilung? Oh, Sie schickt der Himmel, ich bräuchte da noch ein paar Infos..."

Wenn Sie an den Einsatz von Sympathie für Spionage und andere unlautere Zwecke denken, kommen Ihnen vielleicht zuerst ganz bestimmte Filme in den Sinn - mit hübschen Blondinen, die eitle Politiker umgarnen, oder knackigen Beachboys, die Abteilungsleiterinnen etwas älteren Semesters den Urlaub versüßen. Irgendwann tauchen die netten Damen und Herren dann mit der Zugangskarte fürs Vorstandsbüro plötzlich unter, und das Opfer stürzt von Wolke sieben auf den harten Boden der Realität zurück.

Aber immerhin war das Abenteuer schön. Allzu viel Hoffnung in diese Richtung sollten Sie sich allerdings gleich verbieten: Nur wenige Hacker und Social Engineers sehen aus wie Brad Pitt

oder Angelina Jolie, und wenn die Angreifer entsprechendes Profipersonal zusätzlich anwerben müssen, geht die Attacke ins Geld. In den Genuss solcher Versuchungen kommen Sie also nur, wenn Sie wirklich wertvolle Geheimnisse hüten.

Trotzdem - einen guten Film solcher Art zu sehen kann ein durchaus brauchbares Abwehrtraining sein. Die wunderbare Thriller-Komödie "Sneakers" mit Robert Redford etwa liefert ein echtes Lehrstück zum Social Engineering per Sympathie. Der Held, Chef einer leicht chaotischen Sicherheitstruppe, die die Sicherheitsmaßnahmen von Unternehmen überprüft, kommt darin einem Verbrecher auf die Spur und will sich in dessen Firmengebäude einschleichen. Er setzt deshalb seine attraktive Freundin auf einen Hardware-Entwickler des Unternehmens an, der über einen Computerdienst eine Lebenspartnerin sucht. Die junge Frau wickelt ihr Opfer nach allen Regeln der Kunst ein, nimmt dessen Stimme zur Überwindung eines biometrischen Schutzsystems auf und stiehlt schließlich seine Brieftasche samt Karten und Schlüsseln. Die Pointe liegt darin, wie der Coup auffliegt: Der verbrecherische Firmenchef, der die zwei später im Gebäude überrascht, kann einfach nicht glauben, dass ein Computer seinen pedantisch-unbeholfenen Techniker mit solch einer hübschen und eleganten Frau zusammengebracht hat.

*Eine gewisse Ähnlichkeit oder Seelenverwandtschaft sind große Sympathiefaktoren*

Sie wiederum werden vielleicht irgendwann einfach auf einen netten Menschen treffen, der mit Ihnen über dicke Geländewagen in der City schimpft oder, wenn Sie selbst solche Autos mögen, Ihre Abneigung gegen deren Verteufelung teilt. Schon geben Sie bereitwilliger Auskunft über Firmeninterna, als sie es bei einem Ihnen gleichgültigen Menschen tun würden. Vielleicht ist er oder sie auch seit kurzem im gleichen Fitness-Club, fährt wie Sie Motorrad oder kommt mit dem Fahrrad, trägt ähnliche Kleidung, ist Fan des gleichen Fußballvereins oder teilt Ihre Gesundheitsprobleme. Schon lassen Sie sich auf längere Gespräche ein. Eine gewisse Ähnlichkeit oder Seelenverwandtschaft sind große Sympathiefaktoren, die sich mit etwas Übung leicht spielen lassen. Gutes Aussehen allerdings ist auch von Bedeutung, denn hübschen Menschen wird statistisch gesehen eher geholfen als hässlichen, wobei auch hier

der Attraktivitätsfaktor in weiten Grenzen manipulierbar ist - ein strahlendes Lächeln etwa macht schon viel aus.

Die Frage ist nun, was man mit all diesen Erkenntnissen überhaupt anfangen kann. Es hat ja keinen Sinn, nette Menschen aus Prinzip schlechter und misstrauischer zu behandeln als Berufsgrantler oder Fieslinge unter den Kollegen, nur weil ein winziger Bruchteil der angenehmeren Hälfte der Menschheit vielleicht böse Absichten hat.

Sinnvollerweise sollten Sie auch hier bei den Forderungen ansetzen, die der Manipulator Ihnen unweigerlich irgendwann stellt. Wenn Sie jemand um vertrauliche Informationen bittet oder Sie um andere zweifelhafte Hilfestellungen angeht, achten Sie auf sich selbst, warum sie möglicherweise bereit sind, für genau diese Person gesetzte Grenzen zu überschreiten. Hat er oder sie sich dieses Vertrauen wirklich verdient? Sie können sicher sein: Gerade ein wirklich sympathischer Mensch wird Ihnen einen Sicherheitscheck nicht übelnehmen - wenn Sie Ihr Vorgehen freundlich erklären.

Damit haben wir Ihnen jetzt selbst ein mildes Social Engineering vorgeschlagen. Lassen Sie den Sympathiefaktor für sich arbeiten, wenn Sie unangenehme Sicherheitsmaßnahmen durchsetzen müssen. Welch ungeheure Wirkung diese Freundlichkeit hat, können Sie übrigens manchmal erfahren, wenn Sie nach Israel reisen: An den Flughäfen dort gibt es Sicherheitspersonal, das selbst die intensivsten Befragungen und Kontrollen in einer Weise abwickelt, dass man einfach nicht anders kann als selbst freundlich zu bleiben. Social Engineering ist durchaus nicht immer böse!

### **Beeinflussung per Autorität**

"Morgen, Herr Schulze, hier Meier, ich leite die Entwicklung im Labor Freiburg."

"Guten Morgen, ich..."

"Hören Sie, der Schmidt, Ihr werter Kollege, der ist doch glatt in Urlaub gefahren ohne uns die Daten zum neuen Energiesparmodul für die Serie 5 zuzusenden."

"Was? Äh, soll ich ihn..."

"Nein, nichts da. Ich habe gerade schon mit Ihrem Chef telefoniert, dem Müller, der ist auch schon auf hundertachtzig. Sie haben doch das Kennwort für Schmidts Rechner, das müssen Sie doch, Sie sind doch sein Backup!?"

"Ja sicher, aber..."

"Kein aber, hier geht es um

Schadensbegrenzung, und wenn Sie es genau wissen wollen, auch um Schmidts Job, haben Sie das verstanden? Also, jetzt gehen Sie bitte sofort rüber zu seinem Schreibtisch, werfen den PC an, und schicken mir die Pläne zu dem Modul. Ich bin hier im Hilton in Hamburg und muss gleich zum Lieferanten, soll ich mich da für dumm verkaufen lassen? Nehmen Sie tmeier562@rycos.de, an den Firmen-Account kommt man ja nie ran, wenn man ihn braucht. Und schnell bitte, Sie wissen ja warum! Kann ich mich darauf verlassen?"

Was würden Sie in solch einem Fall tun? Das arme Opfer wird wahrscheinlich nachgeben. Dabei spielen zwar auch Faktoren wie der angebliche Zeitmangel und der Wunsch eine Rolle, dem Kollegen den Job zu retten (Hilfsbereitschaft) - aber der stärkste Faktor dürfte in diesem Fall die Autorität des Anrufers sein. Sie äußert sich im Ton und stützt sich auf die angeblich übergeordnete Stellung sowie den Bezug auf den direkten Vorgesetzten. Untermauert wird sie, wie bei fast jedem Social-Engineering-Angriff, durch Insider-Wissen: Der Anrufer hat sich vorher genau über die Hierarchien und Zuständigkeiten in der Abteilung des Opfers informiert und weiß auch, wer notfalls auf wessen PC zugreifen kann.

Wenn im Unternehmen unserer Beispielperson ein autoritärer Führungsstil herrscht, hat Schulze im geschilderten Fall genau eine Chance, einer bössartigen Manipulation zu entkommen: Bevor er die gewünschte Mail schickt, muss er das Gespräch auf jeden Fall unterbrechen. Dazu kann er notfalls einen Verbindungsfehler simulieren, indem er einfach auflegt. Daraufhin sollte er mit der Nummer aus seiner eigenen Telefonliste in Freiburg anrufen und fragen, wo sich Herr Meier gerade aufhält und wie er zu erreichen sei. Nur dann, wenn sich die Hamburg-Geschichte auf diesem Weg unabhängig von Meiers eigenen Angaben erhärten ließe, dürfte Schulze die Erfüllung des Wunsches überhaupt in Betracht ziehen. Selbst ein wirklich cholischer Chef wird solche Vorsichtsmaßnahmen honorieren, wenn er wieder zu Ruhe kommt.

Lassen Sie sich bei Anordnungen, die mit Sicherheitsrichtlinien in Konflikt geraten oder Ihnen auf irgendeine Weise seltsam vorkommen, also nie aus der Ruhe bringen. Fragen Sie sich in jedem Fall, ob der Befehlsgeber tatsächlich berechtigt ist, das Gewünschte von Ihnen zu verlangen. Dies gilt auch, wenn er Ihnen in der typischen Kleidung und dem Verhalten eines Vorgesetzten in Ihrer Organisation gegenüber steht - erinnern Sie sich an den Hauptmann von Köpenick? Oft

reichen schon ein Kittel, ein Klemmbrett und die mürrische Ungeduld eines Controllers, und schon wird man für berechtigt gehalten, in beliebige Büros zu laufen und dort Informationen abzufragen. Gehört das unbedingte Befolgen jedes Befehls nicht ausdrücklich zu ihrem Arbeits- oder Dienstvertrag, wird Ihnen eine gesunde Vorsicht beim Befolgen von Anordnungen selbst in Organisationen mit rauen Sitten erst recht zugute kommen.

*Oft reichen schon ein  
Kittel, ein Klemmbrett und  
die mürrische Ungeduld  
eines Controllers*

Arbeiten Sie in einem Unternehmen, in dem normalerweise kein Befehlston herrscht, sind plötzliche unfreundliche Anweisungen möglicherweise selbst schon ein Hinweis darauf, dass etwas nicht stimmt - vor allem, wenn Ihnen Ihr Gegenüber unbekannt ist. Die Wahrscheinlichkeit dieser Konstellation ist allerdings eher gering, da sich ein guter Angreifer gewöhnlich vorab nach den Sitten und Gebräuchen in der Organisation erkundigt, auf die er es abgesehen hat. Er wird in einem freundlichen Unternehmen also auch freundlich auftreten. Ihr Vorteil: In diesem Fall hat er es schwerer als in einem streng hierarchischen Umfeld, denn Sie können Sicherheitschecks selbstbewusst und ohne banges Gefühl in die Wege leiten.

### **Beeinflussung per Kommitment und Konsistenz**

"Guten Morgen, Frau Meier, Sie holen doch gleich die Post - lassen Sie mich dann schnell mal an Ihren PC? Ich habe meinen Notebook vergessen."

"Aber Herr Müller, das darf ich doch nicht."

"Aber Frau Meier, Sie sagen doch selbst immer, wenn wir uns hier nicht mehr vertrauen, dann ist die Firma sowieso am Ende, und bei den Entlassungswellen müssen wir viel mehr zusammenhalten."

In unserem Kulturkreis gilt es als positiv, zu einer Sache und zu seinem Wort zu stehen und in Grenzen konsequent zu handeln. Eine ganze Reihe von Redensarten dokumentiert dies recht eindrucksvoll: "Er oder sie hält wenigstens Wort", "der oder die verfolgt eine gerade Linie", "auf den oder die kann man sich verlassen", "er oder sie hängt sein Fähnchen

nicht nach dem Wind". Sie könnten diese Reihe wahrscheinlich problemlos ergänzen, und tatsächlich sind wir ja meistens sehr froh, wenn unser Gegenüber fest geglaubte Ziele und Meinungen nicht plötzlich zum "Geschwätz von gestern" erklärt.

*Machen Sie sich dann klar,  
dass Konsequenz allein keinen  
Wert darstellt*

Vorsichtig werden sollten Sie allerdings, wenn jemand einen fragwürdigen Wunsch mit direkten Hinweisen auf Ihre Einstellung oder frühere Aussagen durchzusetzen versucht. Er kann damit rechnen, dass sie unbewusst oder bewusst versuchen werden, verlässlich zu erscheinen. Machen Sie sich dann klar, dass Konsequenz allein keinen Wert darstellt - andernfalls wäre es für Menschen fast unmöglich, aus Fehlern oder neuen Erfahrungen zu lernen oder sich weiter zu entwickeln.

Wenn Sie in einem heiklen Fall dieser Art mit sich selbst kämpfen, hilft vielleicht ein kurzes Stückchen Brecht:

Ein Mann, der Herrn K. lange nicht gesehen hatte, begrüßte ihn mit den Worten:  
`Sie haben sich gar nicht verändert´  
`Oh´ sagte Herr K. und erleichte.

Ganz subtil beherrschen übrigens auch Verkäufer das Spiel mit Kommitment und Konsistenz. Mancher Autokäufer hat das schon zu spüren bekommen: Erst nennt ihm der Händler einen recht günstigen Preis für ein bestimmtes Fahrzeug, dann kommt die Probefahrt. Steigt der Kunde glücklich wieder aus - inzwischen ist er oder sie sich sicher, diesen Wagen fahren zu wollen, und war im Geiste damit schon in den nächsten Urlaub unterwegs - fällt dem Verkäufer urplötzlich auf, dass er ja - hoppla - die Klimaanlage oder die hübsche Sonderlackierung bei der Kalkulation völlig vergessen hat. Ach, ist ihm das peinlich! Von wegen. Er weiß genau, dass es sein Opfer jetzt schwer hat, von der einmal getroffenen Kaufentscheidung wieder zu abzulassen. Die paar Euro mehr, die die 2000 Euro für die Sonderausstattung umgerechnet auf die monatlichen Raten ausmachen, werden jetzt nicht mehr ins Gewicht fallen. Hätte das Opfer den Endpreis aber schon vorher erfahren, hätte es sich vielleicht gar nicht erst in das Auto gesetzt.

Eine in den USA inzwischen verbotene Praxis war es lange Zeit, vor Weihnachten bestimmte Spielzeuge massiv im Fernsehen zu bewerben - und dann kurz vor dem Fest zu behaupten, es gäbe Lieferschwierigkeiten. Die Kunden kauften dann etwas anderes. Nach Weihnachten annoncierten die Firmen dann, der gewünschte Artikel sei nun endlich lieferbar. Welche Mama und welcher Papa konnte dann schon dem Gequengel der lieben Kleinen widerstehen, dieses Spielzeug doch vor Heilig Abend ganz fest versprochen zu haben?

Warum hier ein Verbot ausgesprochen wurde, ist bei näherem Hinsehen klar: Die Eltern waren fast gezwungen, zu ihrem Wort zu stehen, weil sie den Wortbruch zu Weihnachten nicht zu vertreten hatten. Im Unternehmensumfeld aber stehen Sie nur selten unter solchem Druck. Denken Sie dort lieber an ihre Sicherheitslinien und an Brecht und wägen sie ab. Das Ergebnis wird immer besser sein als blinde Konsequenz.

#### **Wie ich Dir, so Du mir**

"Hallo Frau Schulze - kennen Sie mich noch?"  
"Aber ja doch! Wenn Sie mir damals nicht die Computerpanne behoben hätten, mein Gott wäre das ein Ärger gewesen!"  
"Das hab ich doch gern getan. Aber sagen Sie, jetzt habe ich ein Problem. Ich müsste mal ganz kurz einen Blick auf die Mitarbeiterdatenbank werfen - darf ich wohl einmal für nur fünf Minuten an Ihren PC?"

Dass Geschenke verpflichtend wirken, nutzen vor allem Spendensammler gern aus. Zu Weihnachten oder Ostern haben Sie sicher schon einmal Briefe mit Überweisungsformularen bekommen, die als kleine Vorab-Danksagung Weihnachts- oder Osterkarten oder beispielsweise Adressaufkleber enthielten. Diesen durchaus teuren Aufwand würden sich die entsprechenden Institutionen nicht leisten, wenn der Trick die Spendenbereitschaft nicht deutlich erhöhen würde. Auch Sektenmitglieder auf der Straße bei der Mitgliederwerbung überreichen gern erst einmal ein hübsches Buch. Bei den Hare-Krishna-Jüngern war es eine Blume, die sie ihrem Opfer zunächst aufdrängten - fast jeder fühlte sich dann genötigt, wenigstens einen kleinen Betrag locker zu machen. Wer die Blume anschließend im Ärger über die eigene Nachgiebigkeit wegwarf, konnte zu seinem Missvergnügen mitunter beobachten, wie die Spendensammler ihr Hilfsmittel schnell wieder

aus dem Abfallkorb fischten, um damit den nächsten Passanten zu beglücken.

### *Geschenke verpflichten*

Die Reaktion, auf ein Geschenk mit einer Gegenleistung aufzuwarten, ist in vielen Kulturen so tief verankert, dass sich Menschen gegen diesen Mechanismus kaum wehren können. Social Engineers wissen das. Sie geben einem Geschäftsführer auf dem Golfplatz wertvolle Tipps oder helfen Mitarbeitern selbstlos bei lästigen Tätigkeiten. In der Industriespionage versuchen Profis zuweilen, Anwendern im Unternehmen bei der Behebung vermeintlicher oder zuvor eigens herbeigeführter Computerprobleme zu helfen. Später fordern sie dann freundlich, aber bestimmt eine Gegenleistung ein.

Es ist schwer, diesem Trick zu begegnen, denn das Spiel von Geben und Nehmen ist uralte und hält seit jeher soziale Gefüge und die Wirtschaft zu ihrem eigenen Vorteil zusammen. Das Spiel kann den Charakter eines Tauschgeschäfts annehmen, bei dem Personen individuelle Fähigkeiten oder Ressourcen gegenseitig anbieten - ich streiche Deine Tür, dafür ziehst Du mir meine Winterreifen auf - oder es wird einfach als Mittel zum Freundschaftserhalt zelebriert, wie beispielsweise in Form gegenseitiger Einladungen.

Deshalb ist bei der Gegenwehr auch Fingerspitzengefühl gefragt. Aufmerksam werden sollten Sie, wenn jemand, den Sie obendrein nur flüchtig kennen, sehr früh eine ganz bestimmte Gegenleistung für eine Hilfestellung oder ein Geschenk einfordert, die noch dazu geltenden Regeln widerspricht.

Sie dürfen dann nein sagen. Das "Nein" muss sich ja nur auf die Gegenleistung beziehen, die Ihnen unangenehm erscheint oder sogar verboten ist. Wählen Sie selbst, auf welche Weise Sie Ihrem Gegenüber Ihre Dankbarkeit zeigen. Ein Helfer ohne Hintergedanken wird dafür Verständnis haben.

### **Das machen doch alle so!**

"Hallo Herr Fischer, darf ich bei Ihnen auch mal kurz den Patch-Stand checken? In der Mittagspause?"

"Ja - was - geht denn das so einfach?"

"Wir machen das mit Absicht in der Pause - Sie geben mir einfach Ihr Kennwort, und wenn

Sie aus der Kantine kommen, ist das diesmal ganz ohne den üblichen Ärger erledigt. Sie können das Kennwort ja anschließend ändern."

"Aber ich kann Ihnen doch nicht einfach..."

"Wissen Sie, wir haben das in der letzten Woche gemeinsam beschlossen, als Sie noch in Berlin waren. Einfach den kurzen Dienstweg nehmen, damit wir nicht wieder die ganze Woche damit verplempern. Nur die anderen Abteilungen sollten nichts davon wissen, und auch nicht alle Kollegen - sollen sich die Prinzipienreiter doch mit der Bürokratie rumschlagen, wenn sie unbedingt wollen!"

Menschen orientieren sich gern am Verhalten ähnlicher Menschen. Die Auswirkungen sind bekannt: Brave Bürger in Anzug und Krawatte laufen bei rot über die Kreuzung, wenn nur genug andere Anzugträger dasselbe vormachen. Man kauft silbergraue Autos, weil alle anderen Autos auch silbergrau sind. Man wählt die Bank, bei der die Kollegen Kunde sind, orientiert sich beim Restaurantbesuch an guten Freunden, kleidet sich "passend", klatscht mit, wenn andere klatschen - und so weiter. Die Kehrseite: Bevor Menschen bei einem Unfall oder einer Gewalttat helfen, warten sie oft zu lange darauf, was die anderen tun. Hier hat das Prinzip der sozialen Bewährtheit schon Menschenleben gekostet.

Vor allem letzteres Beispiel zeigt, dass soziale Bewährtheit vor allem dann zur Orientierung herangezogen wird, wenn man sich in einer Situation unsicher fühlt. In diesem Fall ist der Blick auf den anderen kontraproduktiv und gefährlich, aber unter weniger dramatischen Umständen erspart das Nachmachen oft genug schmerzliche Irrwege und Peinlichkeiten.

*Nichts sagen und nicht nachfragen zu dürfen, macht die Sache verdächtig*

Will ein Angreifer Sie über dieses menschliche Verhaltensprinzip manipulieren, muss er sich etwas einfallen lassen, denn er kämpft zwangsläufig mit einem prinzipiellen Problem: Er muss Sie glauben machen, dass er jene Gruppe repräsentiert, an der Sie sich orientieren möchten. Deshalb muss er sich, wie im einleitenden Beispiel, etwa als Abgesandter eben dieser Gruppe ausgeben und zugleich mit einem Trick verhindern, dass Sie sich auf einem anderen Weg rückversichern. Genau dieser Trick ist im Beispiel oben auch der Punkt, an dem das Opfer vielleicht aufmerksam wird: Nichts sagen

und nicht nachfragen zu dürfen, macht die Sache verdächtig. Leichter hat es der Angreifer, wenn er die Zugehörigkeit zu einer Gruppe - zu "Ihrer" Gruppe - so glaubhaft verkörpert, dass Sie sie nicht in Zweifel ziehen. Hier überschneidet sich die "soziale Bewährtheit" als Social-Engineering-Technik mit dem Prinzip "Sympathie". Man könnte sich hier etwa auch einen Abteilungsleiter vorstellen, der auf dem Golfplatz einen anderen Abteilungsleiter trifft, der einen "unter Kollegen" unglaublich beliebten Berater empfiehlt - und so einen Spion in ein Unternehmen einschleust.

Die einzige Möglichkeit der Abwehr besteht darin, gerade in Situationen der Unsicherheit eigene Entscheidungen immer dann zu hinterfragen, wenn sie auf dem Rat anderer beruhen. Wenn Sie Rat suchen, suchen Sie ihn vorsichtshalber aktiv bei Ihnen wirklich bekannten Personen oder Gruppen. Fragen Sie sich auch, warum Sie unsicher sind - hat man Sie vielleicht gerade gezielt verunsichert?

Beachten Sie außerdem immer, dass das Prinzip der sozialen Bewährtheit wie im Beispiel der zögernden Helfer auch andersherum problematisch werden kann. Sie haben etwas bemerkt, was Ihnen im Unternehmen ungewöhnlich vorkommt? Sie sagen aber nichts, weil auch sonst niemand etwas sagt? In einem großen deutschen Unternehmen hat schon einmal ein falscher Mitarbeiter geraume Zeit lang in einem Großraumbüro gesessen. Den Kollegen kam er zwar "seltsam" vor, und einige wunderten sich, dass er offenbar in einem Bus auf dem Parkplatz wohnte - aber niemand wollte den ersten Schritt tun. Als es dann endlich so weit kam, hatte der "Mitarbeiter" schon einen ganzen Schrank voller "Sicherheitskopien" angehäuft. Zum Glück war er kein böswilliger Spion, sondern ein leicht verwirrter Ex-Consultant, der sich "weiterbilden" wollte.

### **Bitte schnell, sonst ist alles zu spät!**

"Frau Schulze? Hier Worbach, der Chef von Abteilung 7. Hören Sie, ich habe gleich ein Kundengespräch und brauche sofort die neuesten Statusberichte für die Öko-Spülmaschine."

"Aber die sind doch vertraulich, können Sie nicht..."

"Also Frau Schulze, jetzt kommen Sie mir nicht mit Bürokratie, wenn ich die Infos nicht in fünf Minuten habe, verlieren wir einen Riesenauftrag, und das kann ja wohl nicht in Ihrem Sinne sein, oder? Schicken Sie die

Dateien an meinen Privat-Account, worbach4g17@aol.com. Das VPN tut's hier nicht."

*Wenn Sie nicht gleich seinen  
Wünschen nachkommen,  
geschieht etwas ganz Schlimmes*

Fast jeder, der Sie manipulieren will, macht zugleich die Zeit knapp, in der Sie sich für eine Handlung entscheiden müssen. Die gilt besonders dann, wenn er etwas verlangt, das nicht ganz regelkonform ist oder Risiken mit sich bringt. Der Angreifer will, dass Sie nicht zum Nachdenken kommen. Sie sollen keine Gelegenheit haben, die möglichen Folgen Ihres Tuns vorab auszuloten, die Begründungen dafür zu überprüfen oder zusätzlichen Rat einzuholen. Deshalb baut der Social Engineer Druck auf: Wenn Sie nicht gleich seinen Wünschen nachkommen, geschieht etwas ganz Schlimmes, oder eine Chance ist unwiederbringlich verloren. Und natürlich wollen nicht gerade Sie die Sache zum Scheitern bringen.

Abwägen müssen Sie in solch einem Fall unbedingt, fünf Minuten Zeit haben Sie immer. Fragen Sie sich, ob die geschilderte Situation plausibel ist. Gehen Sie die Situation bei aller Hektik wenigstens einmal komplett durch und überlegen Sie, ob der Zeitdruck tatsächlich so groß sein kann, wie er angeblich ist. Werden Sie misstrauisch, wenn Sie Ihr Gegenüber nicht persönlich kennen - wenn es die entsprechende Person nämlich wirklich eilig hat und weiß, dass sie eine Regelverletzung verlangen muss, wird sie sich allein schon im eigenen Interesse normalerweise zuerst an engere Vertraute wenden. Warum also sind Sie im Spiel? Rufen Sie Ihren Kommunikationspartner außerdem vorsichtshalber über eine Nummer zurück, die in ihrem offiziellen Telefonverzeichnis steht, um wenigstens einen halbwegs sicheren Identitätsbeweis zu haben. Fragen Sie, wenn irgend möglich, auch schnell bei der zuständigen Assistenz nach, ob die Hintergrundgeschichte stimmt - etwa der Aufenthalt in einem Hotel oder bei einem bestimmten Kunden.

Kommen Sie nach diesen Maßnahmen tatsächlich zu dem Schluss, dass Sie dem Wunsch Ihres Gegenübers nachgeben müssen, dokumentieren Sie den Vorfall und den Grund für Ihre Entscheidung und leiten Sie beides so schnell wie möglich an die zuständigen Kollegen von der

Unternehmenssicherheit oder den zuständigen Abteilungsleiter weiter.

Mit dem Prinzip "Knappheit" wird man Sie übrigens auch im privaten Alltag immer wieder zu manipulieren versuchen. Da gibt es Waren nur "solange der Vorrat reicht", sind Serien "limitiert", hat man beim Online-Buchhändler "nur noch drei Exemplare auf Lager" (jeder Buchhändler kann binnen 24 Stunden nachordern!) und so weiter. Schlimmer sind Anlageberater oder Versicherungsvertreter, die Ihnen ein angeblich günstiges Angebot machen, dieses aber nicht aufrechterhalten wollen, wenn Sie sich die Sache noch ein oder zwei Tage überlegen möchten - in diesem Fall war das Angebot bestimmt nicht so gut für Sie, wie es auf den ersten Blick vielleicht erschien.

### **Die Kunst, freundlich Grenzen zu setzen**

Die wirksamste Waffe gegen Social Engineering ist das "Nein".

"Nein, das kann ich Ihnen nicht sagen, ich weiß es nicht" - so sollten Sie reagieren, wenn Sie jemand fragt, ob der Abteilungsleiter in Urlaub ist.

"Leider kann ich Sie nicht durchgehen lassen. Unser Schließsystem lässt nur eine Person pro Karte eintreten" - so könnte die angemessene Reaktion aussehen, wenn Sie ein (möglicher) Lieferant fragt, ob Sie ihm nicht freundlicherweise die Tür aufhalten möchten.

Das Problem mit dem "Nein"-Sagen ist, dass es schwierig ist. Wir sagen insgesamt lieber "Ja" als "Nein", wenn wir um irgendeine Form der Zusammenarbeit oder Hilfe gebeten werden - vor allem, wenn die Bitte überdies mit Normen übereinstimmt, die von Autoritäten vorgegeben sind. Dass wir in solchen Fällen lieber "Ja" sagen, ist auch gut so. Würden wir auf Ansprüche an positives und bewährtes Sozialverhalten grundsätzlich negativ reagieren, würden wir nicht nur persönlich Schaden nehmen, sondern den sozialen Zusammenhalt im Unternehmen oder im Alltag generell aufs Spiel setzen.

Dies wissen die "Sozialingenieure" natürlich auch. Sie nutzen die Tendenz, "Ja" zu sagen, indem sie günstige Situationen dafür herstellen: Autorität, Sympathie, Gefühl der Verpflichtung, soziale Bewährtheit und so weiter - Sie haben diese Möglichkeiten ja in

den vorhergehenden Newslettern nacheinander kennen gelernt.

Es ist nicht leicht, herauszufinden, ob ein "Nein" in einer bestimmten Situation angebracht ist. Die wahrscheinlich einzige Methode, die man wirklich empfehlen kann, ist: Zeit gewinnen. "Ich muss das kurz prüfen und bin dann gleich wieder bei Ihnen", gibt Ihnen Gelegenheit, über das Anliegen eines Anrufers nachzudenken. "Einen kleinen Moment bitte, ich lege nur meinen Mantel ab, dann komme ich wieder zu Ihnen", gibt Ihnen die Zeit, zu prüfen, ob ein Lieferant wirklich von jemanden erwartet wird.

*Wichtig beim Nein-Sagen ist vor allem, klar zu sein, aber nicht brutal*

Wichtig beim Nein-Sagen ist vor allem, klar zu sein, aber nicht brutal. Es gibt eine Reihe von Möglichkeiten, wie man respektvoll "Nein" sagen kann:

- Das Nein begründen: "Oh, jederzeit gerne - nur jetzt besprechen wir gerade etwas, das keinen Aufschub duldet!"
- Verständnis zeigen: "Ich weiß, dass es wichtig für Sie ist, aber ich kann Ihnen erst in etwa 15 Minuten helfen."
- Bedanken: "Das ist ein schönes Kompliment, dass Sie mir das zutrauen, aber ich kann leider nicht."
- Teil-Nein: "Heute kann ich das leider nicht beantworten, wollen Sie mich morgen wieder kontaktieren?"
- Gegenangebot: "Am Telefon kann ich Ihnen leider keine Auskunft dazu geben. Wollen Sie nicht morgen persönlich bei mir vorbeikommen?"
- Humor: In manchen Situationen ist Humor eine wundervolle Möglichkeit, ein "Nein" angenehm zu verpacken.

Wenn Sie sich intensiver mit der Materie befassen wollen oder spüren, dass Ihnen die "Neinsagerei" besonders schwer fällt, hilft Ihnen vielleicht Dietrich Ückermanns 60-Minuten-Trainings-CD "Nein sagen ohne zu verletzen" weiter. Das Hörbuch aus der Reihe "Express-Ratgeber" ist bei "Activecoach Training und Verlag" erschienen und im Buchhandel erhältlich.