Risikofaktor Mensch

DIE KUNST DER TÄUSCHUNG

KEVIN MITNICK

& William Simon

Vorwort von Steve Wozniak

Social Engineering

Social Engineering benutzt Techniken der Beeinflussung und Überredungskunst zur Manipulation oder zur Vortäuschung falscher Tatsachen, über die sich ein Social Engineer eine gefälschte Identität aneignet. Damit kann der Social Engineer andere zu seinem Vorteil ausbeuten, um mit oder ohne Verwendung von technischen Hilfsmitteln an Informationen zu gelangen.

Inhalt

Vorwort

Als menschliche Wesen werden wir mit dem inneren Bedürfnis geboren, unsere Umgebung zu erkunden. In jungen Jahren waren Kevin Mitnick und ich beide zutiefst neugierig auf die Welt und begierig darauf, uns zu beweisen. Oft wurden wir bei unseren Anstrengungen belohnt, neue Dinge zu erfahren, Rätsel zu lösen und bei Spielen zu gewinnen. Aber gleichzeitig brachte uns unsere Umwelt Verhaltensregeln bei, die unserem inneren Forschungsdrang Fesseln anlegten. Sowohl für unsere größten Wissenschaftler und technologischen Vordenker als auch für Leute wie Kevin Mitnick bedeutet es die größte Erregung, diesem Drang nachzugeben, und damit konnten wir Dinge erreichen, die niemand anders für möglich gehalten hatte.

Kevin Mitnick ist eine der großartigsten Personen, die ich kenne. Fragen Sie ihn, und er wird geradeheraus sagen, dass es bei seiner Tätigkeit – Social Engineering – darum geht, andere zu betrügen. Aber Kevin ist kein Social Engineer mehr. Und sogar, als er noch einer war, ging es ihm niemals darum, sich zu bereichern oder anderen Schaden zuzufügen. Das bedeutet nicht, dass dort draußen nicht irgendwelche gefährlichen und destruktiven Kriminelle Social Engineering einsetzen, um einen echten Schaden hervorzurufen. Tatsächlich hat Kevin genau aus diesem Grund dieses Buch geschrieben: Um Sie vor solchen Leuten zu warnen.

Kevin Mitnicks Buch „Die Kunst der Täuschung“ zeigt, wie verletzbar wir alle für die Zudringlichkeiten eines Social Engineers sind – die Regierung, die Geschäftswelt und jeder von uns persönlich! In diesen sicherheitsbewussten Zeiten geben wir eine Menge Geld für die Technologien aus, die unsere Computernetzwerke und Daten schützen sollen. Dieses Buch zeigt auf, wie simpel es ist, die Insider hereinzulegen und den gesamten technologischen Schutz zu umgehen.

Egal, ob Sie bei der Regierung oder in einem Wirtschaftsunternehmen arbeiten – dieses Buch gibt Ihnen die Mittel in die Hand, die Arbeit eines Social Engineers zu verstehen und zu durchkreuzen. Kevin und sein Co-Autor Bill Simon setzen erfundene Geschichten ein, die unterhaltsam sind und

Ihnen gleichzeitig die Augen öffnen. So erwecken sie die Techniken aus der Unterwelt des Social Engineerings zum Leben. Nach jeder Geschichte bieten sie praktische Richtlinien an, mit denen Sie sich gegen die beschriebenen Lücken und Bedrohungen schützen können.

Eine rein technologische Sicherheit übersieht riesige Löcher, die von Leuten wie Kevin geschlossen werden können. Lesen Sie dieses Buch, und Sie werden schließlich erkennen, dass wir alle uns von den Mitnicks unter uns helfen lassen müssen.

Steve Wozniak

Einleitung

Einige Hacker zerstören anderer Leute Dateien oder Festplatten, sie werden *Cracker* oder *Vandalen* genannt. Manche Hacker kümmern sich nicht darum, die technologischen Grundlagen zu erlernen, sondern laden sich einfach Hacker-Programme herunter, mit denen sie in Computersysteme einbrechen – diese werden *Skript Kiddies* genannt. Erfahrenere Hacker mit Programmierkenntnissen entwickeln Hacker-Programme und stellen sie ins Web oder in Newsgroups. Und dann gibt es die Personen, die keine technologischen Interessen haben, sondern den Computer als Hilfsmittel nutzen, um Geld, Waren oder Dienste zu ergaunern.

Trotz des durch die Medien geschaffenen Mythos' „Kevin Mitnick" bin ich kein bösartiger Hacker.

Aber ich greife vor.

DER ANFANG

Mein Weg ist wohl schon früh vorgezeichnet gewesen. Um die Zukunft habe ich mir keine Sorgen gemacht, aber ich langweilte mich. Mein Vater verließ uns, als ich drei war, und seitdem verdiente meine Mutter unseren Lebensunterhalt als Kellnerin. Damals war ich die meiste Zeit meines Wachseins alleine – das Einzelkind einer Mutter, die lange und schwere Tage nach einem manchmal sehr wechselhaften Dienstplan zu arbeiten hatte. Ich war mein eigener Babysitter.

Ich wuchs in einem Ort im San Fernando Valley auf, von wo aus ich ganz Los Angeles erforschen konnte, und als ich zwölf war, hatte ich eine Möglichkeit entdeckt, kostenlos im gesamten Stadtgebiet von Los Angeles herumzufahren. Eines Tages bemerkte ich, dass die Gültigkeit der Tickets dadurch kontrolliert wurde, wie der Fahrer die Tickets lochte, um Datum, Zeit und Wegstrecke zu kennzeichnen. Bei einem freundlichen Fahrer erfuhr ich mit bedacht gewählten Fragen, wo man diesen besonderen Locher kaufen könne.

Mit den Transfertickets sollte man auf seiner Reiseroute in andere Busse umsteigen können, aber ich fand heraus, wie ich sie einsetzen musste, um überall hin fahren zu können, ohne zu bezahlen. Es war ein Kinderspiel, Blankotickets zu organisieren. An jeder Endstation waren die Mülleimer voller halbbenutzter Ticketbücher, die von den Fahrern nach Feierabend weggeworfen worden waren. Mit einem Stapel unbenutzter Tickets und dem Locher konnte ich meine eigenen Transfers stanzen und das gesamte Busnetz von Los Angeles befahren. Nach kurzer Zeit kannte ich den Busfahrplan so gut wie auswendig. Das war ein frühes Beispiel für mein überraschendes Gedächtnis, mit dem ich mir bestimmte Arten von Informationen merken konnte; ich kann mich auch heute noch sehr gut an Telefonnummern, Passworte und andere scheinbar triviale Details erinnern – bis zurück in meine Kindheit.

Ein anderes persönliches Interesse, das sich schon ganz früh herausbildete, war meine Faszination für die Kunst des Zauberns. Hatte ich erst mal herausgefunden, wie ein neuer Trick funktionierte, übte ich solange, bis ich ihn endlich gemeistert hatte. Durch das Zaubern entdeckte ich gewissermaßen, dass es mir Freude machte, geheimes Wissen zu erlangen.

VOM PHONE PHREAK ZUM HACKER

Meine erste Begegnung mit dem, was, wie ich später erfuhr, *Social Engineering* genannt wird, fand während meiner Zeit in der Highschool statt, als ich einen anderen Schüler traf, der sich mit einem Hobby namens *Phone Phreaking* beschäftigte. Das ist eine Art des Hackens, bei dem man das Telefonnetzwerk erforscht, indem man Telefonsysteme und Angestellte der Telefongesellschaften ausnützt. Er hat mir prima Tricks mit Telefonen gezeigt, wie man z.B. alle Informationen herauskriegt, die eine Telefongesellschaft über einen Kunden besitzt, und wie man mit einer Geheimnummer kostenlose Ferngespräche führen kann. (In Wahrheit war es nur für uns umsonst. Viel später fand ich heraus, dass es überhaupt keine Geheimnummer war, sondern die Telefonate auf irgendein Firmenkonto gebucht wurden.)

So lernte ich Social Engineering kennen – das war sozusagen mein Kindergarten. Mein Freund und ein anderer Phone Phreaker, den ich später kennen lernte, ließen mich zuhören, wie sie unter einem Vorwand die Telefongesellschaft anriefen und Dinge erzählten, die ihnen eine gewisse Glaubwürdigkeit verschafften. Ich erfuhr von unterschiedlichen Abteilungen der Telefongesellschaften und lernte Jargon und Abläufe kennen. Aber dieses „Training" währte nicht lange; das war auch nicht nötig, denn ich probierte selbst alles aus und lernte ständig dazu, so dass ich meine ersten Lehrer bald überrundete.

Damit war die Richtung abgesteckt, die mein Leben in den nächsten fünfzehn Jahren nehmen sollte.

In der Highschool hatte ich am meisten Spaß daran, mir den unautorisierten Zugang zu einer Telefonzentrale zu verschaffen und dann die Zugangsberechtigungen eines anderen Phone Phreakers zu verändern. Wenn er dann von zu Hause ein Telefonat führen wollte, hörte er eine Ansage, er solle eine Münze einwerfen, weil die Schaltzentrale der Telefongesellschaft aus der Art der Verbindung geschlossen hatte, er telefoniere von einem Münzfernsprecher aus.

Ich vertiefte mich immer mehr in alles, was mit Telefonen zusammenhing, nicht nur Elektronik, Schaltungen und Computer, sondern auch Organisation und Abläufe der Telefongesellschaften und die Terminologie. Nach einiger Zeit wusste ich wohl mehr über das Telefonsystem als viele Angestellte. Und dabei entwickelte ich meine Geschicklichkeit beim Social Engineering derart, dass ich im Alter von 17 Jahren die meisten Angestellten der Telefongesellschaften praktisch zu allem überreden konnte, egal ob ich persönlich oder am Telefon mit ihnen sprach.

Meine Karriere als Hacker, über die vielfältig berichtet wurde, begann in der Highschool. Ich kann hier nicht auf Einzelheiten eingehen, aber ein wichtiger Beweggrund für meine ersten Hacks war der Wunsch nach Anerkennung durch die Hacker-Gruppe.

Damals benutzten wir den Ausdruck *Hacker* für eine Person, die viel Zeit mit dem Herumbasteln an Hard- und Software verbrachte, um entweder effektivere Programme zu entwickeln oder unnötige Schritte zu vermeiden und schneller mit einer Sache fertig zu werden. Dieser Begriff wird heute sehr abwertend im Sinne eines „bösartigen Kriminellen“ verwendet. In diesem Buch gebrauche ich die Bezeichnung so wie früher – in einem freundlicheren Zusammenhang.

Nach der Highschool studierte ich Computerwissenschaften im *Computer Learning Center* in Los Angeles. Nach einigen Monaten fand der Computermanager der Schule heraus, dass ich mir Schwachstellen des Betriebssystems zunutze gemacht hatte und volle administrative Berechtigungen auf ihren IBM-Minicomputern besaß. Die besten Computerexperten des Lehrkörpers konnten nicht herausfinden, wie mir das gelungen war. Man machte mir ein Angebot, das ich nicht ablehnen konnte, und das war wohl eins der frühesten Beispiele, wie eine Firma einen Hacker angeworben hat. Ich konnte mir aussuchen, ob ich ein Projekt zur Verbesserung der Computersicherheit durchführen wolle oder gesperrt werde, weil ich das System gehackt hatte. Natürlich entschied ich mich für das Projekt und machte später meinen Abschluss *cum laude*.

ICH WERDE SOCIAL ENGINEER

Vielen Leuten ist das Aufstehen morgens eine Qual, weil ihnen vor dem sprichwörtlichen Alltagstrott graust. Mir war das Glück beschert, dass ich meine Arbeit genoss. Sie können sich insbesondere nicht vorstellen, mit welcher Freude mich die Herausforderung und der Lohn einer Tätigkeit als Privatdetektiv erfüllte. Ich verfeinerte meine Talente in der Schauspielkunst namens *Social Engineering* (wie man Leute dazu bringt, Dinge für ihnen fremde Personen auszuführen, die sie normalerweise nicht tun würden) und wurde dafür auch noch bezahlt.

Für mich war es keine Schwierigkeit, als Social Engineer zum Fachmann zu werden. Seit Generationen war meine Familie von der Seite meines Vaters her mit dem Verkaufen beschäftigt, und so könnte die Kunst der Beeinflussung und Überredung eine vererbte Charaktereigenschaft sein. Wenn Sie diesen Wesenszug mit der Neigung kombinieren, andere zu täuschen, haben Sie das Profil eines typischen Social Engineers.

Man könnte sagen, bei der Stellenbeschreibung eines Trickbetrügers gebe es zwei Spezialisierungen. Jemand, der andere anschwindelt und sie um ihr Geld betrügt, gehört zur Unterkategorie des *Grifters* (Gauner). Jemand, der Täuschung, Betrug und Überredung bei Firmen einsetzt, um in der Regel an deren Informationen zu gelangen, wird als *Social Engineer* bezeichnet. Schon in der Zeit, als ich mit den Bustickets herumtrickste (als ich noch zu jung war, um zu erkennen, dass das etwas Böses war), erkannte ich bei mir das Talent, Geheimnisse herauszufinden, die ich eigentlich nicht kennen sollte. Auf dieses Talent baute ich mit Täuschung und dem richtigen Jargon auf und entwickelte ein ausgefeiltes Geschick in der Manipulation.

Um mein Geschick in diesem Gewerbe auszubauen (wenn ich es denn ein Gewerbe nennen darf), wählte ich einen kleinen Aspekt einer Information, die mir eigentlich gleichgültig war, und dann versuchte ich, am Telefon jemanden zu überreden, mir diese Info zu verraten, einfach nur, um meine Fähigkeiten zu schulen. Auf die gleiche Art und Weise, wie ich meine Zaubertricks einstudierte, übte ich den Einsatz verschiedener Vorwände ein. Durch diese Probeläufe fand ich schnell heraus, dass ich praktisch jede gewünschte Information erlangen konnte.

Jahre später beschrieb ich es in meiner Aussage im Kongress vor den Senatoren Lieberman und Thompson folgendermaßen:

> Ich habe unerlaubten Zugang zu einigen der weltweit größten Unternehmen erlangt und erfolgreich einige der hartnäckigsten Computersysteme geknackt, die jemals entwickelt worden sind. Dabei habe ich mich techni-

> scher und nicht-technischer Mittel bedient, um mir den Quellcode verschiedener Betriebssysteme und Telekommunikationsgeräte zu beschaffen, damit ich ihre Schwachstellen und internen Funktionsweisen studieren konnte.

Meine gesamten Aktivitäten sollten nur der Befriedigung meiner eigenen Neugier dienen. Ich wollte meine Möglichkeiten kennen lernen und geheime Informationen über Betriebssysteme, Handys und alles andere, was mich neugierig machte, erfahren.

SCHLUSSBEMERKUNG

Ich habe seit meiner Verhaftung erkannt, dass meine Handlungen illegal waren und ich Verletzungen des Datenschutzes begangen habe.

Meine Neugier hat mich zu den Verbrechen motiviert. Ich wollte so viel wie möglich darüber erfahren, wie Telefonnetze arbeiten und wie es sich mit der Computersicherheit verhält. Ich wurde von dem Kind, das Zaubertricks liebte, zum weltweit berüchtigten Hacker – von Regierungen und Unternehmen gefürchtet! Wenn ich an mein Leben in den vergangenen dreißig Jahren zurückdenke, muss ich mir eingestehen, dass ich durch meinen Wunsch, Technologien zu begreifen, mein Bedürfnis nach guten intellektuellen Herausforderungen und meine Neugier einige sehr schlechte Entscheidungen getroffen habe.

Mittlerweile bin ich ein neuer Mensch geworden. Ich nutze meine Talente und das umfassende Wissen, das ich über Informationssicherheit und Taktiken des Social Engineering angesammelt habe, um Regierungen, Firmen und Einzelpersonen dabei zu helfen, Bedrohungen ihrer Informationssicherheit zu erkennen, zu vermeiden und zu begegnen.

In diesem Buch kann ich auf eine weitere Art und Weise meine Erfahrungen für andere nützlich machen, die sich gegen die weltweiten Aktivitäten bösartiger Informationsdiebe schützen wollen. Ich hoffe, Sie finden die Storys unterhaltsam, erhellend und lehrreich.

Kapitel 1

Das schwächste Glied der Kette

Ein Unternehmen kann sich die besten Sicherheitstechnologien geleistet haben, die für Geld zu kriegen sind. Die Angestellten sind so gut ausgebildet, dass sie alle sensiblen Daten besonders aufmerksam sichern, bevor sie abends nach Hause gehen. Alle Firmengebäude werden von den besten Sicherheitsfirmen des Landes rund um die Uhr bewacht.

Und trotzdem ist dieses Unternehmen immer noch absolut gefährdet!

Sie können alle Expertentipps zur Datensicherheit befolgen, sorgsam alle empfohlenen Sicherheitsprogramme installieren und bei der Absicherung der Systemkonfiguration durch die Aktualisierung der Software durch und durch wachsam sein.

Trotzdem sind auch Sie immer noch absolut gefährdet!

DER MENSCHLICHE FAKTOR

Als ich vor einiger Zeit vor dem amerikanischen Kongress aussagte, führte ich aus, dass ich Passwörter und andere sensible Daten von Firmen oft dadurch bekam, dass ich mich als jemand anderes ausgab und dann *einfach danach gefragt habe*.

Es ist ein natürliches Bedürfnis, sich nach vollkommener Geborgenheit zu sehnen, aber das führt viele Menschen dazu, sich mit einem falschen Sinn von Sicherheit zufrieden zu geben. Nehmen wir den verantwortungsbewussten und fürsorglichen Hausbesitzer, der in seine Tür ein absolut einbruchssicheres Schloss eingebaut hat, um sein Zuhause, seine Frau und Kinder zu schützen. Nun ist er zufrieden, dass er seine Familie gut vor Eindringlingen bewahren kann. Aber was ist, wenn der Einbrecher ein Fenster einschlägt oder den Code für das Garagentor knacken kann? Da könnte man doch ein robustes Sicherheitssystem installieren, oder? Das ist besser, aber immer noch keine Garantie. Ob mit oder ohne teure Schlösser – der Hausbesitzer bleibt gefährdet.

Warum? Weil der *menschliche* Faktor die eigentliche Schwachstelle der Sicherheitskette ist.

Sicherheit ist allzu oft nur eine Illusion, die häufig durch Leichtgläubigkeit, Arglosigkeit oder Ignoranz verschlimmert wird. Vom berühmtesten Wissenschaftler des 20. Jahrhunderts, Albert Einstein, stammt das Zitat: „Zwei Dinge sind unendlich: das Universum und die menschliche Dummheit. Aber bei dem Universum bin ich mir noch nicht ganz sicher." Letzten Endes können Angriffe durch Social Engineering erfolgreich sein, wenn Menschen dumm sind oder – was viel weiter verbreitet ist – einfach keine Ahnung von grundlegenden Sicherheitspraktiken haben. Mit der gleichen Einstellung wie unser sicherheitsbewusster Hausbesitzer halten viele Profis aus der Informationsbranche an dem Irrtum fest, sie hätten ihre Firmen weitgehend gegen Angriffe abgeschirmt, weil sie Standard-Sicherheitsprodukte installiert haben: Firewalls, Zugangsbeschränkungssysteme oder widerstandsfähigere Authentifizierungsgeräte wie zeitbasierte Tokens oder biometrische Smart Cards. Jeder, der glaubt, dass allein die Anwendung von Sicherheitsprodukten ausreiche, echte Sicherheit zu gewährleisten, gibt sich mit der *Illusion* von Sicherheit zufrieden. Damit folgen diese Leute einem Wunschdenken: sie werden unweigerlich früher oder später einen Sicherheitszwischenfall hinnehmen müssen.

Der berühmte Sicherheitsberater Bruce Schneier drückt es so aus: „Sicherheit ist kein Produkt, sondern ein Prozess." Darüber hinaus ist Sicherheit keine technologische Angelegenheit, sondern ein menschliches und ein Management-Problem.

In dem Maße, wie Forscher immer bessere Sicherheitstechnologien entwickeln und damit die Möglichkeit verringern, dass technische Schwachstellen ausgenutzt werden können, werden Angreifer immer mehr den Hebel beim menschlichen Faktor ansetzen. Es ist oft ein Kinderspiel, die menschliche Firewall zu knacken. Das erfordert außer einem Telefonanruf keine Investitionen und beinhaltet nur ein minimales Risiko.

EIN KLASSISCHER FALL VON TÄUSCHUNG

Was ist die größte Bedrohung für die Sicherheit Ihres geschäftlichen Kapitals? Ganz einfach: der Social Engineer – ein skrupelloser Zauberer, der Ihre Aufmerksamkeit auf seine linke Hand zieht, während er mit rechts Ihre Geheimnisse klaut. Diese Type ist oft so freundlich, wortgewandt und entgegenkommend, dass es Ihnen eine Freude ist, ihm begegnet zu sein.

Schauen wir uns ein Beispiel für Social Engineering an. Nicht viele erinnern sich heutzutage noch an den jungen Mann namens Stanley Mark Rifkin und sein kleines Abenteuer mit der jetzt geschlossenen Security Pacific National

Bank in Los Angeles. Über seine Eskapaden ist in sehr unterschiedlichen Versionen berichtet worden. Rifkin selbst hat (wie ich) niemals seine eigene Geschichte erzählt, und so basiert das Folgende auf veröffentlichten Meldungen.

Der Code wird geknackt

Im Jahre 1978 schlenderte Rifkin eines Tages hinüber in die Buchungsabteilung der Security Pacific National Bank, zu dem nur befugtes Personal Zutritt hatte. Dort wurden täglich Überweisungen im Werte von mehreren Milliarden Dollar veranlasst.

Er arbeitete für eine externe Firma, die im Auftrag der Bank ein Datensicherungssystem für die Buchungsabteilung entwickelte, falls die Computer dort einmal abstürzen sollten. Das berechtigte ihn, die Transferprozeduren einzusehen, und somit hatte er Einblick, wie die Bank die Durchführung von Überweisungen abwickelte. Er erfuhr, dass Bankangestellte, die zur Anweisung von Buchungen berechtigt waren, jeden Morgen einen streng bewachten neuen Code erhielten, den sie für die Anrufe in der Buchungsabteilung benötigten.

In der Buchungsabteilung sparten sich die Angestellten die Mühe, jeden Tag einen neuen Code auswendig zu lernen: Sie übertrugen den Code auf einen Notizzettel und brachten diesen an einer leicht sichtbaren Stelle an. An diesem speziellen Tag im November hatte Rifkin einen besonderen Grund für seinen Besuch. Er wollte einen Blick auf dieses Papier werfen.

Er notierte sich einige Dinge über Verfahrensweisen in der Buchungsabteilung, offensichtlich um sicherzustellen, dass sich das Datensicherungssystem korrekt in die regulären Systeme einpasst. Nebenbei las er heimlich den Sicherheitscode für den heutigen Tag und merkte ihn sich. Einige Minuten danach verließ er den Raum. Wie er später aussagte, fühlte er sich, als hätte er den Hauptgewinn einer Lotterie bekommen.

Da gibt es dieses Schweizer Konto ...

Als er den Raum gegen 15 Uhr verließ, marschierte er direkt zu einem Münzfernsprecher im marmornen Foyer des Gebäudes. Er warf eine Münze ein und wählte die Nummer der Buchungsabteilung. Nun wechselte er seine Rolle und verwandelte sich vom Unternehmensberater Stanley Rifkin in den Kollegen namens Mike Hansen aus der Internationalen Abteilung der Bank.

Nach einer Zeugenaussage verlief das Gespräch in etwa wie folgt:

„Hallo“, sagte er zu der jungen Frau am anderen Ende der Leitung, „hier ist Mike Hansen von der Internationalen Abteilung.“

Sie fragte nach der Büronummer. Das war eine übliche Prozedur, und seine Antwort war vorbereitet: „286."

Die junge Frau fragte nun: „In Ordnung. Wie lautet der Code?"

Rifkin meinte später, dass an diesem Punkt sein von Adrenalin getriebener Herzschlag „ordentlich einen zulegte". Er erwiderte geschmeidig: „4789." Dann fuhr er mit den Anweisungen für eine Buchung über „exakt zehn Millionen zweihunderttausend Dollar" an die Irving Trust Company in New York als Gutschrift für die Woschod Handelsbank von Zürich in der Schweiz fort, bei der er schon ein Konto eingerichtet hatte.

„In Ordnung, das habe ich", sagte die Frau. „Jetzt brauche ich noch die bürointerne Abrechnungsnummer."

Rifkin brach der Schweiß aus. Mit dieser Frage hatte er nicht gerechnet. Ihm schien bei seinen Nachforschungen etwas durch die Lappen gegangen zu sein. Aber es gelang ihm, in seiner Rolle die Fassung zu bewahren, tat so, als ob alles in Ordnung sei und antwortete, ohne zu zögern: „Oh, das muss ich gerade mal nachprüfen. Ich rufe gleich wieder an." Erneut tauschte er die Rollen und telefonierte mit einer anderen Abteilung der Bank, wobei er sich diesmal als ein Angestellter aus der Buchungsabteilung ausgab. Er bekam die Abrechungsnummer und rief die junge Frau zurück.

Sie nahm die Nummer entgegen und bedankte sich. (Unter diesen Umständen muss man es als höchst ironisch ansehen, dass sie sich bei Rifkin bedankte.)

Auf der Zielgeraden

Ein paar Tage danach nahm Rifkin ein Flugzeug in die Schweiz, ließ sich das Geld bar auszahlen und übergab für einen Beutel Diamanten mehr als acht Millionen Dollar an eine russische Agentur. Er flog zurück und passierte problemlos mit den Diamanten in einem Geldgürtel den amerikanischen Zoll. Er hatte den größten Banküberfall der Geschichte durchgezogen – und dabei weder eine Waffe und noch nicht mal einen Computer gebraucht. Seltsamerweise brachte ihm diese Eskapade später einen Eintrag im Guiness-Buch der Rekorde in der Kategorie „Größter Computerbetrug".

Stanley Rifkin hat die Kunst der Täuschung eingesetzt – die Fertigkeiten und Techniken, die man heute Social Engineering nennt. Dafür brauchte er bloß eine durchdachte Planung und gute Redegewandtheit.

Und darum geht es in diesem Buch – um die Techniken des Social Engineering (darin bin ich Ihr ergebener Diener) und wie Sie sich und Ihre Firma davor schützen können.

WORIN LIEGT DIE BEDROHUNG?

Die Rifkin-Story macht sehr deutlich, wie irreführend unser Sicherheitsbedürfnis sein kann. *Jeden Tag* kommen solche Fälle vor – gut, vielleicht nicht in der Größenordnung von 10 Millionen Dollar, aber nichtsdestotrotz verursachen sie schwere Schäden. Vielleicht verlieren Sie gerade in diesem Moment Geld oder jemand klaut die Pläne eines neuen Produkts – und Sie erfahren es nicht einmal. Wenn Ihr Unternehmen bisher verschont geblieben ist, stellt sich nicht die Frage, *ob* es passiert, sondern *wann*.

Wachsende Besorgnis

In einem Gutachten über Computerverbrechen aus dem Jahre 2001 berichtete das *Computer Security Institute*, dass 85 % der an der Untersuchung beteiligten Unternehmen in den vergangenen 12 Monaten Verletzungen der Computersicherheit aufgedeckt haben. Diese Zahl ist erstaunlich: Nur 15 von 100 beteiligten Organisationen teilten mit, dass es im vergangenen Jahr keine Sicherheitsverletzungen gegeben hat. Ähnlich verblüffend war die Zahl der Organisationen, die nach eigenen Berichten aufgrund von Sicherheitslücken bei Computern finanzielle Verluste erlitten: 64 %. Mehr als die Hälfte wurden also finanziell geschädigt. *In einem einzigen Jahr!*

Meine eigenen Erfahrungen führen mich zu der Annahme, dass die Zahlen bei solchen Berichten in gewisser Weise aufgebläht sind. Ich habe kein großes Vertrauen in die Art und Weise, wie man diese Untersuchungen durchführt. Das heißt nicht, dass man die Nachteile vernachlässigen kann – die Schäden sind weitreichend! Wer nicht auf Sicherheitsprobleme ausgerichtet plant, hat ein Versagen gleich mit eingebaut.

Die kommerziellen Sicherheitsprodukte, die bei den meisten Unternehmen eingesetzt werden, sollen hauptsächlich Schutz gegen Amateur-Hacker wie die gemeinhin als Skript Kiddies bekannten Jugendlichen bieten. Tatsächlich sind diese Möchtegern-Hacker mit ihrer selbst heruntergeladenen Software kaum mehr als nur ärgerlich. Größere Verluste – und hier liegt die wahre Bedrohung – muss man von erfahrenen Angreifern mit klar definierten Zielen befürchten, die aus Geldgier handeln. Diese Personen konzentrieren sich auf jeweils ein Ziel, wogegen die Amateure versuchen, so viele Systeme wie möglich zu infiltrieren. Die Amateure bei den Computer-Eindringlingen stellen einfach auf Quantität ab, aber die Profis zielen auf qualitativ wertvolle Daten.

Sicherheitsprogramme für Unternehmen benötigen Technologien wie Authentifizierungssysteme (zur Identitätsprüfung), Zugangskontrollen (für die Verwaltung von Zugangsberechtigungen für Daten und Computersysteme) und Frühwarnsysteme gegen Computer-Einbrecher (die elektronische Entsprechung zur Alarmanlage). Dennoch geben Unternehmen heute immer

noch mehr Geld für Kaffeemaschinen aus als für Maßnahmen zum Schutz der Firma gegen Sicherheitsangriffe.

Genau wie ein Ganove einer Versuchung nicht widerstehen kann, reizt es den Hacker immens, einen Weg um die Abschirmungen durch Hochsicherheitstechnologien herum zu finden. Und meistens beginnen sie damit, den Hebel bei den Anwendern dieser Technologien anzusetzen.

Betrügerische Praktiken

Es gibt eine populäre Redewendung, dass nur ein abgeschalteter Computer ein sicherer Computer sei. Clever, aber verkehrt: Der Schwindler überredet einfach jemanden, ins Büro zu gehen und diesen PC einzuschalten. Wenn Ihr Gegner Ihre Daten herauskriegen will, kommt er auch ans Ziel, gewöhnlich auf verschiedenen Wegen. Das ist nur eine Frage von Zeit, Geduld, Hartnäckigkeit und Ausstrahlung. Und hier kommt die Kunst der Täuschung ins Spiel.

Um Sicherheitsmaßnahmen auszutricksen, muss ein Angreifer, Eindringling oder Social Engineer einen Weg finden, einen vertrauensvollen User so zu täuschen, dass er Informationen weitergibt, oder die arglose Zielperson derart zu überlisten, dass sie den Zugang freigibt. Wenn vertrauensvolle Angestellte so getäuscht, beeinflusst oder manipuliert werden, dass sie sensible Daten weitergeben oder Handlungen ausführen, die einem Eindringling ein Schlupfloch bieten, kann keine Technologie der Welt Ihre Organisation schützen. Manchmal kann ein Dechiffrierer den Klartext einer kodierten Botschaft entschlüsseln, wenn er über eine Schwachstelle des Codes die Verschlüsselungstechnologie umgehen kann, und genau so täuschen Social Engineers bei Ihren Angestellten falsche Tatsachen vor, um den Sicherheitstechnologien auszuweichen.

VERTRAUENSMISSBRAUCH

Erfolgreiche Social Engineers besitzen meist sehr gute soziale Kompetenzen. Sie sind charmant, höflich und einem gleich sympathisch – Charakterzüge, mit denen schnell eine Beziehung und ein Vertrauensverhältnis aufgebaut werden kann. Ein erfahrener Social Engineer ist in der Lage, über die Taktiken und Strategien seines Gewerbes sich praktisch alle gewünschten Informationen anzueignen.

Ausgefuchste Techniker haben durchdachte Lösungen für den Bereich der Informationstechnologie entwickelt, um die mit dem Einsatz von Computern verbundenen Risiken zu minimieren. Aber dabei haben sie die signifikanteste Schwachstelle übersehen: den menschlichen Faktor. Trotz unseres Verstandes stellen wir Menschen – Sie, ich und alle anderen – immer noch das bedrohlichste Risiko für unsere gegenseitige Sicherheit dar.

Unser nationaler Charakter

Uns ist diese Bedrohung nicht bewusst, insbesondere nicht in der westlichen Welt. Vor allem in den Vereinigten Staaten sind wir nicht darauf trainiert, argwöhnisch miteinander umzugehen. Wir haben gelernt, dass wir „unseren Nächsten lieben" und einander vertrauensvoll begegnen sollen. Denken Sie daran, wie schwierig es für Organisationen des Nachbarschaftsschutzes ist, die Leute dazu zu bringen, ihre Häuser und Autos abzuschließen. Diese Art von Schwachstelle ist offensichtlich, und sie wird trotzdem von vielen ignoriert, die es vorziehen, in einer Traumwelt zu leben – bis sie auf die Nase fallen.

Wir wissen, dass nicht alle Menschen aufrichtig und ehrlich sind, aber nur allzu oft leben wir so, als ob alle es wären. Diese liebenswürdige Unschuld ist der Grundstoff des amerikanischen Lebens, und es ist sehr schmerzhaft, dies aufzugeben. Als Nation haben wir in unsere Vorstellung von Freiheit eingebaut, dass die Orte am lebenswertesten sind, an denen man am wenigsten Schloss und Riegel braucht.

Die meisten Leute gehen von der Annahme aus, dass sie von anderen nicht getäuscht werden, und gründen dies auf den Glauben, dass die Wahrscheinlichkeit einer Täuschung recht gering sei. Der Angreifer wiederum berücksichtigt dieses weitverbreitete Wunschdenken und lässt seine Bitte so vernünftig erscheinen, dass sie völlig unverdächtig wirkt, während er gleichzeitig das Vertrauen des Opfers missbraucht.

Die Arglosigkeit der Organisationen

Ganz deutlich wurde diese Arglosigkeit, die Teil unseres nationalen Charakters ist, als Computer zum ersten Mal miteinander verbunden wurden. Erinnern Sie sich daran, dass der Vorläufer des Internet – das ARPAnet (das *Advanced Research Projects Agency Network* des Verteidigungsministeriums) – für die Verteilung von Informationen zwischen Regierungs-, Forschungs- und Bildungseinrichtungen konzipiert war. Man hatte sich gleichzeitig mit der Informationsfreiheit den technischen Fortschritt zum Ziel gesetzt. Darum haben viele Bildungseinrichtungen seinerzeit bei den frühen Computersystemen wenig oder gar nicht auf Sicherheit geachtet. Jemand wie der besonders freigeistige berühmte Software-Entwickler Richard Stallman weigerte sich sogar, sein Konto mit einem Passwort zu schützen.

Als dann das Internet für eCommerce eingesetzt wurde, wandelten sich die Gefahren einer schwachen Sicherheit in unserer verdrahteten Welt dramatisch. Der Ausbau der Technologie wird aber nicht das Problem lösen, das der Mensch für die Sicherheit darstellt.

Schauen wir uns nur die heutigen Flughäfen an. Zwar sind Sicherheitsmassnahmen allgegenwärtig, aber trotzdem alarmieren uns Medienberichte über

Reisende, die Sicherheitsvorkehrungen umgehen konnten und potenzielle Waffen an Kontrollpunkten vorbeischmuggelten. Wie kann das sein in einer Zeit, in der sich alle unsere Flughäfen in einem derartigen Alarmzustand befinden? Sind die Metalldetektoren kaputt? Nein. Das Problem liegt nicht bei den Maschinen. Das Problem ist der menschliche Faktor: das Personal an den Maschinen. Die Flughafenbehörden können die Nationalgarde aufstellen und Metalldetektoren und Systeme zur Erkennung von Gesichtern installieren, aber deutlich hilfreicher wäre die Ausbildung des Sicherheitspersonals an vorderster Front, wie man Reisende korrekt überprüft.

Das gleiche Problem findet sich in den Regierungs- und Bildungseinrichtungen und Unternehmen auf der ganzen Welt. Trotz der Anstrengungen aller Sicherheitsprofis bleiben Informationen nicht gut genug geschützt. Bis nicht das schwächste Glied in der Sicherheitskette – der Mensch – gestärkt worden ist, bleiben Daten für Angreifer mit den Fähigkeiten eines Social Engineers leicht zu pflücken.

Mehr als jemals zuvor müssen wir unser Wunschdenken ablegen und uns der Techniken gewahr werden, die diejenigen anwenden, die die Vertraulichkeit, Integrität und Verfügbarkeit unserer Computer und Netzwerke angreifen wollen. Wir haben eingesehen, dass wir im Straßenverkehr defensiv fahren sollten, und nun ist es an der Zeit, die Praxis eines defensiven Umgangs mit Computern zu akzeptieren und zu erlernen.

Die Gefährdung durch einen Einbruch in Ihre Privatsphäre, Ihre Gedanken oder das Informationssystem Ihrer Firma mag solange irreal erscheinen, bis er tatsächlich stattfindet. Um eine derart kostspielige Dosis Realität zu vermeiden, sollte jedem die Bedeutung klar werden, warum wir wachsam und ausgebildet sein müssen, um aggressiv unser Informationskapital, unsere persönlichen Daten und die kritischen Infrastrukturen unseres Landes schützen zu können. Und diese Vorsichtsmaßnahmen müssen wir heute treffen!

TERROR UND TÄUSCHUNG

Natürlich ist Täuschung nicht das exklusive Instrument des Social Engineers. Realer Terrorismus bringt die größten Schlagzeilen, und uns wird so deutlich wie niemals zuvor klar, wie es gefährlich in der Welt zugeht. Die Zivilisation ist immer noch bloß eine dünne Schicht Tünche.

Die Angriffe auf New York und Washington D.C. im September 2001 haben uns allen Furcht und Schrecken eingeflößt – nicht nur in Amerika, sondern bei allen wohlgesinnten Menschen weltweit. Wir sind jetzt alarmiert, dass es überall auf der Welt besessene Terroristen gibt, die gut ausgebildet nur darauf warten, uns mit weiteren Angriffen zu verheeren.

Die kürzlich verstärkten Bemühungen unserer Regierung haben unser Sicherheitsbewusstsein deutlich erhöht. Wir müssen wachsam bleiben und uns gegen jegliche Form von Terrorismus schützen. Wir müssen lernen, wie Terroristen auf bösartige Weise sich falsche Identitäten verschaffen, die Rolle eines Studenten oder Nachbarn einnehmen und mit der Menge verschmelzen. Sie verschleiern ihre wahren Beweggründe, während sie sich gegen uns verschwören – dabei verwenden sie ähnliche Tricks wie die, über die Sie in diesem Buch lesen werden.

Und obwohl sich Terroristen meines Wissens bisher noch nicht aus der Trickkiste des Social Engineers bedient haben, um Unternehmen, Trinkwasserkläranlagen, Kraftwerke oder andere vitale Komponenten unserer nationalen Infrastruktur zu infiltrieren, besteht diese Gefahr auf jeden Fall, denn es ist einfach viel zu leicht. Ich hoffe, dass dieses Buch dazu beiträgt, das nötige Sicherheitsbewusstsein in den oberen Etagen der Unternehmen zu wecken, denn nötige Richtlinien zur Datensicherheit werden kein bisschen zu früh kommen.

ÜBER DIESES BUCH

Die Sicherheit eines Unternehmens ist eine Frage der Balance. Zu wenig Sicherheit macht Ihre Firma angreifbar, aber ein Übermaß an Sicherheit steht bei der Durchführung der alltäglichen Arbeit im Weg und hemmt das Wachstum und den Erfolg des Unternehmens. Die Herausforderung besteht in der Aufgabe, einen Ausgleich zwischen Sicherheit und Produktivität zu schaffen.

Andere Bücher über die Sicherheit von Unternehmen beschäftigen sich vor allem mit der Technologie von Hard- und Software und berücksichtigen nicht genug die größte aller Bedrohungen: dass man Menschen täuschen kann. In diesem Buch habe ich mir dagegen zum Ziel gesetzt, Sie, Ihre Mitarbeiter und andere Angestellte Ihres Unternehmens über die Gefahren der Manipulation aufzuklären und über die Schutzmaßnahmen zu informieren, mit denen Sie verhindern, weiterhin Opfer zu sein. Dieses Buch konzentriert sich hauptsächlich auf nicht-technische Methoden, mit denen Eindringlinge Informationen stehlen und die Integrität von Daten kompromittieren, von denen man fälschlicherweise annimmt, sie seien geschützt, oder die Arbeitsergebnisse Ihres Unternehmens zerstören.

Meine Aufgabe wird durch eine einfache Wahrheit erschwert: Jeder von uns wurde von den größten Social-Engineering-Experten aller Zeiten manipuliert: den eigenen Eltern. Sie haben stets Mittel und Wege gefunden, dass wir das tun – „nur zu deinem Besten!“ –, was sie von uns erwarten. Eltern werden auf die gleiche Art zu großartigen Geschichtenerzählern, wie Social Engineers geschickt absolut plausible Geschichten, Begründungen und Rechtfertigun-

gen entwickeln, um an ihr Ziel zu kommen. Ja, wir sind allesamt durch unsere Eltern geformt worden: mehr oder weniger wohlwollende Social Engineers.

Wir sind anfällig für Manipulationen, weil dieses Training uns darauf konditioniert hat. Unser Leben wäre sehr schwierig, wenn wir dauernd aufpassen, andere verdächtigen und uns darum kümmern müssten, nicht von jemanden reingelegt zu werden, der uns ausnutzen will. In einer perfekten Welt würden wir anderen ohne weiteres vertrauen und davon ausgehen, dass die Menschen, denen wir begegnen, ehrlich und zuverlässig sind. Aber unsere Welt ist weit davon entfernt, perfekt zu sein, und so ist es notwendig, einen hohes Maß an Wachsamkeit zu halten, um die Täuschungsversuche unserer Gegner abzuwehren.

In den Hauptteilen 2 und 3 dieses Buches können Sie die Social Engineers in Aktion erleben. Sie werden über Folgendes lesen:

- Was Phone Phreaks schon vor Jahren herausgefunden haben: eine raffinierte Methode, um von einer Telefongesellschaft eine nicht eingetragene Telefonnummer zu erfahren.
- Verschiedene Methoden, wie ein Angreifer sogar von wachsamen und argwöhnischen Angestellten Benutzernamen und Passwörter ergaunern kann.
- Wie ein Angreifer einen Betriebsleiter dazu brachte, ihm beim Diebstahl geheimster Produktinformationen der Firma behilflich zu sein.
- Mit welchen Methoden ein Angreifer eine Angestellte zum Herunterladen einer Software überreden konnte, die alle ihre Tastatureingaben aufzeichnen kann und die Details per Email an den Angreifer schickt.
- Wie Privatdetektive an private und Firmendaten kommen, so dass es Ihnen zweifellos kalt den Rücken herunterlaufen wird.

Vielleicht denken Sie, wenn Sie einige der Geschichten aus Teil 2 und 3 lesen, das sei unmöglich: Niemand könne wirklich mit diesen Lügen, schmutzigen Tricks und Intrigen durchkommen, von denen Sie auf diesen Seiten lesen. Die Realität ist: Jede Geschichte schildert Ereignisse, die möglich sind und die es schon gegeben hat. Viele davon geschehen jeden Tag irgendwo auf der Welt, vielleicht ja sogar in Ihrer Firma, während Sie dieses Buch lesen.

Das Material aus diesem Buch wird Ihnen wirklich die Augen öffnen, wenn Sie Ihre Firma abschirmen wollen, aber Sie können auch Ihre ganz persönlichen Daten schützen und die Einbruchsversuche eines Social Engineers in Ihr Privatleben abwehren.

In Teil 4 dieses Buches wechseln wir die Gangart. Mein Ziel ist, Sie in Ihrer Firma beim Aufbau und der Umsetzung der nötigen Richtlinien und bei der Durchführung von Aufklärungstrainings zu unterstützen. Dadurch können Sie die Wahrscheinlichkeit verringern, dass Ihre Angestellten jemals wieder von einem Social Engineer hereingelegt werden. Ein Verständnis der Strategien, Methoden und Taktiken eines Social Engineers wird Ihnen dabei helfen, vernünftige Kontrollen einzusetzen, um Ihr informationstechnologisches Kapital abzusichern, ohne die Produktivität der Firma zu unterminieren.

Kurzum, ich habe dieses Buch geschrieben, um Sie vor dem Social Engineering als einer gefährlichen Bedrohung zu warnen, und Ihnen dabei behilflich zu sein, das Risiko für Ihre Firma und Angestellten, auf diese Art ausgenutzt zu werden, zu senken.

Oder vielleicht sollte ich sagen, dass sie überhaupt jemals wieder ausgenutzt werden.