KAPITEL 1
Wer braucht eine Firewall?

Wenn über Computersicherheit gesprochen wird, hört man oft: »Ich habe keine Probleme. Meine Daten sind weder wertvoll noch geheim, und falls jemand meine Festplatte löscht, habe ich kein Problem damit, alles neu zu installieren.«

Wenn dies der Fall ist, so brauchen Sie eigentlich keine Firewall. Oder?

In der Regel ist es aber nicht ganz so einfach. Oft liegen der Vorstellung, nicht von diesen Problemen betroffen zu sein, falsche Annahmen zugrunde:

»Cracker sind Genies.«

Wenn dies der Fall wäre, gäbe es nur einige wenige Cracker, die vermutlich kaum die Zeit und das Bedürfnis hätten, sich unter Millionen Rechnern im Internet ausgerechnet Ihren PC vorzunehmen. Statt dessen würden sie sich viel eher mit ultrageheimen Rechnern von Regierungen und Banken beschäftigen, die sowohl eine Herausforderung als auch ein finanziell lohnenswertes Ziel bieten.

Tatsächlich ist diese Sorte Cracker extrem selten. Der Großteil der Angriffe im Internet rührt von gelangweilten Teenagern her, die Angriffsprogramme benutzen, deren Funktionsweise sie oft nicht einmal verstehen. Diese Programme können problemlos von diversen Servern im Internet heruntergeladen werden und erfordern in der Regel keine tiefergehenden Computerkenntnisse. Diese Angreifer werden daher oft als *Script Kiddies* bezeichnet.

Aus diesem Grund ist das Risiko, das Ziel eines Angriffes zu werden, deutlich größer, als Sie vielleicht zunächst annehmen. Nicht nur existiert eine große Anzahl möglicher Angreifer, diese haben auch automatisierte Werkzeuge, mit denen sie in kürzester Zeit große Bereiche des Internets auf schlecht gesicherte Rechner untersuchen und diese automatisch angreifen können.

»Wenn meine Dateien gelöscht werden, ist das nicht weiter schlimm.«

Viele Anwender gehen davon aus, daß sie keine wichtigen Daten besitzen oder ihre Dateien notfalls neu erstellen können, indem sie auf vorhandene Unterlagen und Notizen zurückgreifen.

Wenn Sie Ihren Rechner beruflich nutzen, könnte diese Einstellung fatal sein. Vermutlich können Sie die meisten Dokumente, Kalkulationen und Präsentationen neu erstellen. Aber wieviel Ihrer kostbaren Arbeitszeit wird Sie das kosten? Und was ist, wenn der Angriff abends erfolgt und Sie am nächsten Morgen eine wichtige Konferenz haben, auf der Sie der Vortragende sind?

Wenn Sie Ihren Computer nicht für berufliche Zwecke einsetzen, so mag es durchaus sein, daß der Verlust aller Dateien auf dem Rechner keine Katastrophe ist. Mit Sicherheit werden Sie dies aber erst wissen, wenn es passiert ist.

Gehen Sie doch einmal in Ruhe den Inhalt Ihrer Festplatte durch und fragen sich, was es bedeuten würde, wenn Sie die dort abgelegten Dateien verlören. Falls Sie ein Office-Paket benutzen, werden Sie sicherlich einige Tabellen und Dokumente finden.

Oder stellen Sie sich vor, daß Sie die Lesezeichenliste Ihres Browsers neu erstellen müßten. Wenn Sie das Netz als Informationsquelle nutzen, dann kann es schon bitter sein, wenn Sie die in Monaten gesammelten Quellen auf einen Schlag verlieren und neu zusammenstellen müssen.

Das beste Mittel gegen einen Datenverlust ist sicher das tägliche Erstellen von Backups. Aber dies ist nur eine Versicherung für den Fall der Fälle. Darüber hinaus sollte man von vorneherein die Wahrscheinlichkeit verringern, daß dieser Ernstfall eintritt. In bezug auf Angriffe aus dem Internet kann dies durch den Aufbau einer Firewall geschehen.

»Das Schlimmste, was meinen Dateien passieren kann, ist, daß sie gelöscht werden.«

Auch hierbei handelt es sich um einen weit verbreiteten Irrtum. Nehmen wir einmal an, es gäbe ein kleines Softwareunternehmen, das branchenspezifische Software für mittelständische Unternehmen schreibt. Jeden Abend werden Backups angefertigt und an einem sicheren Ort hinterlegt.

Wollte nun ein Konkurrent dieser Firma einen Schaden zufügen, so wäre der Effekt, der durch das Löschen der Festplatten der Rechner angerichtet würde, eher gering. Natürlich müßten die Rechner neu aufgesetzt werden, und auch die Arbeit des letzten Tages vor dem Angriff müßte rekonstruiert werden. Dadurch würde aber insgesamt nur eine Verzögerung von wenigen Tagen entstehen. Es wäre aber auch davon auszugehen, daß die Rechner anschließend besser gesichert wären und sich dem Angreifer keine zweite Chance böte.

Anders sieht es aus, wenn sich ein Angreifer Zugang zu den Rechnern verschafft und dort nur kleine Änderungen vornimmt. Er könnte z. B. kleine Fehler in die Programme einbauen, die gerade entwickelt werden. Er könnte auch Programme installieren, die mehr oder weniger zufällig einzelne Bits auf der Festplatte verändern. Wenn so ein Angriff geschickt ausgeführt wird, ist die Chance groß, daß er erst lange Zeit danach bemerkt wird. Zu diesem Zeitpunkt sind aber viele Dateien verändert worden, und es ist nahezu unmöglich, alle Fehler zu finden. Auch die Backups helfen hier wenig. Ist der Zeitpunkt

nicht bekannt, zu dem der Angriff durchgeführt wurde, so kann nicht sicher festgestellt werden, welche Backup-Version die unveränderten Dateien enthält. Aber selbst wenn man ein »sauberes« Backup besitzt, so kann es sein, daß dieses zu alt ist, als daß es viel nützt.

Glücklicherweise sind die Fälle, wo Cracker derartig boshaft vorgehen, extrem selten. Normalerweise begnügen sie sich damit, nur das Betriebssystem zu manipulieren, um bei weiteren Besuchen einfacher in den Rechner eindringen zu können oder die gesamte Festplatte zu löschen, wenn sie sich ertappt fühlen und ihre Spuren verwischen wollen. Hier reicht es vollkommen aus, den Rechner von Grund auf neu zu installieren und die verlorenen Daten aus Backups zu rekonstruieren.

»Cracker sind hinter meinen Dateien her.«

Tatsächlich sind Ihre Dateien vermutlich relativ uninteressant für den durchschnittlichen Cracker. Zwei andere Dinge werden ihn an Ihrem Rechner viel mehr interessieren. Da wären zum einen seine Ressourcen. Einen fremden Rechner, den niemand mit dem Cracker in Verbindung bringen kann, könnte er für viele Dinge benutzen, für die er den eigenen Rechner nur äußerst ungern einsetzen würde. Er könnte dort z. B. eigene Server einrichten, um mit Gleichgesinnten Raubkopien und pornographische Bilder auszutauschen. Auch als Ausgangsbasis für einen Angriff auf Drittrechner sind fremde Rechner viel besser geeignet. So verringert der Cracker die Chance deutlich, derjenige zu sein, bei dem die Polizei nachts vor der Tür steht und unangenehme Fragen stellt, wenn ein bekanntes Internet-Auktionshaus einen Tag nicht erreichbar war oder auf der Homepage eines bekannten westlichen Geheimdienstes plötzlich der Schriftzug »Central Stupidity Agency« prangt.

Als zweites ist es für einen Cracker interessant, die Anwender zu beobachten, die einen Rechner benutzen. Wenn diese sich an fremden Systemen anmelden, so kann er das dabei angegebene Paßwort belauschen. Kaufen Sie aber gar online ein, so kann er die verwendete Kreditkartennummer abfangen und für eigene Einkäufe verwenden. Damit er nicht ständig zugegen sein muß, wird der Angreifer hierzu Programme installieren, die Tastatureingaben oder Pakete im lokalen Netz belauschen, sie nach vorher festgelegten Kriterien filtern und dann in einer Datei ablegen, die bei einem späteren Besuch eingesammelt werden kann. Das Schreiben solcher Programme ist zwar nicht wirklich schwierig, der durchschnittliche Cracker wird allerdings den einfacheren Weg wählen und eines der bereits im Internet verfügbaren Programme verwenden.