Vorwort zur 2. Auflage

Vor langer Zeit, Anfang der 70er Jahre, als das Internet selbst in der Science-Fiction noch kaum eine Rolle spielte, beherrschte eine Firma namens AT&T den Telefonmarkt in den USA. Diese Firma benutzte für die Gebührenabrechnung in ihrem Telefonnetz ein eigenartiges Verfahren: Sobald einer der beiden Gesprächsteilnehmer den Hörer aufgelegt hatte, wurde ein akustisches Signal gesendet, das den Einheitenzähler bei AT&T stoppte, aber nicht die eigentliche Telefonverbindung unterbrach. Normalerweise war dies kein Problem, denn wenn einer der beiden Teilnehmer auflegte, tat das überlicherweise auch sein Gesprächspartner, und so war die Verbindung ohnehin beendet.

Nun gab es aber ein paar findige Hobbytechniker, die versuchten, mehr über dieses rätselhafte Signal herauszufinden. Sie hatten die Hoffnung, durch das Simulieren dieses Signals bei einer bestehenden Telefonverbindung den Zähler anhalten und danach umsonst weiter telefonieren zu können. Auf der Suche nach dem richtigen Ton gelang es schließlich einem gewissen John Draper, die Frequenz von 2.600 Hertz als das verantwortliche Signal zu identifizieren. Etwa zur gleichen Zeit fand er in einer Cornflakes-Packung der Marke *Capt'n Crunch* eine kleine Kinderpfeife, die zufälligerweise genau das richtige Signal produzierte. Unter dem Namen Capt'n Crunch telefonierte Draper von nun an kostenlos in ganz Amerika, indem er, direkt nachdem das Gespräch begonnen hatte, in seine Pfeife blies und so den Gebührenzähler anhalten konnte. Bald darauf verbreitete sich das Wissen um diese günstige Art der Kommunikation schnell in den ganzen USA und führte schließlich zur Entstehung einer eigenen Subkultur: der *Phone Phreaks*.

Mit der Zeit entwickelte Capt'n Crunch sein System immer weiter und führte mit den so genannten *Blue Boxes* Geräte ein, die das 2.600 Hz-Signal automatisch erzeugten und noch über viele zusätzliche Funktionen verfügten. Im Laufe der Zeit allerdings wurde AT&T auf die Phreaks aufmerksam, und schließlich wurde Draper verhaftet und zu einer Gefängnisstrafe verurteilt. Dennoch lebte die Szene noch einige Zeit weiter, bis AT&T schließlich das Abrechnungsverfahren völlig umstellte.

Inzwischen ist John Draper ein überaus erfolgreicher Geschäftsmann im Silicon Valley, für die Hackerszene ist und bleibt er eine absolute Kultfigur.[1] Sogar eine der berühmtesten Hackergruppen ist nach ihm und seiner Entdeckung benannt: *2600.org*.

Was hat nun aber diese Geschichte aus grauer Vorzeit in einem Buch über Sicherheit im Internet zu suchen? Zum einen zeigt sie, dass die oft als Terroristen verteufelten Hacker meist nichts weiter als technisch begabte und unkonventionelle Querdenker sind. Andererseits wird hier aber auch deutlich, wie ein Angriff im Internet überhaupt funktioniert: Voraussetzung ist immer eine durch Programmierfehler verursachte Sicherheitslücke, die dem Hersteller lange genug verborgen bleibt oder als unwichtig und eher theoretisch angesehen wird. Experimentierfreudige Personen versuchen sich dann an dieser Lücke, finden – meist durch Zufall – den nötigen Weg und verbreiten anschließend das Wissen im Netz weiter. Doch innerhalb der letzten Jahre zeichnet sich hier eine dramatische Wende ab. Das Ausnutzen von Sicherheitslücken wandelt sich vom Hobby einiger Computerfreaks zum knallharten kriminellen Geschäft, in dem es um viel Geld geht. Zurecht ist im Fall von Spam, dem Werbemüll, der unser aller E-Mail-Postfächer überflutet, bereits von einer Internet-Mafia die Rede.

Wer aber sind die Datenspione, Hacker, Cracker und anderen zwielichtigen Gestalten, und wie kann man sich gegen sie zur Wehr setzen? Woher kommen eigentlich Viren und Trojaner, und mit welchen Programmen kann ich mich gegen sie schützen? Welche Risiken gehe ich ein, wenn ich online einkaufe oder meine Bankgeschäfte erledige? Welche Internetsoftware sollte ich verwenden, und wie kann ich durch geschickte Konfiguration der Programme eine maximale Sicherheit erreichen? Mit diesen und anderen Themen werden wir uns auf den folgenden Seiten beschäftigen und dabei niemals ein bekanntes Motto aus der Hackerszene aus den Augen verlieren:

> Ein falsches Gefühl von Sicherheit ist gefährlicher als jede Sicherheitslücke.

Über dieses Buch

Sicherheit im Internet richtet sich vor allem an Computernutzer, die sich zuvor erst wenig mit der Sicherheitsproblematik des Internets beschäftigt haben. Da das Buch aber nicht nur an der Oberfläche kratzt, sondern sich um ein tieferes Verständnis der Thematik bemüht und eine Fülle an Informationen und praktischen Tipps bietet, ist es auch für fortgeschrittene Leser geeignet.

Zielsetzung ist es vor allem, Sie als Leser mit einem fundierten Hintergrundwissen und den nötigen, meist kostenlosen Werkzeugen auszurüsten, um Ihnen eine sichere Nutzung des Internets zu ermöglichen. Dabei werden Sie in diesem Buch

1 Die ganze Geschichte inklusive der technischen Details können Sie auf John Drapers Homepage unter *http://www.webcrunchers.com/crunch/* nachlesen.

nur selten pauschale Empfehlungen finden, sondern bekommen das Rüstzeug an die Hand, um Gefahren einschätzen und auf sie reagieren zu können.

Zwar ist das Thema Sicherheit unabhängig vom benutzten Betriebssystem relevant, wann immer aber in diesem Buch konkrete Programme vorgestellt werden oder ein Problem auf Betriebssystemebene diskutiert wird, liegt der Schwerpunkt auf Windows. Dies hat seinen Grund darin, dass die meisten Viren, Würmer und Trojaner auf Windows-Systeme zugeschnitten sind und auch Angriffe auf Implementierungsfehler von Protokollen oder Software-Schwachstellen in den meisten Fällen auf Windows-Rechner stattfinden. Bei der Vorstellung typischer Internetsoftware – wie Browser und Mail-Tools – wurden jedoch Programme ausgewählt, die für möglichst viele Plattformen erhältlich sind.

Keine Regel ohne Ausnahme! Dieser Satz gilt auch für die Rechnersicherheit. Im gesamten Internet gibt es kein System, das nicht auf irgendeine Art angegriffen werden könnte: Selbst auf die Rechner des Pentagon in den USA wurden schon erfolgreiche Crackerangriffe durchgeführt. Wenn wir daher von Sicherheit sprechen oder bestimmte Konfigurationen oder Produkte als »sicher« bezeichnen, bedeutet dies nicht, dass es nicht noch irgendwelche Schwachstellen geben könnte. Sicherheit, vor allem im Computerbereich, ist immer ein relativer Begriff, und es kommt in erster Linie darauf an, kein leichtes Ziel für einen Angriff darzustellen. Dies ist auch dann möglich, wenn ein eingesetztes Programm keine hundertprozentige Sicherheit gewährleistet. Wir wollen daher davon absehen, rein theoretische Sicherheitslücken zu präsentieren. Stattdessen werden wir uns auf die wirklich gewichtigen Probleme konzentrieren.

Wir werden in diesem Buch einige Tools vorstellen, mit denen Sie die Sicherheit Ihres Rechners gezielt verbessern können. Wir haben uns in den meisten Fällen dafür entschieden, die kostenlosen Varianten der Software zu beschreiben, und weisen auf die etwas leistungsfähigeren kommerziellen Produkte lediglich hin. Eine breite Palette dieser Tools finden Sie auch auf der dem Buch beiliegenden CD-ROM, so dass Sie mit der Sicherung Ihres PCs gleich loslegen können. Nichtsdestotrotz sollten Sie sich immer auf dem Laufenden halten, ob es Updates zu der Software gibt, die Sie installiert haben. Aktualität ist ein absolut zentraler Faktor, wenn es um Sicherheit im Internet geht, da bei Angriffen durch Malware immer wieder Sicherheitslücken ausgenutzt werden, die nur mit aktuellen Softwareversionen geschlossen werden können.

Aufbau dieses Buchs

Dieses Buch soll Ihnen nicht nur als einmalige Lektüre, sondern auch als Nachschlagewerk zum sicheren Umgang mit dem Internet dienen. Um Ihnen daher das »Navigieren« zu erleichtern, finden Sie im Folgenden einen kurzen Überblick über die einzelnen Kapitel.

Kapitel 1, *Gefahren und Akteure im Internet*, gibt Ihnen nicht nur einen ersten Einstieg in die Sicherheitsproblematik des Internets, sondern beschäftigt sich auch mit der Frage nach den Akteuren, denen Sie im Netz begegnen können. Außerdem behandeln wir hier die Frage, wie viel Sicherheit man sich überhaupt leisten kann oder möchte.

In Kapitel 2, *Technische Hintergründe*, lernen Sie die grundlegenden Funktionsmechanismen des Internets kennen. Mit dem hier erworbenen Wissen werden Sie in der Lage sein, die in den darauf folgenden Kapiteln angesprochenen Sicherheitsprobleme zu verstehen, und sich selbst ein Bild über mögliche Gefahren machen können. Zu den Themen dieses Kapitels gehören das Client-Server-Modell, Protokolle, Adressierung und Routing.

Kapitel 3, *Sicherheitsbewusstsein*, beschäftigt sich mit der Wahl von Passwörtern, der Absicherung des Betriebssystems und persönlicher Dateien sowie mit der Frage, wie man bereits durch umsichtiges Verhalten Datenspionage und Verlust verhindern kann.

Kapitel 4, *World Wide Web*, soll Sie in die Lage versetzen, Ihr Sicherheitsrisiko beim Surfen selbst einschätzen zu können. Dazu beschäftigen wir uns mit den Grundelementen des World Wide Web: mit der Auszeichnungssprache HTML, dem Webprotokoll HTTP und verschiedenen Programmiersprachen.

Das Kapitel 5, *Browser – einer für alles*, stellt Ihnen die drei führenden Webbrowser vor und geht auf ihre Sicherheitslücken ein. Dabei erfahren Sie nicht nur, wie der Internet Explorer, Firefox und Opera sicher konfiguriert werden, sondern lernen auch einige Testmöglichkeiten kennen, mit deren Hilfe Sie die Auswirkungen der hier empfohlenen Einstellungen nachvollziehen können.

Der im Internet nach wie vor am häufigsten genutzte Dienst ist E-Mail, und gerade deswegen ist dieses Medium für Datenspione und für die Verbreitung von Viren sehr interessant. Kapitel 6, *E-Mail – wer liest mit?*, befasst sich daher mit den Protokollen SMTP und POP, mit der Abhörbarkeit elektronischer Nachrichten, mit Verschlüsselung und mit der Frage, wie man prüfen kann, ob eine Mail auch wirklich vom angegebenen Absender stammt. Zudem werden wir uns die Filterfunktionen verschiedener Mailprogramme ansehen, mit deren Hilfe Sie aufdringliche Werbung loswerden.

Kapitel 7, *E-Commerce und Online-Banking*, stellt Ihnen den heutigen Stand abhörsicherer Übertragungstechniken vor und zeigt anhand mehrerer »virtueller Banküberfälle«, welche Schwächen heutige Shopping- und Banking-Angebote aufweisen und was Sie dagegen unternehmen können.

Das Kapitel 8, *Weitere Internetdienste*, geht auf die Sicherheitsproblematik von Tauschbörsen, Instant Messagern, Online-Spielen, sowie einiger anderer Internetdienste ein.

Kapitel 9, *Anonymität*, behandelt die Frage, welche Inhalte für welche Datensammler von Interesse sein könnten und wie Sie sich vor solcher Spionage mit Hilfe von Proxies schützen können. Außerdem gibt das Kapitel einen kurzen Überblick über die juristische Diskussion und staatliche Abhörsysteme nach dem 11.09.2001.

Kapitel 10, *Viren, Würmer und Trojaner*, skizziert knapp die Geschichte der Computerschädlinge und verdeutlicht anhand zahlreicher Beispiele, wie es hinter den Kulissen eines Wurms oder Trojaners aussieht. In diesem Kapitel werden Sie außerdem den Trojaner *Back Orifice* kennen lernen und einen Überblick über gängige Antivirenprogramme erhalten.

Kapitel 11, *Angriffsszenarien*, zeigt anhand einiger Beispiele, wie aktuelle und zukünftige Sicherheitslücken von Angreifern ausgenutzt werden und gibt Ihnen als Leser einen Einblick in das Zusammenspiel einzelner Angriffsarten bis hin zu einem komplexen Szenario.

Kapitel 12, *Firewalls und erweiterte Sicherheitssysteme*, stellt einige erweiterte Sicherheitsmaßnahmen für kleinere Netzwerke – wie z.B. Paketfilter – vor. Im Zentrum des Kapitels stehen jedoch Personal Firewalls, die Sie effektiv vor Zugriffen von außen schützen, Ihren eigenen Datenverkehr aber passieren lassen. Wir beleuchten die Fähigkeiten und Schwachstellen dieser Programme und geben Anleitungen zu ihrer Konfiguration.

Zu guter Letzt beschäftigt sich Kapitel 13, *Erste Hilfe*, mit der Frage was zu tun ist, wenn ein Angriff stattgefunden hat, woran man dieses erkennen kann und wie man sein System wieder zum Laufen bekommt.

Die Begriffserläuterungen im Glossar helfen Ihnen, die beschriebenen technischen Zusammenhänge besser zu verstehen; eine Sammlung interessanter Quellen im Web unterstützt Sie dabei, sich selbstständig weiter in Sicherheitsthemen einzuarbeiten.

Danksagung

Oft wird das Internet als ein rechtsfreier Raum beschrieben, in dem es von zwielichtigen Gestalten nur so wimmelt und es vor allen Dingen um das große Geld geht. Im Verlauf dieses Buchs werden Sie jedoch entdecken, dass viele tausend Sicherheitsexperten, Entwickler, Internetpioniere und hochmotivierte Nutzer Tag für Tag und meist unbezahlt in ihrer Freizeit dafür kämpfen, das Internet zu einem sicheren Ort freier Informationen zu machen.

Mit dem offenen Projekt Wikipedia (*http://www.wikipedia.org*) gibt es beispielsweise eine kostenlos zugängliche und qualitativ hochwertige Enzyklopädie mit vielen hunterttausend Einträgen, zu der jeder Benutzer nach Belieben etwas beisteuern kann. Mit dem quelloffenen Linux und zahlreichen freien Distributionen ist ein professionelles Betriebssystem im Internet erhältlich, an dessen Sicherheit rund um die

Uhr hunderte von Entwicklern werkeln. Dank OpenOffice, das wir vor allem der Firma Sun verdanken, kann jeder Internetnutzer, ob reich oder arm, in jedem Land dieser Welt Dokumente erstellen und somit aktiv am Informationszeitalter teilnehmen, denn das OpenDocument-Format stellt sicher, dass seine Dokumente weltweit gelesen werden können. Gleiches gilt für den – in diesem Buch ausführlich besprochenen – Firefox-Browser, den Thunderbird-Mailer und das Verschlüsselungstool GnuPG.

Offene internationale Communities, die freie Inhalte vermitteln und fördern, sowie die Open Source-Bewegung sind es, die das Internet mit immer neuen Ideen vorantreiben. Daher gehört diesen Machern im Hintergrund besonderer Dank, denn ohne sie wäre das Internet nicht nur unsicherer, sondern es wäre lediglich eine technische Revolution anstelle der kulturellen, wie wir sie heute erleben.

Für die Mitarbeit, das Korrekturlesen sowie die moralische Unterstützung beim Erstellen der ersten Auflage danke ich insbesondere Carmen Queckbörner, Marion Wilde sowie dem damaligen Lektor Florian Zimniak. Ebenso gilt mein Dank Michael Lutz und Ariane Hesse, durch die ich überhaupt erst dazu gekommen bin, dieses Buch zu schreiben. Nicht unerwähnt sollen auch die Leser der ersten Auflage bleiben, die mit zahlreichen interessanten Anmerkungen und Verbesserungsvorschlägen zum Gelingen dieser zweiten Auflage beigetragen haben.

Was die zweite Auflage angeht, gilt mein Dank insbesondere Inken Kiupel vom O'Reilly Verlag, die mit der richtigen Mischung aus Druck und Geduld dafür gesorgt hat, dass »Sicherheit im Internet« nicht erst im nächsten Jahrtausend erscheint.

Für zahlreiche inhaltliche Anmerkungen und Beispiele möchte ich mich zudem bei meinen langjährigen Freunden Timo Vollmert und Rainer Schwarzbach bedanken. Ingo und Sandra Nahser, Nicole Schwarzbach sowie Rudolf Queckbörner und natürlich meiner gesamten Familie möchte ich für die immer neuen Motivationsversuche und das regelmäßige Nachfragen zum Stand der Dinge danken.

Zuletzt möchte ich mich ganz herzlich bei meiner Freundin Nicole Befurt bedanken, die nicht nur jede einzelne Seite mehrfach Korrektur gelesen, sondern mich über Monate hinweg bedingungslos unterstützt hat.