In diesem Kapitel:

- Angriffsszenarien im Überblick
- Hacker, Cracker und Skript-Kiddies
- Wie viel Sicherheit ist notwendig?

KAPITEL 1

Gefahren und Akteure im Internet

Wenn wir in diesem Buch vom Internet sprechen, müssen wir uns einige wichtige Umstände bewusst machen: Zunächst einmal handelt es sich beim Internet um ein internationales, weltumspannendes Netzwerk. Es wird des Öfteren auch als das »Netz der Netze« bezeichnet, um dem Umstand Rechnung zu tragen, dass das Internet die Gesamtheit aller in Teilnetzen verbundenen Rechner ist. Diese Tatsache mag auf den ersten Blick trivial wirken, sie ist jedoch letztlich der Grund für die zahlreichen Probleme, die bei der Nutzung des Internets entstehen können.

Jeder auch nur temporär an das Internet angeschlossene Computer wird zum vollwertigen Teil des gesamten Netzes und steht theoretisch mit all seinen Ressourcen anderen Nutzern zur Verfügung. Es handelt sich beim Internet also keinesfalls um eine Einbahnstraße, bei der die Benutzer Daten abfragen können, aber selbst unbeteiligt am Gesamtnetz bleiben. Oft erhält man den Eindruck, dass unerfahrene Surfer das Internet für eine Art erweitertes Fernsehen (oder Videotext) halten, bei dem sie zwischen den einzelnen Kanälen (Webseiten) frei wechseln können und das Dargebotene passiv konsumieren können. Besonders deutlich wird diese verdrehte Einstellung in Sätzen wie »Ich habe jetzt auch Internet« oder »Mein Internet funktioniert zurzeit nicht«. In Wirklichkeit müsste es heißen: »Ich bin jetzt auch Teil des Internets.« Die Interaktion zwischen Angebot und Benutzer ist gerade das wesentliche Merkmal dieses Mediums. Im Gegensatz zum Fernsehen ist man als Surfer stets – wenn auch meist unbewusst – aktiver Bestandteil des Netzwerks. Gewöhnen Sie sich also an den Gedanken, weder unbeobachtet noch passiv im Internet sein zu können. Genau so wie sie Anfragen an Computer im Netz senden, werden auch Anfragen an Ihr System gesandt, und manche dieser Anfragen sollten lieber unbeantwortet bleiben.

Weiterhin sollte Ihnen bewusst sein, dass das Internet die gesellschaftlichen Verhältnisse widerspiegelt. Ebenso wie im richtigen Leben werden Sie Nutzer und Anbieter finden, die seriös und Ihnen wohl gesonnen sind. Sicherlich werden Sie aber auch auf zwielichtige Gestalten und illegale Angebote treffen. Neben der Bibel

können Sie bei zahlreichen legalen amerikanischen Internethändlern auch Hitlers in Deutschland verbotenes Buch »Mein Kampf« bestellen. Was in einer Kultur- oder Rechtszone verboten sein mag, ist in anderen vielleicht Teil der Meinungsfreiheit und somit legal. Im Internet gibt es jedoch de facto keine abgegrenzten Rechtsräume. Was in den USA ins Netz gestellt wird, ist in jedem anderen Land der Welt abrufbar. Auf diese Weise ist Nazipropaganda möglicherweise nur wenige Klicks von Seiten mit kommunistischen Manifesten oder einer Sammlung von Papstdogmen entfernt. Zahlreiche Regierungen versuchen hier immer wieder einzugreifen und nur gewünschte Internetinhalte zu erlauben. Wer jetzt an Staaten wie China denkt, liegt sicherlich richtig, übersieht aber, dass auch hierzulande Inhalte unterdrückt werden. In Ländern wie China erreicht diese Zensur jedoch so große Ausmaße, dass von einem freien Netz bedauerlicherweise nicht mehr die Rede sein kann. Der Grund liegt meist darin, dass sich das Internet zu einer mächtigen politischen Bühne verwandelt hat. Der Computer zu Hause ermöglicht plötzlich einen Blick auf andere (freie) Staatsformen oder lässt die vermeintlichen Wahrheiten des eigenen Systems in einem anderen Licht erscheinen. Ein sehr erschreckendes Beispiel für die Macht dieses Mediums und zugleich ein Beleg dafür, wie anfällig es für Progaganda ist, sind die Videos von den Hinrichtungen ausländischer Geiseln, die 2005 von Terroristen im Irak ins Internet geladen wurden.

Im Gegensatz zum Fernsehen sehen Sie im World Wide Web also nicht nur für Sie aufbereitete, mehr oder weniger harmlose und bereits zensierte Informationen, sondern jeden erdenklichen Inhalt, den irgendjemand ins Internet gestellt hat. Wenn Sie im Fernsehen eine Dokumentationsreihe über das Dritte Reich sehen, können Sie mit großer Wahrscheinlichkeit davon ausgehen, dass hier Fakten vermittelt werden und nicht Halbwahrheiten oder gar Propaganda. Im Internet hingegen kann es Ihnen leicht passieren, dass Sie z. B. bei historischen Recherchen plötzlich auf einer Webseite landen, auf der die wohlbekannten Tatsachen verdreht oder geleugnet werden.

Da also jedermann jegliche Information unzensiert ins Internet stellen kann, ist die Frage nach der Seriosität der Quelle für Sie als Surfer von zentraler Bedeutung. Im Gegensatz zum Fernsehen liegt die Verantwortung bei Ihnen. Sie müssen in der Lage sein zu entscheiden, welchen Anbietern und Angeboten Sie Vertrauen schenken möchten. Das gilt für historische Dokumentationen genauso wie für Online-Shops. Auch durch die Möglichkeit, sich durch sein Surfverhalten strafbar zu machen, unterscheidet sich das Medium Internet grundlegend vom passiven Fernsehen oder Zeitunglesen. Da Sie zwar zu allen Inhalten Zugang haben, aber den Gesetzen im eigenen Land verpflichtet sind, müssen Sie stets darauf achten, keine illegalen Inhalte zu betrachten, herunterzuladen oder anzufordern. Ein Beispiel dafür ist der Bezug von verschreibungspflichtigen Medikamenten aus dem Ausland.

Wo liegt dann aber der Vorteil dieses Netzes, in dem Dichtung und Wahrheit so eng beieinander liegen? Nun, Sie haben die Freiheit, zu jedem Zeitpunkt beliebige Infor-

mationen von beliebigen Quellen zu beziehen und zu vergleichen. Dies beinhaltet zwar Verantwortung, birgt aber auch eine großartige Chance in sich. Es ist z.B. erstaunlich und hochinteressant, wie unterschiedlich auf den ersten Blick eindeutige politische Geschehen auf den Internetseiten verschiedener Nachrichtenagenturen dargestellt werden. Oftmals lohnt sich vor allem ein Blick auf ausländische Seiten, um sich ein besseres Bild vom Geschehen machen zu können. Dies gilt jedoch keinesfalls nur für Politik, sondern insbesondere auch für das Einkaufen im Netz. Nahezu bei jedem Produkt lassen sich zwischen fünf und 20 Prozent sparen, wenn man die Preise verschiedener Anbieter gründlich genug vergleicht. Gerade im Bereich elektronischer Produkte wie Digitalkameras sind die Preisunterschiede gewaltig, da das gewünschte Modell mit großer Wahrscheinlichkeit irgendwo in den Weiten des Internets aktuell als Angebot ausgeschrieben ist.

Angriffsszenarien im Überblick

In den späteren Kapiteln werden wir uns ausführlich mit den verschiedenen Gefahren beschäftigen, die das Internet mit sich bringt. Dabei werden wir nicht nur das World Wide Web, sondern auch viele andere Dienste im Internet thematisieren. An dieser Stelle wollen wir deshalb nur einen kurzen Blick auf die verschiedenen Gefahren und Akteure werfen, die für Internetbenutzer gefährlich werden könnten.

Wie bereits erwähnt, ist die Seriosität der Internetanbieter von zentraler Bedeutung. Dies betrifft jedoch nicht nur die Frage nach dem Wahrheitsgehalt der ins Internet geladenen Informationen, sondern in besonderem Maß auch die Frage nach der Sicherheit des eigenen Rechners und persönlicher Daten: Welche Gefahren drohen bereits beim einfachen Besuch einer Webseite, bei welchen Anbietern können Sie problemlos Ihre persönlichen Daten hinterlassen, wem sollten Sie Ihre Kreditkarteninformationen eher nicht zur Verfügung stellen?

Aus der Diskussion über Sicherheit im Internet haben sich im Lauf der Zeit drei Schlüsselbegriffe herauskristallisiert, die mit Hilfe verschiedener Sicherheitsmaßnahmen gewährleistet werden sollen: Vertraulichkeit, Integrität und Authentizität. Hinter dem Schlagwort Vertraulichkeit steht die Frage, wie ich Daten vor unberechtigten Lesezugriffen schützen kann. Integrität fragt nach dem Schutz der Daten vor unberechtigter Manipulation, die Frage nach Authentizität hingegen richtet sich an den Urheber von Daten (zum Beispiel E-Mails): Ist er wirklich der, der er vorgibt zu sein?

Immer dort, wo neue Technologien und Möglichkeiten erforscht werden und zum Einsatz kommen, brodelt auch die Gerüchteküche. Dies gilt umso mehr, wenn auch ein wirtschaftliches Interesse mit im Spiel ist. Natürlich möchten Ihnen die Hersteller von Security-Tools möglichst plausibel weismachen, dass das Internet ein gefährlicher Ort ist, den man – wenn überhaupt – nur unter Anwendung teurer Sicherheitsmaßnahmen aufsuchen sollte. Dieses Buch soll Sie in die Lage versetzen,

mögliche Risiken selbst einschätzen zu können, und zudem eine Auswahl an effektiven und kostengünstigen Lösungen für die Probleme bieten, die im Internet auf Sie zukommen können. Diese Probleme können verschiedenartiger Gestalt sein und sich auf äußerst unterschiedlichen technischen Ebenen bewegen. An dieser Stelle wollen wir uns einige verbreitete Angriffstechniken, auf die wir im weiteren Verlauf des Buchs zurückkommen werden, in einem knappen Überblick ansehen. Technische Details, die zum tieferen Verständnis der einzelnen Attacken nötig sind, finden Sie in Kapitel 2, *Technische Hintergründe*.

Social Engineering

Dies ist eine recht simple, gleichzeitig jedoch sehr gefährliche Angriffsmethode, da es keine technischen Schutzmaßnahmen gibt, mit denen man eine solche Attacke abwehren könnte. Man versteht unter *Social Engineering* den Versuch eines Angreifers, die Unwissenheit des Anwenders auszunutzen, um beispielsweise an Account-Daten zu gelangen. Per E-Mail oder auch über das Telefon gibt sich der Angreifer z. B. als Postmaster eines Freemail-Anbieters aus und fordert den ahnungslosen Benutzer dazu auf, aus »Sicherheitsgründen« seine Account-Daten in ein vorgegebenes Wortpaar zu ändern. Folgt der User dieser Aufforderung, hat der Angreifer vollen Zugriff auf den E-Mail-Account. Daher sollten Sie solchen Aufforderungen, ob von Seiten eines Freemailers oder ihres Systemadministrators, nie nachkommen. Unter dem Begriff des Social Engineering wollen wir jedoch auch unseriöse oder gar illegale Lockangebote verstehen, mittels derer Internetnutzer zum Besuch bestimmter Webseiten oder zu Käufen angeregt werden sollen.

Hoax

Auch diese Methode des Unruhestiftens kommt ohne komplizierte technische Hilfe aus. Als *Hoax* bezeichnet man Falschmeldungen, die gezielt – meist per E-Mail – im Internet verbreitet werden. Es kann sich dabei zum Beispiel um falsche Virenwarnungen handeln, in denen der Empfänger aufgefordert wird, die Nachricht »so schnell wie möglich an alle Bekannten« weiterzuleiten, um die Verbreitung eines »extrem gefährlichen« Virus zu verhindern. Dies führt zum einen zur Verunsicherung unerfahrener Benutzer, zum anderen wird dadurch eine unnötige Netzlast verursacht.

Mailbomben

Unter *Mailbomben* versteht man den Versuch eines Angreifers, einen PC oder auch einen Mailserver mittels einer Unzahl an E-Mails mit Daten zu überfluten und lahm zu legen. Dabei versucht der Angreifer, durch den Gebrauch anonymer Server selbst möglichst im Hintergrund zu bleiben, so dass die Spuren der Mails nicht auf ihn deuten. Mailbomben waren früher eine sehr verbreitete Angriffsart und richteten sich sowohl gegen Privatpersonen als auch gegen Unternehmen. Inzwischen gibt es einerseits weitaus effektivere Arten, jemandem zu schaden, und andererseits Mittel, eine solche Mailbombe recht einfach

wieder loszuwerden. Daher sind diese Angriffe selten geworden und lassen eher auf wenig erfahrene Angreifer schließen.

Viren und Würmer

Viren sind wohl die bekannteste Bedrohung im Internet. Die Namensgleichheit mit den aus der Biologie bekannten Schädlingen rührt daher, dass beide »Organismen« ähnlich funktionieren: Sie infizieren einen Wirt und verändern dessen Funktion so, dass er zur Vermehrung des Virus beiträgt. Computerviren werden an Programme angehängt und aktivieren sich, sobald das Programm gestartet wird. Von diesem Punkt an beginnen sie, das Betriebssystem oder andere Programme zu infizieren. Viele Viren sind harmlos und erzeugen nur unsinnige Anzeigen auf dem Monitor. Einige besonders bösartige Exemplare nisten sich jedoch z. B. im Boot-Sektor des Computers ein und können von dort aus verhindern, dass das Betriebssystem überhaupt noch gestartet werden kann. Inzwischen existieren im Internet zahlreiche »Virus Construction Kits«, mit denen es auch Laien problemlos möglich ist, innerhalb weniger Minuten neue Viren zu bauen.

Würmer funktionieren ähnlich wie Viren, allerdings sind sie eigenständige Programme, die sich oft als andere, ungefährliche Dateien wie Bilder oder Worddokumente tarnen. Meist werden sie in Form von E-Mail-Attachments verbreitet und aktivieren sich in dem Moment, in dem der ahnungslose Empfänger die Datei öffnet, um sich z. B. das vermeintliche Bild anzusehen. Würmer besitzen wie Viren die Fähigkeit, sich selbstständig fortzupflanzen. Dabei verschicken sie sich meist per E-Mail an alle Kontakte im eigenen Adressbuch. Auch unter dieser Spezies gibt es höchst verschiedene Stufen der Bösartigkeit. Im schlimmsten Fall kann auch ein Wurm das Betriebssystem eines Computers zerstören. Computerwürmer sind speziell für Privatpersonen seit einigen Jahren das größte Sicherheitsproblem im Internet. Es gibt jedoch auch gutartige Würmer, die sich auf Servern einnisten, um von dort aus Sicherheitslöcher zu beheben.

Trojanische Pferde

Der Begriff *Trojanisches Pferd* stammt aus der antiken Mythologie: In einem riesigen Holzpferd, das angeblich ein Geschenk an die Einwohner Trojas sein sollte, schmuggelten die Griechen ihre Kämpfer in die verfeindete Stadt und besiegten sie so in nur einer Nacht. Die Angriffstechnik, um die es hier geht, arbeitet ähnlich: In einem regulären Programm, das sich ein User aus dem Netz herunterlädt oder zugeschickt bekommt, versteckt sich ein weiteres Programm mit verschiedenen Komponenten, die es dem Angreifer ermöglichen, den Rechner vollständig fernzusteuern und gleichzeitig dem Opfer beispielsweise vorzugaukeln, dass die Online-Sitzung weiterhin völlig normal verlaufe. Mittels des »entführten« Computers kann der Angreifer dann beispielsweise Einbrüche in andere Netze begehen, ohne dass eine direkte Spur zu ihm zurückführt, oder alle Passwörter des Benutzers aufzeichnen (*loggen*). Trojanische Pferde sind

zum Angriffswerkzeug schlechthin geworden und werden in Zukunft noch an Bedeutung gewinnen. Ähnlich wie für Viren gibt es auch hier zahlreiche Download-Möglichkeiten und Dokumentationen, so dass auch ein Laie ohne weiteres mit diesen gefährlichen Spielzeugen experimentieren kann.

Spyware/Adware

Bei *Spyware* handelt es sich um Programme, die Trojanischen Pferden sehr ähnlich sind, deren Betreiber aber andere Absichten verfolgen. Hier geht es nicht so sehr darum, Kontrolle über einen Rechner und die dort gespeicherten Daten zu erlangen, sondern z.B. darum, die Surf- und Kaufgewohnheiten eines Benutzers auszuspionieren, um ihm dann vollautomatisch die »richtige« Werbung zukommen zu lassen. Dies ist jedoch keineswegs so harmlos, wie es auf den ersten Blick wirken mag, denn unter Umständen ändern Spywareprogramme die Darstellung der von Ihnen besuchten Internetseiten so, dass sie ständig auf einen unseriösen Online-Shop weitergeleitet werden. Mit dem Begriff *Adware* bezeichnet man verschiedene Zusatzprogramme die einem bei der Installation eines Softwarepakets aus dem Internet quasi untergejubelt werden. Manchmal bleibt Ihnen wenigstens die Wahl, selbst zu entscheiden, ob Sie diese Software ebenfalls installieren möchten. Nichtsdestotrotz handelt es sich in den allermeisten Fällen um unerwünschte oder zumindest wenig sinnvolle Applikationen, und daher ist die Grenze zwischen Adware und Spyware schwammig.

Denial-of-Service-Attacken

Bei *Denial-of-Service-Attacken* (DoS) handelt es sich um eine Flut meist sinnloser Anfragen an einen Server, bei deren Abarbeitung dieser irgendwann stecken bleibt und die Arbeit einstellt. Anders als bei Mailbomben, die als Unterart von DoS-Attacken angesehen werden können, kann ein Angreifer hier jedoch beliebige offene Ports und Protokolle benutzen. DDoS-Attacken (*Distributed Denial of Service*) stellen eine Verfeinerung dieser Technik dar, bei der sich der Angreifer meist eines Trojaners bedient, den er zuvor auf mehrere andere Rechner geschmuggelt hat. Mittels des Trojaners kann der Angreifer nun den DoS-Angriff gleichzeitig von verschiedenen Maschinen aus starten und seine Schlagkraft so erhöhen. Selbst die Webserver großer Online-Unternehmen halten diesen Angriffen nicht stand, und daher kann es zu empfindlichen Imageschäden aber auch Umsatzeinbrüchen kommen. Am 1. Februar 2005 überfluteten Angreifer z.B. die Server des heise-Verlags, dessen Online-Angebot in Deutschland zu den wichtigsten Informationsquellen rund um das Thema Computer(sicherheit) zählt.

Sniffing

Unter *Sniffing* versteht man das Abhören von Kommunikationsinhalten in einem Netzwerk. Dabei fängt der angreifende Computer meist den gesamten Datenverkehr im Netz ab und wertet ihn aus. Dadurch kann ein Eindringling beispielsweise an Passwörter gelangen oder Informationen über die Struktur des Netzwerks und lohnende Angriffsziele sammeln.

Spoofing

Unter *Spoofing* versteht man eine Vielzahl unterschiedlicher Angriffstechniken, die als Vorbereitung für einen Angriff dienen oder dem Eindringling Anonymität verleihen. Gemeinsam ist ihnen, dass der angreifende Computer vorgibt, ein anderer zu sein, als er tatsächlich ist. Ein Beispiel für diese Technik ist das *IP-Spoofing*, bei dem der Angreifer Zugriff auf geschützte Dateien erlangt, indem er seinem Computer eine falsche Identität verschafft. So wird in den meisten firmeninternen Netzen den netzeigenen IP-Adressen der angeschlossenen Rechner blind vertraut. Mit gefälschten Datagrammen, die angeblich von einer netzinternen IP-Adresse stammen und die der Angreifer nun in das Netzwerk einspeist, ist es ihm möglich, an Informationen zu gelangen, die eigentlich nur intern zur Verfügung stehen. Spoofing-Attacken zeichnen sich meist dadurch aus, dass der Angreifer blind arbeiten muss, und daher versucht, möglichst schnell einen Rechner in seine Gewalt zu bringen, um dann von dort aus weiterzuarbeiten.

Source-Routing-Attacken

Hierbei gelingt es dem Angreifer, die Route, die die Daten z. B. zwischen einem Surfer und einem Online-Shop nehmen, so zu manipulieren, dass er selbst die Daten abfangen kann. Auf diese Weise ist es möglich, Informationen über Accounts oder gar Kreditkartendaten zu erbeuten.

Man-in-the-Middle-Attacken

Da die Daten auf ihrem Weg von der Quelle zum Ziel einige Zwischenstationen passieren müssen, ist es denkbar, dass sich eine dieser Stationen komplett unter der Kontrolle eines Angreifers (»man in the middle«) befindet. Dieser ist somit in der Lage, ähnlich wie bei einer Source-Routing-Attacke den Datenfluss vor dem Weiterleiten zu lesen und zu manipulieren.

Identitätsdiebstahl

Gerade in den Vereinigten Staaten greift der *Identitätsdiebstahl* im Internet zurzeit stark um sich, und es wird nicht mehr lange dauern, bis dies auch in Europa der Fall sein wird. Dies ist umso schlimmer, als zahlreiche Anbieter anscheinend völlig unvorbereitet und überfordert sind. Allein in der ersten Hälfte des Jahres 2005 sind in den USA bereits über 50 Millionen Kundendaten samt brisanter Details wie Kreditkartennummern gestohlen worden. Das Verschulden liegt in fast allen Fällen bei den Anbietern und Datenhaltern, aber es wird für Sie als Geschädigten schwierig nachzuweisen, dass Sie an dem Diebstahl Ihrer persönlichen Daten keine Schuld tragen. Sie sollten also im Vorfeld handeln und umsichtig mit sensiblen Daten umgehen. Dazu später mehr.

Phishing

Diese Angriffstechnik ist noch sehr jung, zählt aber aktuell zu den größten Bedrohungen im Internet. Phishing läßt sich nicht einfach einordnen, da es eine Kombination oder Anwendung mehrerer Angriffsarten darstellt. Grundsätzlich

beginnt eine Phishing-Attacke mit Social Engineering, also beispielsweise einer E-Mail die den Leser dazu anregt, einem bestimmten Link zu folgen. Diese E-Mail scheint beispielsweise von Ihrer Bank zu stammen, und Sie werden darin aufgefordert Ihre Konto- und Zugangsdaten aus bestimmten Gründen (z.B. zum Schutz vor Phishing) auf der Internetseite der Bank einzugeben. Netterweise ist in der E-Mail auch gleich der Link zur Bank enthalten. Klickt man jedoch auf diesen Link, so landet man auf einer völlig anderen Seite, die eine genaue Nachbildung der Bankseite darstellt. Ahnungslos tappt man daher leicht in die Falle und verschickt seine geheimen Zugangsdaten an Kriminelle. Damit dieser fatale Fehler nicht sogleich auffliegt, werden Sie automatisch (mit Hilfe der eingegebenen Daten) an die echte Bankseite weitergeleitet und wiegen sich in Sicherheit. An dieser Stelle handelt es sich daher quasi um eine Man-in-the-middle-Attacke. Mit Hilfe der erbeuteten Daten kann der Angreifer daraufhin möglicherweise Ihre Identität annehmen. Es gibt zahlreiche Phishing-Arten, und nicht jede besteht aus den drei hier genannten Komponenten.

Hacker, Cracker und Skript-Kiddies

Diese Liste erhebt keinen Anspruch auf Vollständigkeit, und Sie werden festgestellt haben, dass bei weitem nicht jeder Internetnutzer für jede dieser Techniken in gleichem Maße anfällig ist. Wer sind nun aber die Akteure, die einem unbedarften Internetnutzer das Leben dermaßen schwer machen? Wahrscheinlich denken Sie jetzt an bösartige »Hacker«, wie sie in den Medien stets verteufelt und in einigen Ländern (z.B. Großbritannien) neuerdings rechtlich als Terroristen eingestuft werden. Man sollte dies jedoch etwas differenzierter betrachten. Im Computerbereich unterscheidet man üblicherweise zwischen *Hackern* und *Crackern*. Wie Sie im Folgenden sehen werden, liegen zwischen diesen beiden Begriffen Welten. Allerdings sei darauf hingewiesen, dass es keine Standarddefinition gibt und somit die Grenzen manchmal verschwimmen.

Als *Hacker* wollen wir hier jemanden bezeichnen, der als IT-Sicherheitsspezialist eingestuft werden kann (in welchem Teilgebiet auch immer) und einer gewissen »Hackerethik« folgt. Als meistgenannte und wohl auch am weitesten anerkannte Hackerethik zitieren wir die des »Chaos Computer Club e.V.« (*http://www.ccc.de*) im Wortlaut:

1. Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
2. Alle Informationen müssen frei sein.
3. Misstraue Autoritäten – fördere Dezentralisierung.
4. Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.

5. Man kann mit einem Computer Kunst und Schönheit schaffen.
6. Computer können dein Leben zum Besseren verändern.
7. Mülle nicht in den Daten anderer Leute.
8. Öffentliche Daten nützen, private Daten schützen.

Zwei Aspekte sind hier von besonderer Wichtigkeit: erstens der Freiheitsbegriff, der sich in den ersten drei sowie der letzten Maxime ausdrückt, und zweitens die hier nur indirekt angesprochene Motivation des Handelns. Ziel eines Hackers ist es nicht, möglichst viel Schaden anzurichten, sondern einem verantwortungsvollen Umgang mit Computertechnologien Vorschub zu leisten. Das kann z.B. heißen, dass man darauf hinwirkt, das Internet für alle offen zu halten, und neue Entwicklungen kritisch beobachtet und untersucht. In der Regel erwartet man von einem Hacker, dass er vielleicht in Computersysteme einbricht oder Möglichkeiten erforscht, Kreditkarten oder Handys zu manipulieren, mit den erlangten Daten aber keinen Schaden anrichtet. Viele Hacker veröffentlichen die von ihnen gefundenen Sicherheitslücken samt Hilfestellungen und Lösungsansätzen, um ihre Erkenntnisse für die Verbesserung von Sicherheitssystemen nutzbar zu machen. Insbesondere im Bereich Datenschutz und Überwachung hat die Internetgemeinschaft den Hackern viel zu verdanken, da sie zusammen mit anderen Datenschutzgruppen und Organisationen eine Art Gegengewicht zu den teils fragwürdigen Bemühungen des Staates stehen. Daher sollte man mit der pauschalen Verurteilung von Hackern sehr vorsichtig sein und in jedem Einzelfall die zugrunde liegenden Motive prüfen.[1]

Ganz anders hingegen verhält es sich mit den so genannten *Crackern*. Darunter versteht man im Allgemeinen Personen, die versuchen, ihr Wissen zu missbrauchen, um Schaden anzurichten. Wenn Sie im Fernsehen oder in Zeitungen also von »Hackerangriffen« hören oder lesen, sind in Wirklichkeit meist Cracker am Werk. Im Gegensatz zur Hackerszene gibt es hier keine Ethik, sondern nur das Ziel, Daten zu erbeuten, zu beschädigen oder anderweitig für Probleme zu sorgen. Man kann hier also keinesfalls mehr von ehrenhaften Motiven sprechen.

Mit Ausnahme einiger weniger professioneller Cracker, die gegen Bezahlung beispielsweise Wirtschaftsspionage betrieben, bestand das Lager der Cracker früher zu großen Teilen aus jungen Computerprofis, die das Programmieren von Internetwürmern oder das Verunstalten von fremden Internetseiten eher als eine Art Wettkampf untereinander begriffen. Inzwischen ist das Internet jedoch ein sehr großer und

1 Besonders heiß wird derzeit die Frage diskutiert, inwieweit bereits das bloße Einbrechen in ein EDV-System einem Straftatbestand gleichkommt, und ob eventuell das Suchen nach Schwachstellen schon als Tatvorbereitung gewertet werden kann. In der »realen« Welt ist das Einbrechen in ein Firmengebäude oder der Versuch, den Alarmanlagen-Code zu überwinden, eine klare Straftat. Es sei jedoch dringend davor gewarnt, diese Spielregeln unverändert auch auf das Internet anzuwenden. Leider werden zurzeit auf juristischer Ebene für das Internet eher unreflektiert die gleichen Richtlinien wie für die »reale« Welt als Maßstab gesetzt. Bei Interesse lohnt hier ein Blick auf die Paragrafen §202a, §263, §303a und §303b des Strafgesetzbuchs.

umsatzstarker Marktplatz geworden, und Geld lockt bekanntlich Betrüger an. Die Situation hat sich daher innerhalb der letzten Jahre grundlegend geändert, und es kann zurecht von Internetkriminalität gesprochen werden. Das jährliche prozentuale Wachstum elektronischer Straftaten ist sogar zweistellig, und die Beteiligten sind längst nicht mehr die verspielten Computerprofis von damals, sondern gut organisierte Kriminelle.

Neben den Hackern und Crackern lässt sich noch eine dritte Gruppe von potenziellen Angreifern ausmachen, die so genannten *Skript-Kiddies*. Wie der abwertende Name schon vermuten lässt, handelt es sich hierbei um Personen, die – ohne selbst über fundiertes Know-how zu verfügen – Cracker-Tools benutzen oder andere vorgefertigte Programme zum Herumexperimentieren und Schadenanrichten missbrauchen. Merkmal dieser Gruppe ist, dass es sich nicht um Profis, sondern eher um unbedarfte Störenfriede handelt, die ihr Handeln (ähnlich einigen Crackern) als eine Art Sport begreifen, mit dem Ziel, z.B. möglichst viele Rechner »abzuschießen«. Die Anzahl der Skript-Kiddies übersteigt die der Cracker erheblich, so dass Sie es als Privatperson wahrscheinlich eher mit solchen Quälgeistern als mit einem wahren Profi seines Fachs zu tun bekommen. Hier liegt aber auch Ihre Chance, denn wenn Sie die Vorgehensweise und Beschaffenheit der Cracker-Tools kennen und zudem die richtigen Sicherheitsmaßnahmen beachten, sind Sie vor den Skript-Kiddies einigermaßen sicher.

Statistiken zeigen aber, dass die meisten Angriffe nicht von außen, sondern aus dem eigenen Netzwerk, d.h. von Kollegen kommen. Dies liegt vor allem daran, dass die Netze in Firmen in den meisten Fällen kaum nach innen gesichert sind. Darüber hinaus liegt hier ein anderes Motiv vor: Im Gegensatz zu einer Cracker-Attacke ergeben sich die Angriffe nicht zufällig (z.B. weil Sie gerade online sind), sondern sie werden gezielt durchgeführt – sei es aus Missgunst, persönlichen Rache- oder Spionagegelüsten.

Wie viel Sicherheit ist notwendig?

Während wir uns in späteren Kapiteln konkret mit bestimmten Sicherheitsmaßnahmen beschäftigen wollen, soll hier die Frage nach der Verhältnismäßigkeit der Mittel gestellt werden. Dazu muss man sich zuerst bewusst machen, dass Sicherheit erstens kein einmal erreichter und dann konstanter Zustand, sondern ein ständig im Wandel begriffener Prozess ist, und dass zweitens eine erhöhte EDV-Sicherheit auch immer mit geringerem Benutzungskomfort einhergeht. Vollständige Sicherheit bedeutet immer auch Stillstand. Diese Erkenntnis führt dazu, dass man sich nicht mehr fragt, wie man maximale Sicherheit erreichen kann, sondern *wie viel* Sicherheit man sich leisten kann oder muss. Theoretisch müssten jeder Computerstart, jeder Zugriff auf das Internet und jedes Dokument durch Passwörter und weitere Sicherungsmechanismen geschützt werden. Eine effiziente Arbeit wäre dann aber

nicht mehr möglich. Als Benutzer müssen Sie sich also die Frage stellen, wie viel Sicherheit Sie wirklich brauchen.

Wichtig ist es hier vor allem, zwischen privaten PC-Benutzern und Firmennetzwerken zu unterscheiden. Unternehmensdaten sind im Allgemeinen schutzbedürftiger als persönliche Daten und zudem durch das firmeninterne Netzwerk und eine meist ständige Anbindung ans Internet stärker gefährdet. Während aber umgekehrt in einem Unternehmen ein Systemadministrator kontinuierlich für die Sicherheit der Daten sorgt, sind Sie als Privatperson selbst in die Pflicht genommen. Sie müssen sich also darüber klar werden, wie sensibel Ihre Daten sind und welche Vorkehrungen Sie bereit und in der Lage sind zu treffen, um ein höheres Maß an Sicherheit zu erreichen.

Zusätzlich zu absolut erforderlichen Maßnahmen wie der Installation eines aktuellen Virenscanners und einer guten Konfiguration Ihres Browsers können Sie z. B. auch so genannte *Personal Firewalls* auf Ihrem PC installieren und damit die Sicherheit im Netzverkehr erheblich erhöhen. Der Aufwand und Komfortverlust einer Firewall muss allerdings gegen die realen Gefahren im Internet und gegen Ihre Surfgewohnheiten abgewogen werden. Falsch konfigurierte Firewalls machen in der Regel viel Ärger, daher müssen Sie eine gewisse Einarbeitungs- und Wartungszeit einkalkulieren. Doch auch richtig eingestellte Programme verlangsamen zum Teil die Netzwerkanbindung erheblich und melden sich selbst bei unkritischen Vorgängen immer wieder. Als Benutzer werden Sie öfters mit aufspringenden Warnfenstern konfrontiert, deren Bedeutung sich nicht unbedingt direkt erschließt.

In diesem Buch werden Sie daher selten pauschale Aussagen zur Aktivierung oder Deaktivierung bestimmter Funktionen oder zur Installation bestimmter Tools finden, sondern eher Hinweise, die Ihnen als Entscheidungshilfe dienen sollen. Bei allen Sicherheitssorgen, wie sie immer wieder in den Medien und auch in diesem Buch zum Ausdruck kommen, dürfen Sie jedoch nicht vergessen, dass Sie als »gewöhnlicher« Surfer nicht am laufenden Band gecrackt werden. Zwar nimmt die Anzahl der registrierten Vorfälle zu, dies liegt aber zum einen an der wachsenden Zahl von Internetnutzern und zum anderen an der gestiegenen Aufmerksamkeit der Betroffenen. Lediglich die Zahl der Einbrüche in Firmennetze wird immer noch stark unterschätzt. Der Grund dafür ist, dass es meist nicht im Interesse der Unternehmen liegt, Einbrüche öffentlich zu machen und somit ein schlechtes Licht auf die eigene Netzsicherheit zu werfen. Die wirkliche Gefahr für Privatpersonen sind daher nicht so sehr direkte Angriffe von Crackern oder Skript-Kiddies, sondern mehr oder weniger selbstständige elektronische Schadprogramme in Form von Würmern, Spyware und Trojanischen Pferden.

Vielleicht halten Sie nach dem Lesen dieses ersten Kapitels das Buch ratlos in den Händen und fragen sich, wie Sie ohne Informatikstudium und teure Sicherheitstools überhaupt ruhig im Internet surfen sollen. Für diesen Fall sei Ihnen die 80/20-Regel

ans Herz gelegt, die auch maßgeblichen Einfluss auf die Gestaltung dieses Buchs hatte.

Angenommen, es gäbe so etwas wie einen Zustand völliger Sicherheit, in dem Ihnen nichts und niemand im Internet schaden zufügen könnte, quasi hundertprozentige Sicherheit. Um diesen Zustand zu erreichen, müssten Sie eine bestimmte Anzahl Ressourcen investieren, gleich ob Zeit, Geld oder eine Kombination von beiden. Um ein hohes Maß an Sicherheit zu erreichen, geben beispielsweise mittelständische Unternehmen durchaus einige zehntausend Euro aus. Die gute Nachricht ist nun die, dass Sie 80% dieser Sicherheit beim Einsatz von 20% der Ressourcen erreichen können. Was professionelle Sicherheitsmaßnahmen und Programme wirklich teuer macht, sind die letzten 10-20% (wobei vollständige Sicherheit wie erwähnt eine Fiktion bleibt). Für Sie als privaten Internetbenutzer bedeutet dies, dass sie mit deutlich weniger als 100 Euro auskommen, um Ihren PC wirklich effektiv abzusichern. Mehr noch, die wirklich essenziellen Maßnahmen bedürfen keiner Software, sondern einfach des richtigen Bewusstseins im Umgang mit dem Internet, und genau dieses Bewusstsein soll in diesem Buch vermittelt werden.