

Kapitel

5

„Darf ich Ihnen helfen?“

Wir sind alle sehr dankbar, wenn wir uns mit einem Problem herumschlagen und jemand mit Kenntnis und Geschick hilfsbereit vorbeikommt und uns Unterstützung anbietet. Dies nutzt ebenfalls der Social Engineer aus.

Er weiß aber genauso, wie er anderen Probleme *macht* ... und Sie sind dann sehr froh und dankbar, wenn er das Problem wieder löst ... so dass Sie ihm schließlich zu Dank verpflichtet sind und ihm eine kleine Info geben oder ihm einen Gefallen tun, was sich für Ihre Firma (oder auch Sie persönlich) nach der Begegnung deutlich als nachteilig erweist. Und vielleicht erfahren Sie auch niemals, dass Sie etwas Wertvolles verloren haben.

Ich möchte Ihnen einige typische Arten vorstellen, wie ein Social Engineer seine „Hilfe“ anbietet.

NETZWERKAUSFALL

Datum/Uhrzeit: Montag, der 12. Februar, 15:25

Ort: Büro der Schiffbaugesellschaft Starboard

Der erste Anruf: Tom DeLay

„Buchhaltung, Tom DeLay.“

„Hallo Tom, hier spricht Eddie Martin vom Computer-Service. Wir versuchen gerade, ein Netzwerkproblem zu beheben. Wissen Sie zufällig, ob jemand aus Ihrer Abteilung Probleme damit hat, ins Netzwerk zu kommen?“

„Hm, keine Ahnung. Ich glaube nicht.“

„Und Sie selbst haben keine Schwierigkeiten?“

Der erste Anruf: Tom DeLay (Forts.)

„Nein, alles prima.“

„Das freut mich. Hören Sie, wir starten gerade einen Rundruf an Leute, die betroffen sein könnten, weil es ganz wichtig ist, dass Sie uns sofort informieren, wenn Sie Ihre Netzwerkverbindung verlieren.“

„Das hört sich aber nicht gut an. Glauben Sie wirklich, dass das passieren kann?“

„Das wollen wir nicht hoffen, aber bitte melden Sie sich dann bitte gleich bei uns, ja?“

„Aber hallo werde ich das machen.“

„Hört sich so an, als ob es ein großes Problem für Sie ist, wenn Ihre Netzwerkverbindung zusammenbricht ...“

„Darauf können Sie Gift nehmen.“

„Ich gehe Ihnen mal für alle Fälle meine Handy-Nummer, während wir am Problem arbeiten. Dann können Sie mich direkt erreichen, falls es nötig ist.“

„Das wäre große Klasse. Schießen Sie los.“

„Die Nummer ist 555 867 5309.“

„555 867 5309. Hab ich. Vielen herzlichen Dank. Wie war noch mal Ihr Name?“

„Ich bin Eddie. Hören Sie, da ist noch was – ich muss prüfen, über welchen Port Ihr PC verbunden ist. Schauen Sie doch mal auf Ihren Rechner, ob Sie einen Aufkleber mit so was wie ‚Portnummer‘ finden.“

„Warten Sie ... Nein, so was sehe ich hier nicht.“

„Okay, dann schauen Sie doch bitte auf der Rückseite des Rechners, ob Sie ein Netzkabel sehen.“

„Ja, da ist was.“

„Folgen Sie dem Kabel bis dorthin, wo es im Rechner steckt, und schauen, ob der Stecker da ein Etikett hat.“

„Momentchen ... Ja, da ist was, ich muss mich grad mal bücken, damit ich das lesen kann. Ah ja, da steht Port 6.47.“

„Gut, das hatten wir uns auch notiert, wollte nur noch mal sichergehen.“

Der zweite Anruf: Der Kollege aus der IT-Abteilung

Zwei Tage später geht ein Anruf im Netzwerkzentrum der gleichen Firma ein.

„Hallo, Bob am Apparat. Ich bin im Büro von Tom DeLay aus der Buchhaltung. Wir versuchen gerade, ein Kabelproblem zu lösen. Bitte deaktivieren Sie mal den Port 6.47.“

Der Kollege aus der IT-Abteilung meint, das sei in einigen Minuten erledigt, und man möge ihm doch Bescheid sagen, wenn er den Port wieder aktivieren soll.

Der dritte Anruf: Hilfe vom Feind

Etwa eine Stunde später macht der Typ, der sich Eddie Martin nennt, gerade im Baumarkt ein paar Einkäufe, als sein Handy klingelt. Mit einem Blick auf die Anruferidentifikation sieht er, dass der Anruf von der Schiffbaugesellschaft kommt, und eilt an ein ruhiges Plätzchen, bevor der den Anruf annimmt.

„Computer-Service, Eddie am Apparat.“

„Oh, hallo Eddie. Das haltt so, wo sind Sie denn gerade?“

„Äh, bin gerade in einem Schaltschrank. Wer spricht da bitte?“

„Hier ist Tom DeLay. Mensch, bin ich froh, dass ich Sie erreiche. erinnern Sie sich noch, dass wir vor zwei Tagen gesprochen haben? Gerade ist meine Netzwerkverbindung zusammengebrochen, genau wie Sie es gesagt haben, und mir geht hier ganz schön die Düse.“

„Ja, da arbeiten schon ein paar von uns dran. Das sollten wir bis heute Abend wieder repariert haben. Geht das klar bei Ihnen?“

„NEIN! Verdammt, wenn ich so lange raus bin, komme ich total in Verzug! Können Sie das nicht schneller hinkriegen?“

„Wie eilig ist das bei Ihnen?“

„Ich kann ein paar andere Sachen vorziehen. Können Sie das vielleicht in etwa einer halben Stunde hinkriegen?“

„Halbe Stunde!! Sie haben ja gar keine Ansprüche. Hören Sie, ich lasse alles fallen und sehe zu, dass ich das für Sie wieder hinniege.“

„Eddie, das wäre ganz große Klasse, vielen Dank.“

Der vierte Anruf: Volltreffer!

Eine dreiviertel Stunde später ...

„Tom? Hier ist Eddie. Checken Sie mal Ihre Netzwerkverbindung.“

Nach einigen Momenten:

„Oh, super! Es läuft wieder. Das ist fantastisch!“

„Gut, bin froh, dass ich das für Sie wieder hingekriegt habe.“

„Danke vielmals für die Mühe.“

„Hören Sie mal, wenn Sie sichergehen wollen, dass Ihre Verbindung nicht noch mal abbricht, sollten Sie ein kleines Programm laufen lassen. Das geht ganz schnell.“

„Das passt jetzt gerade nicht so gut.“

„Verstehe ... Es könnte uns eine Menge Kopfschmerzen ersparen, wenn dieses Netzwerkproblem das nächste Mal auftritt.“

„Na gut ... wenn es schnell geht.“

„Bitte machen Sie Folgendes ...“

Eddie leitet Tom durch die Prozedur, eine kleine Anwendung von einer Website zu ziehen. Nach dem Download des Programms bittet Eddie, Tom möge darauf doppelklicken. Er macht es, aber sagt:

„Es funktioniert nicht. Da passiert nichts.“

„Verflixt noch mal. Irgendwas stimmt mit dem Programm nicht. Dann lassen wir es fürs Erste sein. Wir können das später noch mal probieren.“ Und dann weist er Tom an, wie er das Programm löschen soll, damit es nicht wiederhergestellt werden kann.

Das Ganze hat etwa zwölf Minuten gedauert.

Die Story des Angreifers

Bobby Wallace fand es immer lächerlich, wenn er einen so guten Auftrag wie diesen bekam und seine Klienten sich um die unausgesprochene, aber naheliegende Frage herumdrückten, zu welchem Zweck diese Informationen gewünscht werden. Bei dieser Sache fielen ihm nur zwei Begründungen ein. Vielleicht waren sie Strohmänner für eine Organisation, die an der Übernahme der Zielfirma, der Schiffbaugesellschaft Starboard, interessiert war und die nun wissen wollte, in welcher finanzielle Lage sie sich genau befindet – insbesondere alles, was die Zielfirma vor einem potenziellen Käufer verbergen will. Oder aber sie repräsentierten Investoren, denen die Art und Weise, wie mit dem Geld in der Firma umgegangen wird, spanisch vorkommt und die

nun herausfinden wollen, ob einer der Geschäftsführer da einen Selbstbedienungsladen führt.

Und vielleicht erzählten seine Klienten ihm die wahren Beweggründe auch deswegen nicht, weil Bobby dann möglicherweise mehr Geld verlangte, wenn er wüsste, wie wertvoll die Daten sind.



Es gibt eine Vielzahl von Wegen, wie man sich Zugang zu den geheimsten Daten einer Firma verschaffen kann. Ein paar Tage lang grübelte Bobby über den Möglichkeiten und recherchierte ein wenig, bevor er sich für einen Plan entschied. Er wählte einen Schlachtplan mit einer ihm sehr gemäßen Herangehensweise, bei dem die Zielperson so vorbereitet wird, dass sie den Angreifer um Hilfe bittet.

Zuallererst kaufte sich Bobby in einem Kaufhaus für 40 Dollar ein Karten-Handy. Er rief den Mann an, den er sich als Zielperson ausgesucht hatte, stellte sich als Kollege vom Computer-Service der Firma vor und richtete die Dinge so ein, dass der Mann Bobby jederzeit auf dem Handy anrufen würde, wenn er mit seiner Netzwerkverbindung ein Problem hat.

Um nicht aufzufallen, ließ er zwei Tage verstreichen und telefonierte dann mit dem Netzwerkrechenzentrum der Firma. Er behauptete, er müsse für Tom, die Zielperson, ein Problem lösen und bat darum, Toms Netzwerkverbindung zu unterbrechen. Bobby wusste, dass dies der heikelste Part des ganzen Unterfangens war – in vielen Betrieben arbeiten die Leute vom Computer-Service sehr eng mit dem Rechenzentrum zusammen; oft ist sogar der Computer-Service ein Teil der IT-Struktur. Aber für den gleichgültigen Kollegen vom Rechenzentrum war es ein Routineanruf, und er fragte nicht nach dem Namen der Person vom Computer-Service, der angeblich an diesem Netzwerk-Problem arbeitete, und deaktivierte bereitwillig den Netzwerk-Port der Zielperson. Somit war Tom vom Intranet der Firma völlig abgeschnitten, konnte keine Daten vom Server holen oder mit den Kollegen austauschen, Emails abrufen oder überhaupt irgend etwas ausdrucken. Heutzutage ist das gleichbedeutend mit einem Rückfall in die Steinzeit.

Wie Bobby schon vorausgesehen hatte, dauerte es nicht lange, bis sein Handy klingelte. Natürlich gab er sich den Anschein, dass er dem armen, leidenden Kollegen liebend gerne helfen wolle. Dann rief er das Rechenzentrum an und veranlasste die erneute Aktivierung des Ports. Schließlich rief er seinen Mann zurück und manipulierte ihn erneut, indem er ihm diesmal ein schlechtes Gewissen machte, Bobbys Bitte abzulehnen, nachdem dieser ihm einen Gefallen getan hatte. Tom stimmte zu, ein kleines Programm auf seinen Computer herunterzuladen.

Natürlich war das, dem er zugestimmt hatte, nicht das, wonach es aussah. Die Software, die nach Bobbys Aussage verhindern sollte, dass die Netzwerkverbindung erneut zusammenbricht, war in Wirklichkeit ein Trojanisches Pferd, eine Anwendung, die auf Toms PC das anrichtete, was in der Geschichte den Trojanern passierte: Damit wurde der Feind ins Lager geholt. Tom berichtete, dass nichts passierte, als er auf das Icon doppelklickte. Tatsächlich war es Absicht, dass auf dem Bildschirm nichts zu erkennen sein sollte, obwohl das kleine Programm eine geheime Anwendung installierte, die dem Eindringling einen verborgenen Zugang zu Toms Computer ermöglichte.

Nach dem Start dieser Anwendung hatte Bobby vollständige Kontrolle über Toms Rechner, was als *remote command shell* bezeichnet wird. Mit diesem Zugang konnte Bobby auf Toms Rechner nach Abrechnungsdateien Ausschau halten und sie bei Bedarf kopieren. Dann konnte er sie gemächlich nach den Informationen durchsuchen, die für seine Klienten nützlich sein könnten.

Und das war noch nicht alles. Er konnte jederzeit zurückkommen und die Emails und privaten Aktennotizen der Firmenchefs auf bestimmte Worte hin durchsuchen, die ihm viele interessante Leckerbissen enthüllen könnten.

Nachdem er seine Zielperson so beschwindelt hatte, dass sie ihm arglos das Trojanische Pferd installierte, warf Bobby später an diesem Tag das Handy in einen Mülleimer. Natürlich war er so umsichtig, dass er vorher den Speicher löschte und die Batterie entfernte, bevor er das Teil wegwarf – es wäre das Letzte gewesen, wenn jemand aus Versehen diese Handy-Nummer anrief und das Handy dann klingelte.

Jargon

Trojanisches Pferd Ein Programm, das böartigen oder gefährlichen Code enthält, mit dem der Rechner oder die Dateien des Opfers beschädigt oder Informationen vom Netzwerk oder PC des Opfers bezogen werden können. Einige Trojaner sind so programmiert, dass sie sich im Betriebssystem verstecken und alle Tasteneingaben oder Mausbewegungen aufzeichnen oder aber Befehle über ein Netzwerk akzeptieren und ausführen – und das alles, ohne dass das Opfer etwas davon ahnt.

Trickanalyse

Der Angreifer spinnt sein Netz, um die Zielperson zu überzeugen, dass sie ein Problem hat, das in Wahrheit nicht existiert – oder das wie in diesem Fall noch nicht eingetreten ist, aber von dem der Angreifer weiß, dass es stattfindet, weil er selbst es verursachen wird. Er präsentiert sich dann als Retter in der Not.

Bei dieser Art des Angriffs ist das Arrangement von besonderer Spannung für den Angreifer: Weil schon im Vorfeld die Saat ausgebracht wird, führt die Zielperson den Anruf aus eigenem Antrieb durch, wenn sie sich mit einem Problem konfrontiert sieht. Der Angreifer lehnt sich einfach zurück und wartet, bis er angerufen wird. Man bezeichnet diese Taktik liebevoll als *reverse social engineering*. Ein Angreifer, der das Opfer dazu bringt, *ihn* anzurufen, erlangt sofortige Glaubwürdigkeit: Wenn ich jemanden anrufe, von dem ich annehme, er sei beim Computer-Service tätig, werde ich nicht von ihm verlangen, seine Identität zu beweisen.

Bei einem Betrug wie diesem wählt der Social Engineer gerne eine Zielperson, die wahrscheinlich wenig Ahnung von Computern hat. Je mehr Kenntnisse vorhanden sind, desto wahrscheinlicher wird man argwöhnisch oder bemerkt den Manipulationsversuch. Wenn Computer für jemanden eine besondere Herausforderung darstellen, weil er wenig Kenntnisse über Technologie und Arbeitsweise hat, ist seine Bereitschaft wahrscheinlich höher, sich anleiten zu lassen. Er ist ebenfalls anfälliger für eine List wie „Laden Sie einfach dieses kleine Programm herunter“, weil er keine Vorstellung davon hat, welchen potenziellen Schaden eine Software verursachen kann. Und obendrein kann er sich wahrscheinlich noch weniger vorstellen, welchen Wert die Daten auf dem Computernetzwerk haben, das er in Gefahr bringt.

Jargon

Remote Command Shell Eine Befehlseingabezeile, die zur Ausführung von bestimmten Aktionen oder Programmstarts textbasierte Eingaben akzeptiert. Ein Angreifer, der technische Schwachstellen ausnutzt oder ein Trojanisches Pferd auf dem Rechner des Opfers installieren konnte, könnte einen Fernzugang zu einer Befehlszeile erlangen.

Reverse Social Engineering Ein Angriff durch einen Social Engineer, bei dem der Angreifer die Situation so einrichtet, dass das Opfer mit einem Problem fertig werden muss und den Angreifer um Mithilfe bittet. Eine andere Form des Reverse Social Engineerings dreht den Spieß um: Die Zielperson erkennt den Angriff und setzt psychologische Prinzipien der Beeinflussung ein, um vom Angreifer soviel Informationen wie möglich zu erhalten, damit das Unternehmen das bedrohte Firmenkapital so gut wie möglich schützen kann.

Mitnick Spot

Wenn ein Fremder Ihnen behilflich ist und Sie im Gegenzug ebenfalls um einen Gefallen bittet, sollten Sie sich nicht einfach so erkenntlich zeigen, ohne dieses Anliegen sorgfältig zu prüfen.

KLEINE HILFE FÜR DIE NEUE

Neue Angestellte sind ein lohnenswertes Ziel für Angreifer. Sie kennen erst ein paar Leute, haben wenig Ahnung von Betriebsabläufen oder was in der Firma so üblich ist. Und weil sie bestrebt sind, einen guten ersten Eindruck zu machen, zeigen sie viel Bereitwilligkeit zur Zusammenarbeit und wie eifrig sie bei der Sache sind.

Die hilfsbereite Andrea

„Personalabteilung, Andrea Calhoun am Apparat.“

„Hallo Andrea, hier ist Alex von der Sicherheitsabteilung.“

„Ja, bitte?“

„Wie geht's uns denn so?“

„Alles prima. Was kann ich für Sie tun?“

„Hören Sie, wir entwickeln gerade ein Sicherheitsseminar für neue Angestellte und suchen ein paar Leute, mit denen wir das ausprobieren können. Dafür brauche ich die Namen und Telefonnummern aller Neueinstellungen aus dem letzten Monat. Können Sie mir dabei helfen?“

„Das kriege ich wohl bis heute Nachmittag hin. Reicht Ihnen das? Wie lautet Ihre Durchwahl?“

„Das ist die 52 ... aber ich bin leider fast den ganzen Tag in irgendwelchen Besprechungen. Wenn ich damit fertig bin, rufe ich Sie heute Nachmittag von meinem Büro aus an, wahrscheinlich ab 16 Uhr.“

Als Alex gegen 16.30 anrief, hatte Andrea die Liste schon zur Hand und las ihm die Namen und Durchwahlen vor.

Eine Botschaft für Rosemary

Rosemary Morgan liebte ihren neuen Job. Sie hatte vorher noch nie für eine Zeitschrift gearbeitet und fand, dass die Leute hier viel freundlicher waren, als sie erwartet hatte, und das war erstaunlich, wenn man den andauernden Druck bedenkt, unter dem die Redaktion monatlich pünktlich eine Ausgabe produziert. Der Anruf, den sie an einem gewissen Donnerstagmorgen erhielt, bestätigte diesen Eindruck von Freundlichkeit.

„Spreche ich mit Rosemary Morgan?“

„Ja, am Apparat.“

„Hallo Rosemary, hier ist Bill Jorday aus der Arbeitsgruppe für Datensicherheit.“

„Ja, bitte?“

Eine Botschaft für Rosemary (Forts.)

„Hat schon mal jemand aus unserer Abteilung mit Ihnen unsere Sicherheitspraktiken besprochen?“

„Nein, ich glaube nicht.“

„Schön, dann wollen wir mal. Zullererst erlauben wir keinem, irgendwelche Software von außerhalb der Firma hier zu installieren. Wir wollen keine Haftungsklagen wegen der nicht-lizenzierten Verwendung von Software. Und natürlich, um Probleme mit Viren oder von Würmern infizierter Software zu vermeiden.“

„Okay.“

„Sind Ihnen unsere Richtlinien in Bezug auf Emails bekannt?“

„Nein.“

„Wie lautet Ihre Email-Adresse?“

„Rosemary@ttrzine.net.“

„Melden Sie sich mit dem Benutzernamen Rosemary an?“

„Nein, der lautet R-Unterstrich-Morgan.“

„Richtig. Wir legen Wert darauf, dass allen unseren neuen Angestellten klar ist, dass das Öffnen von unerwarteten Email-Anhängen gefährlich sein kann. Es werden eine Menge Viren und Würmer versendet, und diese Emails erwecken den Eindruck, dass Sie den Absender kennen. Wenn Sie also eine Email mit einem unerwarteten Anhang bekommen, sollten Sie immer prüfen, ob wirklich die als Absender angegebene Person Ihnen diese Mail geschickt hat. Können Sie das nachvollziehen?“

„Ja, davon habe ich schon gehört.“

„Sehr gut. Unsere Richtlinien besagen, dass Sie Ihr Passwort alle 90 Tage ändern müssen. Wann haben Sie zuletzt Ihr Passwort geändert?“

„Ich bin erst drei Wochen hier, und ich benutze noch das erste Passwort.“

„Das ist in Ordnung. Sie können die 90 Tage voll ausnutzen. Aber wir müssen auf jeden Fall sicherstellen, dass die Leute keine einfach zu ratenden Passwörter verwenden. Verwenden Sie ein Passwort, das aus Ziffern und Buchstaben besteht?“

„Nein.“

„Das müssen wir ändern. Welches Passwort gebrauchen Sie jetzt?“

„Das ist der Name meiner Tochter – Annette.“

Eine Botschaft für Rosemary (Forts.)

„Das ist wirklich kein sicheres Passwort. Sie sollten niemals ein Passwort verwenden, das mit Ihrer Familie zusammenhängt. Schauen wir mal ... Sie könnten es genauso wie ich machen. Es ist okay, Ihr jetziges Passwort als ersten Teil zu benutzen, aber jedes Mal, wenn Sie es ändern, fügen Sie eine Zahl entsprechend des aktuellen Monats hinzu.“

„Wenn ich das also jetzt mache, müsste ich für März eine 3 oder eine 03 hinzufügen.“

„Das bleibt Ihnen überlassen. Womit kommen Sie besser zurecht?“

„Ich glaube, ich nehme Annette3.“

„Prima. Soll ich Ihnen bei der Passwortänderung behilflich sein?“

„Nein, damit kenne ich mich aus.“

„Gut. Da ist noch etwas anderes. Sie haben auf Ihrem Rechner eine Antiviren-Software, und es ist wichtig, dass sie aktuell ist. Sie sollten niemals die automatische Update-Funktion ausschalten, auch wenn Ihr PC gelegentlich etwas langsamer werden sollte. In Ordnung?“

„Sicher, kein Problem.“

„Ganz klasse. Haben Sie unsere Telefonnummer von hier, damit Sie bei Computerproblemen anrufen können?“

Nein, hatte sie nicht, und er gab ihr die Durchwahl, die sie sorgfältig aufschrieb. Danach ging sie wieder an die Arbeit und war ganz zufrieden, wie sorgfältig hier mit ihr umgegangen wird.

Trickanalyse

Diese Geschichte bekräftigt ein Grundthema, das sich durch das ganze Buch zieht. Die grundlegende Information, die ein Social Engineer von einem Angestellten haben will – egal welches Ziel er letzten Endes verfolgt – sind die Daten über die Berechtigungen und Authentifizierung der Zielperson. Mit einem Benutzernamen und dem dazugehörigen Passwort eines einzigen Angestellten aus der richtigen Ecke der Firma hat der Angreifer alles Nötige, um einzubrechen und andere gewünschte Informationen zu lokalisieren. Mit diesem Wissen hat er praktisch einen Generalschlüssel, und damit ausgerüstet kann er frei im gesamten Unternehmen herumspazieren und alle Tresore ausplündern.

Mitnick Spot

Bevor neuen Angestellten ein Zugang zu den Firmennetzwerken gewährt wird, müssen sie in der Befolgung guter Sicherheitsrichtlinien ausgebildet werden, insbesondere der Richtlinie, niemals Passwörter weiterzugeben.

NICHT SO SICHER WIE GEDACHT

„Eine Firma, die nicht auf den Schutz ihrer sensiblen Informationen achtet, handelt grob fahrlässig.“ Diesen Satz würden eine Menge Leute unterschreiben. Und die Welt wäre ein besserer Ort, wenn das Leben so offensichtlich und so einfach wäre. In Wahrheit sind auch solche Firmen ernsthaft gefährdet, die sich viel Mühe geben, vertrauliche Daten zu schützen.

Hier ist ein Fallbeispiel, das erneut illustriert, wie Unternehmen sich täglich selbst in die Tasche lügen, dass ihre von erfahrenen, kompetenten Profis ausgearbeiteten Sicherheitspraktiken nicht umgangen werden können.

Die Geschichte von Steve Cramer

Der Rasen war nicht besonders groß und hatte nie etwas von dieser teuren Saat gesehen. Er rief keinen Neid hervor. Und auf keinen Fall war er groß genug, um als Begründung für den Kauf eines Rasenmähers zu dienen, auf dem man sitzend umherfahren konnte, aber das war schon in Ordnung. So was hätte er sowieso nicht benutzt. Steve genoss es, mit einem handbetriebenen Rasenmäher zu arbeiten, weil das mehr Zeit in Anspruch nahm, und diese Aufgabe lieferte ihm eine nützliche Entschuldigung, seinen eigenen Gedanken nachzuhängen. So musste er Anna nicht zuhören, die ihm Geschichten über die Leute aus der Bank erzählte, bei der sie arbeitete, oder ihm Botengänge auftrug. Er hasste diese „Liebster, würdest Du bitte ...“-Listen, die ein integraler Bestandteil seiner Wochenenden geworden waren. Ihm ging durch den Kopf, dass sein zwölfjähriger Pete ganz schön pfiffig gewesen war, ins Schwimm-Team einzutreten. Jetzt musste er jeden Samstag zum Training oder einem Treffen und konnte sich den samstäglich Aufgaben entziehen.

Für manche Leute könnte Steves Job, medizinische Geräte bei GeminiMed zu entwickeln, eine langweilige Geschichte sein, aber er wusste, dass er damit Leben rettete. Steve sah seine Arbeit als etwas sehr Kreatives an. Künstler, Komponist, Ingenieur – nach Steves Meinung mussten sie sich alle der gleichen Herausforderung stellen: Sie schufen etwas vorher noch nie Dagewesenes. Und auf seine neueste Schöpfung, eine faszinierend ausgeklügelte Herzgefäßprothese (ein sogenannter Stent), war er besonders stolz.

An diesem gewissen Samstag war es gerade halb zwölf, als Steve langsam ärgerlich wurde, weil er beinahe mit dem Rasenmähen fertig war und noch immer keinen Fortschritt dabei gemacht hatte, die letzte Hürde bei der Herzgefäßprothese zu überwinden: die Reduktion der Energieversorgung. Beim Mähen konnte man perfekt über dieses Problem grübeln, aber leider war ihm keine Lösung eingefallen.



Anna erschien an der Tür, die Haare in das rotgemusterte Cowboy-Tuch gewunden, das sie beim Putzen stets trug. „Telefon“, rief sie. „Jemand von der Arbeit.“

„Wer denn?“ rief Steve zurück.

„Irgendein Ralph. Glaub ich jedenfalls.“

Ralph? Steve fiel niemand mit diesem Namen bei GeminiMed ein, der am Wochenende anrufen würde. Aber vielleicht hatte Anna auch den Namen falsch verstanden.

„Steve, hier spricht Ramon Perez vom Technischen Dienst.“ Ramon – wie um alles in der Welt mochte Anna von diesem spanischen Namen auf Ralph kommen, fragte er sich.

„Dies ist nur ein Gefälligkeitsanruf“, sagte Ramon. „Drei von den Servern sind abgestürzt, wir gehen von einem Wurm aus. Wir müssen die Festplatten komplett löschen und die Datensicherung wieder aufspielen. Das heißt, Ihre Dateien werden spätestens Mittwoch oder Donnerstag wieder zugänglich sein. Mit ein bisschen Glück.“

„Absolut inakzeptabel“, sagte Steve nachdrücklich, bemüht, seinen Ärger im Zaum zu halten. Wie konnten diese Leute so naiv sein? Glaubten die denn wirklich, dass er dieses ganze Wochenende und dann noch fast bis zum nächsten ohne Dateizugang klarkommen könne? „Auf gar keinen Fall. Ich werde in spätestens zwei Stunden bei mir zu Hause am Rechner sitzen und brauche definitiv den Zugang zu meinen Daten. Habe ich mich deutlich genug ausgedrückt?“

„Ja, klar, jeder, den ich bisher angerufen habe, will ganz oben auf der Liste stehen. Ich habe mein Wochenende gekippt, um hier wieder alles in Ordnung zu bringen, und es macht echt keinen Spaß, dass alle, mit denen ich spreche, ihren Frust an mir auslassen.“

„Ich habe einen ganz strengen Termin einzuhalten, die Firma hängt davon ab. Ich muss heute Nachmittag einiges geschafft kriegen. Welchen Teil davon haben Sie nicht verstanden?“

„Ich muss noch eine Reihe Leute anrufen, bevor ich überhaupt anfangen kann“, erwiderte Ramon. „Kämen Sie damit klar, wenn Sie kommenden Dienstag wieder an Ihre Daten können?“

„Nicht Dienstag, nicht Montag, heute. JETZT!“ sagte Steve und fragte sich, an wen er sich wenden sollte, wenn er das diesem Dickschädel nicht klarmachen konnte.

„Ist ja gut“, sagte Ramon, und Steve konnte hören, wie er genervt seufzte. „Lassen Sie mich mal sehen, was sich machen lässt. Sie arbeiten auf dem RM22-Server, richtig?“

„RM22 und auf dem GM16. Beiden.“

„In Ordnung. Okay, ich kann das hier beschleunigen, ein bisschen Zeit sparen – ich brauche Ihren Benutzernamen und Ihr Passwort.“

Oha, dachte Steve. Was geht hier ab? Warum braucht er mein Passwort? Warum fragt ausgerechnet einer von der IT-Abteilung danach?

„Wie war noch mal Ihr Name? Und wer ist Ihr Vorgesetzter?“

„Ich bin Ramon Perez. Hören Sie, ich sag Ihnen was: Als Sie eingestellt wurden, da gab es ein Formular, das Sie für Ihr Benutzerkonto ausgefüllt haben, und Sie mussten dort ein Passwort eintragen. Ich könnte da nachschauen und Ihnen zeigen, dass wir das hier in den Unterlagen haben. Okay?“

Steve dachte kurz darüber nach und stimmte dann zu. Er blieb mit wachsender Ungeduld am Apparat, während Ramon die Dokumente aus einem Aktenschrank holte. Als er schließlich wieder am Telefon war, konnte Steve hören, wie er einen Stapel Papier durchblätterte.

„Jawohl, da haben wir's ja“, sagte Ramon schließlich. „Sie haben das Passwort ‚Janice‘ eingetragen.“

Janice, dachte Steve. Das war der Name seiner Mutter, und tatsächlich hatte er es einige Male als Passwort genutzt. Es war gut möglich, dass er es beim Ausfüllen der Einstellungspapiere als sein Passwort eingetragen hatte.

„Ja, das ist richtig“, bestätigte er.

„Okay. Wir verlieren hier einiges an Zeit. Sie wissen nun, dass ich echt bin, Sie wollen, dass ich eine Abkürzung nehmen und Ihre Daten möglichst schnell wieder zugänglich machen soll. Da könnten Sie mich hier ein wenig unterstützen.“

„Meine Kennung ist s, d, Unterstrich, cramer – c-r-a-m-e-r. Das Passwort ist ‚pelikan1‘.“

„Ich mache mich sofort an die Arbeit“, sagte Ramon und hörte sich endlich hilfsbereit an. „Geben Sie mir ein paar Stunden Zeit.“

Steve mähte den Rasen zu Ende, aß zu Abend, und als er sich dann schließlich an seinen Rechner setzte, entdeckte er, dass er tatsächlich wieder auf seine Daten zugreifen konnte. Es war ihm eine Genugtuung, dass er diesen unkooperativen Typ aus der IT-Abteilung so gründlich in den Griff bekommen hatte, und hoffte, dass Anna mitgehört hatte, wie bestimmend er aufgetreten war. Es täte wohl gut, dem Typ oder seinem Boss mal die Hölle heiß zu machen, aber er wusste, das war etwas, zu dem er nie kommen würde.

Die Geschichte von Craig Cogburne

Craig Cogburne war als Vertreter einer High-Tech-Firma recht erfolgreich gewesen. Nach einiger Zeit bemerkte er, dass er gute Antennen dafür hatte, einen Kunden zu durchschauen und ein Gefühl dafür zu entwickeln, wo jemand widerspenstig war oder wo sich Schwächen oder Angriffspunkte auf-tun konnten, die einem den Abschluss einer Transaktion erleichterten. Er begann zu überlegen, wo er dieses Talent weiter nutzen könnte, und sein Weg führte ihn nach und nach in ein weitaus lukrativeres Feld: das der Industriespionage.

Das hier war ein ganz heißer Auftrag. Sah nicht nach einem Zeitfresser aus, und ein Trip nach Hawaii würde auf jeden Fall dabei herauspringen. Oder vielleicht sogar nach Tahiti.

Der Kerl, der mir den Auftrag gab, hat mir natürlich nichts von seinen Hintermännern erzählt, aber es war naheliegend, dass es irgendeine Firma war, die mit einem einzigen großen Sprung die Konkurrenz hinter sich lassen wollte. Meine Aufgabe bestand einfach darin, das Design und die Produktspezifikationen von einem Teil namens Herzgefäßprothese zu kriegen, was immer das auch sein mochte. Das Unternehmen nannte sich GeminiMed. War mir vorher noch nicht untergekommen, aber es gehörte zu den weltweit größten Firmen, den Fortune 500, mit einem halben Dutzend Niederlassungen an verschiedenen Orten. Das macht den Job leichter als bei einer kleineren Firma, bei der es wahrscheinlicher wird, dass der Typ, mit dem ich rede, denjenigen kennt, für den ich mich ausbebe, und mir auf die Schliche kommt. Wie Piloten über einen Zusammenprall in der Luft sagen, kann einem das den ganzen Tag verderben.

Mein Auftraggeber schickte mir ein Fax mit einem Ausschnitt aus so einem Ärztemagazin, in dem stand, das GeminiMed an einer Herzgefäßprothese mit der Bezeichnung STH-100 arbeitete, die ein völlig neues Design besitzen sollte. Super Sache, da hatte schon irgend so ein Reporter für mich die Hufe geschwungen und mir eine Menge Arbeit abgenommen. Eine wichtige Sache hatte ich schon, bevor ich überhaupt angefangen hatte: den Namen des neuen Produkts.

Erstes Problem: die Namen von Leuten herausfinden, die in dieser Firma am STH-100 arbeiten oder für die es wichtig sein könnte, die Pläne zu sehen. Da habe ich in der Telefonzentrale angerufen und gesagt: „Ich habe einem aus Ihrer Arbeitsgruppe versprochen, mich mit ihm in Verbindung zu setzen, und nun fällt mir sein Nachname nicht mehr ein, aber der Vorname beginnt mit einem S.“ Und sie antwortet: „Wir haben einen Scott Archer und einen Sam Davidson.“ Ich ging aufs Ganze und fragte: „Welcher der beiden arbeitet in der Gruppe für das STH-100?“ Sie hatte keine Ahnung, und so entschied ich mich nach Gutdünken für Scott Archer, und sie stellte mich durch.

Als er abnahm, stellte ich mich vor: „Hallo, hier spricht Mike von der Poststelle. Wir haben ein Paket für das Projektteam des Herz-Stent STH-100. Haben Sie eine Idee, zu wem das gehört?“ Er gab mir den Namen des Projektleiters Jerry Mendel. Ich brachte ihn sogar dazu, seine Telefonnummer für mich nachzuschlagen.

Ich rief an. Mendel war nicht erreichbar, aber auf seiner Mailbox hörte ich die Nachricht, dass er bis zum 13. im Urlaub sei, was bedeutete, dass er noch eine weitere Woche beim Skifahren oder wo auch immer zubringen werde, und alle, die in der Zwischenzeit etwas benötigten, sollten Michelle unter 9137 anrufen. Sehr hilfsbereit, diese Leute. Sehr hilfsbereit.

Ich legte auf und wählte Michelles Nummer, bekam sie auch an den Apparat und sagte: „Hier spricht Bill Thomas. Jerry hat mir gesagt, ich solle Sie anrufen, wenn ich mit der Produktbeschreibung fertig bin, die sein Team überarbeiten soll. Sie arbeiten an der Gefäßprothese, nicht wahr?“ Das bestätigte sie.

Jetzt kam der schwerste Teil dieser Trickserei. Falls sie Verdacht schöpfen sollte, war ich bereit, die Karte auszuspielen, dass ich Jerry nur einen Gefallen tun wollte, um den er mich gebeten hatte. Ich fragte: „Auf welchem System arbeiten Sie?“

„System?“

„Welche Art von Computerserver benutzt Ihre Arbeitsgruppe?“

„Oh“, sagte sie, „RM22. Und einige arbeiten auch mit einem GM16.“

Sehr gut. Das habe ich gebraucht, und es war ein Stück Information, das ich ihr aus den Rippen leiern konnte, ohne sie stutzig zu machen. Und das hat sie auch für das nächste Stück weichgekocht, das ich so beiläufig wie möglich ansprach: „Jerry hat gemeint, Sie könnten mir eine Liste der Email-Adressen der Leute vom Entwicklungsteam geben“, sagte ich und hielt den Atem an.

„Sicher. Aber der Verteiler ist zum Vorlesen viel zu lang, kann ich Ihnen das zumailen?“

Huch! Jede Email-Adresse, die nicht mit GeminiMed.com endete, ließe die Alarmsirene losgehen. „Geht das auch per Fax?“ erwiderte ich.

Das könne sie auf jeden Fall einrichten.

„Unser Fax hat leider den Geist aufgegeben. Ich muss die Nummer von einem anderen Gerät herausfinden. Ich rufe gleich zurück“, sagte ich und legte auf.

Jetzt denken Sie vielleicht, ich hätte mir mächtig was eingebrockt, aber das ist bloß ein üblicher Routine-Kniff in unserer Branche. Ich wartete ein bisschen, damit meine Stimme der Frau in der Telefonzentrale nicht bekannt vorkam, und rief sie dann erneut an: „Hallo, hier ist Bill Thomas. Unser Faxgerät hier oben ist kaputt, kann ich ein Fax an Ihren Apparat senden lassen?“ Sie sagte ja und gab mir die Nummer.

Und dann laufe ich da einfach auf und hole das Fax ab, nicht wahr? Auf gar keinen Fall. Erste Regel: Sich niemals an Ort und Stelle blicken lassen, wenn es nicht absolut notwendig ist. Man ist ganz schön schwer zu identifizieren, wenn man bloß eine Stimme am Telefon ist. Und wenn man Sie nicht identifizieren kann, können Sie auch nicht verhaftet werden. Ziemlich schwer, einer Stimme Handschellen anzulegen. Darum rief ich nach einiger Zeit wieder in der Zentrale an und fragte sie, ob das Fax eingetroffen sei. „Ist hier“, sagte sie.

„Hören Sie“, sagte ich. „Ich muss plötzlich dringend zu einem unserer Vertreter rausfahren. Wäre es für Sie möglich, das Fax dorthin weiterzuleiten?“ Sie willigte ein. Und warum auch nicht – könnte man von jemandem aus der Telefonzentrale erwarten, vertrauliche Daten zu erkennen? Während sie das Fax an den „Vertreter“ schickte, habe ich meine tägliche Sportübung gemacht und bin zu dem Papierladen um die Ecke gegangen, bei dem im Fenster das Schild „Hier Faxdienste“ hängt. Das Fax sollte schon vor mir im Laden sein, und wie erwartet lag es schon bereit, als ich eintrat. Sechs Seiten für jeweils 1.75 Dollar. Für einen Zehner und ein bisschen Kleingeld hielt ich die gesamte Namens- und Email-Liste der Arbeitsgruppe in Händen.

Jetzt noch schnell rein

Okay, bis jetzt hatte ich in den vergangenen paar Stunden mit drei oder vier verschiedenen Personen gesprochen und war dem Zugang zu den Firmenrechnern schon einen Riesenschritt näher. Aber einige Teile fehlten noch, bevor ich ganz drin war.

Nummer eins war die Telefonnummer, über die man von außen den Zentralserver anwählen konnte. Ich rief erneut bei GeminiMed an und fragte den Telefonisten nach der IT-Abteilung, und dort erkundigte ich mich nach jemandem, der mir am PC behilflich sein könne. Er stellte mich durch, und ich tat so, als sei ich ziemlich durcheinander und hätte technisch von nichts eine Ahnung. „Ich bin zu Hause und habe gerade einen neuen Laptop gekauft, und ich will ihn so einrichten, dass ich mich von außerhalb einwählen kann.“

Das Verfahren war eigentlich ganz klar, aber ich ließ mich geduldig von ihm durch die Prozedur führen, bis er zu der Einwahlnummer kam. Er gab mir die Nummer, als ob es einfach nur eine weitere Routineinformation sei. Dann ließ ich ihn warten, während ich es ausprobierte. Perfekt!

Nun hatte ich also die Hürde zur Verbindung mit dem Netzwerk genommen. Ich wählte mich ein und fand heraus, dass es einen Terminal Server gibt, über den sich alle Anrufer mit jedem Rechner des internen Netzwerks verbinden konnten. Nach einigen Versuchen stieß ich auf einen Computer von jemandem, der bei einem Gastzugang kein Passwort eingerichtet hatte. Einige

Betriebssysteme führen bei der Erstinstallation den Anwender zur Einrichtung eines Benutzernamens und eines Passworts, stellen aber auch einen Gastzugang bereit. Der Anwender soll sein Passwort auch für den Gastzugang eintragen oder diesen deaktivieren, aber die meisten Leute haben davon keine Ahnung oder es ist ihnen egal. Möglicherweise ist dieses System gerade erst eingerichtet worden, und der Besitzer hatte sich noch nicht darum gekümmert, den Gastzugang zu deaktivieren.

Dank dieses Gastzugesanges hatte ich nun Zugang zu einem Rechner, bei dem sich herausstellte, dass darauf eine ältere Version des Betriebssystems UNIX lief. Unter UNIX richtet das Betriebssystem eine Passwort-Datei ein, in der die verschlüsselten Passworte aller Personen abgelegt sind, die für diesen Computer eine Zugangsberechtigung besitzen. Die Passwort-Datei enthält einen Einweg-Hash (das ist eine nicht umkehrbare Form der Verschlüsselung) von jedem Benutzer-Passwort. Bei einem Einweg-Hash wird ein reales Passwort wie z.B. „tuseinfach“ durch einen Hash in verschlüsselter Form dargestellt; in diesem Fall wird der Hash von UNIX in dreizehn alphanumerische Zeichen konvertiert.

Jargon

Passwort-Hash Eine Folge von sinnlosen Zeichen – das Ergebnis eines Einweg-Verschlüsselungsprozesses, den ein Passwort durchläuft. Dieser Prozess soll unumkehrbar sein, d.h. es wird angenommen, dass es nicht möglich ist, das Passwort aus dem Hash wiederherzustellen.

Wenn der Kollege in der Abteilung nebenan Daten auf einen PC übertragen will, muss er sich identifizieren, indem er einen Benutzernamen und ein Passwort eingibt. Das Systemprogramm, das seine Autorisierung verifiziert, verschlüsselt das eingegebene Passwort und vergleicht dann das Ergebnis mit dem verschlüsselten Passwort (dem Hash) aus der Passwort-Datei. Wenn beides übereinstimmt, wird der Zugang freigegeben.

Weil die Passwörter in der Datei verschlüsselt wurden, ist die Datei selbst jedem User zugänglich, weil angenommen wird, dass es keinen bekannten Weg gibt, die Passwörter zu entschlüsseln. Das ist lachhaft – ich habe die Datei heruntergeladen, einen Wörterbuch-Angriff darauf losgelassen (nähere Angaben zu dieser Methode finden Sie in Kapitel 12) und herausgefunden, dass einer aus dem Forschungsteam, jemand mit dem Namen Steven Cramer, ein aktuelles Konto mit dem Passwort „Janice“ führt. Auf gut Glück habe ich versucht, mich über dieses Passwort auf einem der Forschungsserver einzuloggen; wenn es funktioniert, hätte ich einiges an Zeit gespart. Aber leider klappte es nicht.

Das bedeutete, ich musste den Typ dazu kriegen, mir seinen Benutzernamen und sein Passwort zu verraten. Dafür habe ich bis zum Wochenende gewartet.

Den Rest kennen Sie schon. Am Samstag rief ich Cramer an. Um seinen Argwohn abzulenken, log ich ihm etwas von einem Wurm vor und dass die Server aus der Datensicherung wiederhergestellt werden müssten.

Was mit der Geschichte über das eingetragene Passwort aus den Bewerbungsunterlagen ist, die ich ihm erzählt habe? Ich habe darauf gebaut, dass er sich nicht mehr daran erinnert, ob das überhaupt stattgefunden hat. Ein neuer Angestellter füllt so viele Papiere aus, wer sollte sich Jahre danach noch an Einzelheiten erinnern? Und überhaupt – wenn ich es mit ihm verpatzt hätte, hätte ich immer noch eine lange Liste mit anderen Namen.

Mit seinem Benutzernamen und Passwort gelangte ich auf den Server, sah mich ein wenig um und fand dann die Entwicklungsunterlagen für das STH-100. Ich war nicht ganz sicher, welche Daten richtig wichtig waren, darum habe ich einfach alle Dateien auf einen *Dead Drop* transferiert, eine kostenlose FTP-Site in China, wo sie abgelegt werden konnten, ohne dass jemand Verdacht schöpft. Mein Auftraggeber soll das durchwühlen und sich seine Sachen heraussuchen.

Jargon

Dead Drop Ein Platz zum Ablegen von Informationen, der wahrscheinlich nicht von anderen gefunden wird. In der Welt der traditionellen Spione kann das hinter einem lockeren Mauerstein sein, in der Welt der Computer-Hacker befindet er sich gewöhnlich auf einer ausländischen Internet-Site.

Trickanalyse

Für unseren Mann namens Craig Cogburne oder jeden anderen, der in der diebischen, aber nicht immer illegalen Kunst des Social Engineerings ähnlich beschlagen ist, kommt diese Herausforderung praktisch einer Routinesache gleich. Sein Ziel war, auf einem gesicherten Firmencomputer, der durch eine Firewall und die üblichen Sicherheitstechnologien geschützt war, Dateien zu finden und herunterzuladen.

Das meiste seiner Arbeit verlief so einfach wie Brötchenschmieren. Er begann, indem er sich als Mitarbeiter der Poststelle vorstellte und einen bestimmten Druck mit der Behauptung aufbaute, ein Paket müsse dringend zugestellt werden. Dieser Schwindel brachte den Namen des Projektleiters der Forschungsgruppe für die Herzgefäßprothese. Dieser befand sich im Urlaub, hatte aber – sehr praktisch für jeden Social Engineer, der Infos klauen will – ganz hilfsbereit Namen und Telefon seiner Sekretärin hinterlassen. Als er sie

anrief, entschärfte Craig jeglichen Verdacht, indem er angab, er handle nur im Auftrag des Projektleiters. Wegen dessen Abwesenheit gab es für Michelle keine Möglichkeit zur Überprüfung. Sie akzeptierte es als die Wahrheit und gab ohne Murren eine Personalliste der Arbeitsgruppe heraus – für Craig eine unabdingliche und höchst geschätzte Information.

Sie wurde nicht einmal argwöhnisch, als Craig die Liste nicht per Email, sondern als Fax erhalten wollte, wobei Email normalerweise für beide Seiten bedeutend weniger umständlich gewesen wäre. Warum war sie so leichtgläubig? Wie bei vielen Angestellten wollte sie vermeiden, dass ihr Chef bei seiner Rückkehr herausfindet, sie habe einen Anrufer geblockt, der nur einen Auftrag des Chefs ausführen wollte. Nebenbei bemerkt hatte der Anrufer ebenfalls gesagt, dass der Chef diese Anfrage nicht nur autorisiert habe, sondern auch um seine Unterstützung gebeten habe. Wir finden hier wieder einmal ein Beispiel, wie jemand dem starken Wunsch nachgibt, ein Teamplayer sein zu wollen. Die meisten Menschen werden somit anfällig für einen Betrug.

Craig vermied das Risiko, persönlich im Gebäude zu erscheinen, indem er einfach das Fax an die Empfangsdame senden ließ in dem Wissen, dass sie wahrscheinlich recht hilfsbereit sein werde. Das Empfangspersonal wird in der Regel danach ausgesucht, ob es ein angenehmes Wesen hat und einen guten Eindruck hervorrufen kann. So ein kleiner Gefallen wie die Entgegennahme und die Weiterleitung eines Fax gehört normalerweise zu den Aufgaben im Empfang, und diese Tatsache nutzte Craig für seine Belange aus. Was sie nun schließlich weiterleitete, stellte sich als Information heraus, die bei jedem, der den Wert der Information versteht, die Alarmglocken hätte schrillen lassen – aber wie kann man vom Empfangspersonal erwarten, dass es weiß, welche Informationen vertraulich sind und welche nicht?

Indem er sich dem Kollegen aus dem Rechenzentrum als verwirrt und naiv zeigte, setzte Craig eine andere Art der Manipulation ein, um ihm die Einwahlnummer zum Terminal Server abzuluchsen, der in dieser Firma den Knotenpunkt zur Verbindung mit dem internen Netzwerk und den anderen Computersystemen darstellt.

Mitnick **Spot**

Für jeden hat die Fertigstellung der Arbeit erste Priorität. Unter diesem Druck sind Sicherheitspraktiken oft zweitrangig und werden übersehen oder ignoriert. Darauf verlassen sich Social Engineers bei der Ausübung ihrer Tätigkeit.

Craig konnte sich problemlos einloggen, indem er ein Standard-Passwort verwendete, das noch nie geändert worden war. Diese grell markierten, sperrangelweit offenen Lücken existieren bei vielen internen Netzwerken, die sich nur auf die Sicherheit von Firewalls verlassen. Tatsächlich kann man die Stan-

dard-Passwörter vieler Betriebssysteme, Router und anderer Produkte einschließlich Telefonanlagen im Internet finden. Jeder Social Engineer, Hacker oder Industriespion und auch nur der bloß Neugierige kann diese Liste unter <http://www.phenoelit.de/dp1/dp1.html> finden. (Es ist absolut unglaublich, wie das Internet denjenigen das Leben erleichtert, die wissen, wo sie suchen müssen. Und nun wissen *Sie* es auch.)

Cogburne konnte schließlich sogar einen vorsichtigen, misstrauischen Mann („Wie war noch mal Ihr Name? Und wer ist Ihr Vorgesetzter?“) überreden, seinen Benutzernamen und sein Passwort auszuladern, so dass er den Zugang zu den Servern des Forschungsteams erhielt. Für Craig kam das einem Generalschlüssel gleich, mit dem er an die geheimsten Firmeninformationen kommen und die Pläne für das neue Produkt zum Download abholen konnte.

Was wäre passiert, wenn Steve Cramer Craigs Anruf weiterhin verdächtig gefunden hätte? Es war unwahrscheinlich, dass er schon vor Arbeitsbeginn am Montag morgen irgendetwas über seinen Argwohn weitergegeben hätte, und das wäre viel zu spät gewesen, um den Angriff zu verhindern.

Ein Schlüssel zum letzten Teil des ganzen Schwindels: Craig ließ sich selbst anfangs sehr gleichgültig klingen, als ob ihm Steves Sorgen ziemlich egal wären, änderte dann seine Haltung und klang so, als ob er versuche, Steve bei seiner Arbeit zu helfen. Wenn das Opfer Grund zu der Annahme hat, man wolle ihm helfen oder ihm einen Gefallen tun, wird es meistens vertrauliche Informationen mitteilen, die es anderweitig sonst sorgfältig geschützt hätte.

SCHUTZMAßNAHMEN

Bei einem der mächtigsten Tricks des Social Engineers dreht er den Spieß um. Darum ging es in diesem Kapitel. Der Social Engineer verursacht das Problem und löst es dann auf magische Weise, wobei er das Opfer derart beschwindelt, dass es ihm einen Zugang zu geheimsten Firmendaten ermöglicht. Könnten Ihre Angestellten auf diese Art von Betrug hereinfliegen? Haben Sie sich darum gekümmert, spezifische Sicherheitsregeln zu entwerfen und umzusetzen, die so etwas verhindern können?

Fortbilden, Ausbilden und Weiterbilden ...

Eine alte Anekdote erzählt von einem Besucher in New York, der einen Mann auf der Straße fragt: „Wie komme ich zur Carnegie Hall?“ Der Mann antwortet: „Üben, üben, üben.“ Jeder ist durch Angriffe von Social Engineers so gefährdet, dass die einzige effektive Verteidigung einer Firma nur darin bestehen kann, die eigenen Leute gut auszubilden und zu trainieren und sie dadurch zu schulen, einen Social Engineer zu entdecken. Und dann müssen

alle regelmäßig an die Trainingsinhalte erinnert werden, denn leider wird das nur zu schnell wieder verblassen.

Jede Einzelperson des Unternehmens muss darin unterwiesen werden, bei der Kontaktaufnahme mit einer Person, die nicht persönlich bekannt ist, einen angemessenen Grad an Misstrauen und Vorsicht einzusetzen, insbesondere wenn es dabei um jegliche Art von Zugang zu einem Computer oder Netzwerk geht. Es gehört zur menschlichen Natur, anderen vertrauen zu wollen, aber wie die Japaner es ausdrücken: Business ist Krieg. Ihr Unternehmen kann es sich nicht leisten, die Verteidigungslinien zu vernachlässigen. Die Sicherheitsrichtlinien eines Unternehmens müssen klar definieren, was als angemessenes oder unangemessenes Verhalten gilt.

Sicherheit gibt es nicht von der Stange. Die Angestellten einer Firmen haben gewöhnlich völlig unterschiedliche Rollen und Verantwortlichkeiten, und jede Position hat ihre eigenen Schwachstellen. Es sollte ein Basis-Training geben, das alle aus dem gesamten Unternehmen abzuleisten haben, und darüber hinaus muss das Personal den Arbeitsaufgaben entsprechend weitergebildet werden, um sich gewisse Prozeduren anzueignen, damit sie nicht selbst Teil des Problems werden. Personen, die mit vertraulichen Informationen arbeiten oder Vertrauensstellungen besetzt halten, sollten ein zusätzliches Spezial-Training erhalten.

Wie man vertrauliche Informationen bewahrt

Wenn man einem Fremden begegnet, der einem Hilfe anbietet, wie es in den Geschichten dieses Kapitels verdeutlicht wurde, sollte man auf die Sicherheitsrichtlinien des Unternehmens zurückgreifen, die auf die Größe, Bedürfnisse und Kultur Ihres Unternehmens angepasst worden sind.

Kooperieren Sie niemals mit einer fremden Person, die Sie darum bittet, Informationen zu beschaffen, fremdartige Befehle in einen PC einzugeben, Software-Einstellungen zu verändern oder – hier finden wir das größte Gefährdungspotenzial – einen Email-Anhang zu öffnen bzw. ungeprüfte Software herunterzuladen. Jegliches Software-Programm – auch dasjenige, das scheinbar überhaupt nichts bewirkt – ist vielleicht nicht so harmlos, wie es aussieht.

Hinweis

Ich persönlich bin der Meinung, dass keine Firma irgendeinen Austausch von Passwörtern erlauben sollte. Es ist viel einfacher, eine sehr strenge Regel einzuführen, die es dem Personal generell untersagt, jegliche Passwörter weiterzugeben oder gemeinsam zu nutzen. Das erhöht die Sicherheit. Aber jedes Unternehmen muss bei einer Entscheidung die eigene Kultur und die Sicherheitsbedenken zu diesem Thema selbst abwägen.

Es gibt gewisse Prozeduren, bei denen wir dazu neigen, mit der Zeit nachlässiger zu werden, egal wie gut unsere Ausbildung ist. Dann vergessen wir im Ernstfall unser Training, genau dann, wenn wir es am Nötigsten haben. Sie würden annehmen, dass alle wissen (oder es zumindest wissen sollten), dass man seinen Benutzernamen und das Passwort auf keinen Fall herausgeben soll, und dass man das nicht noch mal extra erwähnen braucht. Das sagt einem einfach der gesunde Menschenverstand. Aber es ist eine Tatsache, dass jeder Angestellte regelmäßig daran erinnert werden muss, dass die Weitergabe von Benutzernamen und Passwort des Computers im Büro oder zu Hause oder einfach nur von der Frankiermaschine in der Poststelle der Weitergabe der PIN bei der Kreditkarte entspricht.

In seltenen Fällen – sehr seltenen! – können gewisse Umstände eintreten, bei denen es eine Berechtigung oder gar Notwendigkeit für die Weitergabe vertraulicher Informationen gibt. Aus diesen Gründen ist es nicht angemessen, ein absolutes Verbot einzurichten. Trotzdem sollten Ihre Sicherheitsrichtlinien und Abläufe äußerst genau benennen, unter welchen Umständen Angestellte ihr Passwort weitergeben dürfen und – das ist das Wichtigste! – wer nach dieser Information fragen darf.

Berücksichtigen Sie die Quelle

Bei den meisten Organisationen sollte die Regel bestehen, dass jegliche Information, die möglicherweise der Firma oder einem Kollegen Schaden zufügen könnte, nur an Personen gegeben werden dürfen, die persönlich bekannt sind oder deren Stimme einem so vertraut ist, dass man sie fraglos wiedererkennt.

Wenn es um besonders hohe Sicherheitsbedürfnisse geht, sollten Anfragen nur dann berechtigt sein, wenn sie persönlich gestellt oder mit einer starken Form der Authentizität begründet werden – z.B. mit zwei verschiedenen Items wie einem geteilten Geheimnis und einem zeitbasierten Token.

Prozeduren zur Datenklassifikation müssen festlegen, dass keine Information aus Bereichen der Organisation, die sich mit vertraulichen Aufgaben beschäftigen, weitergegeben werden dürfen, wenn man die Person nicht persönlich kennt oder es keinen Bürgen dafür gibt.

Wie gehen Sie also mit einer anscheinend berechtigten Anfrage nach Informationen von einem anderen Angestellten der Firma um, so wie nach einer Liste von Namen und Email-Adressen Ihrer Abteilung? Wie schärfen Sie tatsächlich das Bewusstsein, damit ein Punkt wie diese Liste, die ganz klar nicht so wertvoll ist wie z.B. ein Datenblatt mit der Produktbeschreibung eines neuen Forschungsprojektes, als nur zum internen Gebrauch erkennbar wird? Ein wichtiger Bestandteil der Lösung: Bestimmen Sie in jeder Abteilung Per-

sonen, die für Anfragen über Informationen zuständig sind, die die Gruppe verlassen sollen. Dann muss ein Sicherheitstrainingsprogramm für Fortgeschrittene durchgeführt werden, um diese gewissen Angestellten in den besonderen Verifikationsprozeduren zu unterweisen, die sie befolgen sollen.

Hinweis

Unglaublicherweise bürgt sogar das Nachschlagen von Name und Telefonnummer der Anrufer in der Firmendatenbank und ein Rückruf unter dieser Nummer nicht für eine absolute Sicherheit – Social Engineers kennen sich damit aus, Namen in Firmendatenbanken einzufügen oder Anrufe umzuleiten.

Keiner sollte vergessen werden

Jeder kann innerhalb der eigenen Organisation die Bereiche aufsagen, die einen besonders hohen Schutzbedarf gegen böartige Angriffe benötigen. Aber oft übersehen wir die eine oder andere Ecke, die nicht so offensichtlich und trotzdem besonders gefährdet ist. In einer dieser Geschichten erschien die Bitte, ein Fax zu einem Anschluss innerhalb der Firma zu schicken, relativ harmlos und sicher genug, und trotzdem hat der Angreifer sich dieses Schlupfloch zunutze machen können. Hier lautet die Lektion: Von der Sekretärin und den Assistenten bis hoch zum Geschäftsführer und den Managern müssen alle Personen sich einem besonderen Sicherheitstraining unterziehen, damit sie auf diese Art von Tricks vorbereitet sind. Und vergessen Sie nicht, Ihre Haustür zu sichern: Das Empfangspersonal ist oft ein Hauptziel für Social Engineers und muss genauso auf die verführerischen Techniken aufmerksam gemacht werden, die einige Anrufer oder Besucher einsetzen.

Die Verantwortlichen für die Unternehmenssicherheit sollten eine Art zentrale Klärungsstelle für Trickbetrug einführen. Dann können Mitarbeiter, die vermuten, sie seien gerade das Ziel eines Social Engineer gewesen, sich dort melden. Wenn sicherheitsrelevante Vorfälle zentral zusammengetragen werden, stellt das ein effektives Frühwarnsystem dar, mit dem ein koordinierter Angriff rechtzeitig erkannt und jeglichem Schaden vorgebeugt werden kann.

