Vorwort

Unsere Welt ändert sich dramatisch, doch wir nehmen es kaum zur Kenntnis. Natürlich wissen wir, dass die Produktivität durch Computertechnologie und Netzwerke gewachsen ist und das Internet eine ebenso wichtige Schlüsseltechnologie wie die Erfindung und Entwicklung der Elektrizität als Energiequelle geworden ist.

Wir alle wissen, wie viel Geld durch Internet-Startups, durch den Online-Aktienhandel und durch Business-to-Business-Networking verdient worden ist.

Nur wenige sind sich aber darüber klar, in welch gefährliches Fahrwasser wir damit geraten sind.

Wir leben in einer Gesellschaft, die ganz gut in der Lage ist, unsere physische Sicherheit zu gewährleisten. Banken besitzen Tresore und Alarmsysteme, Bürogebäude haben überwachte Eingänge und Türsteher, Einrichtungen der Regierung sind von Zäunen umgeben und werden, wenn nötig, von bewaffnetem Personal bewacht. Inhaber von Schmuckgeschäften nehmen jede Nacht ihre Waren aus dem Schaufenster und verschließen sie in einem Tresor. Geschäfte in berüchtigten Wohngegenden werden rund um die Uhr von Videokameras überwacht und vergittern bei Geschäftsschluss ihre Fenster.

Die Online-Welt jedoch ist nicht so sicher. Unternehmen, die Millionen von Dollar für hochmoderne Alarmsysteme ausgeben, beschäftigen oft nicht einen einzigen Mitarbeiter für die Computersicherheit. Und Unternehmen, die doch Geld für jene Systeme zur Entdeckung von Eindringlingen (IDS) ausgeben, die wie ein Einbruchsalarm im Netz funktionieren, stellen dann niemanden für die Überwachung der IDS-Konsole ein. Die Firewalls, die am Eingang zu den Netzwerken als Wächter fungieren, sind unter Leistungs- und nicht unter Sicherheitsaspekten konfiguriert. Für die meisten Organisationen ist Computersicherheit nur ein Lippenbekenntnis.

Das vorliegende Buch macht diese Punkte überdeutlich. *Attacken im Netz* untermauert mit Untersuchungen, Fallstudien und Geschichten über die wenigen erfolgreich verlaufenen Ermittlungen, wie verwundbar unsere Systeme gegenüber Online-Diebstählen, Einbrüchen, Missbrauch und Manipulationen sind. Obwohl sich die Geschäftswelt auf eine vollständige Online-Präsenz zubewegt, stecken wir immer noch unsere Köpfe in den Sand und hoffen, dass das, was wir nicht sehen, uns auch keinen Schaden zufügen wird.

Was wir jedoch sehen können – der jugendliche Hacker, der über Computer in Chat-Räumen »verfügt«, mit gestohlenen Kreditkarten seine neue Hardware bezahlt und Ihr Netz für die Verbreitung von Spam-E-Mails mit Werbung für pornografische Websites missbraucht –, ist nur die Spitze des Eisbergs. Wenn ein Hacktivist Webserver schädigt, so mögen vielleicht die Abendnachrichten eine halbe

Minute darüber berichten, aber solche öffentlich gewordenen Angriffe sind nicht das eigentliche Problem.

In *Attacken im Netz* erfahren Sie etwas über jene Einzelheiten, die die Abendnachrichten nicht bringen. Sie werden z.B. lesen, wie in den Systemen von zwei Hackern die Befehle gefunden wurden, die im Jahr 1990 das Telefonnetz von AT&T lahmlegten. (Sie hatten doch gedacht, es handele sich nur um einen Software-Fehler.) Und Sie werden erfahren, wie ein Russe mehr als 10 Millionen Dollar per Banküberweisung von der Citibank in die Hände bekam. Oder dass ein Geschäftemacher bereit war, 84 000 Kreditkartennummern zu verkaufen, die er auf eine CD gebrannt und mit Hilfe eines Romans über die Mafia verschlüsselt hatte.

In den Untersuchungen von CSI und FBI, die am Anfang des Buches stehen, künden Statistiken von einem wachsenden Bewusstsein für diese Bedrohung unserer Sicherheit. Die Teilnehmer an diesen Untersuchungen, die sich über einen Zeitraum von fünf Jahren hinzogen, erkennen in zunehmendem Maße nicht nur das Ausmaß der Bedrohung, sondern auch den Umstand, dass sich durch die verschiedenen elektronischen Verbrechen angerichteten Schäden auch in harten Dollars beziffern lassen. Vielleicht wird es Sie bei der Lektüre dieser Kapitel überraschen, dass die größte Bedrohung für die Ressourcen Ihres Unternehmens in all diesen Jahren gleich geblieben ist, während die Gefahr von Internet-Attacken stetig wächst.

Allerdings zeigen die im vorliegenden Buch beschriebenen Zwischenfälle und Statistiken nur den Teil, über den wir etwas wissen. So enthält z.B. das Kapitel über Firmenspionage reichlich Einzelheiten über die Fälle von Datendiebstahl, von denen wir Kenntnis haben. Doch das ist so, als würde man mit einem einzelnen Kokainfund prahlen, während Jahr für Jahr Tausende von Tonnen der Droge durch die Nasen der Süchtigen gehen.

Das tatsächliche Ausmaß der Computerkriminalität kennt niemand. Die meisten Organisationen weigern sich immer noch, den Ermittlungsbehörden Informationen über Computerkriminalität zugänglich zu machen. Und auf jeden erkannten Fall von Systemeinbruch oder unberechtigter Nutzung kommen wahrscheinlich mindestens zehn unerkannte Fälle.

Der einzelne Hacker verfügt über eigene Ressourcen, sammelt Informationen bei Freunden und Komplizen und benutzt das Internet als Arbeitsplattform. Stellen Sie sich nur einmal vor, wie es wäre, wenn Sie einen im Grunde amateurhaften Spezialisten für Computersicherheit hätten und diesem Menschen unbegrenzte Ressourcen zur Verfügung stellen würden: Ausbildung, Zugriff auf geheime Daten, die schnellsten Computer und Netzwerkverbindungen und ein Team von engagierten und begeisterungsfähigen Leuten. Dann hätten Sie so etwas wie die Abteilungen für informationstechnologische Kriegführung, die bereits in mehr als 20 Ländern der Welt existieren.

Wenn diese Teams in ein System eindringen, ist es unwahrscheinlich, dass sie je auffallen werden. Sie wollen kein Aufsehen erregen, sondern Daten stehlen oder

Kontrolle erlangen. Sie kennen die angegriffenen Systeme gut und haben die erforderliche Zeit und Geduld, um sorgfältig vorzugehen und keine Spuren zu hinterlassen. Es sind die Angriffe, die man weder hören noch sehen kann, vor denen jedes Unternehmen mit nennenswerten Online-Ressourcen sich fürchten sollte. Wenn Sie denken, dass dies die Kapazitäten der meisten Nationalstaaten übersteigt, sollten Sie nur einmal lesen, wie sich eine kleine Gruppe, die sich »die Phonemasters« nannte, derart in eine regionale Telefongesellschaft hineinhackte, dass sie alles machen konnte, was sie wollte – sogar Verbrecher warnen, dass ihre Telefone abgehört wurden. Als die Telefongesellschaft ihre Sicherheitsvorkehrungen verbesserte, erstellten die Phonemasters Hintertüren in den geknackten Systemen, mit denen sie diese neuen Sicherheitsmaßnahmen umgehen konnten.

Anstatt sich dagegen besser zu verteidigen, gibt sich der Markt generell wachsweich. Die meisten Unternehmen entscheiden sich heute für Sicherheitsvorkehrungen, die eher für eine Bretterbude taugen. Sie hängen ein Schild aus, auf dem steht: »Geschützt von Smith & Wesson«. Ich habe Unternehmen besucht, bei denen die Firewall-Software, die eigentlich das E-Commerce-Geschäft abschirmen sollte, immer noch in der Originalverpackung herumlag, und andere Firmen, deren Identifikationssysteme nur dazu da waren, um sie den Investoren zu zeigen. Und die verbreitetsten Systeme sind bei weitem nicht immer die sichersten.

Die beiden meistverkauften Firewalls verwenden heute eine Technik namens Stateful Packet Filtering (SPF). Diese besitzt den doppelten Vorteil, schnell und flexibel zu sein, und dies ist auch der Grund für ihre Beliebtheit. Beachten Sie, dass ich das Wort »Sicherheit« nicht erwähnt habe, denn diese spielt bei der Kaufentscheidung für eine Firewall nur eine untergeordnete Rolle. SPF ist deswegen so beliebt, weil es sich leicht installieren lässt und dem »Business as usual« nicht im Wege steht. Es ist, als würden Sie an der Tür Ihres Bürogebäudes einen Wächter postieren, der dafür bezahlt wird, die Leute möglichst schnell durchzuwinken.

Das Marketing spielt bei Sicherheitsversagen eine noch größere Rolle. Zum Schaden für die Welt hat Microsoft das Monopol auf dem PC-Markt und ist eifrig dabei, auch das Monopol bei Servern zu erringen. Microsoft-Programme wie Outlook und Windows Script Host verwandeln jeden Desktop-Computer in ein potenzielles Einfallstor für Viren wie Melissa und Iloveyou oder in eine Quelle für Denial-of-Service-Angriffe. Webserver unter Windows NT, die man unter großem Aufwand relativ sicher machen kann, sind dreimal häufiger Opfer von Hackerangriffen als Unix-Webserver, obwohl sie bis heute nur ein Fünftel aller Webserver insgesamt ausmachen. Anstatt wirklich sichere Systeme zu entwickeln und zu liefern, redet Microsoft nur davon, wozu man in der Lage wäre. Was Microsoft jedoch in Wirklichkeit tut, ist die Einführung erstaunlich flexibler und komplexer Produkte, von denen selbst ihre eigenen Entwickler zugeben, dass sie auf undokumentiertem Quellcode basieren.

Wenn Sie dies noch nicht veranlasst hat, dem Sicherheitsaspekt mehr Aufmerksamkeit zu widmen, so wird die Lektüre dieses Buches dies gewiss erreichen. Sie können es als Werkzeug benutzen, um Ihrem Management das Ausmaß der Gefahr

nur vor Augen zu führen: nicht nur, dass eine wirkliche Gefahr besteht, sondern auch, wie schädlich es sein kann, diese Gefahr zu ignorieren. Ich rede nicht nur vom finanziellen Schaden, der bereits konkret genug ist und hier ausführlich dokumentiert wird, sondern auch davon, wie es ist, wenn die eigenen Sicherheitslücken in der Tagespresse beschrieben werden.

Wenn Sie sich beruflich mit Sicherheit beschäftigen, wissen Sie in der Regel bereits, dass Ihre Firma nicht genug Geld und Aufmerksamkeit auf die Sicherheit verwendet. Kaufen Sie dieses Buch und geben Sie es Ihren Managern zu lesen. Lesen Sie es selbst, um mit Statistiken und Geschichten über die Leute aufwarten zu können, die das Risiko ignorierten, anstatt es zu managen. Lesen Sie über erfolgreiche Ermittlungen und über die wichtigsten Beweise, so dass Sie kein wehrloses Opfer sind, sondern wenigstens die Chance haben, zurückzuschlagen.

Wie Richard Power im Nachwort schreibt, gelangen immer mehr Geschichten über Computerkriminalität ans Licht. Dennoch halten Sie die umfassendste, zurzeit existierende Beschreibung dieses Themas in der Hand. Und vielleicht brauchen wir uns eines nicht allzu fernen Tages unserer Sicherheit nicht mehr zu schämen, sondern können stolz darauf sein, weil wir die Probleme ernsthaft in Angriff genommen haben, anstatt sie weiter zu ignorieren.

Rik Farrow

Vorwort der Übersetzerin

Dieses Buch war überfällig: eine fundierte, aktuelle und umfassende Darstellung der Cyber-Kriminalität unserer Tage, Argumentationshilfe für Sicherheitsexperten in Unternehmen und hochklassige Information für alle Interessierten.

Die detaillierten Insiderkenntnisse des Autors Richard Power waren auch für die Übersetzung eine Herausforderung: Sehr viele Begriffe – insbesondere Namen von Behörden – und etliche der in Amerika so beliebten Abkürzungen mussten eingedeutscht werden, um auch dem deutschen Publikum ein flüssig zu lesendes Buch zu präsentieren. Wer sich dafür interessiert, kann die Originalbezeichnungen im Glossar wiederfinden, das für die deutschen Leser gegenüber dem amerikanischen Original stark erweitert wurde. Und wie in jedem IT-lastigen Buch gibt es auch hier wieder einen Rest von Terminologie, der schlicht unübersetzbar ist. Macht nichts: Hacker, Cracker und Cyberspace sind schon fast ebenso gute deutsche Wörter wie Computer und Software.

Wir danken Richard Power dafür, dass er die Freundlichkeit hatte, exklusiv für die deutsche Ausgabe einen Kommentar zu dem Hackerangriff auf Microsoft zu schreiben, der im Oktober 2000 aufgedeckt wurde. Sie können darin ein paar interessante Neuigkeiten über Passwörter erfahren.

Dank gebührt auch dem zuständigen Lektor, Herrn Rainer Fuchs von Markt+Technik, für die hervorragende Zusammenarbeit und Unterstützung des Projekts.

Anregungen und Kritik sind wie immer willkommen. Sie können, soweit die Übersetzung betroffen ist, an RederTranslations gerichtet werden, ansonsten direkt an den Verlag.

Dorothea Reder
RederTranslations

Bonn, im Dezember 2000
E-Mail: Doro@RederTranslations.com

Aus aktuellem Anlass: Der Microsoft-Hack

Am 27. Oktober 2000, als die Übersetzung von *Attacken im Web* auf Hochtouren lief, meldete die Presse ein Cyber-Verbrechen von außerordentlicher Tragweite: Hacker drangen in die geheimen Quellcode-Archive der Firma Microsoft ein. Die Übersetzerin nahm Kontakt zu Richard Power auf, um die Meinung des Autors zu erkunden. Wir danken Herrn Power dafür, dass er exklusiv für die deutsche Ausgabe diesen Vorfall ausführlich kommentiert hat. Im Folgenden lesen Sie den Wortlaut.

Der Microsoft-Hack

Am Freitag, den 27. Oktober 2000 liefen bei den Nachrichtenagenturen die Drähte heiß: Hacker waren bei Microsoft eingedrungen und hatten sich Zugang zu den Quellcode-Dateien der Firma verschafft. Die Presseagentur Reuters meldete, Microsoft habe den Vorfall als »einen bedauernswerten Akt der Firmenspionage« bezeichnet.

Den Chef von Microsoft, Steve Ballmer, zitiert Reuters mit den Worten: »Es ist offenbar, dass die Hacker einiges von unserem Quellcode gesehen haben.« Noch am selben Tag wurde ich interviewt von der Los Angeles Times, der Washingon Post, der New York Daily News, der San Jose Mercury News, USA Today, Newsweek, BBC, Associated Press, Reuters und anderen. Diese Folgeartikel beherrschten die Wochenendpresse. Sie erhellten einige zentrale Punkte.

Spionage im Informationszeitalter ist nicht mehr Industriespionage

Microsoft selbst hat den Zwischenfall als einen Akt der »Spionage« bezeichnet. Und tatsächlich ist seit einigen Jahren bereits offensichtlich, dass die Spionage des Industriezeitalters (bei der z.B. ein Insider durch Bestechung, Erpressung oder Verlockungen gekauft wird) nachlässt, während die Spionage des Informationszeitalters (bei der z.B. Hacker in die internen Netzwerke von Großunternehmen eindringen, um digitale Geschäftsgeheimnisse zu stehlen) rasch zunimmt.

Egal ob und wann die tatsächlichen Motive der Täter im Microsoft-Fall je ans Licht kommen: Der Hackerangriff auf den Microsoft-Quellcode unterstreicht, wie dringend es nötig ist, dass die Verantwortlichen dieser lebenswichtigen Wirtschaftszweige die Spionage des Informationszeitalters viel mehr als bisher ernst nehmen.

Microsoft hat nicht als einzige Firma bei der Abwehr von Malware[1] versagt

Die ersten Berichte besagten, dass eines der verwendeten Hackertools das trojanische Pferd/der Wurm QAZWSX.HSQ gewesen sei, dessen Name von den Buchstaben abgeleitet ist, die auf der amerikanischen QWERTY-Tastatur am weitesten links stehen. In der Regel nennt man es QAZ. QAZ ist ein bösartiger Code, der bereits bekannt war. Entdeckt wurde er Mitte Juli in China. Alle großen Hersteller von Virenscannern – darunter auch Microsoft – hatten ihre Virensignaturen-Datenbanken so aktualisiert, dass sie QAZ identifizierten. Natürlich machte auch der Jahresbericht zur Untersuchung von CSI und FBI das Problem deutlich. Jahr für Jahr geben mehr als 90 Prozent der Befragten an, dass sie Virenscanner einsetzen, aber gleichzeitig bekennen auch 90 Prozent, dass sie in den letzten zwölf Monaten Virenprobleme hatten. Ich vermute, dass manche dieser Infektionen zwar auf neue Viren zurückzuführen waren, viele aber auch auf ein Scheitern der Anti-Virus-Software. Normalerweise scheitert diese entweder, weil man sich nicht genügend um die unternehmensweite Aktualisierung der Datenbank mit den Virensignaturen gekümmert hat oder weil man die Virenscanner für Telearbeiter und andere Benutzer mit Remote-Zugriff entweder nicht aktualisiert oder gar nicht erst eingesetzt hat.

Ist Schadensbegrenzung eine Gegenmaßnahme?

Es ist kaum zu glauben, dass ausgerechnet der Quellcode von Microsoft von diesem Vorfall betroffen war. Und ebenso schwer zu glauben ist es, dass der Remote-Zugriff auf diesen Microsoft-Quellcode mit wieder verwendbaren Passwörtern »gesichert« war.

Schließlich kann jede Organisation Opfer von Hackern werden, in jeder Organisation kann die Datensicherheit scheitern, aber gerade die Kunden, Partner und Aktionäre von Microsoft hätten doch eine bessere Sicherung des Quellcodes erwarten können. Und diejenigen Kunden, Partner und Aktionäre, die etwas Ahnung von Datensicherheit haben, hätten gewiss erwarten können, dass der Remote-Zugriff auf diesen Quellcode nicht nur mit Passwörtern geschützt wird.

Microsoft kann mich gerne widerlegen und die Dinge klarstellen, falls ich damit Unrecht habe. Aber aus Redmond berichten die Medien nur Ausflüchte und Desinformation, sodass man sich an den Präsidentschaftswahlkampf erinnert fühlt. So hat Microsoft z.B. am Freitag und am darauffolgenden Montag vehement bestritten, dass der Quellcode in irgendeiner Weise geschädigt worden sei. Nun, offen gesagt: Mit solch pauschalen Aussagen wird die Öffentlichkeit für dumm verkauft.

---

1. Diesen Begriff verwendet der Autor für »bösartige Software« (Anm. d. Übers.).

Das Einzige, was Microsoft relativ sicher sagen konnte, war, dass die Quellcode-Kopie auf diesem speziellen Server nicht verändert worden war. Na gut. War sie aber irgendwie kopiert worden? War sie von diesem Server heruntergeladen worden? Und selbst wenn man sie nicht heruntergeladen hatte: Hatte man sie vielleicht lange untersucht? Wenn ja, dann ist der Quellcode in vieler Hinsicht gefährdet.

Wenn er dem Untergrund in die Hände fiel, dann hat man ihn wohl auf Schwachstellen hin analysiert, die dann in zukünftigen Hackerangriffen ausgenutzt werden können.

Die Konkurrenz könnte den Quellcode analysiert haben, um die Eigenschaften der Microsoft-Produkte besser nachahmen und/oder in verbesserter Form herstellen zu können. Eine solche Analyse könnte der Konkurrenz Zeit und Geld für die Forschung und Entwicklung sparen und die Möglichkeit geben, Microsoft auf dem Markt eine Niederlage beizufügen.

Man hätte den heruntergeladenen Quellcode auch mit einem trojanischen Pferd versehen, kompilieren, eindampfen und dann an arglose Kunden verkaufen können.

Ein noch übleres Beispiel für die von Microsoft verbreitete Desinformation ist die Art, wie sich die veröffentlichte Geschichte von Freitag bis Montag verändert hat. Da hat zumindest die PR-Abteilung von Microsoft versagt, wenn nicht noch mehr.

Am Freitag zitierten die Medien Steve Ballmer und andere mit ganz unmissverständlichen Aussagen. Doch am Montag widersprach man mehreren dieser Statements wieder.

So stand in den Presseberichten von Freitag und vom Wochenende, der Zugriff der Eindringlinge habe zwischen fünf Wochen und drei Monaten angedauert. Doch am Montag darauf erklärte Microsoft, der Zugriff habe nur zwölf Tage gedauert; Microsoft habe die ganze Zeit darüber Bescheid gewusst und die Eindringlinge überwacht.

Irgendwie hatte man das Gefühl, dass die Montagsversion der Geschichte mehr mit Schadensbegrenzung zu tun hatte, nachdem sich übers Wochenende mehrere Datensicherheitsexperten zu Wort gemeldet hatten, als mit einem Fortschritt der Nachrichtenlage gegenüber den ersten Berichten am Freitag zuvor.

Auf Grund der »Klarstellungen« vom Montag wurde die Geschichte natürlich heruntergekocht. Sie wurde abserviert. Mein Telefon schwieg wieder.

Passwörter: Die Untoten schlagen wieder zu

Nein, ich werde jetzt nicht abschweifen und mich an der aktuellen Debatte beteiligen, ob es besser wäre, den Quellcode als Open Source offenzulegen oder als Geschäftsgeheimnis zu behandeln. Ich möchte lediglich darauf hinweisen, dass sich Microsoft auf Gedeih und Verderb dafür entschieden hat, seinen Quellcode

geheim zu halten. Das Unternehmen hat ein Vermögen für Rechtskosten ausgegeben, um seinen Quellcode vor dem prüfenden Blick der US-Regierung zu schützen. Und doch konnte es nicht verhindern, dass irgendein russischer Hacker den Code mithilfe einer E-Mail-Vorrichtung sondierte.

Auf der Jahreskonferenz des CSI (dieses Jahr fand sie in Chicago statt) ist es ein Quell steter Freude, mit William Hugh Murray von Deloitt and Touche LLP, einem der ganz Großen auf dem Gebiet der Computersicherheit, zu sprechen. Dieses Jahr erinnerte ich ihn daran, wie ich in den Neunzigerjahren eine seiner Präsentationen zu den Problemen der Benutzerauthentifizierung mitgeschrieben und als Titelstory meiner Publikation *Computer Security Alert* gebracht habe.

Ich nannte den Artikel »Der Tod des Passworts«.

Und tatsächlich hatte Murray in seiner Präsentation das wiederverwendbare Passwort für tot erklärt. Er hielt ihm eine richtige Lobrede (»… es hat uns gute Dienste geleistet …«) und gab es dem Vergessen anheim (»… aber es hat ausgedient …«).

Murray ist ein ungemein praktisch denkender Mensch. Er wusste schon damals, dass die Passwörter nicht verschwinden würden. Er wollte den anderen nur bewusst machen, dass die Passwörter verschwinden *sollten*. Diese Worte Murrays machten tiefen Eindruck auf mich. Seither habe ich allen immer gesagt, dass Passwörter nur ein »Placebo« sind, nur eine Sache, die für ein »besseres Gefühl« sorgt.

Doch die raue Wirklichkeit ist leider, dass die meisten Datensicherheitsleute immer noch in einer Umgebung arbeiten, in der sie auf Fragen wie die folgende antworten müssen: »Wie lange sollten Benutzer ein Passwort verwenden dürfen, bevor sie es ändern müssen? Dreißig Tage? Sechzig Tage? Neunzig Tage?« Unglaublich. Nachdem ich Murray an den »Tod des Passworts« erinnert hatte, schnitt ich daher das Thema Microsoft-Hack an.

»Bei dieser Geschichte dreht sich doch alles darum, dass Microsoft den Zugriff auf seinen Quellcode mit wieder verwendbaren Passwörtern kontrollierte.«

Murray lächelte, nippte an seinem Champagner und sagte: »Ja.«

Was sollte geschehen?

Um noch mehr von der rauen Wirklichkeit zu bekommen, besuchte ich Rik Farrows zweitägiges Seminar über Eindringlingstechniken und Gegenmaßnahmen, das er nach der Konferenz exklusiv für das CSI abhielt und ursprünglich auf Anfrage der NSA entwickelt hatte. Natürlich behandelt Farrow ein breites Spektrum von Gefahren und Gegenmaßnahmen. Als Appetithäppchen und praktische Hilfe gebe ich hier nur ein paar willkürlich ausgewählte Auszüge aus seinen Kursunterlagen über Passwort-Angriffe und Gegenmaßnahmen.

»Am einfachsten kommt man in ein System auf dem üblichen Weg herein: indem man einen Benutzernamen und ein Passwort eingibt.

Passwörter kann man sich mit nicht technischen Mitteln beschaffen, indem man seine Sozialkompetenz einsetzt und Leute beschwatzt.

Auch in Benutzerkonten, in die man eindringt, kann man Benutzernamen und Passwörter finden: die Konten- und Passwortliste eines Administrators oder Benutzers, Dateien, die z.B. in Unix-Systemen auf .netre enden, Passwort-Caches auf Windows 9x-Systemen oder die Ergründung der LSAsecrets auf NT-Systemen.

In früheren Jahren richtete man ein neues System oft ohne Passwörter ein: Kontennamen wie »guest« oder »tutor« waren häufig. Auch heute noch tauchen Systeme ohne Passwörter auf, z.B. NT-Systeme mit MySQL-Server (Kontenname sa, Administratorrechte), Silicon Graphics IRX (Kontenname lp), Unix-Systeme allgemein (adm, bin, uucp, nuucp).

Programme zum Knacken von Passwörtern verwenden oft benutzte Passwörter, Wörterbücher und schnelle Hashing-Algorithmen. Wenn ein solches Programm umfangreiche und relevante Wörterbücher verwendet, besteht der Erfolg darin, dass es auf Grund der vorhandenen Konteninformationen die Kontendaten gut errät und beide nach einem Regelwerk (z.B. 1->1,E->3) modifiziert.

Ein Exemplar des zerhackten Passworts ist für den Einbruch unerlässlich. Es gibt viele Unix-Hackerprogramme, die Unix-Passwörter festhalten.

NT-Server und -Workstations speichern ihre Passwörter im System Accounts Manager (SAM).

Bei SP3 fügte Microsoft den SYSKEY hinzu, die Fähigkeit, als Hash gespeicherte Passwörter mit einem 128-KB-Schlüssel zu verschlüsseln. Wenn Sie sich für diesen Weg entscheiden, haben Sie drei Möglichkeiten, diesen Schlüssel zu liefern: Sie speichern ihn auf einer Diskette, die beim Booten verwendet werden muss, oder Sie geben beim neu Booten eine Pass-Phrase ein, oder Sie veranlassen NT, den Schlüssel in der Registrierung zu speichern.

NT-Passwörter werden als Teil der Netzwerkauthentifizierung verwendet. Bei älteren Windows-Versionen (und Samba) können Passwörter auch als einfacher Text übermittelt werden. Doch häufiger wird zur Authentifizierung eine Frage-und-Antwort-Methode eingesetzt. Wenn sowohl die Frage als auch die Antwort im Netzwerk mit einem Schnüffler ausspioniert werden können, kann man sie beim Knacken von Passwörtern verwenden. Den Internet Explorer kann man so hereinlegen, dass er mit einem korrumpierten Webserver Frage-Antwort-Authentifizierungen vornimmt. Der Remote-Verschlüsselungsalgorithmus von Microsoft, PPT, umfasst auch das Frage-Antwort-Verfahren (und verwendet das Passwort als Grundlage für den Schlüssel). Es gibt ein Tool, das pptpsniff heißt.

Die Existenz von rückwärtskompatiblen Lanman-Passwörtern macht es viel einfacher, Passwörter mit roher Gewalt zu knacken. Der beste Schutz gegen das Erschnüffeln oder Knacken von Passwörtern besteht darin, sie nur einmal zu benutzen: z.B. Passwörter, die nicht gespeichert oder wieder verwendet werden. So können die Authentifizierungsverfahren viel mehr Sicherheit bieten. Die zweit-

beste Lösung sind vorausschauende Lösungen zur Passwortüberprüfung: z.B. Passwörter zu überprüfen, wenn die Benutzer sie zu ändern versuchen. Das Verbergen von Passwörtern (Schatten-Passwortdateien und SYSKEY) ist immerhin besser als gar nichts.

Wie stark basiert denn Ihre Sicherheit auf wieder verwendbaren Passwörtern? Und wie wertvoll sind die Daten, die diese Passwörter »schützen« sollen?

Kriminalität, Krieg und Terror im Informations-zeitalter

1.
Kapitel

Die Schattenseiten des Cyberspace

Im Jahr 1991 proklamierte Alvin Tofflers Buch *The Third Wave* das heraufziehende Informationszeitalter. Zehn Jahre später ist der Cyberspace eine ungewöhnliche, neue Erfahrungswelt des Menschen geworden.

Sie können online an der Börse spekulieren. Sie können sich online um eine Stelle bewerben. Sie können online Spitzenhöschen kaufen. Sie können online arbeiten. Sie können online lernen. Sie können online Kredite aufnehmen. Sie können online Sex haben. Sie können online Tauschgeschäfte machen. Sie können online Immobilien kaufen und verkaufen. Sie können Ihre Flugtickets online erwerben. Sie können online an Glücksspielen teilnehmen. Sie können online lange aus den Augen verlorene Freunde wiederfinden. Sie können online Informationen, Erkenntnisse und Spaß finden. Sie können online eine Pizza bestellen. Sie können online Ihre Bankgeschäfte abwickeln. Und an einigen Orten dürfen Sie sogar online an Wahlen teilnehmen.

Die Menschheit hat nicht nur ihre Geschäfte, sondern auch ihre Selbsterfahrung in das Internet verlagert. Und in der digitalen Welt hat die Menschheit – genauso wie überall sonst – auch ihre Schattenseiten gefunden. Wirtschaft, Politik und Kultur haben im Informationszeitalter besondere Formen von Verbrechen, Krieg und sogar Terror nach sich gezogen.

Sie können online Finanzbetrug begehen. Sie können online Geschäftsgeheimnisse stehlen. Sie können online Erpressung und Nötigung begehen. Sie können online Übergriffe starten. Sie können jemanden online verfolgen. Sie können online den Besitz anderer Menschen verwüsten. Sie können online Verleumdungen ausstoßen. Sie können online eine Bank ausrauben. Sie können jemandem online etwas in die Schuhe schieben. Sie können jemanden online zerstören. Sie können online Verbrechen aus Hass begehen. Sie können jemanden online sexuell belästigen. Sie können online Kinder belästigen. Sie können jemandes Glaubwürdigkeit online zerstören. Sie können online Geschäfte stören. Sie können online rauben und plündern. Sie können online Unruhen vom Zaun brechen. Sie könnten sogar einen Krieg online beginnen.

Die Arten der Cyber-Kriminalität

Es gibt ein breites Spektrum der Cyber-Kriminalität, das die folgenden Punkte umfasst:

- Unberechtigter Zugriff von innen (z.B. durch Angestellte)
- Systemeinbruch von außen (z.B. durch Hacker)
- Diebstahl schutzwürdiger Daten (angefangen von einer einfachen Benutzer-ID und dem entsprechenden Passwort bis hin zu Geschäftsgeheimnissen, die zig Millionen Dollar wert sind)
- Finanzbetrug mithilfe von Computern

- Daten- oder Netzwerksabotage
- Störung des Netzwerkverkehrs (z.B. durch Denial-of-Service-Attacken)
- Erfindung und Verbreitung von Computerviren, Trojanischen Pferden und anderem bösartigen Code
- Softwarepiraterie
- Identitätsdiebstahl
- Hardwarediebstahl (z.B. Entwendung von Laptops)

In den Kapiteln 3 und 4 werden Sie sehen, dass diese und andere Verbrechen im Cyberspace nicht nur weit verbreitet, sondern auch teuer sind.

In den USA fällt ein Großteil dieser kriminellen Aktivitäten unter das Gesetz über Computerbetrug und -missbrauch (Artikel 18, Abschnitt 1030) und das Gesetz über die Wirtschaftsspionage (Artikel 18, Abschnitt/Kapitel 90) des amerikanischen Strafgesetzbuchs. Näheres darüber finden Sie in Anhang A.

Gemäß dem Gesetz über Computerbetrug und -missbrauch ist es ein Verbrechen, absichtlich unbefugt oder unter Überschreitung seiner Befugnisse auf einen Computer zuzugreifen und dadurch Informationen zu erlangen, auf die man kein Anrecht hat. Das Gesetz erstreckt sich nicht nur auf den unrechtmäßigen Zugriff auf Regierungscomputer oder Computer regierungsnaher Institutionen zum Zwecke der Beschaffung von Daten (insbesondere Geheiminformationen), die die Bundesregierung erzeugt hat oder besitzt, sondern auf alle Computer, die im zwischenstaatlichen oder internationalen Geschäftsleben zum Einsatz kommen.

Dieses Gesetz erlangte im Jahr 1986 Rechtskraft. Es wurde 1988, 1989, 1990, 1994 und 1996 geändert, um sprachliche Korrekturen vorzunehmen und neue Entwicklungen zu berücksichtigen.

Viele Fälle, die Sie in *Attacken im Web* lesen, fallen unter das amerikanische Gesetz über Computerbetrug und -missbrauch. Manchmal waren Computer der Regierung oder der Universitäten betroffen, manchmal auch Finanzinstitutionen und Telefongesellschaften. Sehr oft waren auch Computer in mehreren Umgebungen zugleich (darunter Regierung, Universität, Finanzbranche und Telekommunikation) betroffen.

Die meisten Bundesstaaten der USA haben ihre eigenen Gesetze gegen Computerkriminalität. So ist z.B. im einschlägigen Gesetz von Iowa Folgendes zu lesen:

> *Jemand begeht einen Computereinbruch, wenn er wissentlich und unbefugt auf einen Computer, ein Computersystem, ein Computernetzwerk oder einen Teil desselben zugreift oder einen solchen Zugriff bewirkt, um Dienste, Informationen oder Eigentum zu erlangen, oder wissentlich und unbefugt den Besitz eines Computers, Computersystems, Computernetzwerks oder Computerprogramms jeder Art oder der darin enthaltenen Daten an sich nimmt, überträgt, verheimlicht oder einbehält mit der Absicht, diesen dem Eigentümer dauerhaft zu verwehren.*

Das Gesetz über die Wirtschaftsspionage (EEA) wurde 1996 rechtskräftig und definierte es als ein Verbrechen nach Bundesgesetz, aus der Veruntreuung von Handelsgeheimnissen eines Dritten Kapital zu schlagen. Zwar ist das EEA kein explizites »Gesetz über Computerkriminalität«, aber es enthält neben den traditionellen Begriffen wie »Fotokopien« und »Lieferungen« spezielle Sprachregelungen über unberechtigte »Downloads«, »Uploads« und »E-Mails«. (Wirtschaftsspionage wird immer mehr zum Computerverbrechen. Mehr über das EEA und die unter diesem Gesetz geahndeten Verbrechen finden Sie in Kapitel 10.)

Manche Cyber-Verbrechen dringen in jeden Winkel und schädigen jeden:

- Die E-Commerce-Kriminialität (z.B. der Diebstahl Hunderttausender von Kreditkartendaten) bedroht den Internetboom, der die beispiellose wirtschaftliche Erholung der USA in den letzten zehn Jahren geschürt hat.
- Wirtschaftsspionage (z.B. der Diebstahl von digital gespeicherten Geheiminformationen der Biotechnologie) gefährdet die Wettbewerbsfähigkeit der USA auf dem Weltmarkt.
- Angriffe auf die Infrastruktur (z.B. ein Anschlag auf das Stromnetz eines Landes) bedrohen die Sicherheit und das Wohlbefinden der gesamten Bevölkerung.

Andere Cyber-Verbrechen wie z.B. Identitätsdiebstahl oder Menschenjagd im Cyberspace zielen auf Einzelpersonen, um diese finanziell, seelisch oder gar körperlich zu schädigen.

Natürlich findet auch ein breites Spektrum unappetitlicher Online-Aktivitäten statt, die zwar nicht illegal sind, aber dennoch große finanzielle Verluste verursachen könnten. So könnte z.B. ein kostspieliges Verfahren wegen sexueller Belästigung folgen, wenn ein Mitarbeiter die Firmen-E-Mail missbräuchlich verwendet.

Der Typus des Cyber-Kriminellen

Im Jahr 1994 stand ich in der Tür eines überfüllten Konferenzraums bei einer vom National Institute of Standards and Technology (NIST und der National Security Agency (NSA durchgeführten Tagung über Computersicherheit. Donn B. Parker, früher bei SRI International und jetzt bei der SRI-Tochter Atomic Tangerine (www.atomictangerine.com) beschäftigt, einer der großen Pioniere auf dem Gebiet der Datensicherheit, hielt eine zukunftsweisende Rede über »Wildwest in NetSec«.

Vieles von dem, was Parker an jenem klaren Herbstmorgen vorhersagte, ist eingetreten. So trugen z.B. automatisierte Hackerwerkzeuge dazu bei, dass es heute nicht mehr so viel Können erfordert, ernsthafte Angriffe zu starten. Doch eine Unstimmigkeit fiel mir auf: In einem Teil seines Vortrags zeichnete Parker ein Profil von der Psyche »jugendlicher Hacker«, das er unmittelbar aus seinen Untersuchungen und Befragungen abgeleitet hatte. Ich zweifelte nicht an seinen Schluss-

folgerungen. Natürlich konnten jugendliche Hacker Chaos und Zerstörung anrichten. Und gewiss spielen psychologische Faktoren bei jeder Art von Verbrechen eine Rolle. Dennoch sagte ich mir: »Irgendetwas stimmt nicht an diesem Bild.«

Es war gar nicht Parkers Präsentation, es war die spürbare Ablehnung, die sie in dem gewaltigen Saal erzeugte. Es ging nicht nur um halbwüchsige Hacker. Es gab da noch ein anderes und weit heimtückischeres Problem, das in der Öffentlichkeit nur selten zur Sprache kam.

Der typische, jugendliche Hacker lieferte nur das passende Bild, er war ein Sündenbock, ein Platzhalter für die Berufsverbrecher und ausländischen Agenten, die ähnliche Online-Einbrüche verübten. Diese digitalen Söldner waren nicht auf das technologische Abenteuer, sondern auf den technologischen Vorteil aus.

Danach behielt ich das Gesamtbild im Blick. Es stimmt, normalerweise ist es der jugendliche Hacker, der letztlich Schlagzeilen macht, aber der Profi macht weniger Fehler als so ein impulsiver, halbstarker Übeltäter. Profis arbeiten im Verborgenen und sind besser für die Durchführung von Geheimmissionen trainiert. Nur selten findet man Hinweise auf ihre Aktivitäten. Wenn doch einmal Profis entdeckt werden, dann gibt die betroffene Organisation deren Aktivitäten nur selten zu. Sie befürchtet, die schlechte Presse könnte ihre Geldgeber, Kunden und dergleichen abschrecken.

So, wie es unterschiedliche Arten der Cyber-Kriminalität gibt, gibt es auch unterschiedliche Arten von Cyber-Verbrechern, die diese verüben.

Unehrliche oder verärgerte Insider (z.B. Mitarbeiter, Ex-Mitarbeiter, Lieferanten, Zeitarbeiter) wollen Ihre Geschäftsgeheimnisse verkaufen, Geld veruntreuen oder einfach nur aus Rache Ihre Daten oder Computernetze zerstören.

Der Begriff »Hacker« wird natürlich mittlerweile überstrapaziert. In der Cyber-Kultur machen manche einen Unterschied zwischen »Hacker« und »Cracker«. Politisch korrekt bezeichnet man jemanden, der nur aus Neugier in ein System eindringt, als Hacker, und jemanden, der eindringt, um Daten zu stehlen oder zu zerstören, als Cracker. Doch selbst jene Hacker, die nur aus Neugier ein System knacken, machen sich zumindest des Einbruchs und Eindringens schuldig.

Wenn Sie mitten in der Nacht ein Geräusch hören, das Licht einschalten und jemanden entdecken, der in Ihrem Schlafzimmer herumkriecht, dann wäre es Ihnen doch wohl egal, dass dieser Eindringling ein Student der Innenarchitektur auf der Suche nach neuen Inspirationen ist, oder etwa nicht?

Berufsspione und -saboteure sind vielleicht die am schwersten zu fassende Tätergruppe. Sie arbeiten für gegnerische Regierungen und Konkurrenzunternehmen. Sie werden bezahlt. Sie sind Meister ihres Fachs. Sie können Ihr Unternehmen ruinieren, Ihre Regierung stürzen oder Ihre Börse zusammenbrechen lassen. Und sie werden kaum jemals gefasst.

Im Cyberspace tummeln sich mehr und mehr Berufskriminelle. Organisierte kriminelle Unternehmungen haben auf den E-Commerce ein Auge geworfen, wie zuvor bereits auf Speditionen, Spielkasinos und Banken. Und ebenso wie das Organisierte Verbrechen hinter dem E-Commerce her ist, zielen Kleinkriminelle mittels Online-Manipulationen auf den Geldbeutel der Privatleute ab.

Terroristen können es auf wichtige Infrastruktureinrichtungen wie z.B. das Telefonnetz, die Stromversorgung oder das Luftverkehrskontrollsystem abgesehen haben. All diese Systeme laufen auf Computern und sind für Cyber-Attacken verwundbar.

Attacken im Web ist eine Reise zu den Schattenseiten des Cyberspace.

2.
Kapitel

Die Gedankenwelt des Cyber-Verbrechers

Von Verbrechen im Cyberspace ist jeder fasziniert. Alle möchten wissen: Warum? Doch als ich den Inhalt dieses Buchs konzipierte und die Überschrift »Die Gedankenwelt des Cyber-Verbrechers« eingab, dachte ich: »Das wird ein kurzes Kapitel.« Warum? Aus drei Gründen:

Erstens: Warum sollte man den psychologischen Wurzeln der Cyber-Kriminalität oder auch den bewussten Motiven der Cyber-Verbrecher selbst so viel Aufmerksamkeit schenken, wenn man in einer Welt lebt, wo so wenig Zeit aufgewendet wird, um die psychologischen Wurzeln und bewussten Motive zu ergründen, die zum Beispiel hinter Völkermord oder sexuellem Missbrauch von Kindern stecken?

Zweitens: Ein Verbrechen bleibt ein Verbrechen, egal ob es in der physischen Welt oder im Cyberspace verübt wird. Wenn Sie irgendwo einbrechen, dann brechen Sie ein, egal ob Sie einen mit Kette gesicherten Zaun oder eine Firewall überwinden. Wenn Sie eine pharmazeutische Formel stehlen, dann stehlen Sie eine pharmazeutische Formel, egal ob sie auf Papier gedruckt oder auf einem Server gespeichert ist. Viele wollen diese einfache Wahrheit nicht begreifen: Verbrechen bleibt Verbrechen.

Warum sollten die psychischen Ursachen oder die bewussten Motive von Cyber-Kriminalität anders aussehen als jene, die bei Verbrechen in der physischen Welt eine Rolle spielen?

Wenn Sie jemandem sagen würden, Sie hätten die psychologischen Motive von Hackern oder Crackern ernsthaft erforscht, dann wäre dieser wahrscheinlich beeindruckt. Er würde alles darüber wissen wollen. Wenn Sie aber demselben Menschen erklärten, Sie hätten die psychologischen Motive von Hausfriedensbruch und Einbruchdiebstahl ernsthaft untersucht, würde er wahrscheinlich auf seine Uhr schauen und eine Ausrede stammeln, um einen schnellen Abgang zu machen.

Drittens gibt es nicht sehr viele zuverlässige Informationen darüber.

Ich werde Ihnen dennoch zwei Expertenmeinungen zu diesem Thema vorstellen: Sarah Gordon, Mitarbeiterin am Watson Research Center von IBM, und Donn Parker von Atomic Tangerine haben beide lange und hart an diesen Fragen gearbeitet. Wir wollen einmal schauen, was sie herausgefunden haben.

»Stereotypenbildung kann gefährlich sein«

Sarah Gordon ist etwas Besonderes. Sie ist eine der faszinierendsten Persönlichkeiten, die für die Datensicherheit arbeiten. Wer sich auskennt – auf beiden Seiten des Gesetzes –, nimmt Sarah Gordon sehr ernst. Niemand hat mehr Zeit als sie damit verbracht, die Motive von Hackern und Virenschreibern zu erforschen.

Von *Forbes ASAP* wird sie wie folgt charakterisiert:

> *Sarah Gordon hat einen erstklassigen Ruf als eine Virusexpertin, die sich meisterhaft mit den fatalen Schöpfungen junger Hacker auskennt. Jahrelang hat sie in ihrer Arbeit als Beraterin für Jugendliche in Krisensituationen ihre eigenen PCs von Viren befreit. Seit 1997 arbeitet sie in dem führenden Antivirus-Labor des Landes: im Thomas J. Watson Research Center in Hawthorne, New York.*
>
> *»Das Labor«, so Gordon »befindet sich tief im Innern der IBM-Forschungsabteilung. Die Tür ist nicht zu verfehlen: Sie ist mit Warnungen zugepflastert. Ich habe sogar ein Poster mit der Warnung ›Raum für die Autopsie von Aliens‹ aufgehängt. Es soll daran erinnern, welch ernste Dinge hinter dieser Tür passieren.*
>
> *Es gibt strenge Sicherheitsvorkehrungen, aber die sind auch nötig. In diesem Labor befindet sich eine der vollständigsten Virus-Sammlungen der Welt. Hackerwerkzeuge können Chaos anrichten, wenn sie dem Falschen in die Hände fallen, Viren hingegen brauchen noch nicht einmal in irgendwelche Hände zu gelangen: Sind sie erst einmal im System, verbreiten sie sich fast genauso wie ein biologischer Virus. Sie können nur durch Einsatz des richtigen Gegenmittels gestoppt werden.«*

Gordon willigte ein, für *Attacken im Web* einige meiner Fragen zu beantworten.

»Was bringt Kinder dazu, sich lieber in ihrem Computer als im Einkaufszentrum herumzutreiben?«

Gordon: »Anfang der Achtzigerjahre bis in die Neunzigerjahre hinein waren Computer in den Haushalten Amerikas noch nicht üblich. Es gab nur wenige Kinder, die tatsächlich einen Computer benutzen konnten. Die meisten Jugendlichen hingen noch in den Einkaufszentren herum, um sich zu treffen und dort ihre Freizeit zu verbringen. Inzwischen finden Treffen und Freizeit jedoch im Internet statt und viel mehr Haushalte verfügen über Computer. Es ist nur natürlich, dass mehr Kinder in Computer eindringen. Man braucht keinen Führerschein, um dort hinzukommen. Und im Internet gibt es viel mehr zu entdecken als im lokalen Einkaufszentrum.

Überlegen Sie einmal, wie die Situation in anderen Ländern ist. In vielen Ländern gibt es keine Einkaufszentren, gesellschaftlichen Ereignisse in Schulen oder Ähnliches, sodass junge Leute und Internet-Sozialisierung ganz natürlich zusammenfinden. Darüber hinaus bietet das Internet Kommunikation ohne wirklichen ›Kontakt‹ und bietet jungen Leuten, die sich in sozialen Beziehungen unsicher fühlen eine exzellente ›Deckung‹. Oder wollten Sie fragen, was die Kids veranlasst, mit Computern ›Böses‹ zu tun? Das ist ein ganz anderes, sehr kompliziertes Thema.«

Ich fragte weiter: »Haben Sie in Ihrer ganzen Erfahrung irgendeinen gemeinsamen Nenner von Belang bei jenen Leuten gefunden, die die Medien als ›Hacker‹ bezeichnen würden?«

Gordon: »Nun, auch ich bin ein Hacker (denken Sie daran, dass nicht jede Hackeraktivität kriminell ist). Demnach müsste ich überlegen, was ich mit dem Rest gemeinsam habe. Ich würde sagen, wir alle sind neugierig, was unsere Computersysteme angeht.«

»Haben Sie in Ihrer ganzen Erfahrung irgendeinen gemeinsamen Nenner von Belang bei jenen Menschen gefunden, die Viren schreiben?«

Gordon: »Auch die treibt der Faktor ›Neugier‹. Der Unterschied besteht darin, dass der Virenschreiber, der seinen Virus zur Verfügung stellt, damit sein ›Geschenk‹ erst verteilt. Vergessen Sie nicht, dass ein Unterschied besteht zwischen einem Virenschreiber und einem Virenverbreiter. Und es besteht auch ein Unterschied zwischen einem Verbreiter und jemandem, der den Virus tatsächlich aktiviert. Das sind zwar feine, aber wichtige Unterschiede, vor allem, wenn wir anfangen, die Gesetzgebung zum Thema Viren zu betrachten.«

»Was würde Ihrer Meinung nach jemanden veranlassen, einen Virus zu schreiben, anstatt zu hacken? Oder ist das eine ein Resultat des anderen«, wollte ich wissen.

»Das eine ist definitiv *nicht* der natürliche Ausfluss des anderen«, so Gordon. »Jahrelang haben die Leute gesagt, Viren seien langweilig. Ich glaube, das ist nicht ganz richtig. Viren sind interessant, vor allem, wenn Sie sie nicht verstehen, und es ist cool, einen Virus zum ersten Mal in Aktion zu sehen.

Dies vorausgeschickt: Sobald Sie Viren verstehen, sind sie tatsächlich langweilig. Und wenn Sie das langweilige Zeugs erst einmal hinter sich gelassen und gemerkt haben, dass es sehr realen Menschen sehr realen Schaden zufügen kann, sind Sie dem normalerweise bereits entwachsen. In der Vergangenheit haben die meisten Virenschreiber diese Entwicklung durchgemacht. Wenn der Zeitpunkt gekommen ist, sind die Raubzüge im Untergrund zuende.

Das Hacken hingegen (und ich meine echtes Hacken, nicht das, was Skriptschreiber machen) erfordert ein viel tiefgehenderes Verständnis von Systemen und ist interessant. Die erhaltenen Informationen und die Leute, die man in dieser Subkultur trifft, sind wesentlich faszinierender. Leute, die mit Hacking – echtem Hacking – zu tun haben, ›entwachsen‹ dieser Szene normalerweise nicht. Sie können ihre Fachkenntnisse nutzen, um eine legale Arbeit zu finden, auch wenn manche bezweifeln, dass dieses Vorgehen ›richtig‹ ist.«

Ein anderer wichtiger Faktor ist laut Gordon, dass das Schreiben von Viren relativ einfach ist und von Leuten mit wenig oder gar keinen Systemkenntnissen erledigt werden kann. Manche Virenschreiber nutzen mittlerweile die Netzverbindungen und andere kommen durch die allgemein verbreiteten Hackertools und -techniken schneller zum Hacken, allerdings nicht in großer Zahl. Dennoch sei der Trend steigend.

Gordon glaubt also, dass sich diese beiden Welten zu überschneiden beginnen. Und das Wesen der digital vernetzten Welt bedingt, dass auch eine kleine Überschneidung große Auswirkungen haben kann. Es ist so einfach (und verantwor-

tungslos), ein Programm zu replizieren, dass die meisten Hacker damit nichts zu tun haben wollen.

»Welche Unterschiede bestehen zwischen den gemeinsamen Nennern von Hackern einerseits und Virenschreibern andererseits?«, fragte ich.

»Hacker sind in der Regel viel fähiger und verstehen die Systeme insgesamt viel besser. Die Virenschreiber, die ich bei DEFCON traf, haben normalerweise nur ein sehr elementares technisches Wissen über Viren und kümmern sich Jahr für Jahr um dasselbe Material.«

Gordons Arbeit zeigt, dass es falsch wäre, Hacker oder Virenschreiber zu stereotypisieren. Dennoch frage ich sie, ob ihr ein Motiv oder ein Bündel ähnlich gelagerter Motive aufgefallen sei, das bei Hackern oder Virenschreibern vorherrschend oder zumindest verbreitet sei.

»Ich denke, Stereotypenbildung kann gefährlich sein. Ich habe festgestellt, dass es nicht korrekt wäre, zu sagen, alle Virenschreiber sind unmoralisch, und es ist sowohl falsch als auch unpassend, alle Hacker als kriminell zu bezeichnen.

Es gibt jedoch unter Hackern ein vorherrschendes Motiv und das ist auch hier wieder die Neugier. Sie wollen einfach wissen, wie die Dinge funktionieren!

Virenschreiber sind in der Regel irgendwann dem Schreiben von Viren entwachsen. Hacker dagegen vervollständigen ihr Wissen und gehen dazu über, mit Computern systemnah zu arbeiten.«

Ich befrage Gordon auch nach ihrer Meinung über die Motive, die David Smith bewegten, Melissa zu schreiben und zu starten, oder die de Guzman (oder wer auch immer verantwortlich war) bewegten, den Liebesbrief-Virus zu erschaffen.

»Im Allgemeinen machen sich Leute, die Viren schreiben, keinen Begriff von deren potenziellen Auswirkungen auf andere. Das ist wie ein Videospiel, in dem die Dinge zwar geschehen, aber nicht ›real‹ sind. Die Leute sind von dem ›Spiel‹ ganz gefesselt und merken erst dann, wenn sie den Konsequenzen Auge in Auge gegenüberstehen, dass es gar kein Spiel gewesen ist. Um sie zu stoppen, müssen sie entweder diese Konfrontation durchmachen oder einfach erwachsen werden.

Die meisten von ihnen entwachsen diesem Spiel. Manchmal bleiben aber auch Ältere dabei und erkennen anscheinend nicht die Folgen ihres Tuns oder sie kümmern sich nicht darum. Das kann zwar, muss aber nicht bedeuten, dass sie absichtlich Probleme verursachen möchten. Bei Smith habe ich zum Beispiel keine Ahnung, ob er irgendwelche besonderen Schwierigkeiten verursachen wollte. Aber ich bin mir ziemlich sicher, dass Smith nicht wusste, welche Auswirkungen sein Virus haben würde.

Das heißt nicht, dass er keine Verantwortung trägt. Er hat zugegeben, das Virus in Umlauf gebracht zu haben, und dafür muss er sich auch verantworten. Und es ist sicher, dass er den Code gut genug verstand. Aber verstand er tatsächlich auch die Implikationen seiner Interaktion mit diesem gewaltigen Monstrum, das wir

›das Netz‹ nennen? Nein. Das ist eine ganz andere Sache. Es ist etwas, um das wir als Gesellschaft uns noch nicht einmal ansatzweise Gedanken gemacht haben.«

Mehr Erkenntnisse von Sarah Gordon bezüglich der Motive von Hackern und Virenschreibern und ähnlicher Themen finden Sie in ihren einschlägigen Veröffentlichungen unter www.badguys.org.

Der Schlüssel: »Große persönliche Probleme«

Donn Parker enthüllt in seinem ausgezeichneten *Buch Fighting Computer Crime: A New Framework for Protecting Information* einige der Motive, die verschiedene Arten von Cyber-Verbrechern ihm gegenüber offenbarten.

Einige Beispiele:

- »Die Banker brauchten unbedingt meine Dienste als Datensicherheitsspezialist, aber sie wollten es nicht wahrhaben. Ich wollte demonstrieren, wie einfach es war, in den ersten Schritt eines Geldtransfers hinein zu gelangen, und ihnen die Ergebnisse zeigen, damit sie mich einstellen. Der erste Schritt war so einfach, dass ich beschloss, auch den zweiten Schritt zu versuchen, um zu sehen, ob das auch möglich war. Die Banker wären dann wohl noch mehr beeindruckt. Niemand bemerkte, was ich getan hatte. Da der nächste Schritt genauso einfach war, wollte ich sehen, wie weit ich gehen konnte. Ich hätte nie geglaubt, dass ich es schaffen würde, das gesamte Verbrechen durchzuführen. Ich hatte den Plan, das gestohlene Geld zurückzugeben und als Held dazustehen.«
- »Ich wusste: Wenn ich nicht das Rechenzentrum unseres Konkurrenten zerstörte, würde ich aus meinem Job als Computer-Operator entlassen, und mein Verhältnis mit der Frau unseres Vorstands wäre zu Ende. Schließlich war er es, der den Anlass lieferte.«[1]

Parker stellt fest, dass Cyber-Kriminelle (genau wie die Kriminellen in der realen Welt) das Bedürfnis haben, ihre Verbrechen rational zu begründen.

> *Zum Beispiel änderte der untreue Bankangestellte in Minneapolis nicht seinen Kontensaldo. Er modifizierte nur das Computerprogramm so, dass es seine Kontoüberziehungen eine Zeitlang nicht bemerkte. Er behauptete, es würde ja kein Geld gestohlen und niemand geschädigt – solange er sein Konto wieder auffüllte, bevor irgendjemand etwas merkte.*

1. *Fighting Computer Crime: A New Framework for Protecting Information,* Donn Parker, John Wiley & Sons, S. 147

> *Internationale Piraten, die geistiges Eigentum stehlen, erklären ihre Spionage- und Diebesaktivitäten oft damit, dass man im Ausland ruhig die Gesetze brechen könne, solange man das Recht des eigenen Landes nicht verletzt. Darüber hinaus fühlen sie sich im Recht, weil andere Länder so reich seien und das eigene so arm.*[1]

Laut Parker gibt es zwar nicht »den typischen Cyber-Kriminellen«, aber es existieren einige Gemeinsamkeiten.

Diese Menschen zeigen möglicherweise das psychologische Symptom, dass ihnen das rechte Maß abhanden kommt (Differential Association Syndrome). So nimmt z.B. jemand, der Veruntreuungen begeht, am Anfang nur Kleinigkeiten mit: Büroklammern, Papier und Bleistifte für den Hausgebrauch. »Das macht doch jeder.« Doch die Diebstähle des Veruntreuers eskalieren, bis er am Ende tausende Dollar vom Firmenkonto der Bank stiehlt.

Das Gleiche gilt auch für den Diebstahl von Computerdiensten. Zwei Programmierer kamen ins Gefängnis, weil sie auf Firmencomputern nebenbei ihr eigenes Geschäft betrieben. »Aber das macht doch jeder«, sagten sie. Klar, auch andere Angestellte nutzten die Firmencomputer, um persönliche E-Mails zu senden oder zu spielen, aber diese beiden belegten zum Schluss drei Viertel der Großrechner ihrer Firma für ihren Handel mit Musiknoten.

Parker beobachtet, dass Cyber-Verbrecher oft dazu neigen, die von ihnen angegriffenen Computer zu vermenschlichen, und dennoch das Gefühl haben, dass ein Angriff auf einen Computer anderen Menschen keinen Schaden zufügt.

> *Die meisten Cyber-Kriminellen, die ich traf, könnten sich, auch wenn ihr Leben davon abhinge, nicht an Verbrechen an Menschen beteiligen. Sie könnten keinem Opfer ins Auge schauen, während sie es ausrauben oder angreifen, aber sie haben kein Problem damit, einen Computer anzugreifen oder auszurauben. Ein Computer starrt nicht zurück und zeigt keine Angst. Cyber-Kriminelle unterscheiden oft zwischen der untragbaren Praxis, anderen Menschen Schaden zuzufügen, und dem unpersönlichen Akt, auf oder mittels Computern Schaden anzurichten. Dennoch ziehen manche bei ihren Verbrechen auch ein gewisses Maß an Befriedigung daraus, dass sie die angegriffenen Computer personifizieren, in ihnen Gegner sehen und Spaß daran haben, sie zu berauben.*[2]

Viele Cyber-Kriminelle haben auch das Robin-Hood-Syndrom und machen sich vor, dass sie nur denen etwas nehmen, denen es nichts ausmacht. Doch diese Sicht ist verdreht, wie Parker bemerkt. Nach den Begriffen der Cyber-Kriminalität äußert sich das Robin-Hood-Syndrom nicht darin, »von den Reichen zu nehmen und den Armen zu geben«, sondern darin, »von den Reichen zu nehmen und die Beute selbst zu behalten«.

---

1. *Fighting Computer Crime*, S. 146 und 148
2. *Fighting Computer Crime*, S. 141

> *Oft sind die Opfer von Cyber-Kriminalität Organisationen, die – zumindest nach Auffassung des Verbrechers – einen kleinen Verlust verschmerzen können, damit er seine großen persönlichen Probleme lösen kann.*[1]

Diese »großen persönlichen Probleme« sind laut Parker der Schlüssel zum Denken des Cyber-Kriminellen.

> *Trotz der verbreiteten Ansicht, dass Individuen normalerweise aus Geldgier Wirtschaftsverbrechen begehen, habe ich herausgefunden, dass die meisten Cyber-Verbrecher nur versuchen, große persönliche Probleme zu lösen. In dem Moment, wo ein Verbrecher das Verbrechen wirklich begeht, versucht er tatsächlich, sich in irgendeiner Form zu bereichern. Die Gerichtsbarkeit und die Medien sehen darin normalerweise Geldgier oder den Wunsch nach einem Leben in Luxus. Doch die meisten Verhöre solcher Verbrecher zeigen, dass nicht Gier, sondern dringende Not sie zu den Verbrechen veranlasst hat. Die Probleme, die sie zu lösen versuchen, decken das ganze Spektrum menschlicher Schwierigkeiten ab: Sie haben Eheprobleme oder Liebeskummer, schaffen es nicht, so schnell wie die anderen Karriere zu machen, brauchen Geld, um fällige Schulden zu begleichen, müssen eine Sucht finanzieren und so weiter. Insgesamt sieht der Cyber-Kriminelle sich selbst nicht als Verbrecher, sondern als jemanden, der nur seine Probleme zu lösen versucht.*[2]

Das Problem des Sport- oder Spaß-Hackers erfordert im Gegensatz zu verärgerten Angestellten oder Betrügern eine andere Art von Aufmerksamkeit.

Viele dieser Hacker sind Jugendliche und sollten deshalb anders behandelt werden. Darüber hinaus sind viele Spaß-Hacker, egal ob jugendlich oder erwachsen, eigentlich nur irregeleitet; sie haben nicht die Absicht, jemandem Schaden zuzufügen, und sehen nichts Schlimmes oder Gefährliches in ihren »Forschungen«.

Vieles deutet darauf hin, dass auch diese Eindringlinge ein paar ernste Probleme haben.

Als Parker 1996 bei SRI arbeitete, schloss er eine Studie ab, die auf Befragungen von mehr als 80 Hackern in den USA und Europa beruhte.

---

1. *Fighting Computer Crime*, S. 142–143
2. *Fighting Computer Crime*, S. 142

Seine Untersuchung jugendlicher Hacker förderte einige Gemeinsamkeiten zu Tage:

- Die Täter waren frühreif, neugierig und hartnäckig.
- Sie waren es gewohnt, zu lügen, zu betrügen, zu stehlen und zu übertreiben.
- Sie hatten jugendlichen Idealismus und äußerten »Alle Macht dem Volk!« oder »Erlaubt ist, was gefällt!«.
- Sie waren hyperaktiv.
- Sie neigten zu Drogen- und Alkoholmissbrauch.

Im Verlauf der Neunzigerjahre wandelte sich nach Parkers Beobachtungen die Hackerkultur zum Schlechteren.

> *In den Interviews wurde klar, dass der einst ehrenhafte Ansatz der Hacker (den Stephen Levy 1984 in seinem Buch Hackers beschrieb) größtenteils verlorengegangen war. In der modernen Hackerkultur beteiligen sich die Hacker regelmäßig an Fälschungen, Übertreibungen, Diebstahl und Fantasterei. Den Medien und der Öffentlichkeit präsentieren sie sich gerne als Wohltäter, Anwälte der Benachteiligten und »die kleinen Leute«, die den großen Computerherstellern die Stirn bieten und dabei noch Gutes tun. Jugendliche Hacker träumen oft, sie seien eine Art Clark Kent und würden Supermänner des Cyberspace. Leider ist ihre Darstellung nach außen hin von der Wirklichkeit weit entfernt.*
>
> *Bösartige Hacker gibt es zwar in allen Altersgruppen von unter zehn Jahren bis zum Senior, aber sie zeichnen sich allesamt durch eine unreife, übertrieben idealistische Geisteshaltung aus. Unabhängig vom Alter verhalten sie sich wie unverantwortliche Kinder, die Räuber und Gendarm in einer Fantasiewelt spielen, die plötzlich Wirklichkeit wird, wenn man ihnen auf die Schliche kommt.*[1]

Zu Ihrer genaueren Orientierung lege ich Ihnen eine Matrix über Täter in der Computerkriminalität vor, die ursprünglich vom FBI als Werkzeug zur Ermittlung von Täterprofilen entwickelt wurde. Alle Tabellen sind dem Buch *Computer Crime: A Crimefighter's Handbook* von David Icove, Karl Seger und William VonStorch (ISBN 1-56592-086-4) entnommen.

1. *Fighting Computer Crime*, S. 162-163

Täter in der Computerkriminalität – organisatorische Besonderheiten

Täterkategorien	Organisation	Zulauf durch/Hauptanziehungskraft	Internationale Verbindungen
Cracker			
Gruppen	Unstrukturierte Organisation, neigt einer Gegenkultur zu	Peergruppe	Interagiert und korrespondiert mit anderen Gruppen in aller Welt
Einzeltäter	Keine, diese Menschen sind echte Einzelgänger	Suchen die intellektuelle Herausforderung	Abonnieren Cracker-Zeitschriften und interagieren manchmal mit Bulletin Boards von Crackern
Kriminelle			
Spionage	Werden von feindlichen, ausländischen Geheimdiensten unterstützt	Arbeiten meist für Geld, manchmal aus ideologischen Gründen oder um Aufmerksamkeit zu erregen	Dringen mithilfe von Computernetzwerken in Zielcomputer in aller Welt ein
Betrug/ Missbrauch	Arbeiten manchmal als kleine, organisierte kriminelle Gruppe, bisweilen auch einzeln	Geld, Macht	Benutzen drahtgebundene Dienste für internationale Überweisungen
Vandalismus			
Außenstehende	Einzeltäter oder kleine Gruppe, eventuell sehr jung	Rache, intellektuelle Herausforderung, Geld	Brechen über Computernetzwerke und Telefonsysteme in die Zielcomputer ein
Benutzer	Oft Mitarbeiter oder Ex-Mitarbeiter	Rache, Macht, intellektuelle Herausforderung, Verärgerung	Keine

Täter in der Computerkriminalität – Besonderheiten in der Vorgehensweise

Täterkategorien	Planung	Professionalisierungsgrad	Methoden
Cracker			
Gruppen	Manchmal sorgfältig geplant	Hoch	Brechen über Computernetzwerke in die Zielcomputer ein, tauschen mit anderen Crackern oder Gruppen Informationen aus
Einzeltäter	Untersuchen vor Einbruchsversuch die vorhandenen Netzwerke	Mittel bis hoch, erlangen Wissen über soziale Netzwerke	Verwenden zwar auch Netzwerke, öfter jedoch Versuch und Irrtum statt sorgfältiger Untersuchung und Planung; tauschen sich über BB-Sites über andere Systeme aus
Kriminelle			
Spionage	Teilweise wie Cracker	Hoch	Manchmal Auftraggeber von Crackern wegen Information und Sammlung von Daten
Betrug/ Missbrauch	Verbrechen werden im Vorfeld sorgfältig geplant	Mittel bis hoch, doch manchmal mehr Erfahrung in Betrugsdingen als in Computerprogrammierung	Manchmal traditionellere Methoden, z.B. Telefonüberwachung und Falltüren, Systemeinbrüche mit eher elementaren Methoden
Vandalismus			
Außenstehende	Keine besondere Planung, eher Gelegenheitstäter	Unterschiedlich	Beobachtet so lange, bis Systemzugriff möglich
Benutzer	Eventuell sorgfältige Planung und Ausführung	Unterschiedlich, manchmal sehr professionell	Falltürenprogramme und Trojanische Pferde, Veränderung von Daten

Täter in der Computerkriminalität – Besonderheiten im Verhalten

Täterkategorien	Motive	Persönlichkeitsmerkmale	Potenzielle Schwächen
Cracker			
Gruppen	Intellektuelle Herausforderung, Spaß in der Peergruppe, Unterstützung einer bestimmten Sache	Hochintelligente Individuen, Anhänger einer Gegenkultur	Halten ihre Übergriffe nicht für Verbrechen, reden ganz frei darüber
Einzeltäter	Intellektuelle Herausforderung, Lösung eines Problems, Macht, Geld, Unterstützung einer bestimmten Sache	Durchschnittlich bis hochintelligent	Behalten eventuell Notizen und andere Dokumentationen ihrer Handlungen
Kriminelle			
Spionage	Geld und die Möglichkeit, das System anzugreifen	Eventuell Cracker, die alleine oder in Gruppen operieren	Täter will immer mehr Informationen und wird dadurch unvorsichtig
Betrug/ Missbrauch	Geld oder andere persönliche Vorteile, Angriff auf die Mächtigen	Dieselbe Persönlichkeit wie andere Betrüger	Täter wird gierig und macht dann Fehler
Vandalismus			
Außenstehende	Intellektuelle Herausforderung, Geld, Macht	Wie Cracker	Wird manchmal zu frech und macht dann Fehler
Benutzer	Rache an einer Organisation, Lösung von Problemen, Geld	Normalerweise einige Computerkenntnis	Hinterlässt manchmal eine Spur von Buchungen in den Log-Dateien

Täter in der Computerkriminalität – besondere Ressourcen

Täterkategorien	Ausbildung	Mindestausrüstung	Unterstützung
Cracker			
Gruppen	Informelle Ausbildung auf hohem Niveau	Elementare Computerausstattung mit Modem	Unterstützung durch Peergruppe
Einzeltäter	Kenntnisse durch Erfahrung erlangt	Elementare Computerausstattung mit Modem	BB-Sites, Informationsaustausch
Kriminelle			
Spionage	Unterschiedlicher Professionalisierungsgrad	Elementare Computerausstattung mit Modem, manchmal auch bessere Geräte	Unterstützung durch den auftraggebenden Geheimdienst
Betrug/ Missbrauch	Etwas Programmiererfahrung	Computer mit Modem oder Zugriff auf Zielcomputer	Peergruppe, manchmal auch ein Unternehmen des Organisierten Verbrechens
Vandalismus			
Außenstehende	Von Grundkenntnissen bis hin zu absolutem Profiniveau	Einfacher Computer mit Modem	Unterstützung durch Peergruppe
Benutzer	Computerkenntnisse, wenig bis fortgeschrittene Programmierkenntnisse	Zugriff auf Zielcomputer	Keine

3.
Kapitel

Reichweite und Ausmaß der Cyber-Kriminalität

Im Mai 2000 berichtete das FBI von einem Rekord: Die Kriminalität in den USA war 1999 im achten Jahr in Folge rückläufig. Tötungsdelikte, Überfälle, Raub und andere Kapitalverbrechen seien um sieben Prozent zurückgegangen. Nie zuvor konnte das FBI, das seit den Dreißigerjahren Verbrechensstatistiken erstellt, in acht aufeinander folgenden Jahren einen solchen Rückgang vermelden.

Doch obwohl die Kriminalität in der physischen Welt Amerikas zurückgeht, steigt leider die Kriminalität im Cyberspace weiter an.

Die folgenden vier unterschiedlichen Quellen liefern faszinierende Daten zu diesem Phänomen:

- Die Untersuchung über Computerkriminalität und Sicherheit von CSI und FBI (CSI/FBI Computer Crime and Security Survey
- Die Statistiken des CERT (Computer Emergency Response Team) über Zwischenfälle, Verwundbarkeit von Systemen, Alarmfälle usw.
- Dan Farmers Untersuchung über Sicherheit im Internet
- Die Untersuchung über Datensicherheit von WarRoom Research

Die Untersuchung über Computerkriminalität und Sicherheit von CSI und FBI

Im Sommer 1995 erhielt ich einen Anruf von FBI-Spezialagent Pat Murphy, Mitglied der neu eingerichteten Abteilung für Computereinbruch des FBI in San Francisco. Diese Abteilung war erst die zweite ihrer Art in ganz Amerika. (Die erste befand sich in Washington, D.C., und die dritte in New York.)

Die regionalen FBI-Abteilungen für Computereinbruch untersuchen Verstöße gegen das Gesetz gegen Computerbetrug und -missbrauch (Artikel 18, Abschnitt 1030), darunter Einbrüche in öffentliche Netzwerke, Eindringen in große Computernetzwerke, Verletzungen der Privatsphäre, Industriespionage, Softwarepiraterie und andere Verbrechen.

Wenige Tage darauf traf ich Murphy und den Spezialagenten für Überwachung George Vinson im 13. Stock des Staatlichen Bürogebäudes in Tenderloin, Golden Gate Avenue 450. Die beiden hatten viele Fragen: Wie gravierend ist das Problem der Computerkriminalität? Wie oft werden Unternehmen angegriffen? Welche Computerverbrechen sind am häufigsten? Welche Art von finanziellen Schäden richten sie an?

Ich sagte Murphy und Vinson, dies seien zwar alles wichtige Fragen, aber niemand könne sie beantworten. Zudem seien Antworten schwer zu bekommen. Die Firmen geben schlechte Neuigkeiten nur höchst ungern zu.

Ich schlug vor, eine anonyme Untersuchung unter den Mitgliedern des CSI durchzuführen. (Dies sind Leute aus der Praxis der Datensicherheit in den Fortune-500-

Unternehmen und großen Regierungsbehörden.) Murphy und Vinson forderte ich auf, die Fragen zu stellen, auf die sie eine Antwort wollten. So einfach fing alles an.

Die Untersuchung über Computerkriminalität und Sicherheit von CSI und FBI wurde als Service für die Öffentlichkeit vom Institut für Computersicherheit (CSI, Computer Security Institute) unter Beteiligung der FBI-Abteilung für Computereinbruch durchgeführt. Diese ständige Einrichtung zielt darauf ab, das Sicherheitsbewusstsein zu stärken und bei der Bestimmung des Ausmaßes der Computerkriminalität in den USA zu helfen.

Der Erfolg der Untersuchung ist auf dem Gebiet der Informationssicherheit beispiellos.

In ihrem fünften Jahr ist die alljährliche Veröffentlichung der Ergebnisse der Untersuchung über Computerkriminalität und Sicherheit von CSI und FBI ein Ereignis, das international Schlagzeilen macht und in den wichtigsten Print- und Hörfunkmedien ausführlich behandelt wird. Der CSI/FBI-Bericht ist wohl die meist zitierte Untersuchung über das Ausmaß und die Reichweite der Cyber-Kriminalität und der damit verbundenen Sicherheitsprobleme. Darüber hinaus zitieren das ganze Jahr lang viele Präsentationen, Presseartikel und Papers über das Wesen und Ausmaß der Computerkriminalität die Untersuchungsergebnisse.

Die Ergebnisse dieser Studie von CSI und FBI führten zu meiner Aussage vor dem US-Senat im Jahr 1995. Sie waren Anlass meiner Reisen nach Südafrika, Japan, Brasilien, Portugal, Norwegen und anderen Orten, an denen ich mit Managern Briefings zu den Themen Cyber-Kriminalität und digitale Kriegführung abhielt.

Die Antworten von 643 Praktikern der Datensicherheit in amerikanischen Firmen und Behörden führten zu Erkenntnissen aus der Untersuchung über Computerkriminalität und Sicherheit von CSI und FBI bezüglich der Trends, die sich in den letzten Jahren herauskristallisierten:

- Organisationen werden von innerhalb und außerhalb der Grenzen ihrer Elektronik attackiert.
- Eine große Bandbreite von Cyber-Attacken wurde entdeckt.
- Cyber-Attacken können schwere finanzielle Schäden verursachen.
- Um sich gegen solche Attacken erfolgreich zu wehren, ist mehr als nur der Einsatz von Datensicherheitstechnologien erforderlich.

Patrice Rapalus, Direktorin von CSI (und meine Vorgesetzte), führt dazu aus: »Die Untersuchung von CSI und FBI hat über die Jahre entstandene Trends offengelegt. Cyber-Kriminalität und Verletzungen der Datensicherheit sind weit verbreitet und treten in unterschiedlichen Formen auf. Hinzu kommt, dass solche Zwischenfälle ernste Schäden verursachen können.

Natürlich muss auch daran gearbeitet werden, dass die Organisationen zuverlässige Verfahren installieren, fortschrittliche Technologien einsetzen und vor allem

genügend und ausreichend geschultes Personal für die Datensicherheit beschäftigen. Das gilt für den privaten ebenso wie für den staatlichen Sektor.«

Bruce J. Gebhardt ist der Leiter des FBI-Büros für Nordkalifornien. Er hat seinen Hauptsitz in San Francisco und ist für 15 Counties zuständig, darunter der permanent expandierende Bezirk des Silicon Valley. Die Computerkriminalität stellt für ihn eine der größten Herausforderungen dar.

»Wenn das FBI und andere Strafverfolgungsbehörden dieses stetig wachsende Problem erfolgreich bewältigen sollen, dann können wir nicht immer nur reagieren und Computerattacken erst behandeln, wenn sie eintreten. Die Ergebnisse der Studie von CSI und FBI liefern uns wertvolle Daten. Diese Informationen wurden nicht nur dem Kongress vorgelegt, um die Notwendigkeit zusätzlicher Ermittlungswerkzeuge im ganzen Land zu unterstreichen, sondern sie identifizieren auch neue Trends in der Kriminalität und helfen mir zu entscheiden, wie ich diese Ermittlungswerkzeuge am vorausschauendsten und aggressivsten einsetzen kann, bevor sich diese ›Trends‹ zu ›Krisen‹ auswachsen.«

Inmitten des Medienrummels um die Veröffentlichung des fünften Jahresberichts über die Untersuchung von CSI und FBI fragten einige Journalisten: »Was ist für Sie die größte Überraschung an den diesjährigen Daten?«

Meine Antwort: »Die einzige Überraschung ist, dass es keine Überraschungen gibt.«

So stieg zum Beispiel die Zahl der Untersuchungsteilnehmer, die ihre Internetanschlüsse als häufigen Angriffspunkt meldeten, seit fünf Jahren immer weiter an.

Die Möglichkeit, über einen Zeitraum von mehreren Jahren Antworten auf dieselben Fragen zu erhalten, bietet wertvolle, nie dagewesene Einblicke in das, was da draußen tatsächlich passiert.

Im Folgenden gebe ich eine Zusammenfassung der Erkenntnisse, die wir bisher während der gesamten Lebensdauer das Projekts gewonnen haben.

Wen wir fragten

Die meisten Untersuchungsteilnehmer arbeiten für große Unternehmen. Die stärkste Konzentration findet sich in der Finanzdienstleistungs- und in der Hightech-Branche (je 17 Prozent der Befragten). Die nächstgrößte Teilnehmerzahl stammt aus der produzierenden Industrie (10 Prozent).

Der staatliche Sektor ist stark vertreten. Insgesamt stellen Regierungsbehörden des Bundes (9 Prozent), der Einzelstaaten (7 Prozent) und der lokalen Ebene (2 Prozent) weitere 18 Prozent der Befragten.

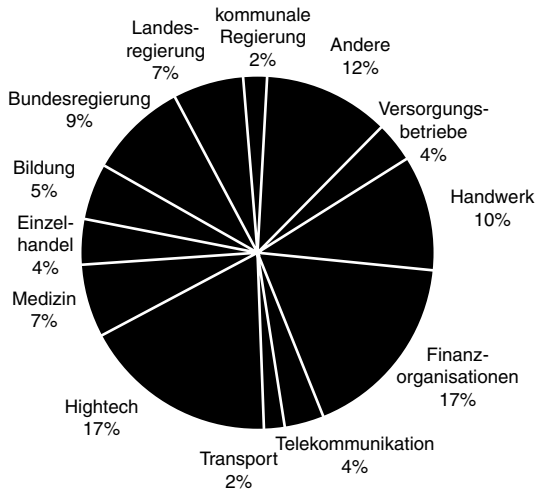

Abbildung 3.1: Befragte nach Branchen. Quelle: CSI/FBI-Untersuchung 2000. 100% = 643 Befragte

Auch andere Organisationen aus lebenswichtigen Bereichen der nationalen Infrastruktur waren beteiligt, darunter z.B. Gesundheitswesen (7 Prozent), Telekommunikation (4 Prozent) und Stadtwerke (4 Prozent).

Die Antworten kommen von großen Arbeitgebern – 30 Prozent der befragten Organisationen haben 10 000 oder mehr Arbeitnehmer; zwölf Prozent haben zwischen 5 001 und 9 999 Beschäftigte.

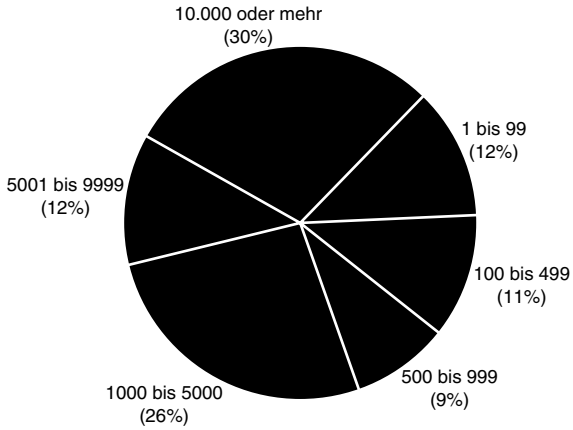

Abbildung 3.2: Befragte nach Zahl der Beschäftigten. Quelle: CSI/FBI-Untersuchung 2000. 99% = 640 Befragte

Dreiundvierzig Prozent der Teilnehmer aus der Wirtschaft haben einen Bruttoertrag von mehr als einer Milliarde Dollar. Bei elf Prozent liegt der Bruttoertrag zwischen 501 Millionen und einer Milliarde. (Interessanterweise ist dies genau umgekehrt wie 1999: Seinerzeit hatten 40 Prozent zwischen 501 Millionen und einer Milliarde und 16 Prozent mehr als eine Milliarde Dollar Bruttoertrag. Ist dies ein weiterer Beweis für den wirtschaftlichen Wohlstand Mitte der Neunzigerjahre?)

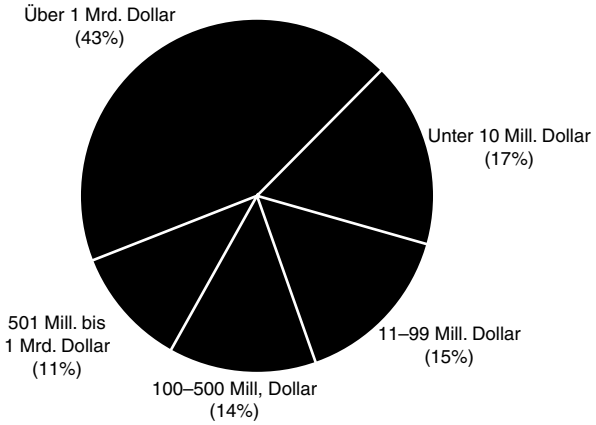

Abbildung 3.3: Befragte nach Bruttoertrag.
Quelle: CSI/FBI-Untersuchung 2000.
65% = 422 Befragte

Betrachten Sie nun einmal die 643 Antworten im Hinblick auf Branche, Beschäftigtenzahl und Bruttoertrag. Die Ergebnisse verdienen ganz klar Ihre Aufmerksamkeit. Die Art der gemeldeten Zwischenfälle (seien sie illegal, strittig oder einfach nur ungehörig) und die Trends, die sich über die fünfjährige Lebensdauer der Untersuchung bestätigt haben, können der wirtschaftlichen Wettbewerbsfähigkeit der USA potenziell ernsthaft schaden.

Solange die Datensicherheit nicht im gesamten Staat und in der gesamten Wirtschaft in das Zentrum konzertierter Bemühungen rückt, werden im Cyberspace die Rechtsstaatlichkeit ebenso wie die führende Rolle der USA auf den Weltmärkten untergraben.

Der Outlaw-Blues

Wie weit verbreitet sind Cyber-Attacken und andere Verstöße gegen die Datensicherheit?

Über fünf Jahre haben wir die folgende Frage gestellt: »Haben Sie in den letzten zwölf Monaten eine unbefugte Nutzung Ihrer Computersysteme beobachtet?« Im Jahr 1996 antworteten 42 Prozent mit »ja«. Im Jahr 2000 waren es 70 Prozent. (Aus diesen Zahlen wurden solche Fälle herausgerechnet, wo sich das »ja« lediglich auf Zwischenfälle mit Computerviren, Laptop-Diebstahl und/oder andere Formen einer missbräuchlichen Verwendung von Netzwerkberechtigungen durch Benutzer bezog.)

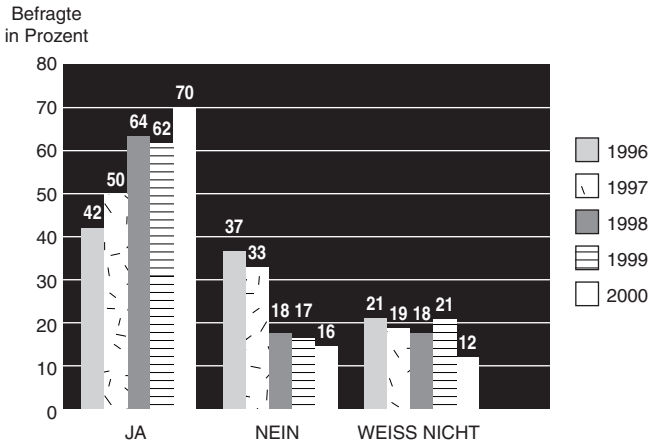

Abbildung 3.4: Unbefugte Benutzung von Computersystemen in den vergangenen zwölf Monaten. Quelle: CSI/FBI-Untersuchung 2000. 2000: 91% = 585 Befragte 1999: 98% = 512 Befragte 1998: 99% = 515 Befragte 1997: 69% = 391 Befragte 1996: 96% = 410 Befragte

Es bestärkt uns zu sehen, wie schnell die Anzahl derer, die diese Frage mit »nein« beantworteten, von 37 Prozent im Jahr 1996 auf 16 Prozent im Jahr 2000 zurückging. 1997 antworteten noch 33 Prozent der Befragten mit »nein«. In den »Randbemerkungen« zur 1997 erstellten Studie schrieb ich: »Letztlich sind ›ja‹ und ›weiß nicht‹ wahrscheinlich die einzigen ehrlichen Antworten auf diese Frage.« Im Jahr darauf fiel die Anzahl der »nein«-Antworten auf 18 Prozent.

Heute, im fünften Jahr der Untersuchungsergebnisse, ist die Anzahl derer, die mit »weiß nicht« geantwortet haben, endlich gesunken: von 21 Prozent in 1999 auf 12 Prozent in 2000.

Was bedeutet all das? Die Menschen leugnen die Gefahr nicht mehr. Sie beobachten die Aktivitäten auf ihren Netzwerken genauer. Sie setzen dafür bessere Werkzeuge ein und sind eher bereit, mit »ja« zu antworten.

Und der Ursprung der Angriffe? Nun, zwar mögen immer noch viele der althergebrachten Weisheit anhängen, dass »80 Prozent der Probleme von Insidern und nur 20 Prozent der Probleme von Außenstehenden« verursacht werden, aber die Anzahl derer, die ihre Internetanbindung als häufiges Angriffsziel melden, ist Jahr für Jahr gestiegen: von 37 Prozent 1996 auf 59 Prozent 2000. Indessen sank die Anzahl derer, die ihre internen Systeme als häufiges Angriffsziel meldeten, von 51 Prozent in 1999 auf 38 Prozent in 2000.

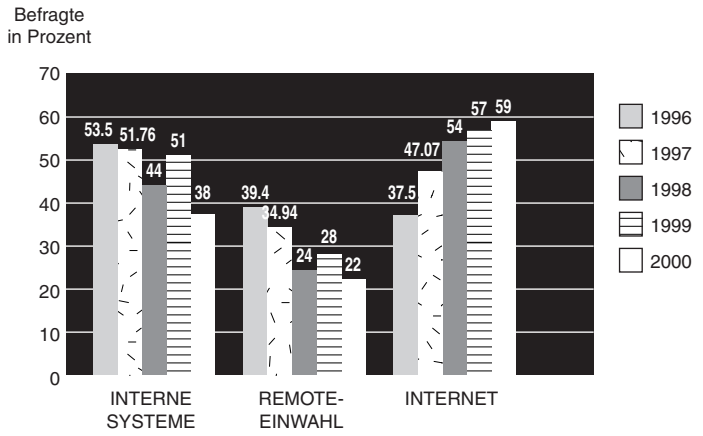

Abbildung 3.5: Immer häufiger wird die Internetanbindung als häufiges Angriffsziel gemeldet.
Quelle: CSI/FBI-Untersuchung 2000.
2000: 68% = 443 Befragte
1999: 62% = 324 Befragte
1998: 54% = 279 Befragte
1997: 69% = 391 Befragte
1996: 40% = 174 Befragte

Die alte Weisheit, dass 80 Prozent der Angreifer Insider und 20 Prozent Außenstehende seien, wird von den Fakten einfach nicht mehr gestützt. Nicht, dass die Bedrohung durch Insider nachgelassen hätte, aber die Bedrohung von außen ist mit zunehmender Bedeutung des Internets als Mittel der Unternehmenskommunikation dramatisch gewachsen.

Bob Dylan prahlte 1965 in seinem »Outlaw Blues«: »Stell mir bloß keine Fragen, ich könnte die Wahrheit antworten.«

Formen von Cyber-Attacken

In den letzten vier Jahren haben wir immer gefragt: »Welche der folgenden Formen elektronischer Angriffe oder elektronischen Missbrauchs hat Ihre Organisation in den vergangenen zwölf Monaten entdeckt?«

Im Jahr 2000 meldeten die Befragten ein breites Spektrum an Angriffen und missbräuchlichen Nutzungen. Einige Beispiele:

- 11 Prozent entdeckten Finanzbetrügereien
- 17 Prozent entdeckten Daten und/oder Netzwerksabotage
- 20 Prozent entdeckten Diebstahl personenbezogener Daten
- 25 Prozent entdeckten einen Systemeinbruch von außen
- 27 Prozent entdeckten Denial-of-Service[1]-Angriffe
- 71 Prozent entdeckten unbefugten Zugriff von Insidern
- 79 Prozent entdeckten Missbrauch von Internetrechten durch Mitarbeiter
- 85 Prozent entdeckten Viren

Berichten oder nicht berichten?

Die Untersuchung über Computerkriminalität und Sicherheit von CSI und FBI will nicht nur Daten über die dunkle Seite des Cyberspace sammeln, sondern auch die Zusammenarbeit von Gerichtsbarkeit und privater Wirtschaft fördern, damit beide die Cyber-Kriminalität wirksam bekämpfen können

In den ersten drei Jahren zeigten nur 17 Prozent der Organisationen, die Opfer ernsthafter Angriffe wurden, diese Attacken auch an. In der Studie von 1999 antworteten 32 Prozent, sie hätten solche Zwischenfälle den Strafverfolgungsbehörden angezeigt. Im Jahr 2000 sank die Zahl der Befragten, die Anzeige wegen solcher Übergriffe erstatteten, wieder auf 25 Prozent.

1. »Denial of Service«: Wenn ein Server in einer Flut von Daten geradezu ertrinkt, muss er seinen Dienst verweigern.

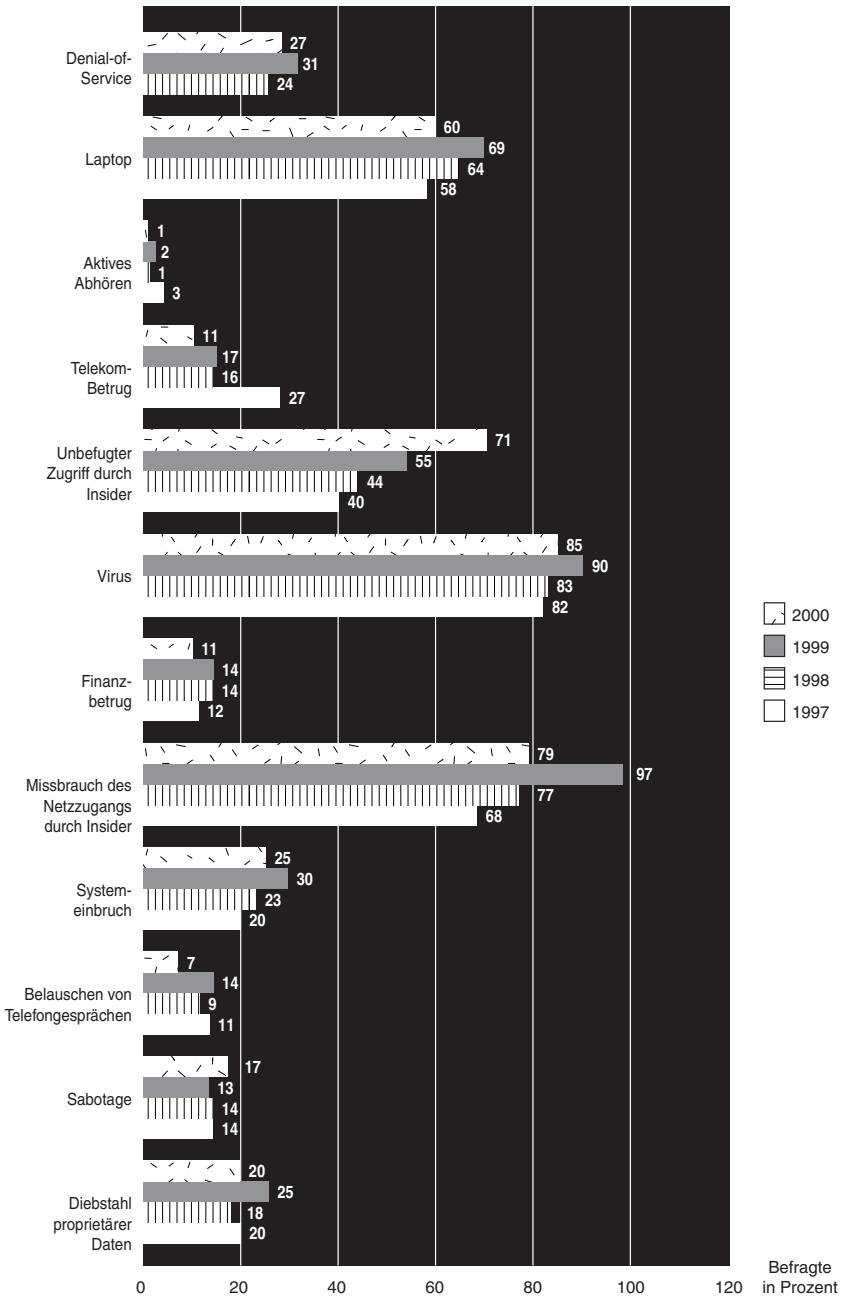

Abbildung 3.6: Arten von Attacken oder missbräuchlicher Verwendung, die in den vergangenen zwölf Monaten gemeldet wurden (in Prozent). Quelle: CSI/FBI-Untersuchung 2000.
2000: 90% = 581 Befragte
1999: 78% = 405 Befragte
1998: 89% = 458 Befragte
1997: 87% = 492 Befragte

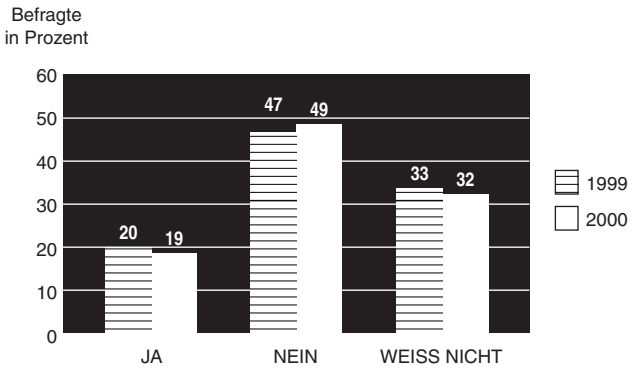

Abbildung 3.7: Verzeichnete Ihre Website in den vergangenen zwölf Monaten unbefugten Zugriff oder sonstige missbräuchliche Verwendung? 99% der Befragten haben Websites, 43% stellen auf ihren Websites E-Commerce-Dienste zur Verfügung. Im Jahr 1999 waren nur 30% im E-Commerce tätig.
Quelle: CSI/FBI-Untersuchung 2000.
2000: 93% = 603 Befragte
1999: 92% = 479 Befragte

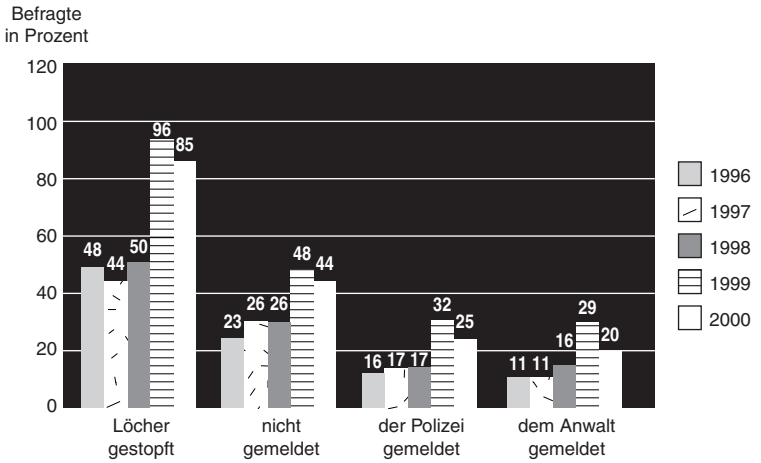

Abbildung 3.8: Falls Ihre Organisation in den vergangenen zwölf Monaten unbefugte(n) Computerzugriff(e) verzeichnete: Welche der folgenden Maßnahmen haben Sie ergriffen?
Quelle: CSI/FBI-Untersuchung 2000.
2000: 63% = 407 Befragte
1999: 57% = 295 Befragte
1998: 72% = 321 Befragte
1997: 56% = 317 Befragte
1996: 76% = 325 Befragte

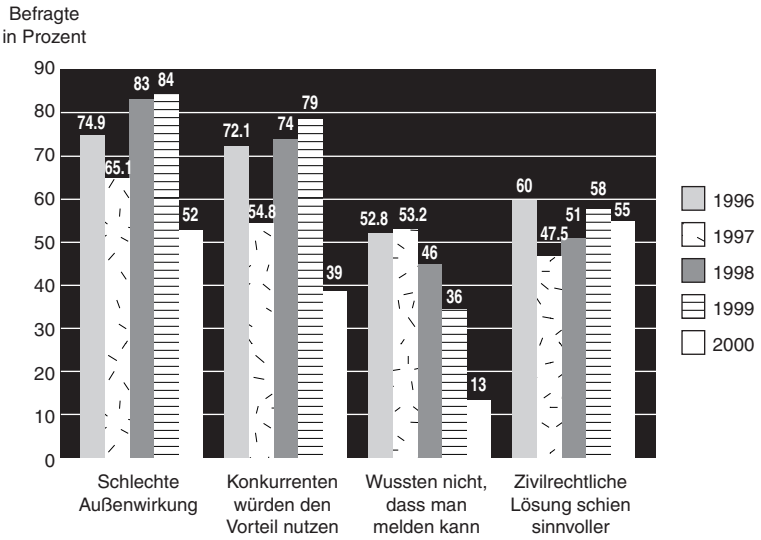

Abbildung 3.9: Die Gründe, aus denen Unternehmen unbefugte Zugriffe nicht den Strafverfolgungsbehörden gemeldet haben. Quelle: CSI/FBI-Untersuchung 2000. 2000: 32% = 209 Befragte 1999: 20% = 107 Befragte 1998: 19% = 96 Befragte 1997: 25% = 142 Befragte 1996: 15% = 64 Befragte

Dr. Dorothy Denning von der Universität Georgetown (Washington D.C.) erklärt, es hätten zwar im Jahr 2000 prozentual weniger Unternehmen als im Jahr 1999 Zwischenfälle angezeigt, aber die absolute Anzahl sei dennoch höher als in den vorangegangenen Jahren, während der Prozentsatz der Unternehmen rückläufig sei, die von einer schlechten Presse oder ihrer Sorge berichten, die Konkurrenz könne dies ausschlachten. Denning folgert: »Dass weniger Anzeigen als im Vorjahr erstattet wurden, könnte auch andere Ursachen haben, z.B. die Kosten einer Ermittlung oder die Erwartung, dass eine Ermittlung erfolglos bleiben würde.«

Tatsächlich sieht es nach Auffassung von Dr. Denning zumindest bei den Teilnehmern an der CSI/FBI-Untersuchung so aus, als sei es immer weniger ein Tabu, Vorfälle anzuzeigen. Der Prozentsatz der Teilnehmer, die »Negativschlagzeilen« befürchteten, sank von 84 Prozent auf 52 Prozent und der Prozentsatz der Befragten, die befürchteten, »die Konkurrenz würde die Nachricht von dem Computereinbruch nutzen, um sich einen Wettbewerbsvorteil zu verschaffen«, sank von 79 Prozent auf 39 Prozent.

Rik Farrow vom CSI (www.spirit.com) gibt weitere Einblicke:

»Das FBI hat mehrere Ermittlungen abgeschlossen, in denen die Identität der Opfer nie preisgegeben wurde. Dies ist ein ermutigendes Zeichen für jene, die eine

schlechte Außenwirkung befürchten. Gleichzeitig kann jedoch jemand, der einen gewaltigen Schaden angerichtet hat und verurteilt wird, mit einer viel leichteren Strafe davonkommen als jemand, der mit einer kleinen Menge Marihuana aufgegriffen wird. Ein für die Sicherheit zuständiger Bankdirektor erwähnte, die Bank würde möglichst immer zivilrechtlich vorgehen, da diese Strafen (plus Anwaltskosten des Verteidigers) in der Regel viel strenger seien.«

Die Wahrheit ist irgendwo da draußen

Die Untersuchung über Computerkriminalität und Sicherheit von CSI und FBI ist eine zwar nichtwissenschaftliche und informelle, aber äußerst fokussierte Datenerhebung unter Praktikern der Datensicherheit.

Bestenfalls liefert diese Untersuchung eine Momentaufnahme, die uns ein Gefühl dafür gibt, welche Fakten zu einem bestimmten Zeitpunkt »auf dem Tisch liegen«. Diese Fakten werden größtenteils durch Daten aus anderen seriösen Untersuchungen und durch die realen, in allgemein zugänglichen Veröffentlichungen dokumentierten Vorfälle bestätigt. Ich finde, dass die Ergebnisse von CSI und FBI zusätzlich dadurch erhärtet werden, dass sie aus den Daten von fünf aufeinander folgenden Jahren schöpfen können.

Das CSI stellt die Untersuchungsergebnisse der Öffentlichkeit zur Verfügung. Jeder, der den Bericht anfordert, erhält ein kostenloses Exemplar. Das FBI in San Francisco hat dazu einen unschätzbaren Beitrag geleistet, indem es sich an der Entwicklung der Studie selbst beteiligte und sich mit uns gemeinsam um Antworten bemühte. Es gibt jedoch zwischen CSI und FBI keine vertraglichen oder finanziellen Beziehungen. Es war lediglich eine übergreifende und auf Erkenntniszuwachs ausgerichtete, gemeinsame Anstrengung beider Organisationen. Der CSI trägt die Kosten und die alleinige Verantwortung für die Ergebnisse.

Hoffentlich finden Sie in der Mischung aus wahren Horrorgeschichten und Datenmaterial, die dieser Bericht enthält, einige für die Datensicherheit in Ihrem Unternehmen relevante Informationen, die Ihnen helfen, Ihren Cyberspace-Quadranten für Neuschöpfung, Kommunikation und Handel sicherer zu machen.

Ein Wort zur Methodik

Wir haben Fragebögen mit Freiumschlägen an 4 284 Datensicherheitsprofis versandt, von denen 643 (oder 15 Prozent) geantwortet haben. 1998 erhielten wir 520 Antworten (13 Prozent von 3 890 versandten Fragebögen). 1997 waren es 563 Antworten (11 Prozent von 4 899 versandten Fragebögen). 1996 antworteten 428 Befragte (8 Prozent von 4 971 versandten Fragebögen).

Die Antworten waren anonym. Die Befragten bezeichneten sich als Manager für die Datensicherheit, als Datensicherheitsbeauftragte oder als Chef-Systemanalytiker. Unter den teilnehmenden Organisationen waren Großunternehmen, Finanzinstitutionen, Regierungsbehörden und Universitäten in den USA.

Andere Quellen zum Thema

Folgende Daten habe ich aus seriösen Untersuchungen anderer Organisationen herausgepickt.

Statistiken von CERT/CC

Das im Kielwasser des Morris-Wurms (siehe Kapitel 5) an der Carnegie Mellon-Universität gegründete CERT (Computer Emergency Response Team) ist ein Vorreiter bei der Verbreitung von Informationen über Sicherheit im Internet. Solche Informationen umfassen Warnungen vor bevorstehenden oder laufenden Angriffen und Hinweise auf Patches, die Sicherheitslücken in Betriebssystemen und Anwendungen schließen können. Die CERT-Daten, die ich hier vorstelle, wurden aus den vielen Anrufen zusammengestellt, die das Team von Systemadministratoren aus dem gesamten Cyberspace rund um die Uhr erhält.

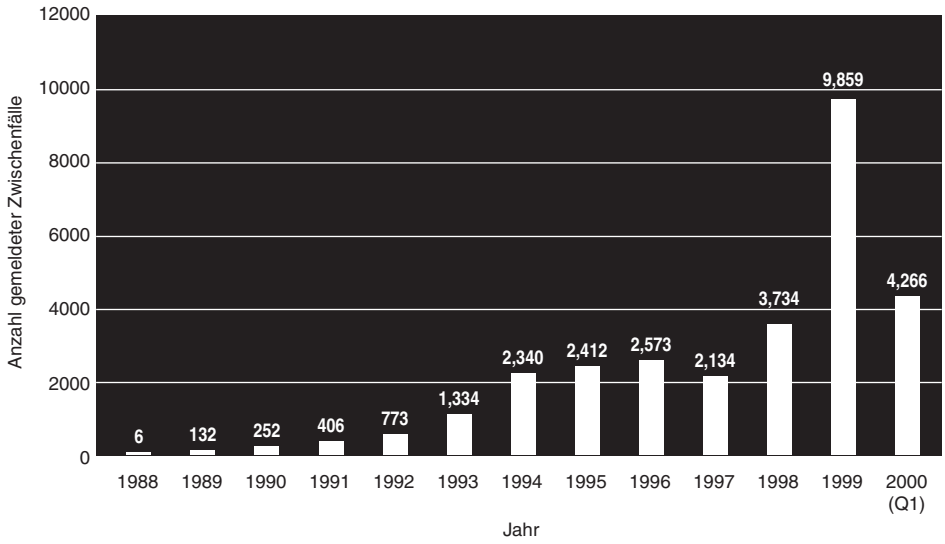

Abbildung 3.10: Anzahl der angezeigten Zwischenfälle.
Quelle: CERT/CC-Statistik 1988–2000
Gesamtzahl der gemeldeten Zwischenfälle (1988–2000): 30 261

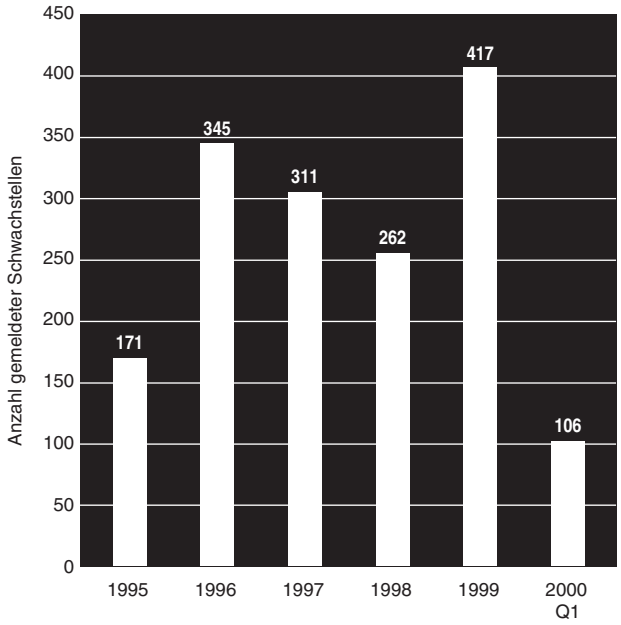

Abbildung 3.11: Angezeigte verwundbare Stellen.
Quelle: CERT/CC-Statistik 1988–2000
Gesamtzahl der gemeldeten verwundbaren Stellen (1988–2000): 1 612

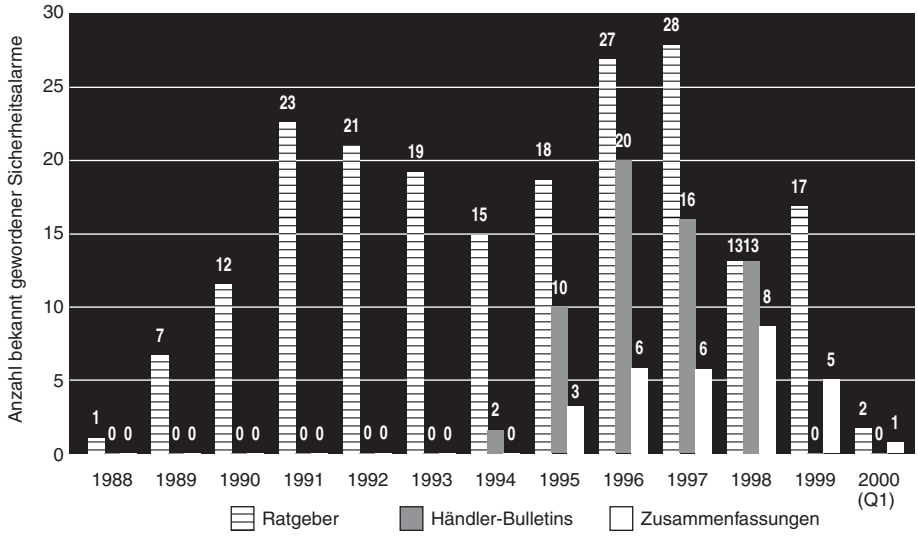

Abbildung 3.12: Öffentlich gewordene Sicherheitsalarme.
Quelle: CERT/CC-Statistik 1988–2000
Gesamtzahl der gemeldeten Sicherheitsalarme (1988–2000): 293

Dan Farmers Untersuchung über Sicherheit im Internet

Dan Farmer ist ein führender – wenngleich umstrittener – Experte für Sicherheit im Internet. Er schrieb das Tool »SATAN«, mit dem sich verwundbare Stellen in Netzwerken und im Internet aufspüren und offenlegen lassen. Dan Farmer führte seine Untersuchung über Sicherheit im Internet (»Internet Security Survey«) durch, indem er frech und ungebeten seit 1996 Websites im Internet durchsuchte.

Laut Farmer weist die Kennzeichnung »rot« auf Websites hin, die »jedem potenziellen Angreifer weit offen stehen« (»Red Web«), und »gelb« kennzeichnet solche Websites, die »zwar nicht ganz so ernsthafte, aber immer noch sehr Besorgnis erregende Probleme aufweisen« (»Yellow Web«).

Zusammenfassung der Untersuchung über Sicherheit im Internet

Art der Website	Gesamtzahl der untersuchten Hosts	davon verwundbar (%)	gelb (%)	rot (%)
Banken	660	68,33	32,73	35,61
Kreditvereine	274	51,09	30,66	20,44
Staatliche Websites der USA	47	31,70	23,40	38,30
Zeitungen	312	69,55	30,77	38,78
Sex	451	66,08	40,58	25,50
Gesamt	**1 734**	**64,94**	**33,85**	**31,08**
Vergleichsgruppe	**469**	**33,05**	**15,78**	**17,27**

Der Datensicherheitsbericht von WarRoom Research

WarRoom Research ist eine im Gebiet von Washington D.C. ansässige Gruppe von Nachrichten- und Datensicherheitsberatern. Sie stellt ihre Daten ähnlich wie CSI/FBI aus den Fortune-500-Unternehmen zusammen. Die Tabellen in diesem Abschnitt geben Antworten auf die folgenden Fragen.

»Haben Sie in den vergangenen zwölf Monaten irgendwelche Versuche von »Außenstehenden« entdeckt, auf eines Ihrer Computersysteme zuzugreifen?«

Ja	119	58,0 Prozent
Nein	25	12,2 Prozent
Weiß nicht	61	29,8 Prozent
Gesamt	205	100,0 Prozent

Zusammenbruch wegen Verwundbarkeit nach Typ der Website (Prozent).
Quelle: Dan Farmer, www.fish.com[1]
(Die Denial-of-Service- und Yellow-Web-Verletzungen wurden als »gelb« und die anderen Verletzungen als »rot« gekennzeichnet.)

Art der Website	Denial of Service	FTP	Yellow Web	INND	REXD access	Send-mail	Red Web	YPup-dated	statd
Banken	57,12	0,15	9,85	3,18	0,15	9,70	1,52	0,91	29,39
Kredit-vereine	43,43	0,00	8,03	1,46	0,00	4,01	0,73	1,09	16,42
Staatliche Websites der USA	44,68	0,00	36,17	0,00	0,00	12,76	2,12	6.38	31,91
Zeitungen	52,88	0,32	14,42	2,24	0,00	16,67	1,28	0,64	30,77
Sex	56,54	0,00	6,65	1,33	0,00	11,97	0,67	0,00	18,85
Gesamt	**53,63**	**0,12**	**10,32**	**2,19**	**0,06**	**10,67**	**1,1**	**0,81**	**24,91**
Vergleichs-gruppe	**28,14**	**0,00**	**1,92**	**0,64**	**0,64**	**7,25**	**0,00**	**0,64**	**13,65**

»Wenn ja, wie viele erfolgreiche, unauthorisierte Zugriffe von »Außenstehenden« haben Sie entdeckt?«

1–10	41	41,8 Prozent
11–20	24	24,5 Prozent
21–30	16	16,3 Prozent
31–40	10	10,2 Prozent
41–50	5	5,1 Prozent
>50	2	2,0 Prozent
Gesamt	98	100,0 Prozent

1. Auf dieser Website finden Sie unter »Internet Security Survey 1996« die Fachbegriffe im Zusammenhang erklärt (Anm. d. Übers.).

»Wenn jemand von außen in Systeme Ihrer Organisation eingedrungen ist, geben Sie bitte an, in welcher Weise der Eindringling aktiv geworden ist.«

Datenintegrität manipuliert	41	6,8 Prozent
Schnüffelprogramm installiert	40	6,6 Prozent
Passwortdateien gestohlen	34	5,6 Prozent
Systeme sondiert/durchsucht	88	14,6 Prozent
Trojanische Logons	35	5,8 Prozent
IP-Schwindel	29	4,8 Prozent
Virus eingeführt	64	10,6 Prozent
Nutzung von Diensten unterbunden	38	6,3 Prozent
Daten heruntergeladen	49	8,1 Prozent
Geschäftsgeheimnisse verletzt	59	9,8 Prozent
Geld gestohlen/umgeleitet	2	0,3 Prozent
E-Mails/Dokumente gelesen	76	12,6 Prozent
Das Eindringen veröffentlicht	3	0,5 Prozent
Personal belästigt	27	4,5 Prozent
Sonstiges (Beschreibung)	18	3,0 Prozent
Gesamt	603	100,0 Prozent

»Wie viele ›Insider‹ haben Sie bei einem Missbrauch der Computersysteme Ihrer Organisation entdeckt? (Eigenes Geschäft auf dem Firmencomputer betreiben, missbräuchliche Verwendung von Online-Accounts oder personenbezogenen Daten etc.)«

Unbekannt	20	9,8 Prozent
0	56	27,3 Prozent
1–5	24	11,7 Prozent
6–10	46	22,4 Prozent
11–15	32	15,6 Prozent
16–20	13	6,3 Prozent
21–25	9	4,4 Prozent
>25	5	2,4 Prozent
Gesamt	205	100,0 Prozent

»Wenn ja, welche Disziplinarmaßnahmen haben Sie ergriffen?«

Mündliche Verwarnung	70	54,3 Prozent
Schriftliche Abmahnung	27	20,9 Prozent
Beurlaubung	7	5,4 Prozent
Kündigung	8	6,2 Prozent
Entlassung	11	8,5 Prozent
Justiz eingeschaltet	2	1,6 Prozent
Außergerichtlicher Vergleich	0	0,0 Prozent
Keine Maßnahmen	4	3,1 Prozent
Sonstiges (Beschreibung)	0	0,0 Prozent
Gesamt	129	100,0 Prozent

Fazit

Diese drei unterschiedlichen Quellen bieten verschiedene Einblicke in dasselbe Problem. Die Daten des CERT spiegeln wider, worüber Systemadministratoren in der Internetgemeinschaft berichten. Farmers Daten zeigen, wie ein auf eigene Faust arbeitender, frecher Hacking-Experte das Maß der Verwundbarkeit im Web beurteilt. Die Daten des WarRoom Research liefern eine zweite Meinung zu den Daten der CSI/FBI-Untersuchung über den Zustand der Datensicherheit in amerikanischen Firmen. Zusammengenommen führen diese drei sehr unterschiedlichen Wege der Datenerhebung alle zur selben Schlussfolgerung: Kriminalität im Cyberspace ist real und wird nicht angemessen bekämpft.

4.
Kapitel

Kosten von Computerkriminalität und Sicherheitsverletzungen

Welche Kosten verursacht die Computerkriminalität? Wie gliedern sich diese Kosten auf? Antworten auf diese brennenden Fragen sind nicht leicht zu bekommen.

In den vergangenen vier Jahren unserer Studie über Computerkriminalität und Sicherheit von CSI und FBI fragten wir immer: »Welche der folgenden Arten von elektronischen Angriffen oder missbräuchlicher Verwendung Ihrer Elektronik hat Ihrer Organisation in den vergangenen zwölf Monaten finanzielle Schäden zugefügt?«

Im Jahr 1997 antworteten 75 Prozent der Befragten, ihre Organisationen seien finanziell geschädigt worden. Im Jahr 1998 räumten 73 Prozent finanzielle Schäden ein. 1999 fiel der Anteil derer, die finanzielle Schäden angaben, auf 51 Prozent. 2000 stieg dieser Prozentsatz jedoch wieder auf 74 Prozent.

Jedes Jahr sind mehr Leute eher bereit, finanzielle Schäden einzuräumen, als diese auch zu quantifizieren.

1997 waren nur 59 Prozent bereit oder in der Lage, einen Teil ihrer finanziellen Schäden zu beziffern. Im Jahr 1998 waren es nur 42 Prozent, 1999 nur 31 Prozent und 2000 nur 42 Prozent.

Im vergangenen Jahr (2000) bezifferten sich die Verluste dieser 273 Befragten auf insgesamt $265 589 940. (Im Durchschnitt betrug der gesamte Verlust über die vergangenen drei Jahre ingesamt $120 240 180.)

2000 waren die finanziellen Schäden in acht von zwölf Kategorien größer als im Vorjahr. Zudem waren die Schäden in vier Kategorien höher als der kombinierte Gesamtbetrag in den drei vorherigen Jahren. So bezifferten 61 Befragte ihre Verluste durch Daten- oder Netzwerksabotage mit insgesamt $27 148 000, während sich der Gesamtschaden der vorangegangenen Jahre insgesamt nur auf $10 848 850 belaufen hatte.

Wie schon in den Jahren zuvor gingen auch hier die größten finanziellen Schäden auf das Konto von Diebstahl schutzwürdiger Daten (66 Befragte zeigten Verluste von insgesamt $66 708 000 an) und Finanzbetrügereien (53 Befragte zeigten Verluste von insgesamt $55 996 000 an).

Im Dezember 1999 hielt ich auf einem Nationalen Sicherheitsforum mit dem Thema »Internationale Zusammenarbeit zur Bekämpfung von Cyber-Kriminalität und Terrorismus« einen Vortrag über die »Einschätzung der Kosten der Cyber-Kriminalität«. Dieses vom Konsortium zur Erforschung von Datensicherheit und Datenstrategie (CRISP, Consortium for Research on Information Security and Policy) gesponserte Treffen fand auf dem Campus der Stanford University im Zentrum für Internationale Sicherheit und Zusammenarbeit des Hoover-Instituts (CISAC, Hoover Institute Center for International Security and Cooperation) statt.

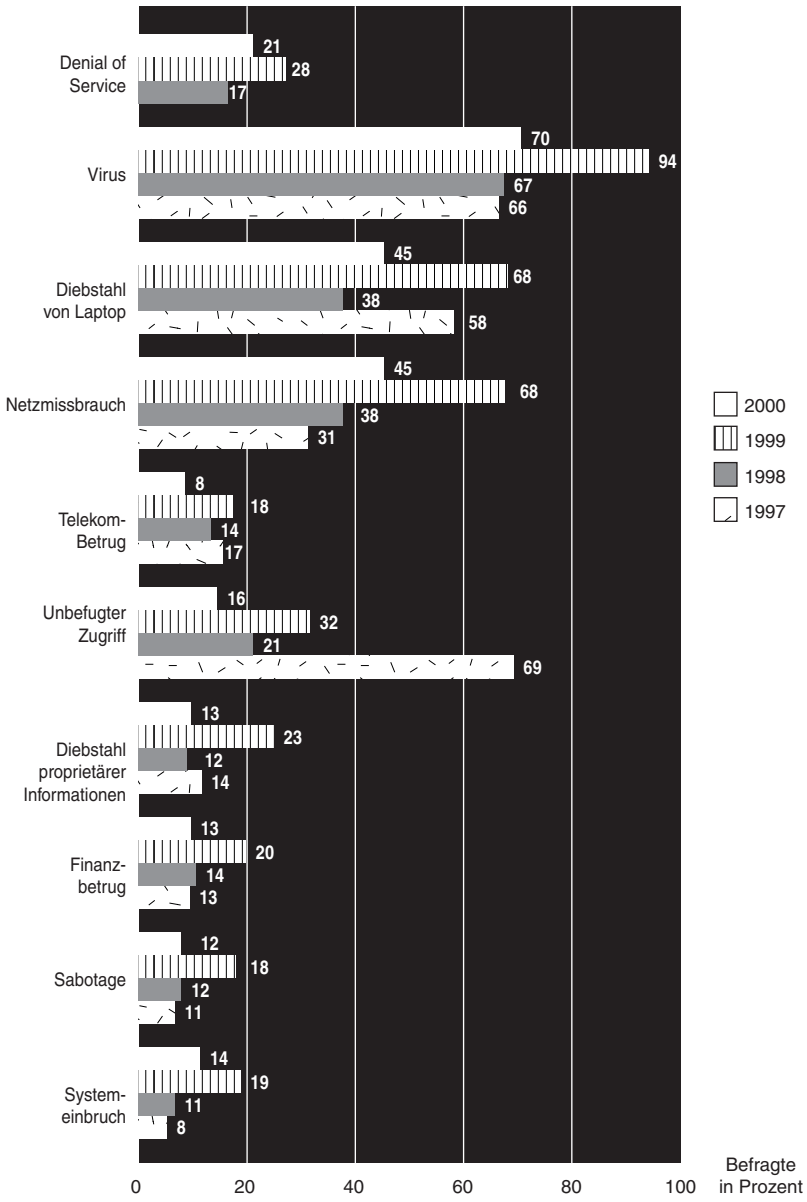

Abbildung 4.1: Finanzielle Schäden nach Art des Angriffs oder Missbrauchs. Quelle: CSI/FBI-Untersuchung 2000.
2000: 74% = 477 Befragte
1999: 51% = 265 Befragte
1998: 73% = 376 Befragte
1997: 75% = 422 Befragte

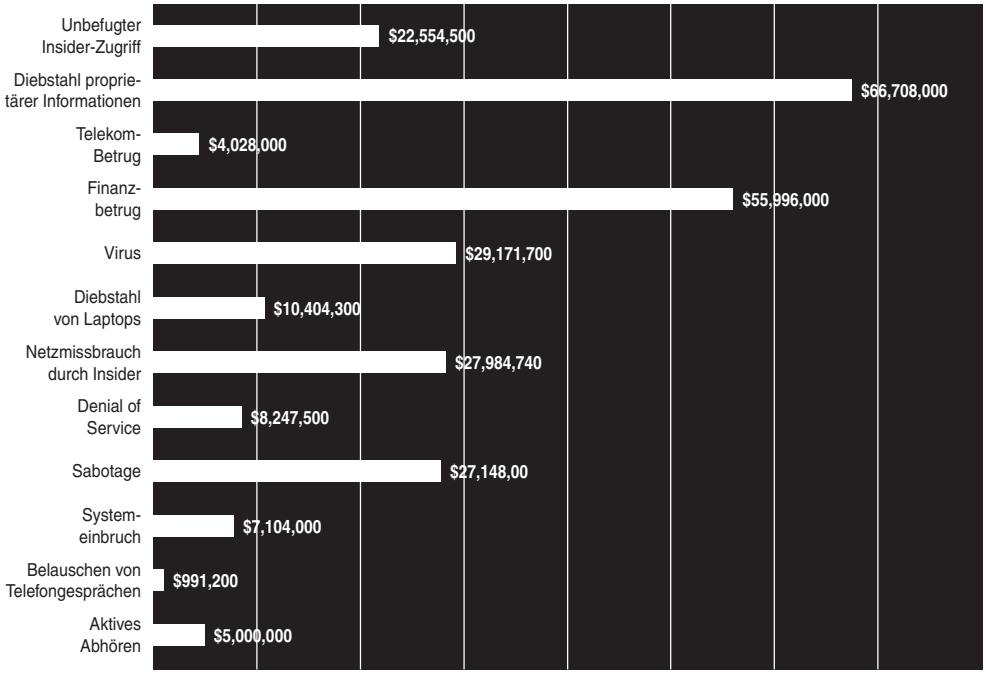

Abbildung 4.2: Schadenshöhe in Dollar nach Schadenskategorie. Quelle: CSI/FBI-Untersuchung 2000. 2000: 42% = 273 Befragte

Ich teilte mit, welche finanziellen Schäden bis zu diesem Zeitpunkt an die CSI/FBI-Untersuchung berichtet worden waren, bot jedoch zusätzlich noch weitere Beweise an, um unsere Daten in ein Verhältnis zu stellen.

Ich ging die Nachrichten noch einmal durch, die ich zwei Jahre lang – von November 1997 bis November 1999 – in der Publikation *Computer Security Alert* in der Rubrik »In Case You Missed It« veröffentlicht hatte. Dabei hielt ich nach Meldungen Ausschau, die finanzielle Schäden durch Cyber-Attacken und andere Verletzungen der Datensicherheit in Dollarbeträgen bezifferten.

Unter den mehreren hundert Meldungen fand ich elf Stück:

- Die so genannten Phonemasters waren in die Telefonnetze von AT&T, British Telecommunications, GTE, MCI, Southwestern Bell und Sprint eingedrungen. (In Kapitel 7 können Sie eine Fallstudie über die Phonemasters lesen.) Ihre Kunden waren unter anderem Privatdetektive, so genannte Informationsbroker, und – über Mittelsmänner – die sizilianische Mafia. Nach Auskunft des FBI verursachten sie bei den genannten Unternehmen Verluste in Höhe von mindestens 1,85 Millionen Dollar.

- Die 26-jährige Nikita Rose wurde von einem Bundesgericht dafür verurteilt, dass sie in einen Computer des Salomon Brothers Investor Fund eingedrungen war und Aktionärsgelder in Höhe von 538 325 Dollar veruntreut hatte.
- Jay Satiro, ein 18-jähriger High-School-Abbrecher, wurde festgenommen, nachdem Mitarbeiter von AOL Anzeige erstattet hatten. Satiro wurde beschuldigt, Daten und Programme bei AOL beschädigt zu haben, deren Wiederherstellung 50 000 Dollar kosten würde.
- Einundfünfzig Menschen wurden verhaftet, weil sie in den Computer einer chinesischen Eisenbahngesellschaft eingedrungen waren. Sie hatten mehr als 8 000 Fahrscheine im Wert von 54 000 Dollar gefälscht, bevor sie entlarvt wurden.
- Zwillingsbrüder wurden von einem chinesischen Gericht zum Tode verurteilt, weil sie in das Computersystem einer Bank eingebrochen waren und 720 000 Yuan gestohlen hatten. Es war der erste Cyber-Bankraub in der Geschichte Chinas.
- Shakuntla Devi Singla, 43, war die erste Frau, die in den USA als Hacker überführt wurde. Sie wurde verurteilt, weil sie eine Personaldatenbank der amerikanischen Küstenwache zerstört hatte. 115 Mitarbeiter der Küstenwache benötigten mehr als 1 800 Arbeitsstunden, um die verlorengegangenen Daten wieder herzustellen. Die Aktion kostete 40 000 Dollar.
- Die Königlich Kanadische Berittene Polizei erklärte nach 14 Monate währenden Ermittlungen, dass ein Hacker in die Computersysteme des NASA-Zentrums, der Staatlichen Gesellschaft für Ozeanographie und Atmosphäre (NOAA, National Oceanographic and Atmospheric Association) und des Hughes STC eingebrochen sei. Eines der Opfer meldete, dass an Dateien ein Schaden von 50 000 Dollar entstanden sei.
- In China sitzt ein Hacker im Gefängnis, der beschuldigt wird, von seinem Arbeitgeber Informationen gestohlen und diese für 100 000 Yuan an die Konkurrenz verkauft zu haben.
- Ein verärgerter Programmierer namens Timothy Lloyd wurde angeklagt, aus Rache das Computersystem seines ehemaligen Arbeitgebers zerstört und damit einen Schaden von zehn Millionen Dollar verursacht zu haben. Lloyd hatte als Netzwerkprogrammierer bei der Firma Omega Engineering Corp. gearbeitet, die modernste Mess- und Regeltechnik für die US-Marine und die NASA herstellt.
- Kürzlich wurde einem Computertechniker zur Last gelegt, in die Computer des Verlags Forbes, Inc., bei dem die Zeitschrift *Forbes* erscheint, eingedrungen zu sein und einen Systemabsturz verursacht zu haben, der das Unternehmen mehr als 100 000 Dollar kostete.

- Vier High-School-Schüler im Alter zwischen 14 und 16 Jahren hackten sich in einen Internet-Server in der Bay Area hinein und veranstalteten dann mit den gestohlenen Kreditkartennummern eine gigantische Einkaufsorgie bei einem Online-Auktionshaus. Sie bestellten Computer im Wert von 200 000 Dollar und ließen diese von United Parcel an leer stehende Häuser in San Carlos liefern, wo sie die Pakete nach Schulschluss abholten.
- Tausende von Menschen, die astronomische Telefonrechnungen dafür erhielten, dass sie erotische Bilder auf ihre Computer heruntergeladen haben sollten, erhalten eine Entschädigung in Höhe von 2,4 Millionen Dollar von Gesellschaften, die die Anrufe dieser Opfer über das osteuropäische Land Moldavien umgeleitet hatten. Die amerikanische Handelskommission teilte mit, die Erstattungen seien Teil zweier Vereinbarungen, die sie mit Unternehmen und Privatleuten geschlossen habe, die eine nach ihrer Ansicht kostenlose Software benutzt hatten, um mehr als 38 000 Verbraucher mit teuren internationalen Telefonnummern zu verbinden. In Wirklichkeit wurden diese Leute über ihre Modems ausgeraubt.

Der Gesamtschaden aus diesen elf Vorfällen beläuft sich auf 15 452 025 Dollar.

Im selben Zeitraum gab es natürlich noch zwei weitere, äußerst kostspielige Verbrechen im Cyberspace, die mehr im Mittelpunkt des Interesses standen.

- Kevin Mitnicks Hacker-Orgie kostete die betroffenen Hightech-Unternehmen innerhalb von zwei Jahren mindestens 291,8 Millionen Dollar, bevor man ihn dingfest machen konnte. Dies besagen die Schätzungen, die NEC America, Nokia Mobile Phones, Sun Microsystems und Novell dem FBI zur Verfügung stellten. NEC beziffert den Wert der gestohlenen Software mit 1,8 Millionen Dollar, aber Nokia errechnet einen Verlust von mindestens 135 Millionen Dollar, einschließlich eines Schadens von 120 Millionen Dollar »auf Grund verzögerter Markteinführung neuer Entwicklungen«.
- David L. Smith, ein 31-jähriger Programmierer aus New Jersey, bekannte sich schuldig, den Computervirus Melissa erschaffen und über eine pornografische Website im Internet verbreitet zu haben, wo er schätzungsweise 80 Millionen Dollar Schaden anrichtete.

Wenn man den Gesamtschaden in Höhe von 15 452 025 Dollar aus den zuvor beschriebenen elf Vorfällen, 291,8 Millionen Dollar aus dem Mitnick-Fall und 80 Millionen Dollar aus dem Fall des Melissa-Virus zusammenrechnet, kommt man auf die ungeheure Summe von 387 252 025 Dollar. (Das bedeutet, dass 13 Fälle von Cyber-Kriminalität zu Verlusten von fast 400 Millionen Dollar geführt haben.)

Im Jahr 2000 meldeten die Befragten in der CSI/FBI-Untersuchung Schäden von insgesamt 265 589 940 Dollar.

Der kumulierte Gesamtbetrag der im Verlauf von vier Jahren an die CSI/FBI-Untersuchung gemeldeten Schäden beläuft sich auf 626 309 795 Dollar.

Und der Sinn dieser Übung?

Wenn Sie den Ergebnissen der CSI/FBI-Untersuchung die in den Medien dokumentierten 13 Fälle gegenüberstellen, erweitern Sie Ihren Blickwinkel: Die von CSI und FBI gemeldeten Daten über finanzielle Schäden sind recht konservativ geschätzt.

In Abbildung 4.3 sehen Sie eine Tabelle mit den kumulierten Schäden aus Computerverbrechen und Sicherheitsverletzungen über einen Zeitraum von 48 Monaten. Beachten Sie bitte, dass im Jahr 2000 zwar 74 Prozent der Befragten in der Untersuchung finanzielle Schäden einräumten, aber nur 42 Prozent der Befragten diese Schäden auch quantifizieren konnten.

Wie Geld verloren ging

	Befragte mit qualifizierten Verlusten				Niedrigste Angabe				Höchste Angabe				Durchschnittliche Verluste				Gesamtjahresverlust			
	'97	'98	'99	'00	'97	'98	'99	'00	'97	'98	'99	'00	'97	'98	'99	'00	'97	'98	'99	'00
Diebstahl proprietärer Informationen	21	20	23	22	$1K	$300	$1K	$1K	$10M	$25M	$25M	$25M	$954,666	$1,677,000	$1,847,652	$1,136,409	$20,048,000	$33,545,000	$42,496,000	$66,708,000
Daten- und Netzwerkspionage	14	25	27	28	$150	$400	$1K	$1K	$1M	$500K	$1M	$15M	$164K	$86K	$163,740	$535,750	$4,285,850	$2,142,000	$4,421,000	$27,148,000
Belauschen von Telefongesprächen	8	10	10	15	$1K	$1K	$1K	$200	$100K	$200K	$300K	$500K	$45,423	$56K	$76,500	$33,346	$1,181,000	$562,000	$765,000	$991,200
Systemeinbruch durch Außenseiter	22	19	28	29	$200	$500	$1K	$1K	$1.5M	$500K	$500K	$5M	$132,250	$86K	$103,142	$172,448	$2,911,700	$1,637,000	$2,885,000	$7,104,000
Missbrauch von Netzzugang durch Insider	55	67	81	91	$100	$500	$1K	$240	$100K	$1M	$3M	$15M	$18,304	$56K	$93,530	$164,837	$1,006,750	$3,720,000	$7,576,000	$27,984,740
Finanzbetrug	26	29	27	34	$5K	$1K	$10K	$500	$2M	$2M	$20M	$21M	$957,384	$388K	$1,470,592	$617,661	$24,892,000	$11,239,000	$39,706,000	$55,996,000
Denial of Service	n/a	36	28	46	n/a	$200	$1K	$1K	n/a	$1M	$1M	$5M	n/a	$77K	$116,250	$108,717	n/a	$2,787,000	$3,255,000	$8,247,500
Spoofen	4	n/a	n/a	n/a	$1K	n/a	n/a	n/a	$500K	n/a	n/a	n/a	$128K	n/a	n/a	n/a	$512,000	n/a	n/a	n/a
Virus	165	143	116	162	$100	$50	$1K	$100	$500K	$2M	$1M	$10M	$75,746	$55K	$45,465	$61,729	$12,498,150	$7,874,000	$5,274,000	$29,171,700
Unbefugter Insider-Zugriff	22	18	25	20	$100	$1K	$1K	$1K	$1.2M	$50M	$1M	$20M	$181,437	$2,809,000	$142,680	$1,000,050	$3,991,605	$50,565,000	$3,567,000	$22,554,500
Telekom-Betrug	35	32	29	19	$300	$500	$1K	$1K	$12M	$15M	$100K	$3M	$647,437	$539K	$26,655	$157,947	$22,660,300	$17,256,000	$773,000	$4,028,000
Aktives Abhören	n/a	5	1	1	n/a	$30K	$20K	$5M	n/a	$100K	$20K	$5M	n/a	$49K	$20K	$5M	n/a	$245,000	$20,000	$5,000,000
Diebstahl von Laptops	165	162	150	174	$1K	$1K	$1K	$500	$1M	$500K	$1M	$1.2M	$38,326	$32K	$86,920	$6,899	$6,132,200	$5,250,000	$13,038,000	$10,404,300
																Jährliche Verluste insgesamt:	$100,119,555	$136,822,000	$123,779,000	$265,586,240

Gesamtsumme der gemeldeten Verluste (1997-2000): 626,306,795 Dollar

Abbildung 4.3: Die Kosten der Computerkriminalität. Quelle: Institut für Computersicherheit, CSI/FBI-Untersuchung 2000.

Quantifizierung des wirtschaftlichen Schadens durch Datensicherheitsverletzung

Es gibt kein Patentrezept zur Quantifizierung der finanziellen Schäden auf Grund von Sicherheitsverletzungen. In vielen Fällen berücksichtigen die gemeldeten Schäden nicht die gesamte Tragweite des Vorfalls. Es existiert einfach keine klar umrissene Möglichkeit, die Kosten dieser üblen Taten aufzuschlüsseln – jedenfalls bisher.

Um etwas zur Entwicklung einer solchen Methodik beizutragen, habe ich kürzlich mehreren Kennern der Materie einige Bemerkungen entlockt.

Sie kennen den Schaden nur, wenn Sie den Wert der Ressource kennen

Chris Grillo von der Firma Minnesota Power and Light (Duluth, Minnesota), beschreibt die Grundlagen.

»Ehe wir die Kosten beziffern können, müssen wir zuerst den Wert jeder gegebenen, computergebundenen Ressource sowie den Wert der Daten selbst identifizieren. Möglicherweise wurden diese Werte bereits zu einem großen Teil bei Katastrophenszenarios oder Umstellungen auf das Jahr 2000 festgestellt.«

Laut Grillo sehen viele Unternehmen leider keine Ressourcen für die Feststellung und Bewertung der Gesamtkosten auf dieser Ebene vor. »Manche denken vielleicht, man könne bestimmte IT-Ressourcen nicht messen. Ich hingegen bin der Ansicht, was man beobachten kann, kann man auch zählen, und was man zählen kann, kann man auch messen.«

Er fügt hinzu, dass die Frage der Quantifizierung von finanziellen Schäden durch Sicherheitsverletzungen jedweden an einer computergebundenen Ressource entstandenen Schaden berücksichtigen muss, der die Erträge oder Aufwendungen eines Unternehmens beeinflusst, auch den Verlust durch die auf Grund verlorengegangener Arbeitseffizienz gestiegenen Kosten und den Verlust durch die Unmöglichkeit, Ressourcen anderswo einzusetzen (d.h. Opportunitätskosten).

»Sie können dies sogar auf die immateriellen Schäden z.B. in der Kundenbetreuung oder am Image der Firma ausdehnen (wenn beispielsweise Kunden irgendeine Form der Kommunikation oder E-Commerce-Transaktionen nicht mehr durchführen können, eine Webseite entstellt ist usw.« Auch solche Ereignisse beeinflussen in irgendeiner Form den Aufwand und Ertrag.

»Um die Kosten zu schätzen«, so Grillo weiter, »würde ich mir die gesamten Eigentumskosten meiner Ressourcen ansehen. Da wir das für die Buchhaltung ohnehin tun: Warum nicht für die verschiedenen Konten ein Diagramm der Gesamteigentumskosten erstellen? Man könnte die Kosten auf viele Arten kategorisieren.«

Grillo schlägt vor, die verschiedenen Kostenarten in vier Kategorien einzuteilen:

- Kapitalkosten wie z.B. für Hardware, Software, Netzwerke, Server, Schaltungen.
- Verwaltungskosten, z.B. für die Verwaltung der Vermögenswerte, die Sicherheitsüberwachung und -nachverfolgung, Kosten der Rechtsberatung und der Revisionsabteilung.
- Kosten für den technischen Support, wenn z.B. alle Welt bei der Hotline anruft; Kosten der Dokumentation dieser Anrufe, der Benutzerschulung usw.
- Betriebliche Kosten bei den Benutzern, wie z.B. für die Verwaltung der Benutzerdaten oder der Ressourcen, in die eingebrochen wurde; Kosten für die Förderung des Problembewusstseins auf Seiten der Benutzer.

Zwar gibt es viele Möglichkeiten, die Kosten zu betrachten, um sie zu beziffern, aber Sie können sie auch auf naheliegendere Weise bestimmen, indem Sie z.B. einfach Ihren Kunden fragen oder in diese Gleichung auch das Konzept des Risikos miteinbeziehen. So könnten Sie z.B. den Eigentümer eines Gegenstands fragen, wie viel Sie ihm für diesen Gegenstand bezahlen müssten. Damit hätten Sie zumindest einen Ausgangspunkt für die »Verhandlung«, in welcher Höhe Sie den betreffenden Gegenstand versichern müssten. (Gehört Ihnen z.B. ein Kunstwerk, so versichern Sie möglicherweise nicht den gesamten Wiederbeschaffungswert. Sie wählen eventuell stattdessen eine niedrigere Zahl, um im Falle eines Diebstahls wenigstens einen Großteil der Kosten gedeckt zu haben. Immerhin müssten Sie sich dann nicht so grämen wie bei einem Totalverlust.) Darüber hinaus können Sie die Wahrscheinlichkeit eines solchen Vorfalls bewerten und dann entscheiden, wie viel Sie für den Schutz des betreffenden Gegenstands ausgeben sollten.

Grillo führt als Beispiel ein Handelsgeheimnis an:

»Für welchen Betrag würden Sie zum jetzigen Zeitpunkt dieses Handelsgeheimnis verkaufen? Eine Milliarde Dollar. Wie groß ist die Wahrscheinlichkeit, dass das Handelsgeheimnis zur Entwicklung eines marktfähigen Produkts eingesetzt würde? 75 Prozent. Somit hätten Sie einen (bereinigten) Marktwert von 750 Millionen.«

Dann gibt er ein weiteres Beispiel mit einem eher materiellen Vermögenswert.

»Wie viel würde es kosten, den Server und die darauf gespeicherten Daten zu ersetzen? 150 000 Dollar. Wie groß ist die Gefahr einer Sicherheitslücke, die diesen Server vollständig zerstört? 10 Prozent. Was sollte ich also für die Versicherung des Servers ausgeben? Zehn Prozent von 150 000 macht 15 000 Dollar. Wir wollen ihn also mit 15 000 Dollar bewerten und versichern und diese Kosten als Schadensanteil ansetzen.

Wenn Geschäftschancen verpasst werden oder wegen des Verlusts einer Computerressource Verzögerungen auftreten, die finanzielle Schäden bewirken, so würde ich die Auswirkungen der Verzögerung analysieren. Bei dieser Analyse würde ich

die geschätzten Verzögerungen jeweils mit ihren nach dem oben beschriebenen Verfahren berechneten Kosten in eine Beziehung setzen. Was würde es z.B. kosten, wenn unsere E-Commerce-Website einen Tag lang ausfällt? Oder eine Woche lang? Oder einen Monat?«

Einbruch in Systeme von außen

Ein Hacker kriecht tage- oder wochenlang durch Ihre Netzwerke, setzt Schnüffelprogramme ab, belegt Speicherplatz im Netz, benutzt Rechenleistung oder greift auf andere Organisationen zu und dergleichen mehr. Wie lassen sich die dadurch verursachten Verluste quantifizieren?

Markus Ranum von der Firma Network Flight Recorder (www.nfr.com) macht kurzen Prozess:

»Zuerst würde ich Kategorien für die Teilverluste einführen:

- Ausfallzeiten/verpasste Geschäftschancen/Geschäftstätigkeit
- Arbeitszeit (Gehälter)
- Berater (wenn welche eingesetzt werden)
- Kosten der Rechtsberatung (Stundensatz)

Eventuell kann es vernünftig sein, diese auf die einzelnen Phasen der Bereinigung umzulegen:

- Entdeckung
- Reaktion
- Reparatur
- Strafverfolgung

Sie könnten sagen: ›Wir haben 1 120 Dollar für Berater ausgegeben, die entdeckten, was der Hacker gemacht hat. Danach haben wir 2 200 Dollar für Berater gezahlt, die unseren Leuten geholfen haben, richtig zu reagieren und den Hacker zu ermitteln. Wir haben 3 000 Dollar darin investiert, das Betriebssystem auf unserer Firewall neu zu installieren. Dann haben wir 2 929 Dollar an Berater bezahlt, die unserem Anwalt geholfen haben, die Strafverfolgung des Hackers vorzubereiten.‹

Jede Ausgabenart lässt sich auf diese Phasen umlegen. Zum Beispiel: ›Wir hatten keine Rechtskosten bei der Entdeckung und Reaktion. Während der Reparatur schalteten wir Rechtsanwälte ein und erklärten ihnen die Lage; diese berechneten für ihre Arbeitsstunden 39 393 Dollar. Dann hatten wir bei der Vorbereitung der Strafverfolgung des Hackers noch Anwaltskosten in Höhe von 81 238 Dollar.‹

Hier lassen sich die Ausgaben ziemlich gleichmäßig umlegen auf die Phase, in der die Taten aufgedeckt wurden, und die Phase, in der der Schaden repariert wurde.

Zwar könnte man auch argumentieren, dass ein Teil der Ausgaben vom Opfer selbst zu tragen wären, da sie auch ohne den Hackerangriff wertvoll für die Infrastruktur seien (nach dem Motto: ›Das hätte ich ohnehin tun müssen.‹). Dann würde man allerdings am Ende sagen: ›Wir haben für 331 311 Dollar einen neuen Silo für die Backups gekauft.‹«

Unberechtigter Zugriff von innen

Welche Art von finanziellem Schaden würde entstehen, wenn ein Insider – vielleicht ein Angestellter oder im Hause arbeitender freier Mitarbeiter – auf schutzwürdige Daten (etwa Handelsgeheimnisse, Verkaufszahlen, Marketingpläne, Forschung & Entwicklung) über das Netzwerk zugriffe, diese Daten herunterladen und dann an den Wettbewerb verkaufen würde?

Laut Ranum ist dies »dasselbe Paradigma«. Auch hier stellt man den Vorfall fest (Entdekkung), ermittelt, was passiert ist (Reaktion), findet die Auswirkungen des Zugriffs auf die Geschäftstätigkeit heraus und installiert Gegenmaßnahmen (Reparatur) und leitet eventuell eine Strafverfolgung ein, was eine Menge Arbeit macht.

»Die meisten Ausgaben bei einem unbefugten Zugriff eines Insiders hängen davon ab, was dieser getan hat. Insiderangriffe wieder in Ordnung zu bringen, ist nicht schwer, da Insider nicht so viel Schaden ausrichten müssen, um die Informationen zu bekommen, die sie brauchen. Es ist auch weniger wahrscheinlich, dass sie Trojanische Pferde und solches Zeugs über das ganze Netzwerk verteilen.«

Daten- oder Netzwerksabotage

Welche finanziellen Verluste würden auftreten, wenn ein wichtiger Server oder ein Netzwerk von innen oder von außen zerstört würde?

Nach Ansicht von Ranum ist die Ausfallzeit der Hauptfaktor bei einer Sabotage. Zu ermitteln, wer es wie und wann getan hat, ist sekundär. »Wenn es keine Backups gibt, werden Sie wohl irgendwie versuchen, den Wert des Systems festzusetzen und die Daten darauf wiederherzustellen. (Wenn allerdings ein Opfer behaupten würde, das System sei zwar wichtig gewesen, aber es seien keine Backups gemacht worden, dann würde es mich schon sehr wundern, wenn dies vor Gericht nicht für Heiterkeit sorgen würde.)«

Bösartiger Code

Wie lässt sich ein ernster Befall mit dem Melissa-Virus quantifizieren? Wie würden Sie den Schaden überhaupt berechnen?

Ranum dazu: »Auch hier müssen Sie feststellen, welche Systeme infiziert sind, wie Sie sie reparieren und hinterher schützen können. Natürlich sollten die Kosten der Verhütung nicht zu den Schäden gerechnet werden. Ist ein Virus ausgebrochen, so müssen Sie die Kosten für die Wiederherstellung der Daten und die Ausfallzeiten

betrachten. Wenn allerdings Daten verlorengingen, kann es selbstverständlich viel teurer werden.«

Doch Ranum hat wenig Mitleid mit jenen, die größere Datenverluste beklagen.

»Das Opfer ist immer selbst schuld, wenn es Daten verliert. Wenn die Daten wichtig sind, sollten Sie davon genügend Kopien besitzen, um nur einen kleinen Teil Ihrer neuesten Arbeit einzubüßen.«

Unterschätzen Sie nicht die »weichen Kosten«

Keith Allan Rhodes vom U.S. General Accounting Office betont, wie wichtig es sei, die »weichen Kosten« nicht zu unterschätzen.

»Sie haben da eine tiefgreifende Frage aufgeworfen«, so Rhodes. »Denn diese Kostenanalyse ist es, auf der die Entscheidung basiert, ob die Sicherheitsanstrengungen der Mühe wert sind. Man kann für jeden der Fälle, die Sie erwähnten, eine grundlegende Personalkostenschätzung anstellen. Oberflächlich betrachtet sieht das ganz einfach aus, aber andererseits ist damit auch die Kostenschätzung noch sehr unvollkommen.

Nehmen wir z.B. an, Sie haben eine Website, ein Hacker dringt ein und Sie müssen die Site neu erstellen. Ganz einfach. Zehn Leute arbeiten einen Tag daran, um die Website wieder online zu bringen (das sind zehn Manntage Arbeit). Unter diesen zehn Mitarbeitern gibt es einen Manager, einen Systemadministrator, einen Webadministrator, einen Netzwerkingenieur, zwei Inhaltsspezialisten und noch vier andere. Stellen Sie deren Kosten fest und rechnen Sie sie zusammen. Mit dem Endergebnis haben Sie die direkten Personalkosten, die entstehen, um diese spezielle Website nach diesem speziellen Einbruch wieder ins Internet zu stellen. Die Schwierigkeit ist hier herauszufinden, wer für wie lange daran beteiligt war. Befand sich z.B. das gesamte Personal vor Ort oder waren auch Leute von der Firmenzentrale beteiligt?«

Rhodes fügt hinzu, dass in dieser Berechnung vieles noch nicht abgedeckt sei.

»In all unseren Szenarien (Außenstehende, Insider, Sabotage, bösartiger Code) sind immer auf irgendeiner Ebene Ermittlungen beteiligt. Die Kosten der Ermittlungen hängen davon ab, wie viel Energie Sie auf die Untersuchung verwenden, und ob die Leute und die Ressourcen, mit denen die Untersuchung vorgenommen wird, Ihre eigenen oder externe Mitarbeiter sind. Doch auch hier ist die Gleichung wieder klar: Wie viele Leute? Wie lange? Zu welchen Kosten?«

Rhodes mahnt, dass diese Kosten erst dann klar seien, wenn Sie über Ressourcen reden, die nur für dieses eine Ereignis eingesetzt werden. »Wenn die Ressourcen, mit denen Sie diesen Einbruch untersuchen, Teil eines ständigen Sicherheitsteams sind, dann müssen Sie die Personalkosten miteinbeziehen, die ein Datensicherheitsteam verursacht. Nun müssen Sie auch den Verwaltungsaufwand einrechnen, der mit einem ständigen Sicherheitsteam verbunden ist.«

Dann führt Rhodes aus, man dürfe die versteckten Kosten einer außerhalb der Firma stattfindenden Rechtsverfolgung nicht ignorieren. So waren z.B. im Falle des Melissa-Virus auf lokaler, staatlicher und bundesstaatlicher Ebene Ressourcen der Gerichtsbarkeit involviert.

Das Justizministerium der USA betreibt eine Website mit dem Titel »Costs of Crime«, Kosten der Kriminalität (*http://www.ojp.usdoj.gov/ovc/ncvrw/1999/cost.htm*), die entsprechende Statistiken zeigt. »So haben z.B. 1997 Raubüberfälle 0,5 Milliarden Dollar Schaden angerichtet, Brandstiftungen 7 Milliarden Dollar Schaden usw. Diese quantifizierbaren Kosten sind klar verständlich. Sie entsprechen unserer Erörterung, wie viel es kostet, eine Website wieder zum Laufen zu bringen.

Doch es sind die ›weichen‹ Kosten, die in Wahrheit die Bank sprengen. So verursachen z.B. Verbrechen an Personen jährlich schätzungsweise 105 Milliarden Dollar an Kosten für medizinische Versorgung, entgangene Einkünfte und öffentliche Hilfsprogramme für die Opfer. Wenn man dann noch den Schmerz, das Leid und den Verlust an Lebensqualität hinzurechnen würde, dann stiegen die Kosten auf schätzungsweise 450 Milliarden Dollar jährlich.

Es mag vielleicht trivial erscheinen, ist es aber nicht. Die durch Gewaltverbrechen entgangenen Löhne und Gehälter machen in den USA ein Prozent der Einkünfte, drei Prozent der Gesundheitsausgaben und 14 Prozent der medizinischen Versorgung von Verletzungen aus.«

Rhodes fährt fort, dass hier auch die Verluste in Höhe von 45 Milliarden Dollar jährlich einzurechnen seien, die den Versicherungen durch Verbrechen entstehen. (Das macht ungefähr 265 Dollar pro Kopf der erwachsenen Bevölkerung.) Die Regierung der USA zahlt jährlich 8 Milliarden Dollar für Nothilfe und Wiedereingliederung der Opfer plus vielleicht ein Viertel der 11 Milliarden Dollar Krankenversicherungsbeiträge.

»Die Statistik über Computerverbrechen muss solche ›weichen‹ Kosten berücksichtigen. Das heißt, dass die betroffenen Firmen oder anderen Organisationen auch den Wert dieser Faktoren verstehen müssen.

Ein Beispiel: Angenommen, Sie und ich sind Mitarbeiter bei der Firma P&R, Inc. Einer unserer ›vertrauenswürdigen‹ Sachbearbeiter für Geschäftspläne ist im Außendienst und steht in einer Telefonzelle, um seiner Frau eine Terminänderung mitzuteilen. Alles ist wunderbar, bis er sich umdreht und plötzlich die leere Stelle sieht, wo eben noch seine Aktentasche mit dem Laptop gestanden hat.

Also beginnen wir, einen Zeitraum zu rekonstruieren. Angenommen, der Mitarbeiter hat einen Fünf-Jahres-Geschäftsplan für ein Unternehmen geschrieben. Der Plan und alle Backup-Daten befinden sich auf dem Laptop, den er dabei hatte. Wie wollen Sie die Kosten beziffern, um diesen verlorengegangenen Geschäftsplan wiederherzustellen? Wie hoch setzen Sie den Schaden an, wenn er in die Hände der Konkurrenz fällt?

Hinzu kommt: Wenn in allen von Ihnen erwähnten Szenarien die Organisation wirklich versucht, den Übeltäter erfolgreich zu belangen, dann wird auch die gerichtliche Auseinandersetzung wahrscheinlich zeitaufwändig und kostspielig – vor allem, wenn die Strafverfolgung bei einem firmeninternen Missbrauchsszenario vorgesehen ist.

Ein anderes Beispiel: Angenommen, eine Person benutzt das Firmen-Intranet für sexuelle Belästigung oder Kinderpornographie. Jetzt reden wir über eine Strafverfolgung, die Ihre Firma oder Sie selbst als deren Chef betrifft. Vergessen Sie nicht: Wenn Sie leitender Mitarbeiter der Firma sind und Ihr Unternehmen etwas Illegales tut, dann kann man Sie sowohl strafrechtlich als auch zivilrechtlich für diese Handlungen belangen.«

Wenn wir Verluste beziffern können, können wir auch den ROI berechnen

Laut Keith Allan Rhodes hat es noch einen weiteren Vorteil, wenn man in der Lage ist, finanzielle Schäden durch solche Sicherheitsverletzungen zu beziffern.

»Was wir letztlich versuchen, ist, den Return on Investment (ROI) herauszufinden, den ein Sicherheitsteam oder ein anderer, von der Firma gewählter Sicherheitsapparat bedeutet. Ist es sein Geld wert? Was ist, wenn keine Gefängnisstrafe verhängt wird? Ist es denn der Mühe wert, wenn meine Website nach wie vor von Hackern belagert wird? Ist das nicht einfach nur der Preis, den man zahlt, um seine Geschäfte abzuwickeln? Ein Risiko, das man bei allen Geschäftsentscheidungen zu tragen hat? Dies ist ein Aspekt geschäftlicher Entscheidungen, mit dem sich nur die wenigsten Unternehmen auseinander setzen.

Wenn man Geschäfte machen will, ist Sicherheit der Preis. Wie sicher Sie letztlich sind, hängt davon ab, welches Unternehmerrisiko Sie zu tragen bereit sind.

Wir wissen z.B. alle, dass bei Mobilfunkdiensten Betrug an der Tagesordnung ist. (Wenn Sie es nicht schaffen, ein Handy auszuplündern, sollten Sie das Plündern besser ganz bleiben lassen.)

Wenn Sie bis drei zählen können, können Sie auch in ein Handy einbrechen. Dennoch boomen die Mobilfunkdienste in einem Maße, das zu dem Risiko offenbar in überhaupt keinem Verhältnis steht. Zum Teil liegt das daran, dass die Anbieter drahtloser Dienste ihre Verluste unmittelbar ins Nirwana abschreiben können, wo niemand einen Zusammenhang zwischen den hohen Telefongebühren und dem Telefonbetrug erkennt.

Bloß weil Ihre Telefongesellschaft so ›nett‹ war, die Kosten der unbefugten Nutzung von Ihrer Telefonrechnung abzuziehen, bedeutet das noch lange nicht, dass Sie nicht dafür bezahlen.«

Hacker, Cracker, Virenschreiber

5.
Kapitel

Begannen die Neunzigerjahre mit einer einzigen großen Lüge?

Attacken im Web konzentriert sich auf eine Anzahl Ereignisse, die Mitte der Neunzigerjahre ihren Anfang nahmen. Die historischen Ereignisse und Persönlichkeiten, von denen dieses Kapitel handelt, bezeichne ich als »Vorgeschichte«. Mit dieser Vorgeschichte meine ich die Jahre vor der Kommerzialisierung des Internets, vor der ungehemmten Verbreitung des World Wide Web und vor dem Heraufdämmern des E-Commerce-Zeitalters.

Diese »vorgeschichtlichen« Themen sind Gegenstand dieses Kapitels: die Hintergründe des mysteriösen Zusammenbruchs des Telefonnetzes am Martin Luther King-Tag 1990, eine kurze Chronik des langen, wilden Treibens von »Superhacker« Kevin Mitnick und der folgenschwere Morris-Virus im Jahr 1988. Es gab natürlich zwischen 1980 und dem Anfang der Neunzigerjahre auch noch andere Verbrechen im Cyberspace. Diese sind jedoch an anderer Stelle gut dokumentiert.

Zu allen drei hier dargestellten Vorfällen gehören Lektionen, die gelernt wurden, und Lektionen, die nicht gelernt wurden.

Der erste ernsthafte Angriff auf eine Infrastruktur?

Am 15. Januar 1990, dem Martin-Luther-King-Feiertag in den USA, brach das AT&T-Telefonnetz für Ferngespräche zusammen, was landesweite Auswirkungen auf die Telefondienste hatte. Dieser Zustand dauerte neun lange Stunden und hatte zur Folge, dass rund 70 Millionen Anrufe nicht getätigt werden konnten. Sicherheitsexperten der Telefongesellschaften und Beamte der Strafverfolgungsbehörden nahmen an, Hacker aus dem Untergrund hätten das System zum Absturz gebracht, doch eine Anklage wurde nie erhoben. Die offiziellen Verlautbarungen beharrten darauf, der Systemzusammenbruch sei Folge eines Softwareproblems gewesen.

Angespornt durch diesen Vorfall bündelten Strafverfolgungsbehörden im ganzen Land ihre Anstrengungen, um »hart gegen Hacker vorzugehen«. Der amerikanische Geheimdienst, das Sonderdezernat der Polizei in Chicago und die Abteilung für Organisiertes Verbrechen und Erpressung im Staat Arizona (Deckname: Operation Sundevil) durchsuchten Hackerwohnungen zwischen Texas und New York. Legendäre »Cyberpunks« aus zwei berüchtigten Hacker-Gangs, der Legion of Doom (LOD) und der Masters of Deception (MOD), wurden festgenommen.

Bruce Sterling berichtet in seinem Artikel *Hacker Crackdown* von den Ereignissen rund um die Zerschlagung von LOD und MOD (siehe Anhang C).

Der folgende Bericht einer absolut zuverlässigen, aber anonymen Person beleuchtet einige zuvor unveröffentlichte Aspekte der Ermittlungen im Fall des Telefonsystem-Absturzes am Martin-Luther-King-Tag.

Ich habe sowohl die Namen der beiden erwähnten Hacker als auch die Hinweise auf den speziellen, in diesem Fall involvierten Zweig des Militärs weggelassen.

Es gab da einen Knaben von der LOD, den sie in New York geschnappt haben. Seine Hacker-Namen waren [redacted] und [redacted].

Er wurde von der örtlichen Telefongesellschaft NYNEX erwischt. Die Polizei und der Richter jagten ihm eine fürchterliche Angst ein und sagten ihm, er müsse entweder ins Gefängnis oder zum Militär. So kam er zur Einheit der amerikanischen [redacted].

Später erhielt ein Militärermittler einen Anruf von jemandem, der in diesem Falle ermittelt hatte und in der Sicherheitsabteilung von NYNEX arbeitete. Der Anrufer sagte: »Sie kennen mich zwar, aber der Tipp, den ich Ihnen gebe, ist anonym. Sie haben ein Problem. Der Mann heißt [redacted] und absolviert gerade die Grundausbildung.«

Der Militärermittler begann mit Erkundigungen bei Stubenkameraden usw. Bei den Streitkräften können Sie testen, welchen Karriereweg Sie einschlagen sollten. Der Betreffende wollte mit Computern arbeiten und machte seine Tests so gut, dass er nicht zur Ausbildungseinrichtung zu gehen brauchte.

Er konnte direkt seinen Posten antreten. Er sagte dem Informanten, er wolle in das Hauptquartier der [redacted]. Er könne es »gar nicht erwarten, diese Computer aufzumischen«.

Die Ermittler schickten ihn auf einen anderen Posten auf einer [redacted]-Basis in Florida zur »Kampfkommunikation«. Das bedeutete, dass er in Zelten schlafen musste usw.

Ein auf dieser Basis stationierter Informant der Ermittler teilte mit, der Betreffende würde im Tageszimmer der Baracken Telefonate verkaufen.

Wenn man einen Anruf tätigen wollte, ging man zu [redacted], der die Verbindung herstellte und einen stundenlang kostenlos Ferngespräche führen ließ.

Nun begannen die Ermittler, mit dem amerikanischen Geheimdienst und dem Staatsanwalt von [redacted], Florida, zusammenzuarbeiten.

Sie erhielten einen Anruf folgenden Inhalts: »Wir möchten Ihnen einen Tipp geben. Wir wissen, dass Sie in dieser Sache ermitteln und einen Durchsuchungsbefehl erwirken wollen. Es geht das Gerücht, nächste Woche sei eine große Sache geplant, aber wir wissen nicht, worum es sich handelt. Sie sollten die Hausdurchsuchung am besten Anfang nächster Woche durchführen.«

So planten die Militärermittler die Durchsuchung für den Mittwoch. Doch am Montag ging AT&T kaputt. Auf einmmal interessierte sich jeder für sie.

BellSouth, AT&T, Bell Labs und andere Gesellschaften kamen. Die Militärermittler hatten nun jede Menge technische Berater, um diesen Durchsuchungsbefehl für diese kleine Baracke eines Teenagers auszuführen. Sie bekamen seinen Apple IIC und ein Modem mit 300 Baud Übertragungsrate. Sie gingen seine Notizbücher durch. Die Leute von BellSouth und Bellcore warfen einen Blick darauf

und sagten: »Mein Gott, das ist der Befehl, dieser Befehl ist es, der das System abstürzen ließ. Dieser Bengel hatte Zugriff.«

Ein Mitarbeiter einer der Telefongesellschaften ging aus dem Zimmer nach draußen zu den Telefonen und rief seine Vorgesetzten an.

Einer der Ermittler folgte ihm und hörte, was dieser am Telefon sagte: »Ich weiß nicht, ob der Junge es wirklich getan hat, aber er hatte den Zugriff und er hatte auch den Computerbefehl.«

Bei der Vernehmung sagte der Junge, er habe für eine Prüfung in Wahrscheinlichkeitsrechnung gelernt und der Hacker [redacted] habe ihn etwa 15 Minuten nach dem Systemzusammenbruch bei AT&T angerufen, nur gesagt »Wir haben sie!« und wieder eingehängt.

Niemand wurde je für den Systemzusammenbruch am Martin-Luther-King-Tag vor Gericht gestellt. AT&T beharrt darauf, dass es sich um ein »Softwareproblem« gehandelt habe. Dies ist die offizielle Version der Geschichte. Auch Sterling hat in seinem ansonsten herausragenden Buch diese Sprachregelung übernommen.

Begannen die Neunzigerjahre mit einer einzigen, großen Lüge? Wollte AT&T durch Einräumen eines »Fehlers« nur seine Verwundbarkeit übertünchen, die es aus Sicherheitsgründen nicht zugeben konnte? War der Zusammenbruch des AT&T-Telefonnetzes an jenem Feiertag wirklich der erste Hackerangriff, der eine Infrastruktur zum Ziel hatte?

Vielleicht werden wir dies nie mit Gewissheit erfahren. Ich neige dazu, der Geschichte meines anonymen Informanten Glauben zu schenken.

Cyber-Staatsfeind Nr. 1?

Kevin Mitnick (Deckname Condor) ist der legendärste Kriminelle in der noch jungen Geschichte des Cyberspace. Seine Story umfasst bereits drei Jahrzehnte und ist noch nicht zu Ende.

Im Jahr 1981 wurde Kevin Mitnick, 17 Jahre, zu einer Bewährungsstrafe verurteilt, weil er aus einer Schaltzentrale von Pacific Bell Computerhandbücher gestohlen hatte.

1982 wurde Mitnick landesweit berühmt, weil er in den Computer der nordamerikanischen Flugabwehr eingedrungen war. Zeitweise erlangte er auch die Kontrolle über drei Zentralstellen einer Telefongesellschaft in Manhattan und Zugriff auf sämtliche Telefonzentralen in Kalifornien. Das Telefon eines Opfers programmierte er so um, dass dieses immer, wenn es den Hörer abnahm, gebeten wurde, eine Münze einzuwerfen.

Im Jahre 1988 überwachte der mittlerweile 25-Jährige heimlich den E-Mail-Verkehr der Sicherheitsexperten von MCI und Digital Equipment. Digital Equipment beschuldigte ihn, dem Computersystem einen Schaden von 4 Millionen Dollar

zugefügt und Software im Wert von einer Million Dollar gestohlen zu haben. Mitnick wurde verurteilt und zu einer Haftstrafe von einem Jahr im Gefängnis von Lompoc, Kalifornien, verurteilt.

Im Jahr 1993 erließ die Polizei von Kalifornien Haftbefehl gegen Kevin Mitnick. Er wurde beschuldigt, Telefonate zwischen dem FBI und der kalifornischen Kraftfahrzeugzulassungsbehörde abgehört und die dabei gesammelten Codes der Strafverfolgungsbehörden missbraucht zu haben, um illegal in die Führerscheindatenbank einzudringen.

Am ersten Weihnachtstag im Jahr 1994 brach Kevin Mitnick, mittlerweile 31, in das System von Tsutomu Shimomura im Zentrum für Supercomputer der Stadt San Diego ein. Daraufhin verfolgte Shimomura den Hacker Mitnick so lange im Cyberspace, bis er im Januar 1995 festgenommen werden konnte.

Im Jahr 1996 bekannte sich Kevin Mitnick vor einem Gericht in Los Angeles schuldig im Sinne der Anklage der betrügerischen Verwendung von Handys und gab zu, gegen die Bewährungsauflagen einer vorherigen Verurteilung wegen Computerbetrugs verstoßen zu haben.

1997 wurde Mitnick zu knapp zwei Jahren Freiheitsentzug verurteilt, weil er gegen Bewährungsauflagen verstoßen und sich mit gestohlenen Mobilfunk-Telefonnummern in Computerdatenbanken eingewählt hatte. Die Anklage umfasste 25 Fälle von Computer- und Telefonbetrug, den Besitz rechtswidriger Zugangsgeräte, die Beschädigung von Computern sowie das Abfangen von elektronischen Nachrichten in einem weiteren Fall.

Dann drangen Hacker in Yahoo! – die meistbesuchte Website im Internet – ein und verschickten einen verhängnisvollen Urlaubsgruß. Eine Gruppe, die sich selbst als PANTS/HAGIS-Allianz bezeichnete, behauptete, einen Computervirus eingeschleust zu haben, der am ersten Weihnachtstag umfangreichen Schaden anrichten würde, wenn Mitnick nicht freigelassen würde.

Im Dezember 1998 berichtete das Szenemagazin *Wired*, Mitnick hätte gesagt, auch ein dreimonatiger Prozessaufschub gäbe seinem Verteidiger nicht genug Zeit, die Anklageschrift zu prüfen. In einem seiner wenigen telefonischen Interviews erklärte Mitnick: »Ich glaube nicht, dass wir bis zum 20. April fertig sein können. Ich hasse es, hier im Knast zu sitzen, vor allem ohne Kautionsanhörung.«

Im März 1999 gab Mitnick zu, den Firmen, in deren Computer er eingebrochen war, Millionen Dollar Schaden verursacht zu haben, und bekannte sich vor dem US-Distriktgericht in fünf Verbrechen für schuldig. Seit seiner Verhaftung 1995 in North Carolina hatte Mitnick im Gefängnis gesessen. Zwar wurde er zu drei Jahren und zehn Monaten Haft verurteilt, aber die Untersuchungshaft wurde ihm angerechnet.

Am 21. Januar 2000 wurde er nach 1 792 Tagen (fast fünf Jahren) im Gefängis auf freien Fuß gesetzt.

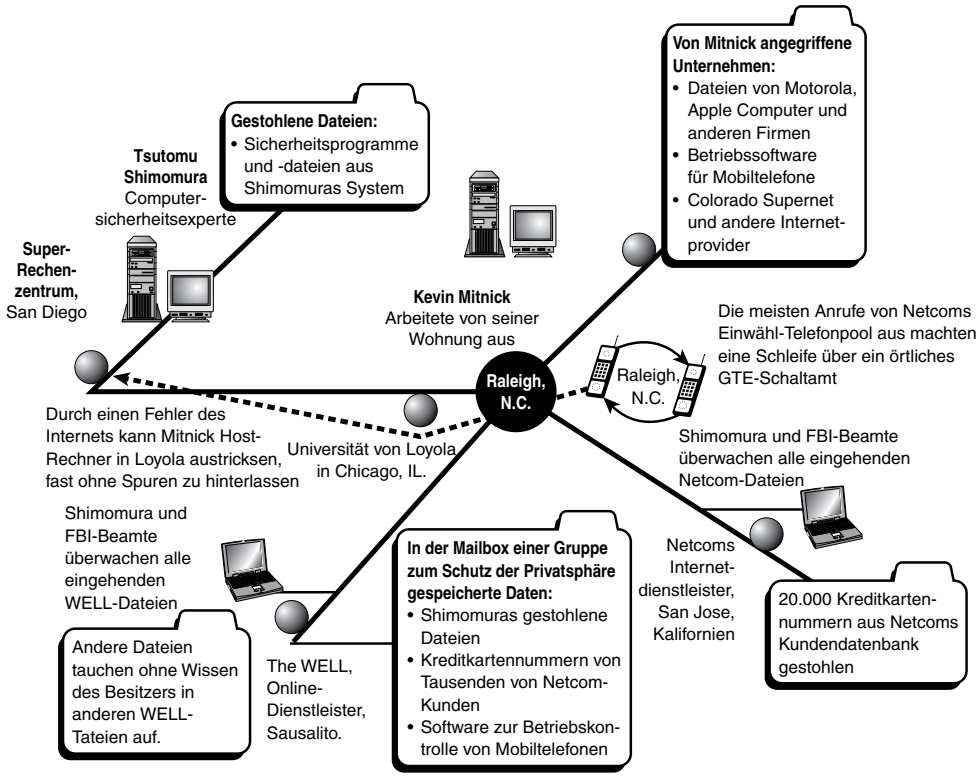

Abbildung 5.1: Mitnicks letzte Verbrechensserie. Quelle: San Francisco Chronicle.

Im April 2000 strich ein Bundesrichter Mitnick von der Teilnehmerliste einer Konferenz über Computersicherheit, die die Vereinigung für Informationstechnologie in Utah unter dem Thema »Netztrends 2000: Die digitale Revolution« veranstaltete. Die Auflagen für Mitnicks Haftentlassung verboten es ihm, als »Consultant oder Berater« für irgendwelche Computerangelegenheiten zu fungieren. Bis zum 20. Januar 2003 bleibt er unter »Aufsicht«.

Laut Staatsanwaltschaft hat Mitnicks Hackerorgie die Hightech-Unternehmen in den zwei Jahren vor seiner Verhaftung mindestens 291,8 Millionen Dollar gekostet (siehe Kapitel 3).

In den Medien und vor Gericht wurde Mitnick von vielen als Cyber-Staatsfeind Nummer eins präsentiert. Im Hacker-Untergrund und der Sympathisantenszene sah man ihn hingegen als Opfer und Fall für die Menschenrechtsorganisationen. Die Wahrheit liegt natürlich wie immer irgendwo dazwischen.

Mehr Einzelheiten zum Mitnick-Fall können Sie den folgenden drei Büchern entnehmen (siehe auch Anhang C):

- *Cyberpunk: Outlaws and Hackers on the Computer Frontier* von Katie Hafner und John Markoff

- *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw—By the Man Who Did It* von Tsutomu Shimomura und John Markoff
- *The Fugitive Game: Online with Kevin Mitnick* von Jonathan Littman

Würmer kommen, Würmer gehen

Im Jahr 1988 schrieb Robert Tappan Morris jr, ein 23-jähriger Diplomand der Informatik aus Cornell und Sohn eines Sicherheitsexperten der NSA (National Security Agency) ein experimentelles, selbst replizierendes und selbst verbreitendes Programm, einen so genannten Wurm, mit einem Umfang von 99 Codezeilen (Objektdateien nicht mitgerechnet), und brachte es in das Internet. Er entschied sich, es vom MIT aus abzusetzen, um die wahre Herkunft aus Cornell zu vertuschen.

Bald entdeckte Morris, dass sich das Programm weitaus scheller, als er gedacht hatte, replizierte und neue Rechner befiel: Es hatte einen Fehler. Am Ende stürzten viele Rechner an etlichen Standorten im ganzen Land entweder ab oder wurden »katatonisch«. Unsichtbare Tasks überlasteten VAX- und Sun-Maschinen im ganzen Land und sorgten dafür, dass die Benutzer diese Rechner wenn überhaupt nur eingeschränkt nutzen konnten. Zum Schluss waren die Systemadministratoren gezwungen, viele ihrer Rechner komplett offline zu nehmen, um die Infektionsquelle auszuschalten.

Als Morris begriff, was geschah, setzte er sich mit einem Freund in Harvard in Verbindung, um eine Lösung zu finden. Schließlich sendeten die beiden von Harvard eine anonyme Nachricht über das Netzwerk, in der sie den Programmierern Anweisungen gaben, wie der Wurm zu vernichten und eine Neuinfektion zu vermeiden sei. Da jedoch das Netz zu überlastet war, drang diese Nachricht erst durch, als es bereits zu spät war. Computer an vielen Standorten, darunter Universitäten, Militärbasen und medizinische Forschungseinrichtungen, wurden befallen. Die geschätzten Folgekosten des Wurms für jede dieser Installationen rangierten zwischen 200 und mehr als 53 000 Dollar.

Der Hauptunterschied zwischen Würmern und so genannten Viren ist die Art, wie sich das Programm reproduziert und verbreitet. Wenn ein normaler Computervirus in ein System eindringt, ändert er eine Systemdatei oder irgendeine andere, passende Datei, die aller Voraussicht nach in naher Zukunft benutzt werden wird. Die Änderung an dieser Datei besteht normalerweise in der Hinzufügung von Befehlen, die den Virus – wo auch immer er sich auf dem Computer befinden mag – aktivieren. Dann nimmt der Virus seine unheilvolle Arbeit auf. Der wesentliche Unterschied zu Würmern ist hier, dass der Virus so lange im Computer schlummert, bis der Benutzer ihn aktiviert. Ja mehr noch: Bevor nicht die geänderte Datei aufgerufen wird, kann der Virus keinerlei Aktivität entfalten.

Dagegen ist ein Wurm weitaus mächtiger. Wenn ein Wurm Zugriff auf einen Computer bekommt (normalerweise, indem er über das Internet eindringt), setzt er ein Programm ab, das nach anderen Internetadressen sucht und diese wenn mög-

lich infiziert. Da der Wurm zu keinem Zeitpunkt die (unfreiwillige oder freiwillige) Unterstützung eines Benutzers benötigt, besteht für alle mit der infizierten Maschine verbundenen Computer Infektionsgefahr. Wenn man die Konnektivität des Internets als Ganzes betrachtet, dann sind ungeheuer viele Computer bedroht, deren einzige Verteidigung darin besteht, alle Sicherheitslücken zu verschließen, über die der Wurm eindringen kann. Zweitens kann sich ein Wurm ohne jede Hilfe verbreiten. Hat er erst eine Internetverbindung erkannt, so braucht er nur noch eine Kopie seiner selbst auf die betreffende Adresse herunterzuladen und ganz normal weiterzulaufen.

Der Morris-Wurm benutzte Sicherheitslöcher in zwei Unix-Programmen: Sendmail und Finger. Angestellte der California University in Berkeley und des MIT hatten Kopien des Programms und waren eifrig beschäftigt, es zu zerlegen, um seine Arbeitsweise herauszufinden.

Programmierteams arbeiteten rund um die Uhr, um wenigstens eine provisorische Gegenmaßnahme zu finden und die weiterhin ungehemmte Verbreitung des Wurms zu unterbinden. Nach etwa 12 Stunden hatte das Team von Berkeley Schritte ersonnen, die die Verbreitung des Wurms verzögern würden. Ein Team von der Purdue University erfand noch ein anderes Verfahren und veröffentlichte es überall. Doch diese Informationen hätten noch schneller herauskommen können, wenn nicht so viele Standorte ihre Internetverbindung vollständig getrennt hätten.

Nach ein paar Tagen begannen sich die Dinge zu normalisieren und jeder wollte wissen, wer das eigentlich alles angerichtet hatte. Die *New York Times* nannte später Morris als Autor. (Obwohl dies offiziell noch nicht bewiesen war, deutete alles auf Morris als Täter hin.)

Was der Morris-Wurm in den Systemen anrichtete

Der Wurm hatte keine Dateien verändert oder zerstört, keine von ihm geknackten Passwörter gespeichert oder übermittelt und keine besonderen Versuche unternommen, Root- oder Administrator-Zugriff auf ein System zu erhalten. (Wenn er diesen Zugriff erhielt, machte er von seinen Rechten keinen Gebrauch.) Er legte keine Kopien seiner selbst oder anderer Programme in den Arbeitsspeicher, damit sie später ausgeführt werden sollten. (Programme, die dies tun, nennt man *Zeitbomben*.) Der Wurm befiel ausschließlich Sun-3-Systeme und VAX-Computer unter 4-BSD-Unix (oder Äquivalent) oder aber Rechner ohne Verbindungen zum Internet. (Mit anderen Worten: Computer ohne Internetadresse wurden nicht befallen. Modems zählen in dieser Hinsicht nicht als Internetverbindungen.) Der Wurm reiste nicht über die Festplatte von Rechner zu Rechner und verursachte keinen physikalischen Schaden an Computersystemen.

Eigentlich war der Sinn des Wurms (nach dekompilierten Versionen seines Codes und den Aussagen seiner Designer zu urteilen), überhaupt nichts zu machen. Zumindest nichts Sichtbares. Er war dazu geschaffen, einfach nur möglichst viele

Computer zu befallen, ohne auch nur den kleinsten Hinweis auf seine Existenz zu geben. Wäre der Code korrekt gelaufen, so wäre es nur ein winziger Prozess gewesen, der andauernd auf Computern im gesamten Internet gelaufen wäre.

Aber der Code arbeitete nicht perfekt. Offenbar enthielt er zu dem Zeitpunkt, als der Wurm abgesetzt wurde, immer noch etliche Fehler. Experten glauben darüber hinaus, dass der Programmierer unterschätzt hatte, mit welcher Geschwindigkeit sich der Wurm ausbreiten würde.

Das Ergebnis ist, dass diese scheinbar harmlosen Prozesse, die einzeln für sich genommen nur wenig Prozessorzeit benötigten, die Systeme in dem Maße immer mehr belasteten, wie mehr und mehr dieser Prozesse dieselben Rechner infizierten. Die befallene Maschine verlangsamte ihre Arbeit rapide, wenn immer mehr Kopien des Wurms ihre jeweilige Funktion ausführten.

Im nachfolgenden Beispiel können Sie die Auswirkungen des Würmerbefalls sehen. Die folgende Tabelle ist für sämtliche Infektionen im ganzen Land repräsentativ.

Tagebuch eines Wurmbefalls auf einem einzelnen System. Alle Ereignisse traten am Abend des 2. November 1988 ein[1].

Zeitpunkt	Ereignis
18:00 Uhr	Ungefähr zu diesem Zeitpunkt wurde der Wurm abgesetzt.
20:49 Uhr	Der Wurm infiziert eine VAX 8600 an der University of Utah (cs.utah.edu).
21:09 Uhr	Der Wurm startet von der infizierten VAX aus den ersten Angriff auf andere Computer.
21:21 Uhr	Die Durchschnittslast auf dem System erreicht den Wert 5. (Die Durchschnittslast ist ein Maß dafür, wie hart der Computer arbeitet. Normalerweise war die Last auf dieser VAX um 21:21 abends immer 1. Jede Last, die höher als 5 ist, führt zu verzögerter Datenverarbeitung.)
21:41 Uhr	Die Durchschnittslast erreicht den Wert 7.
22:01 Uhr	Die Durchschnittslast erreicht den Wert 16.
22:06 Uhr	Nun haben so viele Würmer das System befallen, dass kein neuer Prozess gestartet werden kann. Das System ist jetzt nicht mehr benutzbar.
22:20 Uhr	Der Systemadministrator löscht die Würmer.
22:41 Uhr	Das System wird erneut infiziert; die Durchschnittslast wächst bis auf 27 an.
22:49 Uhr	Der Systemadministrator fährt das System herunter. Es wird danach neu gestartet.
23:21 Uhr	Eine erneute Infektion erzeugt eine Durchschnittslast von 37.

1. Siehe *A Tour of the Worm, Paper von Donn Seely* (*http://sunsite.org.uk/packages/athena/virus/seely.n*)

In noch nicht einmal 90 Minuten ab dem Zeitpunkt der Infektion hatte der Wurm das System lahmgelegt. Dasselbe passierte mit mehr als 6 000 Rechnern im ganzen Land. Zwar hatte der Wurm keinen physikalischen Schaden angerichtet, aber die Verluste, die auf Grund des Abbruchs der Internetverbindung bei infizierten Host-Rechnern entstanden, schwankten laut dem Bundesrechnungshof der USA zwischen 100 000 und zehn Millionen Dollar.

Was der Morris-Wurm gezeigt hat

Wenn ein Computerprogramm 6 000 Computer im ganzen Land abstürzen lässt – darunter solche in Forschungs- und Militäreinrichtungen –, dann machen sich zwangsläufig einige Menschen Gedanken darüber, dass etwas mit dem *status quo* ganz und gar nicht stimmt. Der Wurm von 1988 war da keine Ausnahme. Er legte mehrere eklatante Sicherheitslöcher in Unix-Netzwerken offen, die vermutlich verborgen geblieben oder als unbedeutend ignoriert worden wären, wenn dieser Wurm diese »kleinen« Fehler nicht so plastisch ausgenutzt hätte.

Manche möchten Morris sogar für seine Aktionen danken, weil sie Systemadministratoren überall im Lande wachgerüttelt haben. Natürlich wiesen wieder andere darauf hin, dass er diese Botschaft auch auf andere Weise hätte rüberbringen können. Vor Ende 1988 hat sich die Internetgemeinschaft nicht sonderlich um die Sicherheit von Computern gekümmert – zumindest nicht in demselben Maße wie nach dem 2. November. Der Wurm nutzte zwar mehrere andere Sicherheitslöcher nicht aus, aber bei einer intensiven Neubetrachtung der Betriebssysteme wurden auch diese gefunden und (hoffentlich) geflickt. Dank des Morris-Wurms versuchte man nicht nur, alle Sicherheitslöcher in einem System zu finden, sondern fand auch einige andere Dinge heraus.

Erstens sollte der Zugriff auf bestimmte Dateien nur jenen Benutzern gewährt werden, die diesen Zugriff auch benötigen. Bei einem seiner Angriffe nutzte der Wurm die Tatsache aus, dass die Datei mit den verschlüsselten Passwörtern sämtlicher Benutzer auf den meisten Systemen nicht lesegeschützt war. Folglich konnte der Wurm mehrere Verschlüsselungen möglicher Passwörter mit den verschlüsselten Passwörtern in dieser Datei vergleichen, ohne die Sicherheitswarnungen auszulösen, die normalerweise auftreten, wenn viele unrichtige Login-Versuche bemerkt werden.

Darüber hinaus lag diese Datei auf fast allen Systemen in demselben Verzeichnis, was dem Wurm die Arbeit viel leichter machte. Zum Glück wurde in den meisten Computernetzwerken dieses Versäumnis mittlerweile korrigiert.

Viele Netzwerkadministratoren stellten fest, dass es vorteilhaft ist, wenn mehrere unterschiedliche Computer im Netzwerk laufen, da eine Infektion eines Rechners mit großer Wahrscheinlichkeit nicht sonderlich viele verschiedene Rechner befallen kann. Je heterogener das Netzwerk ist, desto weniger Gefahr droht durch derartige Attacken. (Natürlich ist auch die Softwarekompatibilität in solchen Netz-

werken eingeschränkt; da wir uns hier jedoch auf die Sicherheit konzentrieren, werden wir diesen Umstand einstweilen ignorieren.)

Eine andere, weniger technische Lektion aus dem Wurmbefall ist, wie immens hilfreich es ist, wenn mehrere Institutionen gemeinsam nach geeigneten Gegenmaßnahmen forschen (so wie in diesem Fall MIT und Berkeley gemeinsam versuchten, das Programm zu dekompilieren). Am Ende war es dieses Netz von Computerfreaks und -gurus, das die Speerspitze im Kampf gegen den Wurm bildete.

Hüten Sie sich bei Computerproblemen vor Reflexhandlungen. Als die Systemadministratoren entdeckten, dass der Wurm über das Sendmail-Programm in ihre Systeme eingedrungen war, reagierten viele, indem sie ihre Mailserver herunterfuhren. Diese Medizin hat die Krankheit nur noch schlimmer gemacht. Da der Wurm noch mehrere andere Angriffspunkte kannte, hat ihn der Verlust des Mailprogramms nicht wirklich behindert.

Das Ausschalten des Mailprogramms führte nur dazu, dass die Mails, in denen die Bekämpfung des Wurms und die Behebung der Fehler beschrieben war, vielerorts verspätet eintraf. Die Protokollierung von Daten ist zum Entdecken von Infektionsquellen wie diesem Wurm lebenswichtig. Viele Server wurden dadurch behindert, dass sie nicht sagen konnten, von wo der Wurm gekommen war und wie er in das System eindrang. (Natürlich bleiben die meisten protokollierten Daten zu 99 Prozent der Zeit ungenutzt und da einige Anwendungen ihre eigenen Protokolldateien erfordern, können sich eine ganze Menge Daten ansammeln, die normalerweise nutzlos sind. Auch dies ist wieder ein Punkt, wo man abwägen muss.)

Robert T. Morris wurde schuldig gesprochen, das Gesetz über Computerbetrug und -missbrauch (Artikel 18) verletzt zu haben. Er wurde zu drei Jahren auf Bewährung, 400 Stunden Sozialdienst und einer Geldstrafe in Höhe von 10 050 Dollar verurteilt und musste die Kosten seiner Überwachung tragen.

Mehr über den Fall des Morris-Wurms können Sie in *Cyberpunk* von Katie Hafner und John Markoff nachlesen.

Fazit

Die hier aufgezeigten Probleme sind noch nicht überwunden.

Wie Sie in Kapitel 12 noch lesen werden, ist die Möglichkeit von Infrastrukturangriffen gegen Ziele wie z.B. das Telefonnetz, die Energieversorgung und das Luftverkehrskontrollsystem sehr real. Die Kapitel 6 und 8 zeigen, dass einzelne Hacker immer noch genug Schaden anrichten können, um die Strafverfolgungsbehörden zu beschäftigen und ihnen eine wilde Jagd quer durch den Cyberspace zu liefern. Kapitel 9 schließlich demonstriert, dass der Morris-Wurm nur das erste bösartige Programm gewesen war, das ganze Netzwerke auszuschalten vermochte.

6.
Kapitel

Die Joy Rider: eine Spur der Verwüstung

Eines der größten Missverständnisse, das die Verteidigung des Cyberspace behindert, ist die Vorstellung, Hacker seien nur jugendliche Joy Rider: Junge Genies, die gerne das Rechtssystem und das Militär in Verlegenheit bringen. Natürlich wird dieses Missverständnis unter anderem über die allgemeinen Medien transportiert. In die meisten Fälle, die ans Tageslicht kommen, waren letztlich jugendliche Hacker verwickelt.

Warum? Nun, die Fälle, in die echte Cyber-Terroristen, informationstechnische Kriegführung, Geheimdienste und Firmenspione verwickelt sind, kommen gar nicht erst in die Schlagzeilen. Sie versinken im Sumpf der »Geheimoperationen« oder werden in den betroffenen Firmen unter den Teppich gekehrt. (In den Kapiteln 12 und 13 können Sie mehr über solche Fälle nachlesen.)

Jugendliche oder »Sport«-Hacker (so bezeichnet man Hacker, die zwar aus denselben Motiven in Systeme eindringen, aber nicht mehr minderjährig sind) kommen in die Zeitung, weil sie geschnappt werden. Und sie gelangen in die Schlagzeilen, weil sie gerne im Rampenlicht stehen. Hinzu kommt, dass die betroffene Firma oder Regierungsbehörde nicht gerade eine Büchse der Pandora öffnet, wenn sie solche Hackeraktivitäten zugibt. Gäbe eine Regierungsbehörde hingegen eine Geheimdienstoperation eines anderen Landes zu, so könnte dies ernsthafte diplomatische oder gar militärische Folgen haben. Gäbe ein Großunternehmen einen Hackerangriff zu, bei dem Firmengeheimnisse gestohlen wurden, so wäre dies katastrophal für ihre Außenwirkung: Ihr Aktienkurs könnte z.B. abstürzen, strafrechtliche Ermittlungen könnten aufgenommen werden etc.

Dennoch haben im Laufe der Jahre auch jugendliche oder Sport-Hacker, so genannte Joy Rider, eine Menge Unheil und Verderben angerichtet.

Dieses Kapitel enthält Einzelheiten zu drei herausragenden Fällen, die sich über die Jahre 1994 bis 1999 erstrecken. Diese Fälle veranschaulichen nebenbei, welche Lektionen gelernt und welche nicht gelernt wurden.

Der Rome Labs-Fall: Datastream-Cowboy und Kuji gegen die US Air Force

Das Rome Air Development Center (Rome Labs in der Griffiss-Luftwaffenbasis (New York) ist die wichtigste Forschungseinrichtung des Oberkommandos der US Air Force.

Die Forscher von Rome Labs arbeiten zusammen mit Universitäten, Lieferanten von Verteidigungsgütern und kommerziellen Forschungsinstitutionen an Projekten zu Künstlicher Intelligenz, Radarleitsystemen und Zielerfassungs- und -verfolgungssystemen.

Am 28. März 1994 bemerkten die Systemadministratoren von Rome Labs, dass ein Passwort-Schnüfflerprogramm, ein Hackertool zum Sammeln von Login-Daten, heimlich auf einem mit dem Netzwerk der Rome Labs verbundenen System instal-

liert worden war. Laut James Christy, Direktor der Ermittlungsbehörde für Computerkriminalität des Sonderermittlungsbüros der Air Force (AFOSI), hatte das Schnüfflerprogramm so viele Daten gesammelt, dass es die Festplatte füllte und das System zum Abstürzen brachte.

Die Systemadministratoren informierten die Verteidigungsbehörde für Informationssysteme (DISA) darüber, dass sich ein noch unbekannter Eindringling in das Netzwerk der Rome Labs hineingehackt hatte. Das Team für Computernotfälle (CERT) der DISA wiederum informierte das AFOSI über den Bericht zu dem Einbruch. Dieses informierte seinerseits das Zentrum für informationstechnologische Kriegführung der US Air Force (AFIWC) mit Hauptquartier in San Antonio, Texas.

Das AFOSI schickte ein Team von Cyber-Kriminalitätsermittlern und Sicherheitsexperten zu den Rome Labs. Diese sahen sich Spuren an und befragten die Systemadministratoren. Aus ihren Vorermittlungen zogen sie sehr beunruhigende Schlüsse.

Zwei Hacker waren in sieben verschiedene Computer im Netz der Rome Labs eingedrungen. Sie hatten unbegrenzten Zugriff erlangt, Datendateien heruntergeladen und auf jedem dieser Computer verborgene Schnüffelprogramme abgesetzt. Diese sieben Schnüffler hatten insgesamt 30 Systeme der Rome Labs unsicher gemacht.

Diese Systeme enthielten schutzwürdige Forschungs- und Entwicklungsdaten.

Die systemeigenen Sicherheitsprotokolle zeigten, dass der Hackerangriff auf die Rome Labs tatsächlich bereits am 23. März gestartet wurde, fünf Tage vor seiner Entdeckung am 28. März.

Weiterhin ergaben die Ermittlungen, dass die sieben Schnüffler mehr als hundert Benutzerkonten unsicher gemacht hatten, indem sie die Benutzer-Logons und -Passwörter festhielten. Sie hatten E-Mails von Benutzern ausspioniert, dupliziert und gelöscht. Sie hatten geheime Programmdaten von Kampfsimulationen nachvollzogen und gestohlen. Zudem hatten die Eindringlinge die Systeme der Rome Labs als Sprungbrett für eine Reihe weiterer Hackerangriffe auf andere Militär-, Regierungs- und Forschungseinrichtungen in aller Welt benutzt. Auch auf diesen Systemen brachen sie in Benutzerkonten ein, installierten Schnüfflerprogramme und luden enorme Mengen von Daten herunter.

Die Ermittler stellten den kommandierenden Offizier der Rome Labs vor die Wahl, entweder die Sicherheit aller Systeme, die Ziel der Hacker gewesen waren, wiederherzustellen, oder eines oder mehrere davon für zukünftige Angriffe offen zu lassen. Wenn einige Systeme offen blieben, könnte man das Kommen und Gehen der Hacker nachvollziehen und hätte die Hoffnung, diese bis zu ihrem Ursprung zurückzuverfolgen und zu identifizieren.

Der Kommandeur entschied sich dafür, einige der Systeme offen zu lassen, um den Eindringlingen eine Falle zu stellen.

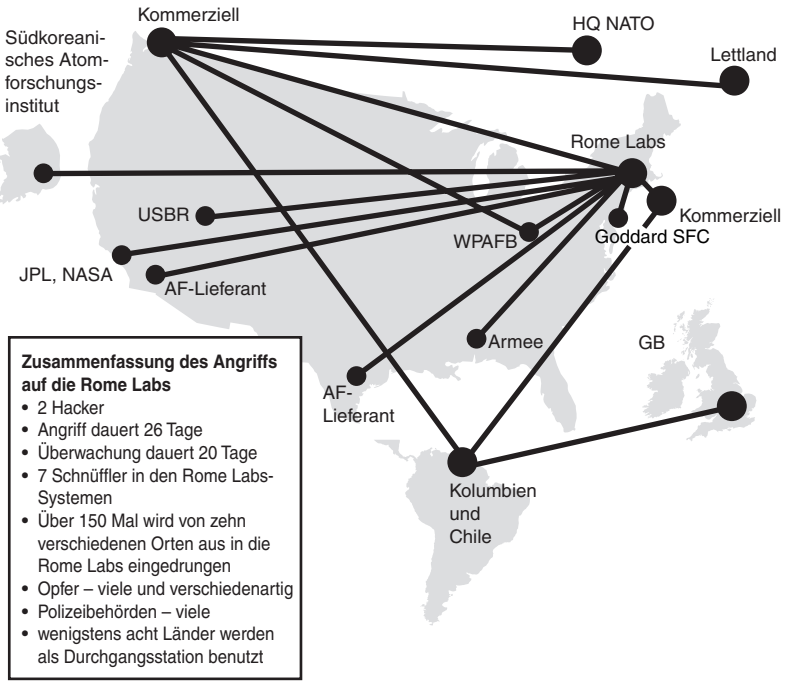

Abbildung 6.1: Nach den Rome Labs wurden mehr als 100 Opfer angegriffen. Quelle: Sonderermittlungsbüro der US Air Force

Ermittler kämpfen mit Rechtsfragen und technischen Grenzen

Mit Standardsoftware und Systembefehlen ließen sich die Angriffe zunächst um eine Etappe ihres Weges zurückverfolgen. Die meisten Angriffe wurden bis zu zwei kommerziellen Internetprovidern zurückverfolgt: cyberspace.com in Seattle, Washington, und mindvox.phantom.com in New York City.

In Zeitungsartikeln stand, dass sich die Leute, die bei mindvox.phantom.com für die Computersicherheit zuständig waren, selbst als »ehemalige Mitglieder der East Coast Legion of Doom« bezeichneten.

Die Legion of Doom (LoD) war ein loser Verband von Computer-Hackern. Mehrere Mitglieder waren für Einbrüche in Firmentelefonzentralen in den Jahren 1990 und 1991 verurteilt worden. Da die Ermittler nicht wussten, ob die Inhaber des New Yorker Internetproviders in die Einbrüche bei Rome Labs wissentlich verwickelt waren oder nur als Zwischenstation gedient hatten, beschlossen sie, diese nicht einzuweihen. Stattdessen überwachten sie einfach die betroffenen Computer im Netzwerk der Rome Labs, um das Ausmaß der Zugriffe festzustellen und alle Opfer zu identifizieren.

Nachdem das Hauptquartier, die Rechtsberater von AFOSI, die Air Force-Rechtsabteilung und die Abteilung für Computerkriminalität im Justizministerium das rechtliche Vorgehen koordiniert und abgestimmt hatten, stellte man ein Netzwerk der Rome Labs unter Echtzeitüberwachung. Die Echtzeitüberwachung von Inhalten ist dasselbe wie das Abhören eines Telefons, weil es ermöglicht, die Kommunikation zu belauschen oder, in diesem Falle, den Text auszuspionieren. Zudem startete das Ermittlerteam in den Rome Labs eine vollständige Tastendrucküberwachung: Es installierte ein ausgefeiltes Schnüfflerprogramm, das jeden aus der Entfernung ausgeführten Tastendruck eines jeden Eindringlings in die Rome Labs festhielt.

Diese Überwachung eines eingeschränkten Kontexts bestand darin, die Dienste des kommerziellen Internetproviders zu abonnieren und nur solche Programmbefehle und Dienstprogramme einzusetzen, deren Benutzung der Provider jedem Abonnenten gestattet. Das Team konnte den Weg des Eindringlings nur um eine Etappe zurückverfolgen. Um die nächste Etappe zu ermitteln, war der Zugriff auf das nächste System auf der Route des Hackers notwendig. Wenn der Hacker über Telefonsysteme auf den Provider zugriff, war eine gerichtlich angeordnete Fangschaltung notwendig.

Da eine solche gerichtliche Anordnung nicht schnell genug zu bekommen war, schied diese Option aus. Hinzu kam: Wenn die Hacker ihren Weg änderten, würde eine solche Fangschaltung ihren Nutzen verlieren. Im Verlauf der Einbrüche überwachte das Ermittlungsteam die Hacker beim Eindringen in das System und versuchte, diese bis zu ihrem Ausgangspunkt zurückzuverfolgen. Sie fanden heraus, dass die Eindringlinge über das Internet kamen und dazu Telefonsysteme in betrügerischer Weise missbrauchten (so genanntes »phone phreaking«).

Da die Eindringlinge ihre Angriffe auf mehreren Wegen starteten, konnte das Ermittlungsteam sie nicht in Echtzeit zu ihren Ursprüngen zurückverfolgen, da es zu schwierig war, mehreren Systemen in mehreren Ländern auf der Spur zu bleiben.

In dem Interview, das ich mit James Christy für dieses Buch führte, gewann ich faszinierende Einblicke in das Vorgehen bei den Ermittlungen.

»In dem Rome Labs-Fall arbeitete das AFIWC mit uns zusammen«, so Christy. »Sie entwikkelten das Hackback-Tool direkt bei Rome.« Laut Christy ist Hackback ein Programm, das auf das System zurückverweist, von dem der Angriff kam, dann ein Hackerskript auf dieses System loslässt, es überwacht, die nächste Etappe herausfindet und dann auf dieses nächste System sein Hackerskript loslässt. Hackback wurde geschaffen, um den Weg der Hacker durch das ganze Internet bis zu ihrem Ausgangspunkt zurückzuverfolgen.

»Nun, AFIWC hat dieses Tool entwickelt«, so Christy weiter, »aber wir haben denen gesagt, das dürft ihr nicht benutzen, das ist illegal. Ihr macht dasselbe wie der Hacker: Ihr brecht in Systeme ein. Sie antworteten, General Minihan [damals Chef der NSA] habe gesagt: ›Wir befinden uns im Krieg und wir werden es benutzen.‹

Meine Leute mussten für den Fall, dass das Tool benutzt würde, mit Verhaftung drohen. Also haben wir alle gesagt, wir wollen etwas ausprobieren.«

Es gab eine große Konferenz mit dem Justizministerium, dem Geheimdienst, dem FBI, AFOSI und den Leuten von Rome Labs. »Alle beriefen wir uns auf besondere Dringlichkeit, eine schnelle Verfolgung. Scott Charney [damals Chef der Abteilung für Computerkriminalität im Justizministerium] gab uns die Genehmigung, Hackback ein einziges Mal laufen zu lassen. Wir taten es, aber es hat uns nichts gebracht. Die Hacker drangen nicht über das Internet in diese Maschinen ein. Sie kamen über Telefon-Einwählverbindungen. Also endete es an dem Ausgangspunkt, von dem wir bereits wussten.«

Der größte Fehler des Datastream-Cowboys

Durch die Überwachung konnten die Ermittler feststellen, dass die Hacker die Spitznamen Datastream und Kuji verwendeten. Mit diesem Hinweis wandten sich die AFOSI-Ermittler für Computerkriminalität an ihr Netz von Geheimdienstinformanten, die im Internet surfen. Die Informanten sollten die beiden Hacker mit den Decknamen Datastream und Kuji identifizieren.

Christy erinnert sich: »Unsere Ermittler gingen zu ihren Informanten und sagten: ›Helft uns mal da draußen: Hat irgendjemand eine Ahnung, wer diese Typen sind?‹ Und anderthalb Tage später kam einer dieser Informanten an und sagte: ›Ich habe diesen Typen. Hier ist seine E-Mail.‹«

Laut Christy haben diese Informanten unterschiedliche Motive. Einige möchten gerne Polizei spielen, einige möchten etwas Rechtes tun, einige finden Hacking einfach spannend und einige werden wegen eigener Gesetzesverstöße unter Druck gesetzt.

Egal, was seine Motivation war: Am 5. April 1994 erklärte ein Informant den Ermittlern, er habe mit einem Hacker geredet, der sich als Datastream Cowboy vorstellte.

Es handelte sich um eine E-Mail-Korrespondenz und die Person erzählte, sie sei aus England. Diese Online-Konversation war bereits drei Monate her. In der E-Mail, die der Informant bereitstellte, erklärte Datastream, er sei 16 und er liebe attack.mil-Websites, weil sie so schön unsicher seien.

Datastream hatte dem Informanten sogar seine Telefonnummer für die eigenen Bulletin-Board-Systeme gegeben, die er für Hacker eingerichtet hatte.

Der größte Fehler von Datastream Cowboy sei es gewesen, mit seinen Hackergeschichten anzugeben, so Christy.

»Es war die einzige Möglichkeit, den Fall zu lösen. Durch Überwachung alleine hätten wir die beiden niemals zurückverfolgen können, weil sie so viele Schleifen und Windungen durch Südamerika gedreht hatten. Wir hätten mit mehreren Ländern zusammenarbeiten müssen.

Haben die südamerikanischen Staaten Gesetze gegen Hacker? Nein. Wären sie in der Lage gewesen, eine Fangschaltung einzurichten? Vielleicht auch das nicht. Denken Sie daran, dass die Hacker Telefonleitungen verwendeten.«

Die Air Force hatte sich zuvor mit Scotland Yard verbündet. Scotland Yard konnte die Personen identifizieren, die in dem Gebäude lebten, zu dem die Telefonnummern des Datastream Cowboys gehörten.

Scotland Yard ließ von der British Telecom die Telefonleitungen der betreffenden Personen mit so genannten Pen-Registern überwachen. Ein solches Register zeichnet alle Nummern auf, die die Bewohner des Gebäudes wählen. Fast sofort stellte sich heraus, dass jemand aus dem Gebäude Telefonleitungen der British Telecom missbrauchte. Dies ist auch in England strafbar.

Innerhalb von zwei Tagen wussten Christy und das Ermittlungsteam, wer der Datastream Cowboy war. Die nächsten 24 Tage lang überwachten sie die Online-Aktivitäten von Datastream und sammelten Daten.

Während der 26 Tage, die die Angriffe gedauert hatten, begingen Datastream Cowboy und Kuji mehr als 150 Computereinbrüche.

Scotland Yard umzingelt den Datastream-Cowboy

Scotland Yard stellte fest, dass bei jedem Computereinbruch in die Rome Labs die betreffende Person in England die Telefonleitungen für Gespräche ins Ausland missbrauchte. Ausgehend von England führte sie ihr Weg über Systeme in mehreren südamerikanischen und europäischen Ländern sowie durch Mexiko und Hawaii. Zum Schluss gelangte sie zu den Rome Labs. Von dort aus konnte sie über das Internet in das NASA-Labor für Antriebstechnik in Kalifornien und dessen Goddard-Raumfahrtzentrum in Greenbelt, Maryland, gelangen.

Die fortlaufende Überwachung durch die englischen und amerikanischen Behörden ergab, dass Datastream am 10. April 1994 erfolgreich in das heimische Computersystem eines Zulieferers für Luft- und Raumfahrttechnik eingedrungen war. Die Angreifer zeichneten mit Schnüfflerprogrammen das Logon des Lieferanten bei Rome Labs auf, als dieser sich bei Computersystemen in Kalifornien und Texas anmeldete. Die Schnüffler hielten nicht nur die Adressen des Lieferantencomputers, sondern auch das Logon und das Passwort für dieses System fest. Nachdem beides ausspioniert war, konnten sich die Angreifer als authorisierte Benutzer des Computersystems des Lieferanten ausgeben. In Kalifornien wurden vier und in Texas ein fünftes System dieses Lieferanten ausspioniert.

Darüber hinaus startete Datastream auf mehreren Systemen dieses Lieferanten einen Angriff mit Internet Scanning Software (ISS)[1]. ISS ist ein Hackertool, das ent-

1. Heute ist ISS ein millionenschweres Unternehmen, das ID-Software verkauft. Die Firma leugnet ihre Wurzeln in der Hackerszene und beschäftigt angeblich auch keine Hacker.

wickelt wurde, um ein System auszuspionieren. Es versucht, Daten über das Betriebssystem des Computers und andere Informationen herauszubekommen, die dem Angreifer bei der Entscheidung helfen könnten, mit welchem Tool er in dieses spezielle System am erfolgreichsten eindringen könnte. Außerdem versucht diese Software, die Passwortdatei des durchsuchten Systems zu lokalisieren und dann zu kopieren.

Der Diebstahl einer Passwortdatei ist deshalb so schwerwiegend, weil man Passwörter, obwohl sie verschlüsselt gespeichert sind, normalerweise leicht knacken kann. Mehrere Hackerprogramme zum Knacken von Passwörtern sind im Internet erhältlich. Wenn eine Passwortdatei gestohlen oder kopiert und geknackt wird, dann kann der Angreifer sich so bei dem System anmelden, dass das System von einem rechtmäßigen Benutzer ausgeht.

Die Überwachung ergab, dass Datastream am 12. April einen ISS-Angriff von den Rome Labs auf die Energieversorgungsabteilung der Brookhaven National Labs in New York startete. Zudem war Datastream zwei Stunden lang mit dem System des Zulieferers für Luft- und Raumfahrttechnik verbunden, das er zuvor geknackt hatte.

Kuji hackt sich in das Goddard-Raumfahrtzentrum hinein

Am 14. April 1994 meldete die Remote-Überwachung, die die Air Force von dem Provider in Seattle aus durchführte, dass sich Kuji über einen litauischen Internetprovider mit dem Goddard-Raumfahrtzentrum verbunden hatte. Die Überwachung ergab, dass von dem Raumfahrtzentrum aus Daten an den Provider übermittelt wurden. Um den Verlust geheimer Daten zu verhindern, brach das Überwachungsteam die Verbindung ab. Man weiß immer noch nicht, ob die von dem NASA-System übermittelten Daten tatsächlich für Litauen bestimmt waren. (Litauen als Destination dieser Daten löste bei den Ermittlern natürlich Besorgnis aus. Schließlich hatte dieses kleine baltische Land erst kurz zuvor seine Unabhängigkeit von Russland erlangt.)

Die weitere Remote-Überwachung von cyberspace.com zeigte, dass Datastream auf das National Aero-Space Joint Program Office zugriff, ein gemeinsames Projekt unter der Leitung der NASA und der Air Force, das auf der Air Force-Basis Wright-Patterson in Ohio durchgeführt wurde. Daten wurden von Wright-Patterson über cyberspace.com nach Litauen übertragen.

Kuji versucht, sich in das NATO-Hauptquartier einzuschleichen

Am 15. April ergab die Echtzeitüberwachung, dass Kuji von Rome Labs aus die ISS-Attacke gegen das NATO-Hauptquartier in Brüssel, Belgien, sowie gegen Wright-Patterson führte. Anscheinend erhielt Kuji durch diesen speziellen Angriff keinen Zugriff auf irgendwelche Systeme der NATO. Doch bei einer Befragung am 19. April