In diesem Kapitel:

- Einsatzgebiete professioneller Firewall-Systeme
- Minimallösung mit privaten IP-Adressen
- Paketfilter
- Application Level Gateways (ALG)
- Personal Firewalls
- Grenzen von Firewalls
- Fazit

KAPITEL 12

Firewalls und erweiterte Sicherheitssysteme

Dieses Kapitel befasst sich mit erweiterten Sicherheitsvorkehrungen, die über die Basisausstattung eines Mediums mit einem Virenscanner hinausgehen. Dabei werden wir einige Grundprinzipien der Funktionsweise von Firewalls erläutern, um dann auf die verschiedenen Strukturen professioneller Firewalls zu sprechen zu kommen. Dabei beschränken wir uns aber auf das Wesentliche und lassen zahlreiche Details außen vor. Anschließend werden wir die so genannten Personal Firewalls besprechen und einige Produkte aus diesem Bereich kennen lernen.

Einsatzgebiete professioneller Firewall-Systeme

In Kapitel 2, *Technische Hintergründe*, haben wir den Unterschied zwischen privaten IP-Adressen (oder besser Adressbereichen) und öffentlichen IP-Adressen kennen gelernt. Der wichtigste Umstand dabei war die Eindeutigkeit der öffentlichen IPs, über die man direkt im Internet erreichbar ist. Diese ständige Erreichbarkeit ist aber nicht nur ein Vorteil, sondern setzt uns auch allen Gefahren aus, die im Internet lauern.

Stellen wir uns einmal ein kleineres Firmennetzwerk mit einigen dutzend Rechnern vor: Es gibt dort einen Fileserver, auf dem die Unternehmensdaten und eine Datenbank mit Kundeninformationen gespeichert sind. Ein Mailserver sorgt für den Nachrichtenaustausch im lokalen Netz, und ein HTTP-Server bietet den Mitarbeitern Zugang zu den firmeninternen Intranetseiten. Solange dieses Netzwerk vom Rest der Welt abgetrennt ist, gibt es keinerlei Probleme, da alle Ressourcen nur innerhalb des lokalen Netzes zugänglich sind.

Vergeben wir jedoch öffentliche IP-Adressen und sorgen für einen Internetzugang über einen Router, ändert sich die Situation schlagartig, denn die Computer werden zum aktiven Bestandteil des Internets. Alle Clients und Server sind nun durch ihre eindeutige Adresse im weltweiten Netz erreichbar und bieten ihre Ressourcen nicht mehr nur dem lokalen Netzwerk, sondern dem gesamten Internet an. Die Konse-

quenz ist, dass beispielsweise die Datenbank mit den Kundendaten durch fremde Benutzer ausgespäht werden oder der Mailserver zum Spammen missbraucht werden könnte. Auch wenn wir davon ausgehen, dass der Zugang zu allen Diensten durch sichere Passwörter geschützt und die Kommunikation im Firmennetz komplett verschlüsselt ist, ergeben sich nach wie vor zahlreiche Möglichkeiten für potenzielle Angreifer.

Es muss also eine Möglichkeit geschaffen werden, eine künstliche Trennung zwischen dem Internet und dem lokalen Netz zu erzeugen. Dazu bedient man sich unterschiedlicher Taktiken.

Minimallösung mit privaten IP-Adressen

Gerade für kleine Unternehmen oder Heimnetzwerke bietet sich die Lösung an, im lokalen Netz private IP-Adressen zu vergeben. Der Router, der für den Zugang ins Internet sorgt, verfügt dann über zwei Anschlüsse: einen mit einer privaten IP-Adresse zum LAN und einen anderen mit einer öffentlichen Adresse zum Internet (bzw. zum Provider) hin. In Kapitel 2, *Technische Hintergründe*, haben wir diese Möglichkeit bereits kurz angesprochen und wollen das Prinzip dahinter nun etwas genauer unter die Lupe nehmen.

Wenn ein Client eine Verbindung zu einem HTTP-Server im Internet aufbauen will, schickt er seine Datenpakete an den Router. Dieser leitet daraufhin die Anfrage an den Server im Internet weiter, ersetzt zuvor jedoch die Ursprungsadresse durch seine eigene (öffentliche). Für den angesprochenen HTTP-Server scheint also die Anfrage vom Router zu stammen, und daher schickt er die Antwort auch an diesen. Eine Zuordnungstabelle im Router sorgt nun dafür, dass dieser erkennt, an welchen Teilnehmer im lokalen Netz er die Ergebnisse weiterleiten soll, und so gelangen die Datenpakete schließlich an ihr Ziel.

Dieses Verfahren wird im Fachjargon *Masquerading* oder *Network Address Translation* (NAT)[1] genannt und kommt auch bei größeren Netzwerken im Zusammenhang mit anderen Sicherheitslösungen zum Tragen. Aus sicherheitstechnischer Sicht liegt der Vorteil von Masquerading und NAT unabhängig von der Art der im LAN verwendeten IP-Adressen darin, dass nur der Router nach außen hin sichtbar wird und nicht der anfragende Client selbst. Dem Kommunikationspartner scheint es daher immer so, als ob er nur mit dem Router verbunden wäre.

Oftmals wird daher behauptet, dass Masquerading und NAT Schutz vor Angriffen bieten würden, oder die entsprechenden Lösungen werden sogar als Firewalls »verkauft«. Zwar bieten diese Techniken einen gewissen Grundschutz, sind aber allein noch völlig unzulänglich. Das liegt vor allem daran, dass der Router in einem sol-

1 Der Unterschied zwischen beiden Ansätzen liegt darin, dass Masquerading n:1 Adressen (viele private IPs auf eine öffentliche) und NAT n:m umsetzt.

chen Fall einfach alles weiterleitet oder empfängt, was bei ihm ankommt, ohne den Datenstrom auf eventuell gefährliche Anfragen oder Datenpakete hin zu untersuchen.

Zum Problem werden maskierende Router, wenn der Verbindungsaufbauwunsch nicht von innerhalb des Netzes, sondern von außerhalb kommt. Dies ist zum Beispiel bei Online-Spielen häufig der Fall. Der lokale Computer schickt eine Anfrage an den Spieleserver mit der Bitte, einen geeigneten Gegenspieler zu finden und mit diesem Kontakt herzustellen. Der Server sucht nun einen weiteren Spieler, der zurzeit online und seinerseits auf der Suche ist und teilt ihm die Adresse des Gegenspielers mit. Nun versuchen die PCs (genauer gesagt die Spiele auf den jeweiligen Rechnern), eine Verbindung zueinander aufzubauen. Da sie aber den jeweiligen Router für den Rechner halten, schicken sie ihre Anfrage an ihn, ohne dass der Router die Datenpakete zuordnen könnte, und daher kommt eine Verbindung nicht zustande. Wie Spiele diese Probleme umgehen und wie Router so genannte *demilitarisierte Zonen* für einzelne Rechner erstellen, ist zwar ein spannendes Thema, würde den Umfang dieses Buches jedoch sprengen. Pragmatisch gesehen sollen Sicherheitsmaßnahmen Zugriffe von außen blockieren – somit tut der Router eigentlich nur seine Arbeit.

Paketfilter

Die logische Konsequenz aus dem oben erwähnten Problem ist die Kontrolle der erlaubten Verbindungen. Wie der Name schon andeutet, führen Paketfilter Untersuchungen auf der Ebene der einzelnen Datenpakete durch. Diese Tatsache muss man sich immer vor Augen führen, wenn es um die Fähigkeiten solcher Filter geht. Moderne Paketfilter können u. a. die im Internet üblichen Protokolle wie UDP, FTP und ICMP lesen und analysieren. Dabei können die Quelladresse, also die IP-Adresse der Anfragequelle, die Zieladresse sowie das Protokoll und die benutzten Ports erkannt werden. Mit diesen Informationen können nun Filterregeln erstellt werden, die den Datenstrom kontrollieren und Entscheidungen darüber treffen, ob das Paket verworfen wird oder nicht. Schauen wir uns dies anhand eines einfachen Beispiels an.

In unserem Beispielnetzwerk wird ein Paketfilter installiert, der dafür sorgen soll, dass die Mitarbeiter zwar im Web surfen und E-Mails verschicken, nicht jedoch FTP nutzen können. Zugriffe von Außen sollen grundsätzlich verboten werden. Grob dargestellt müssten dazu folgende Paketfilterregeln aufgestellt werden:

1. Erlaube Weiterleitung von TCP-Paketen aus dem lokalen Netz an Port 80 einer IP-Adresse außerhalb des eigenen Netzes, wenn der eigene Port über 1.024 liegt.

2. Erlaube Weiterleitung von TCP-Paketen von Port 80 aus dem externen Netz an einen Port über 1.024 eines Clients im lokalen Netz, wenn es sich dabei um keinen Verbindungsaufbauversuch handelt.
3. [Hier können Sie weitere Regeln definieren.]
4. Unterbinde den Transfer von ausgehenden Paketen aus dem lokalen Netz außer denen, die mit den Regeln 1-3 übereinstimmen.
5. Unterbinde den Transfer von eingehenden Paketen aus dem externen Netz außer denjenigen, die weiter oben explizit erlaubt wurden.

Diese Paketfilterregeln sind weder vollständig, noch würden sie genau so funktionieren, da für jede Netzwerkkarte eigene Regeln definiert werden müssen. Für unser Beispiel reichen sie aber aus, denn wir wollen nur die Grundzüge veranschaulichen.

Die Regeln 1 und 2 beziehen sich auf den »Handshake«, d.h. den Verbindungsaufbauwunsch und seine Beantwortung durch den angefragten Server (siehe dazu auch Kapitel 2, *Technische Hintergründe*). Wie Sie an den beiden letzten Regeln sehen können, verfahren wir auch hier nach dem Motto »Alles, was nicht explizit erlaubt ist, gilt als verboten«. Daher finden Sie in unserem Beispiel auch keine Regel für das Verbot von FTP-Zugriffen. Die Firewall-Regeln werden bei den meisten Produkten von oben nach unten abgearbeitet, und sobald die erste Regel zutrifft, wird der dort verlangte Befehl ausgeführt und die Regelkette nicht weiter gelesen. Daher würden Sie alle Zugriffe von innen und außen sperren, wenn die beiden letzten Regeln direkt an Position 1 und 2 stehen würden.

Betrachten wir nun die beiden Richtlinien für den HTTP-Zugriff. Dort werden Aussagen darüber getroffen, über welche Ports (80 und größer als 1.024) kommuniziert werden kann, und dass Verbindungsaufbauwünsche nur vom internen Netz ausgehen dürfen. Wie Sie an den dargestellten Regeln erkennen können, werden Pakete entweder verboten (abgewiesen) oder akzeptiert (durchgelassen). In der Praxis unterscheidet man noch einen weiteren Zustand (Befehl): Dieser ist quasi eine Spezialform des Abweisens und besteht darin, das Paket stillschweigend zu verwerfen. Der Unterschied liegt darin, dass der anfragende Computer beim Abweisen eine Rückmeldung erhält, in der ihm mitgeteilt wird, dass und warum sein Paket nicht akzeptiert wurde (ICMP-Message `destination unreachable`). Beim Verwerfen hingegen wird das Paket still und heimlich gelöscht, ohne dass eine Antwort generiert wird. Für den Kommunikationspartner sieht es daher so aus, als ob der angefragte Port oder Host gar nicht existiert. In der Fachwelt wird seit vielen Jahren darüber diskutiert, ob das stille Verwerfen aus Sicherheitssicht Vorteile mit sich bringt, da ein potenzieller Angreifer gar keine Informationen darüber erhält, ob der Dienst oder Host überhaupt online ist.

Andererseits sind die Informationen beim Abweisen einer Verbindung sehr wichtig für die allgemeinen Regelungsmechanismen im Internet. Viele Mailserver prüfen

beispielsweise die Identität der anfragenden Clients anhand des *auth*-Dienstes auf Port 113. Wenn dort die Verbindung zurückgewiesen wird, erkennt der Server, dass sich der Client nicht ausweisen kann, und fährt dennoch mit dem Empfang der Nachrichten fort. Verwirft man dagegen das Paket an Port 113 einfach, wartet der Mailserver meist noch 30 Sekunden auf eine Antwort und arbeitet erst nach dieser Timeout-Zeit weiter. Die Verzögerung ist zwar in diesem Fall nicht weiter schlimm, auf die Dauer aber störend. Generell sollte man daher die Statusmeldungen nicht künstlich unterdrücken, wenn es dafür keine triftigen Gründe gibt. Die Behauptung, dass das Abweisen von Datenpaketen im Gegensatz zum stillen Verwerfen DoS-Attacken begünstige, hat sich nie wirklich nachweisen lassen. Es gibt aber auch einige Spezialfälle, in denen die Pakete zwingend verworfen werden müssen, um keine Endlosrückkopplungen aus `destination unreachable`-Nachrichten zu bewirken.

Aus unserer clientseitigen Sicht als Privatanwender sollen solche Fragen aber keine allzu große Rolle spielen; viel wichtiger ist es, sich klarzumachen, wo die Grenzen der eben vorgestellten Paketfilter liegen. Denn tatsächlich bietet ein solcher Filter allein noch keinen ausreichenden Schutz. Der Grund hierfür liegt auf der Arbeitsebene dieser Lösungen, die mit der eigentlichen Anwendungsschicht nichts zu tun haben. Konkret bedeutet dies, dass ein Paketfilter eine Verbindung nicht »verstehen«, sondern nur ihre Rahmenbedingungen überwachen kann. Ob auf dem von uns freigegebenen Port 80 auch tatsächlich HTTP übertragen wird, ist unklar und kann vom Paketfilter nicht festgestellt werden.

Wir wollen uns diese überraschende Tatsache an einem kleinen Beispiel verdeutlichen: In unser Beispielnetzwerk wurde ein Trojaner eingeschleust, der nun versuchen soll, firmeninterne Daten nach außen zu schicken. Da aber alle Ports außer Port 80 für den Verkehr in externe Netze gesperrt worden sind, bleibt ihm nur noch besagter HTTP-Port übrig. Der Angreifer wird daher seinen Trojaner so konfigurieren, dass dieser eine Verbindung zu einem Server über Port 80 aufbaut. Dabei muss er noch nicht einmal HTTP verwenden, um Kontakt aufnehmen zu können, denn der Paketfilter versteht die Inhalte der Datenpakete ohnehin nicht. Auf dem besagten Server könnte auch ein spezieller Dienst an Port 80 lauschen, an den der Trojaner Informationen oder sogar komplette Dateien übermitteln kann. Auf diese Weise wurden (und werden) übrigens unzählige Paketfiler und darauf basierende Firewalls ausgetrickst.

Der Vollständigkeit halber sei noch erwähnt, dass so genannte *Stateful Packet Filter* Beziehungen zwischen den einzelnen Datenpaketen herstellen können. Dadurch wird es möglich, jedes Paket nicht nur für sich, sondern im Gesamtzusammenhang zu betrachten. Dies ist ein überaus wichtiger Schritt, um Angriffe und vor allem Angriffsvorbereitungen frühzeitig zu erkennen. Nichtsdestotrotz versteht der Filter den Inhalt der Pakete nicht.

Application Level Gateways (ALG)

Die *Application Level Gateways* (*ALG*) gehören zur großen Familie der Proxy-Systeme, die Sie in Kapitel 9, *Anonymität*, bereits kennen gelernt haben. Im Gegensatz zu generischen oder cachenden Proxys wie *Squid*, die entweder nur Zugangsberechtigungen abfragen oder Verbindungen beschleunigen, handelt es sich bei ALG um »intelligente« Systeme, die den dienstspezifischen Inhalt, den sie übertragen, auch verstehen.

Ein HTTP-Proxy dieser Art kann daher die eintreffenden Datenpakete untersuchen und ist teilweise in der Lage, offensichtlich gefährliche Inhalte zu eliminieren. Die Konsequenz daraus ist, dass Application Level Gateways immer nur für einige ganz bestimmte Dienste tauglich sind. Zwar gibt es auch Produkte wie *DeleGate* (*http://www.delegate.org*), die mit zahlreichen Protokollen zurechtkommen, aber auch ihr Einsatz ist anwendungsspezifisch. Je nachdem, welchen Dienst der Proxy vertreten soll, hat er auch verschiedene Kontroll- und Eingriffsmöglichkeiten. So kann er z. B. angeforderte HTML-Seiten auf ActiveX-Controls oder Java-Applets hin untersuchen und diese aus dem Datenstrom herausfiltern. Ebenso könnte der Proxy die Header-Felder von HTTP manipulieren oder Verweise auf Grafiken bestimmter (Werbe-) Server löschen. Man darf allerdings nicht davon ausgehen, dass ALGs alle gefährlichen Inhalte filtern können, daher gibt es keine Garantie eines absolut »sauberen« Datenstroms. Da solche Analysen zudem einen großen Aufwand bedeuten und sich außerdem Fehler in die Implementierung solcher intelligenten Proxys eingeschlichen haben könnten, gelten ALGs als sehr empfindlich gegenüber DoS- und anderen Attacken, so dass sie stets durch Paketfilter zu schützen sind. Da ein ALG den Inhalt der Pakete jedoch verstehen kann, ist der Schutz um ein Vielfaches höher als der durch einen reinen Paketfilter. Professionelle Firewalls bestehen daher immer aus beiden (und weiteren) Komponenten. Da es sich bei dem ALG keineswegs um eine Art künstliche Intelligenz handelt, vermag er natürlich nur solche Inhalte als gefährlich zu klassifizieren, die wir ihm vorher beigebracht haben, für neuartige Angriffe sind ALGs daher meist »blind«.

Neben den hier nur kurz angesprochenen Themen gibt es noch zahlreiche andere Faktoren, die erst zusammen mit der richtigen Netzwerkstruktur ein sicheres Firewall-System bilden.[2] Aus unserer Sicht soll dies aber ausreichen, um zu verstehen, wie die im Folgenden vorgestellten Personal Firewalls funktionieren.

2 Ein wesentliches Merkmal einer Firewall-Struktur ist die Aufteilung des Systems in mehrere Bereiche, zu denen z. B. auch so genannte *demilitarisierte Zonen* (*DMZ*) gehören. In diesen befinden sich unter anderem die Server, die nach außen hin Dienste bereitstellen und die sowohl gegen Angriffe von außen als auch von innen gesichert werden müssen.

Personal Firewalls

Noch vor wenigen Jahren war der Einsatz von Firewall-Systemen nur Firmen vergönnt, denn das Produkt kostete meist zwischen einigen tausend und zehntausend Euro. Zusätzlich waren die damit verbundenen Installations- und Wartungskosten zu berücksichtigen. Mit zunehmender Zahl an privaten Internetnutzern und vor allem immer mehr schutzbedürftigen Diensten steigt auch das Interesse an Sicherheitsmaßnahmen für private Zwecke oder kleine Firmennetzwerke. Damit war die Stunde der Personal Firewalls gekommen, jener Produkte, die die Aufgabe haben, Paketfilter- und ALG-ähnliche Funktionen auf dem heimischen Desktop umzusetzen.

Mittlerweile gibt es einige dutzend konkurrierende Produkte auf dem Markt, die sich in Funktionsumfang, Qualität und Preis beträchtlich unterscheiden. Wir werden uns daher im Folgenden vier repräsentative, jedoch zum Teil höchst unterschiedliche Ansätze anschauen und anschließend noch einen Blick auf das Produkt *BackOfficer Friendly* der Firma NFR werfen.

ZoneAlarm

Die Firma ZoneLabs brachte mit ihrem Produkt *ZoneAlarm* eine der ersten Personal Firewalls überhaupt auf den Markt. Zurzeit existieren verschiedene Versionen der Software. Wir wollen uns hier nur mit der kleinsten, für den privaten Gebrauch kostenlosen Version befassen. Ursprünglich war der Mehrwert der kostenpflichtigen Versionen eher gering und bezog sich nur auf zusätzliche Einstellungsmöglichkeiten, ein Modul gegen Spyware und einen Virenscanner. Inzwischen hat ZoneLabs die kostenlose Variante jedoch deutlich heruntergeschraubt, um mehr Anreize für den Kauf der erweiterten Versionen zu schaffen. Herunterladen können Sie die etwa 8 MByte schlanke Software unter *http://www.zonelabs.com*.

Nach der Installation des Programms, dem Ausfüllen einiger Angaben und dem unter Windows üblichen Neustart erscheint ein Symbol in der Taskleiste, das sich per Doppelklick in den Vordergrund holen lässt. Das eigentliche Tool ist in zwei Bereiche aufgeteilt: den orangenen Übersichtsrahmen (siehe Abbildung 12-1) und den Hauptbereich mit dem eigentlichen Inhalt, der sich je nach gewähltem Menüeintrag in weitere Bausteine verzweigt. Da die Standardkonfiguration von ZoneAlarm gut gewählt ist, können Sie gleich loslegen, nachdem Sie einige im Folgenden beschriebene Kleinigkeiten umgestellt haben.

Im Bereich FIREWALL können Sie zwischen drei verschiedenen Sicherheitsstufen wählen. Für den Internetbereich sollten Sie unbedingt die Einstellung HIGH belassen; für das lokale Netz hingegen ist bereits die Stufe MIDDLE zu viel, hier sollten Sie LOW einstellen, da es sonst mit hoher Wahrscheinlichkeit zu Störungen in Ihrem lokalen Netz kommen wird. Als weiteren Schritt sollten Sie im erweiterten Menü

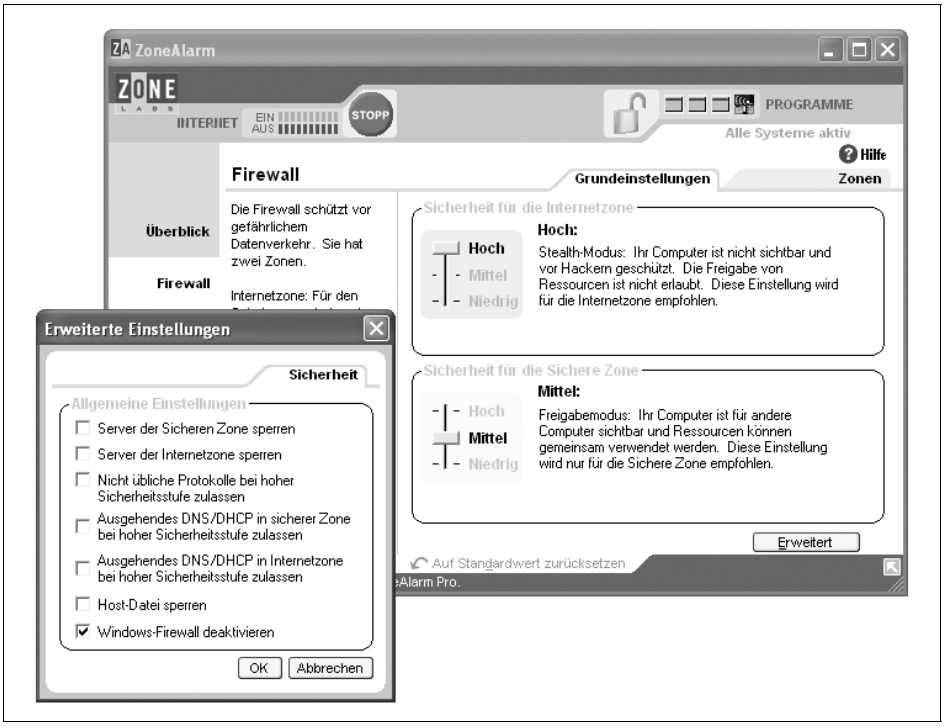

Abbildung 12-1: Das Hauptfenster von ZoneAlarm inklusive Not-Aus-Button

unbedingt die *hosts*-Datei sperren lassen. (Dass ZoneAlarm diese Option anbietet, ist vorbildlich!) Kommen wir nun zum allgemeinen Umgang mit ZoneAlarm.

Wenn Sie versuchen, mit einem Programm auf eine Ressource im Internet oder lokalen Netz zuzugreifen, poppt zuerst ein Informationsfenster der Firewall auf (siehe Abbildung 12-2). Anhand der dort angegebenen Informationen können Sie sich entscheiden, ob die Kommunikation erlaubt werden soll oder nicht. Wahlweise können Sie auch bestimmen, dass eine bestimmte Applikation immer Zugriff auf das Internet erhält. Interessant sind zudem die Einstellungsmöglichkeiten, die Sie im Menü PROGRAMMEINSTELLUNGEN finden. Dort kann man einerseits überprüfen, welchem Programm man den Zugriff erlaubt oder gesperrt hat und diese Einstellungen eventuell verändern, zum anderen kann man aber auch die Funktion UMGEHUNG DER INTERNETSPERRE für einzelne Tools aktivieren. Mittels dieser Funktion legt ZoneAlarm fest, welche Programme trotz aktivierter Sperrung des Internetzugangs weiterarbeiten dürfen.

Das Sperren an sich funktioniert auf zweierlei Arten. Entweder können Sie es direkt manuell auslösen, indem Sie im Hauptfenster der Firewall auf das STOP-Zeichen klicken, oder Sie können einstellen, nach wie vielen Minuten ohne Aktitität die Sperre automatisch greifen soll. Besonders, wenn man häufig größere Downloads

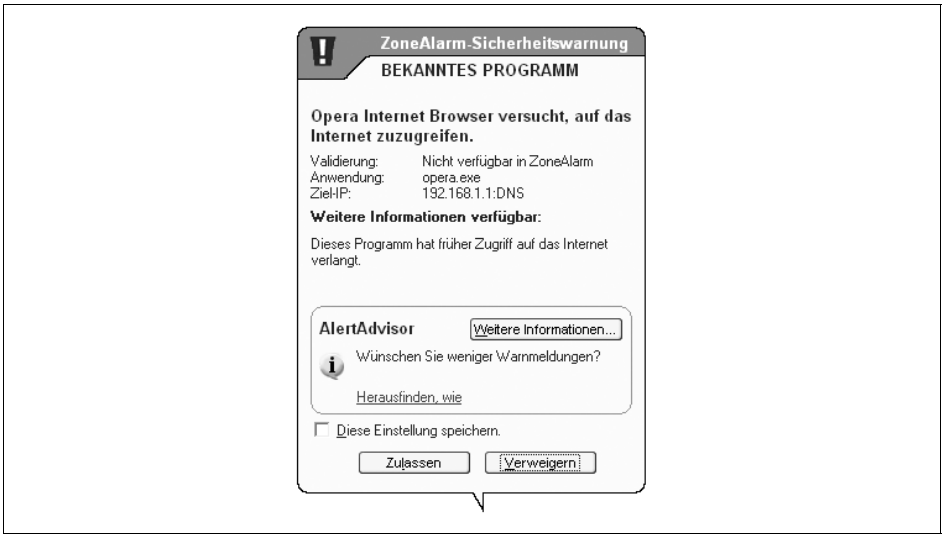

Abbildung 12-2: Soll Opera der Zugriff auf den DNS-Server erlaubt werden?

durchführt, ist diese Funktion sehr nützlich. Während allen anderen Programmen der Zugang zum Internet untersagt wird, läuft z. B. der FTP-Client ungestört weiter.

Ein weiteres Beispiel für den Einsatz der Locking-Option ist das Empfangen von E-Mails bei Nutzung einer Flatrate. Jeglicher Datenverkehr bis auf den Ihres E-Mail-Clients kann verboten werden, und Sie können trotz aktivierten Lockings Nachrichten empfangen.

Schauen wir uns nun noch an, was passiert, wenn jemand aus dem Internet oder dem lokalen Netzwerk heraus versucht, auf Ihren Computer zuzugreifen. Als Beispiel soll uns hier der versuchte Aufbau einer Telnet-Verbindung dienen. Sobald ZoneAlarm entdeckt, dass ein Zugriff aus dem (in diesem Fall: lokalen) Netz stattfindet, poppt ein Informationsfenster auf (siehe Abbildung 12-3). Dort wird nicht nur angegeben, welcher Host versucht hat, eine Verbindung aufzubauen, sondern auch, welche Ressource er angefragt hat. ZoneAlarm unterbindet solche Versuche von vornherein, daher brauchen Sie das Fenster nur noch mit OK zu verlassen und können beruhigt weiterarbeiten. Da auf der höchsten Sicherheitsstufe aber auch zahlreiche ICMP-Pakete gesperrt werden, springt ZoneAlarm gern häufiger mal auf und vermittelt so das Gefühl, dass tatsächlich ein Angriff stattfindet.

Generell sollten Sie sich unbedingt darüber im Klaren sein, dass sich hinter den meisten Verbindungsversuchen und ICMP-Nachrichten nicht gleich böse Absichten verbergen. Selbst in dem Fall, dass immer wieder der gleiche Host Verbindungen zu Ihnen aufzubauen versucht, sollten Sie Ruhe bewahren und zunächst keine Schritte unternehmen. Eine Möglichkeit, sich einen potenziellen Angreifer vom Hals zu schaffen, ist auch hier wieder das einfach Trennen der Verbindung mit anschließen-

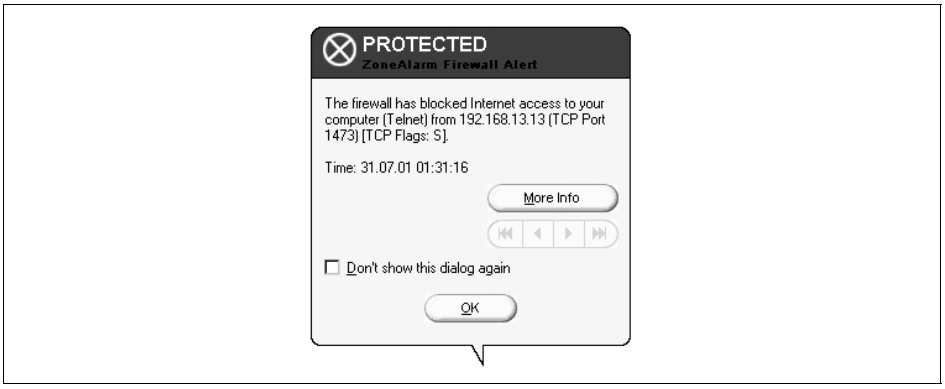

Abbildung 12-3: Ein fremder Host versucht, eine Telnet-Verbindung aufzubauen.

der Neueinwahl. Unter keinen Umständen sollten Sie auf eigene Faust versuchen, herauszufinden, wer der potenzielle Angreifer ist. Das Anpingen oder Tracen solcher Rechner wirkt höchstens provozierend und liegt zudem rechtlich gesehen in einer Grauzone, da Sie hiermit bereits anfangen, einen anderen Rechner zu untersuchen.

Die Entwicklung der Malware verschont leider auch die Hersteller von Sicherheitssoftware nicht: Inzwischen gibt es zahlreiche Würmer und Trojaner, die in der Lage sind, ZoneAlarm schlichtweg auszuschalten und so die Sicherheitsmechanismen zu umgehen. Der Hersteller versucht dies natürlich zu verhindern, das funktioniert aber nur bei bekannten Schädlingen wirklich gut.

Norton Internet Security

Die Firma Symantec ist eine feste Größe im Bereich der Antiviren- und Firewall-Software. Seit einigen Jahren gibt es nun innerhalb der Norton-Reihe auch eine Personal Firewall. Die Software ist in drei verschiedenen Versionen erhältlich: Norton Personal Firewall 2005, Norton AntiVirus 2005 und Norton Internet Security 2005.[3]

Wir wollen uns im Weiteren mit der letztgenannten und umfangreichsten Version befassen. Enthalten sind die Pakete Personal Firewall (inkl. Intrusion Detection), Virenscanner, Datenschutz, Werbeblocker, Kindersicherung und ein Spam-Filter (siehe Abbildung 12-4). Bei dem erwähnten Virenschutz handelt es sich um die vollständige *Norton-Antivirus-Software*. Der Preis für diese komplette Suite ist mit rund 60 Euro sehr fair, zumal Sie gleichzeitig das Recht erwerben, ein Jahr lang automatische Viren- und Programm-Updates zu erhalten. Da das Paket zum einen sehr

3 Die verschiedenen Versionen der letzten Jahre lassen sich automatisch auf dem neuesten Stand halten und unterscheiden sich teilweise nur marginal im Umfang. Sie können also ohne schlechtes Gewissen die Version von 2003 aktuell halten und dazu die Update-Verlängerung bei Symantec online kaufen. Allzusehr sollte man es damit natürlich nicht übertreiben.

umfangreich und zum anderen ausgezeichnet dokumentiert ist, wollen wir uns an dieser Stelle nur grob mit dem Funktionsumfang vertraut machen und lieber einige interessante Details betrachten.

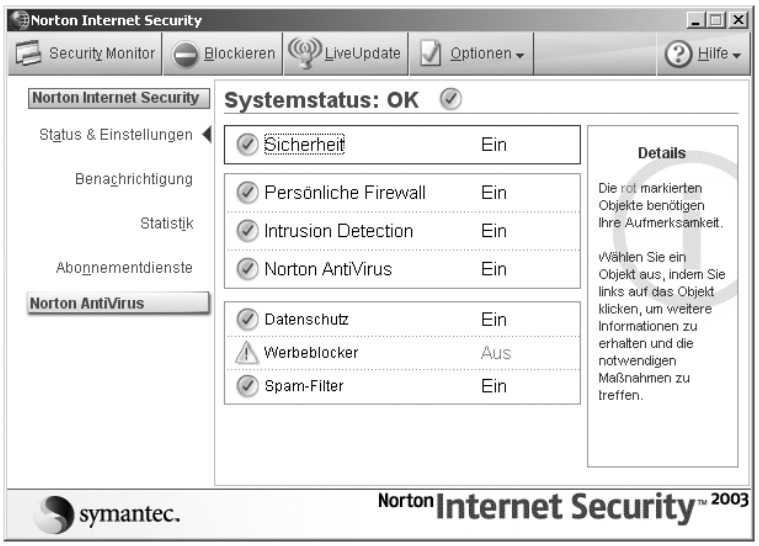

Abbildung 12-4: Der Startbildschirm von Norton Internet Security

Werbeblocker

Mit dieser Funktion können Sie die Anzeige von Bannern und Popup-Fenstern im Browser unterdrücken. Dies ist zwar bei Bannern sehr angenehm und funktioniert meist zuverlässig, manchmal kommt es jedoch zu Falschdarstellungen. Insgesamt können Sie die Funktion jedoch getrost deaktivieren und stattdessen besser den Popup-Blocker von Opera oder Firefox benutzen.

Personal Firewall

Ähnlich wie bei ZoneAlarm fragt die Norton-Firewall bei jedem Programm erst einmal nach, ob der Zugang zum Internet gestattet werden soll. Das aufspringende Fenster ist in der Standardversion nicht sonderlich informativ und das Programm schätzt das Risiko teils als zu gering ein (siehe Abbildung 12-5). Daher lohnt es sich, bei der Norton Firewall immer die höchste Sicherheitsstufe einzustellen.

Per Klick auf DETAILS bekommen Sie aber sehr ausführliche Informationen über das verwendete Protokoll, Ziel- und Quelladresse sowie die genutzten Ports. In einem zusätzlichen Text bewertet die Firewall zudem, ob das Programm vertrauenswürdig ist oder nicht. Dabei spielen einerseits Zertifikate, aber vor allem auch die Frage nach dem Hersteller eine wichtige Rolle. Erkennt Norton den Hersteller, liefert die Firewall Daten über ihn, ansonsten wird dar-

auf hingewiesen, dass der Anbieter nicht ermittelt werden konnte. In Zusammenhang mit einer Virenprüfung gelingt es Norton damit erstaunlich gut, auch die exotischsten Trojaner oder andere Cracker-Tools, die von Ihrem Rechner aus versuchen, auf das Internet zuzugreifen, als unseriös zu entlarven.

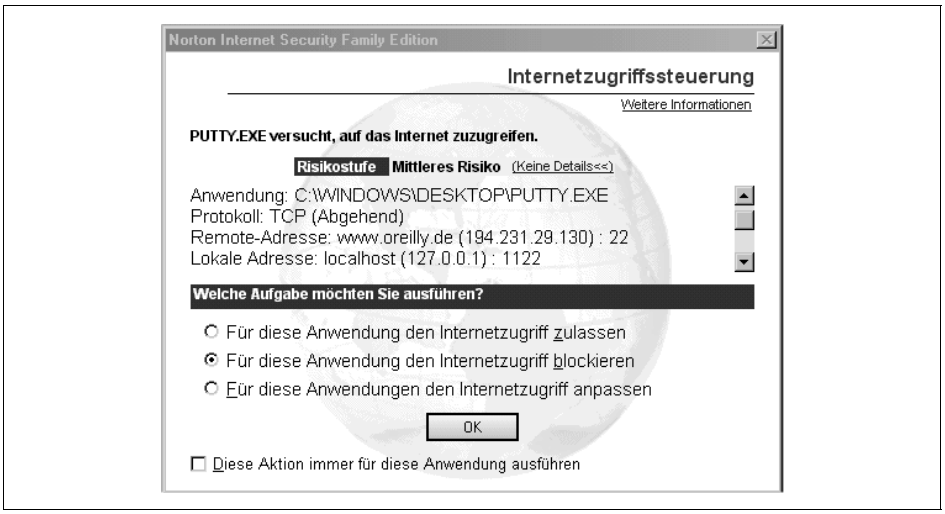

Abbildung 12-5: Darf eine SSH-Verbindung zu http: //www.oreilly.de aufgebaut werden?

Zugriffe von außen

Versucht ein Angreifer, von außen auf Ihren Computer zuzugreifen, blockt die Norton-Firewall solche Verbindungen standardmäßig ab (siehe Abbildung 12-6). Dabei fällt zwar positiv auf, dass Sie als Benutzer nicht mit Popup-Fenstern auf jeden Zugriff aufmerksam gemacht werden, bei einem gehäuften Zugriff oder Verbindungswünschen zu kritischen Ports würde man sich allerdings eine solche Warnmeldung wünschen. Die Warnstufe der Benachrichtigungen lässt sich bei der Firewall dafür vom zu schwachen Standard (»Niedrig«) auf »Mittel« oder »Hoch« setzen; hierzu klicken Sie auf der linken Seite im Menü INTERNETSTATUS den Link BENACHRICHTIGUNG an und bringen dort den Schieber auf die gewünschte Einstellung. Mittels benutzerdefinierter Konfigurationen der Firewall können Sie außerdem genau festlegen, ob eventuell auch Ports von außen erreicht werden dürfen. Dies ist immer dann wichtig, wenn Sie zum Beispiel einen Webserver betreiben oder bei Online-Spielen als Server fungieren möchten.

Datenschutzfunktionen

Unter dieser Rubrik fasst Norton einerseits das Verhalten gegenüber Cookies zusammen, andererseits können Sie hier steuern, wie »geschwätzig« der Browser sich nach außen hin gibt, d.h., welche Informationen er an Webserver weitergibt. Standardmäßig ist hier die Stufe MITTEL eingestellt. Während Sie damit

Abbildung 12-6: Norton blockt den Zugriff auf den NetBus-Port ab.

eine ausgewogene Mischung aus Datenschutz und Komfort erreichen, ist von der Verwendung der hohen Stufe abzuraten. Manche Online-Shops sind dann beispielsweise nicht mehr richtig zu bedienen, und Webseiten können ihr Design nicht an Ihre Vorgaben anpassen.

Symantec-Internetseite

Die Internetseite von Symantec können Sie selbstverständlich auch in vollem Umfang nutzen, wenn Sie kein Symantec-Produkt Ihr Eigen nennen. Dort finden sich zahlreiche relevante Sicherheitsinformationen, die sowohl für Anfänger als auch für Experten aufbereitet sind. Ein guter Einstiegspunkt ist etwa *http://www.symantec.com/region/de/avcenter/index.html*. Von dieser Seite aus können Sie zudem Removal-Tools für bestimmte Viren und Würmer herunterladen, ohne Kunde von Symantec zu sein.[4] Symantec bietet Ihnen zudem die Möglichkeit, Ihren Computer online auf Schwachstellen oder Viren zu prüfen (*Symantec Security Check*). Dazu müssen Sie jedoch den Internet Explorer benutzen. Der Security Check soll zwar angeblich auch Versionen ab Netscape 4.5 unterstützen, erkennt aber beispielsweise Firefox nicht (obwohl alle beide Browser denselben Kern haben). Betrachten Sie diese Art von Scans jedoch bitte eher als eine nette Spielerei, um Benutzern ohne Firewall einen Schrecken einzujagen. Es ist keinesfalls ein Ersatz für eine Firewall und einen Virenscanner auf Ihrem eigenen System und hilft zudem auch erst, nachdem Sie befallen worden sind.

4 Einen ähnlichen Dienst bieten auch einige andere der großen Sicherheitsfirmen an.

McAfee Internet Security

Neben Symantec zählt McAfee sicherlich zu den renomiertesten Firmen im Security-Bereich und bietet daher ähnlich wie ZoneLabs und Symantec eine ganze Palette an Sicherheitsprodukten für Endkunden an. All diese vereint McAfee zur Internet Security Suite, die aus Virenscanner, Spamfilter, Privacy-Service und Firewall besteht. Das komplette Paket kostet weniger als 70 Euro, daher lohnt es sich nicht, die Komponenten einzeln zu kaufen. Sowie die anderen vorgestellten Produkte finden Sie die McAfee-Suite nach der Installation in der Taskleiste wieder. Dort erscheinen (genau wie bei der Komplettlösung von Symantec) zwei Symbole: eines für die Firewall und eines für den Virenscanner. Wir wollen hier wiederum nur auf einige Besonderheiten eingehen und verweisen ansonsten auf das umfangreiche Handbuch und die Online-Hilfe.

Wie Sie anhand Abbildung 12-7 erkennen können, ist das McAfee-Produkt deutlich kompakter und richtet sich eher an fortgeschrittene Benutzer als an Anfänger. Gerade diese werden mit den Einstellungen der Firewall und des Virenscanners Probleme haben. Wer sich jedoch einmal zurechtgefunden hat, stößt auf eine große Anzahl interessanter Einstellungsmöglichkeiten wie etwa den Pufferüberlaufschutz oder den Zugriffsschutz für bestimmte kritische Systemordner.

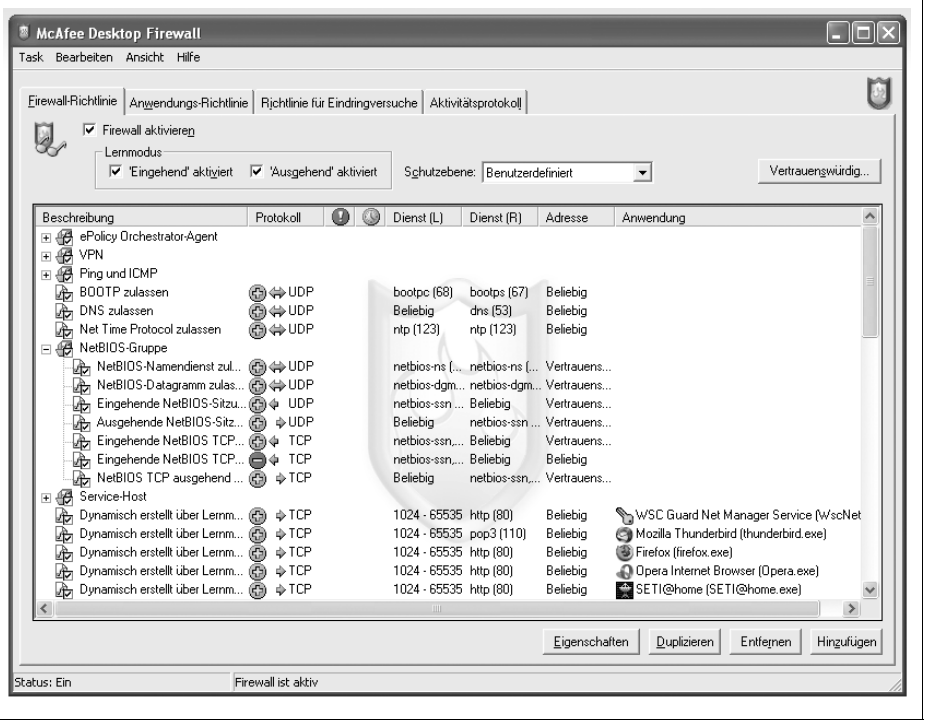

Abbildung 12-7: Der Hauptbildschirm der McAfee-Firewall

Quelle ermitteln

Sollten Sie einmal angegriffen werden, bietet Ihnen die Firewall die Möglichkeit, eigenhändig nachzuverfolgen, von wo aus der vermeintliche Angriff stattgefunden hat (siehe Abbildung 12-8). Wenn Sie sich von diesem Werkzeug ein Spionageprogramm oder gar ein Tool zum Gegenschlag erhofft haben, werden Sie (glücklicherweise) enttäuscht. McAfee sammelt nur Informationen, die Sie selber ohne zusätzliche Programme innerhalb weniger Minuten erhalten können. Betrachten Sie diese Funktion daher eher als nette Spielerei, immerhin ersparen Sie sich damit »Whois«-Anfragen (siehe dazu Kapitel 2, *Technische Hintergründe*). Zudem können Sie in demselben Fenster einstellen, wie lange der Angreifer komplett blockiert werden soll. Es ist wichtig, dass sie hier keineswegs die Option »bis entfernt« wählen, sondern nur eine kurze Zeitspanne von wenigen Minuten. Sie können die Default-Einstellung außerdem im Menü unter BEARBEITEN → OPTIONEN → ANGREIFER AUTOMATISCH BLOCKIEREN bearbeiten. Wie schon erwähnt, sind fast alle Angriffe, die Schutzsysteme (insbesondere Personal Firewalls) melden, keine Angriffe, sondern man könnte sie ein »allgemeines Informationsrauschen« im Netz nennen. Möglicherweise ist es ein

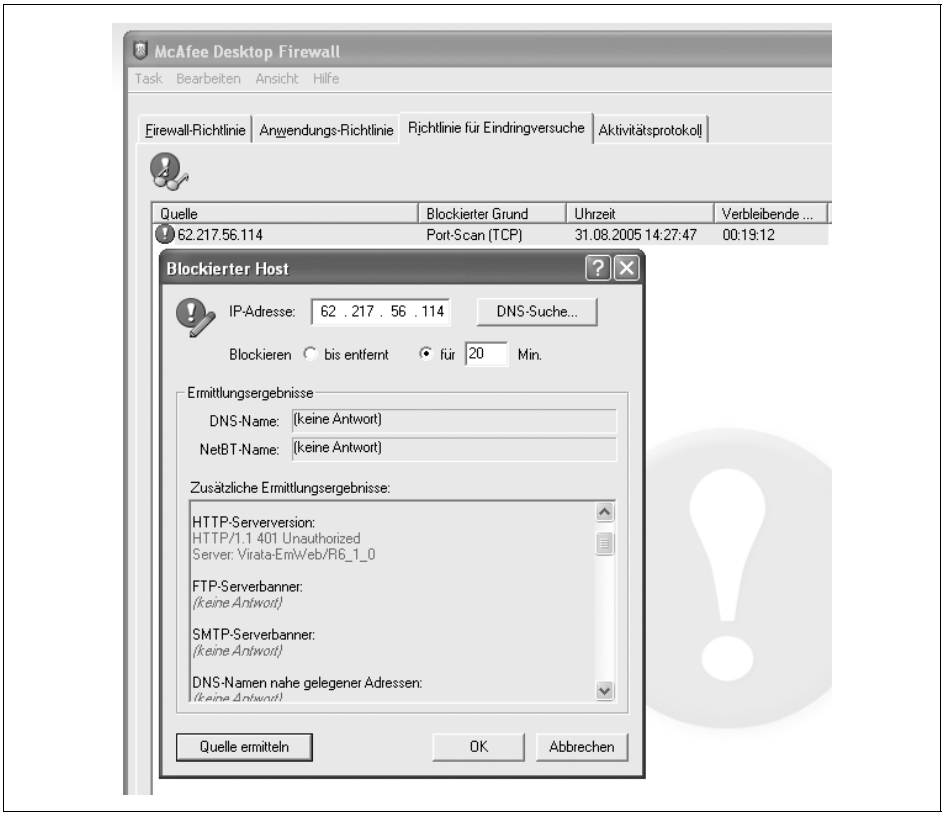

Abbildung 12-8: Mit MacAfee den Angriff zurückverfolgen

Verwaltungsdatenpaket von Ihrem Provider oder das Paket richtet sich an einen Benutzer, der vor Ihnen die dynamische IP-Adresse hatte. Blockieren Sie die IP-Adresse langfristig, kann das unter Umständen zu Problemen mit Ihrer Internetverbindung oder Software kommen (vor allem, wenn man vergisst, die Blockade wieder aufzuheben).

Bei-Zugriff-Scanner

Diese Funktion des integrierten McAfee-Virenscanners folgt eigentlich einer hervoragenden und mittlerweile weit verbreiteten Idee, nämlich Daten direkt beim Zugriff zu untersuchen. Öffnet man also eine bestimmte Datei oder führt ein bestimmtes Programm aus, prüft McAfee automatisch ob dabei Risiken auftreten könnten. Leider ist diese Funktion nicht ganz unproblematisch: Bei größeren oder mehreren zeitgleichen Downloads kann es sowohl bei dem Symantec- als auch dem McAfee-Scanner zu Problemen oder zumindest Verzögerungen kommen. Während der Symantec-Scanner im schlimmsten Fall an Ihren Nerven sägt, kommt es bei dem von McAfee immer wieder zu Problemen mit der Internetverbindung. Dies führt beispielsweise dazu, dass Sie trotz richtiger Firewall-Regeln bestimmte Spiele nicht online spielen können. Wenn Programme also keine Verbindung zum Internet aufbauen können oder sehr langsam laufen (z.B. Thunderbird), ist aller Wahrscheinlichkeit nach der Bei-Zugriff-Scanner das Problem. Sie können diesen daher entweder umkonfigurieren (z.B. das Blocken ausschalten) oder für die Zeit, in der Sie mit dem Programm arbeiten, komplett deaktivieren. Da es inzwischen aber bereits für eine Infektion reicht, eine E-Mail zu lesen oder eine »falsche« Webseite zu besuchen, sei davon dringend abgeraten.

Abbildung 12-9: McAfee erkennt einen Port-Scan von einem fremden Rechner.

Eindringversuch erkannt
: Erkennt McAfee einen Angriffstyp, springt unter lautem Sirenengeheule (nicht erschrecken!) ein Warnfenster auf (siehe Abbildung 12-9). In diesem Fenster haben Sie die Möglichkeit, die IP-Adresse des Angreifers zu sperren und sich zudem das Datenpaket des Angreifers im Detail anzuschauen. Besonders vorbildlich ist, dass McAfee Ihnen eine Einschätzung der Angriffsart und einen verständlichen Text dazu liefert. Kein anderes System bietet Ihnen so viele Informationen und Komfort. Während die Firewall den Port-Scan jedoch noch richtig erkennt, gelang es beim Testen auch, völlig falsche Ergebnisse zu erzielen. Insbesondere geht McAfee allzu schnell von einem DoS-Angriff aus (also einem Angriff, bei dem das Opfer mit sinnlosen Datenpaketen überflutet werden soll).

McAfee-Internetseite
: Die Internetseite von McAfee könnte vom Informationsgehalt leicht mit der Symantec-Seite mithalten, ist jedoch überwiegend in Englisch gehalten und richtet sich zudem eher an fortgeschrittene Benutzer.

Microsoft Windows-Firewall

Seit dem zweiten Service Pack von Windows XP verfügt das Betriebsystem von Haus aus über eine eigene Firewall. Dabei handelt es sich um den ersten Schritt einer sehr umstrittenen Strategie, nach der auch alle Sicherheitslösungen (Firewall, Virenscanner und Spywarefilter[5]) direkt aus dem Hause Microsoft kommen sollen und über kurz oder lang fester Bestandteil des Betriebssystems werden. Dies weckt Erinnerungen an die so genannten Browser- und Instant Messenger-Kriege, in denen es Microsoft mittels dieser Zwangsheirat gelang, in kürzester Zeit sehr große Marktanteile zu gewinnen.

Unabhängig davon wollen wir hier nur sehr kurz auf die Windows-Firewall eingehen, da es sich dabei erstens um eine Minimallösung handelt und das Produkt zweitens noch jung auf dem Markt ist und es daher schwer fällt zu beurteilen, wie die weitere Entwicklung aussehen wird.

Die Windows-Firewall spielt ihre Trümpfe ganz klar bei der Integration aus, sie fügt sich nahtlos in Windows ein und lässt sich für jede Netzwerkverbindung einzeln aktivieren und deaktivieren. Ob eine Netzwerkkomponente (und damit auch die darüber laufende Verbindung) geschützt ist, erkennt man an einem kleinen gelben

5 Zurzeit gibt es Gerüchte, dass sich Microsoft mit einem der größten Spyware-Hersteller geeinigt haben soll und daher bestimmte Spyware nicht mehr als solche gemeldet wird. Inwieweit dies tatsächlich der Fall ist, ist im Augenblick schwer zu beurteilen. Zumindest geht es um viel Geld, und derzeit scheint es fast so, als ob der Begriff der Spyware bald aufgeweicht wird. Spyware könnte also jeweils als das definiert werden, was der Hersteller des Antispyware-Scanners als solches verstehen möchte. Der Fairness halber soll nicht unerwähnt bleiben, dass es ähnliche Vorwürfe auch gegen andere Hersteller von Scannern gibt.

Schlosssymbol rechts oben in der Ecke. Ansonsten gibt es bei der Windows-Firewall nicht viel einzustellen: Sie können Programme explizit freischalten oder sperren, im Grunde genommen arbeitet die Firewall aber selbstständig im Hintergrund. Das schärft zwar nicht unbedingt das eigene Sicherheitsbewusstsein, im Gegensatz zu den Firewalls anderer Hersteller fällt es jedoch positiv auf, dass man beim Surfen eigentlich nicht durch immer neu aufspringende Fenster gestört wird. Leider meint es die Firewall zu gut mit dem Nutzer und meldet sich selbst bei eindeutigen Angriffsvorbereitungen oder DoS-Attacken nicht zu Wort. Es gibt jedoch eine Protokolldatei, in der man einige Informationen über den problematischen Datenverkehr einsehen kann.

Ebenfalls neu (seit Service Pack 2) ist das Sicherheitscenter in der Systemsteuerung (siehe Abbildung 12-10). Dieses kann nicht nur die eigenen Microsoft-Produkte überwachen, sondern arbeitet auch mit den Sicherheitsprodukten anderer Hersteller zusammen und kümmert sich um Updates (sowohl der externen Produkte als auch des Windows-Betriebssystems und des Internet Explorers). Der jeweilige Sta-

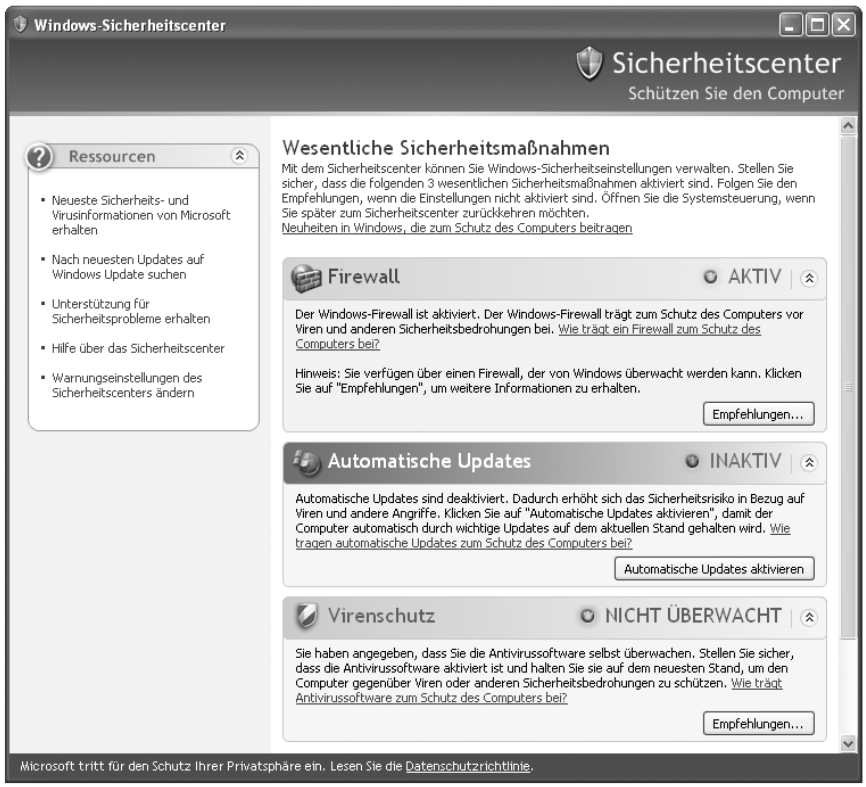

Abbildung 12-10: Das Microsoft-Sicherheitscenter

tus wird durch ein Schildsymbol in der Taskleiste angezeigt. Erscheint das Symbol gelb, gibt es neue Updates, bei Rot ist eine Funktion deaktiviert oder ausgefallen und man sollte dringend nach dem Rechten sehen. Die Updates können zudem völlig automatisiert werden, so dass der Benutzer gar nicht vergessen kann, wichtige Systemupdates herunterzuladen.[6]

Einerseits sollte man skeptisch sein, wenn alle sicherheitsrelevanten Informationen und Tools über ein einziges (noch dazu recht junges) Tool gesteuert werden, andererseits verspricht es endlich den Grad an Einfachheit und Komfort, den gerade Einsteiger dringend brauchen. Insgesamt hinterlässt das Microsoft-Sicherheitscenter daher einen positiven Eindruck. Fortgeschrittene Benutzer können natürlich weiterhin auf andere Lösungen ausweichen und alle wichtigen Einstellungen selber vornehmen.

BackOfficer Friendly

Bei dem Tool *BackOfficer Friendly* (*BOF*) der Firma NFR handelt es sich nicht um eine Firewall im eigentlichen Sinn, sondern um einen so genannten *Honey Pot* (Honigtopf), an dem ein Angreifer sozusagen »kleben« bleibt. BOF täuscht wahlweise einen Back Orifice-Trojaner, HTTP-, Mail(POP/SMTP/IMAP)-, FTP- oder Telnet-Server vor. Versucht nun ein Angreifer auf Ihren Computer zuzugreifen, findet er die angegebenen Ports und wird entweder versuchen, sich Zugriff zu Ihrem System zu verschaffen oder den Trojaner dazu zu benutzen. In Wirklichkeit landen aber alle Anfragen nur bei dem BOF-Tool und stellen daher keine Gefahr für Ihr System dar.

Da BOF sich aber dem Angreifer gegenüber sehr geschickt verhält und den gesuchten Serverdienst vortäuscht, ist es wahrscheinlich, dass dem Angreifer nicht sofort klar wird, dass er einer Täuschung unterliegt. Während der Cracker nun vergeblich versucht, z. B. den Telnet-Zugang zu knacken oder die Antwort des wirklich unendlich langsamen »Webservers« abwartet, sehen Sie auf der Anzeigemaske von BOF, von wo der Angriff ausgeht und welche Daten der Cracker gerade in Ihren »Honigtopf« tippt (siehe Abbildung 12-11).

Zwar bietet dies keinen wirklichen Schutz vor Angreifern, das Tool ist aber ein nettes und für den privaten Einsatz kostenloses Gimmick. Auch wenn BOF nur als eine Spielerei erscheinen mag, soll nicht unerwähnt bleiben, dass Honey Pots sehr häufig als zusätzliche Sicherheitsmaßnahme eingesetzt werden. Dabei bedient man sich

6 Einer solchen Funktion sollten Sie jedoch grundsätzlich skeptisch gegenüberstehen: Zwar ist die Idee sehr gut, jedoch musste Microsoft (auch in der jüngsten Vergangenheit) Updates immer wieder vom eigenen Updateserver zurückziehen, da es zu massiven Problemen bei Kunden gekommen war. Lädt Ihr Betriebsystem alle Updates vollautomatisch, kann das unter Umständen zu einem Problem werden. Noch dazu wäre es denkbar, dass es gelingt, die Updateanfragen des Sicherheitscenters umzuleiten und so beliebig Schad-Code auf den Computer zu bringen. Bis jetzt ist so ein Angriff aber noch nicht aufgetreten.

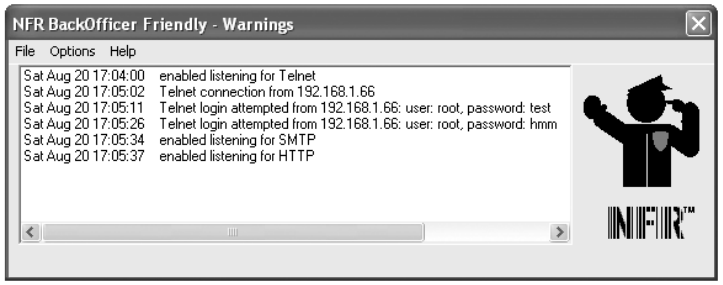

Abbildung 12-11: BOF meldet einen Angreifer, der versucht, sich als root einzuloggen.

professioneller Software, die vortäuscht, dass sich auf diesem Host oder sogar Netzwerk wichtige Informationen befinden, um den so geköderten Cracker genau lokalisieren zu können. Da der vermeintliche Rechner eine Menge bekannter Schwachstellen aufweist, ist er für den Angreifer sehr reizvoll, und dieser verschont so die wirklich wichtigen Systeme.

Erhältlich ist BOF unter *http://www.nfr.com.*[7] Weitere Informationen über professionelle Honey Pots finden Sie im Web unter *http://project.honeynet.org*.

Grenzen von Firewalls

Im Folgenden wollen wir uns anhand von drei Tests vor Augen führen, was Personal Firewalls leisten können und an welchen Stellen ihre Grenzen erreicht sind. Alle beschriebenen Szenarios beziehen sich auf die kostenlose Version der ZoneAlarm-Firewall. Wenn Sie die Tests mitverfolgen möchten, laden Sie sich die Firewall aus dem Internet herunter und installieren Sie diese. Nach dem Test können Sie das Programm bei Bedarf leicht wieder von der Festplatte entfernen oder als Firewall-Lösung behalten.

Shields Up!

Die wichtigste Aufgabe einer Personal Firewall ist, unerwünschten Datenverkehr von Ihrem Computer ins Internet, aber auch umgekehrt den Zugriff von außen auf Ihr System zu kontrollieren und, wenn erwünscht, zu sperren. Dabei ist es auch von Bedeutung, dass die Firewall die Gefahr automatisch einschätzen und dem Benutzer eine Empfehlung geben kann, ob eine Verbindung zugelassen oder abgelehnt werden soll. Gerade bei dieser Aufgabe zeigen sich aber schnell die Grenzen der Personal Firewalls.

7 Leider müssen Sie vor dem Download Ihre persönlichen Daten eingeben, wonach Ihnen eine E-Mail mit dem Download-Link zugeschickt wird.

Um einschätzen zu können, wie sich die Installation einer Firewall auf Ihre Systemsicherheit auswirkt, sollten Sie einmal die verschiedenen Sicherheitstests der *Gibson Research Corporation* unter *https://grc.com/x/ne.dll?bh0bkyd2* durchführen. Diese so genannten »Shields Up!«-Tests bieten Ihnen verschiedene Überprüfungen an. Zum einen können Sie einen Scan Ihrer offenen Ports durchführen (»Common Ports«), zum anderen kann »Shields Up!« versuchen, Zugriff auf Ihr System zu erlangen (»File Sharing«). Beide Tests sollten Sie zuerst ohne und anschließend mit gestarteter Firewall durchführen. Ist diese richtig konfiguriert, werden beide Tests keine Sicherheitslücken aufzeigen.[8]

Besonders interessant ist der File Sharing-Test. Hierbei versucht das Programm, über Port 139 mit dem NetBIOS-Protokoll auf die von Ihnen freigegebenen Ordner zuzugreifen. Dabei handelt es sich zwar um keine Sicherheitslücke im eigentlichen Sinn, Fakt ist jedoch, dass viele Einbrüche in Windows-Systeme auf diesem Weg erfolgen. Im Internet finden sich auch zahlreiche so genannte *Sharescanner*, mit deren Hilfe Angreifer über das weltweite Netz heimlich Zugriff auf Ihre freigegebenen Daten erlangen und so Daten ausspionieren oder sogar verändern können. Dies funktioniert selbst dann, wenn diese Daten passwortgeschützt sind.

Alle hier vorgestellten Firewalls absolvieren den Test ohne Probleme, mit der Einschränkung, dass Norton die davon ausgehende Gefahr herunterspielt und für ein »geringes« Sicherheitsrisiko hält.

Angriff auf die Host-Datei

Nehmen Sie sich einen Moment Zeit und schauen sich die Abbildung 12-12 genauer an, was stimmt dort nicht?

Wahrscheinlich haben Sie nun zwei Ungereimtheiten entdeckt, denn sowohl in der Adressleiste als auch in der Statusleiste steht »ebay« anstelle von »O'Reilly«. Wenn Sie nun die Adresse aus der oberen Leiste (*http://www.ebay.de/catalog/sii2ger/index.html*) direkt in Ihren eigenen Browser tippen, werden Sie feststellen, dass es diese Seite bei eBay überhaupt nicht gibt. Wenn Sie aber nun »ebay« durch »oreilly« ersetzen, landen Sie auf der richtigen Seite – was ist passiert?

Bei der Beschreibung der ZoneAlarm-Firewall sind wir kurz auf die *hosts*-Datei zu sprechen gekommen. Die *hosts*-Datei ist eigentlich ein längst vergessenes Überbleibsel aus einer anderen Computerära und verstaubt seit vielen Jahren im Windows-Betriebssystem.[9] Ursprünglich war die *hosts*-Datei (und ist es unter anderen

8 Einen Blick Wert ist auch der »Messenger Spam«-Test mit dessen Hilfe Sie prüfen können, ob »net send« nach außen verfügbar ist. Dies macht sich in der Regel durch merkwürdige Windows-Popup-Meldungen bemerkbar, in denen Sie aufgefordert werden, angebliche Windows-Updates herunterzuladen. Über einige Monate hinweg war dies eine sehr beliebte Art, Spam zu verbreiten oder Socal Engineering-Attacken zu starten, ist jetzt jedoch weitgehend ausgestorben.

9 Unter WinXP befindet Sie sich unter *C:\Windows\system32\drivers\etc*.

Abbildung 12-12: Die Suchfunktion des Online-Katalogs von O'Reilly

Betriebssystemen immer noch) ein Ort, an dem man lokal (vergleichbar mit DNS und WINS) die IP-Adresse einem durch Menschen lesbaren Rechnernamen zuordnen konnte. Als einziger Eintrag findet sich dort nur noch der *localhost*, also Ihr eigener Rechner. Die Zeile »127.0.0.1 localhost« (siehe Abbildung 12-13) bedeutet also, dass Sie Ihren eigenen PC sowohl über die IP 127.0.0.1 als auch über *localhost* ansprechen können. Während man früher beispielsweise den Server eines lokalen Netzwerks in diese Datei eintrug, wird sie heutzutage unter Windows nicht mehr benutzt. Nichtsdestotrotz kann man dort Einträge vornehmen, die anschließend von Windows ausgewertet werden. Trägt man dort nun die IP-Adresse von *www.oreilly.de* (62.206.71.33) ein und behauptet, dabei handele es sich um *www.ebay.de*, so übernimmt Windows diese Informationen.

Sie können dem Beispiel in Abbildung 12-13 gern folgen, es birgt keinerlei Risko in sich. Wenn Sie nun »www.ebay.de« in Ihren Browser tippen, so stellt dieser keine Anfrage an den DNS-Server um herauszufinden, wie die Adresse des Rechners *www* in der Domain *ebay.de* lautet, da er diese Information bereits von Windows bekommt (eben über besagte *hosts*-Datei). Daher verbindet sich der Browser direkt mit *62.206.71.33* und landet folglich auf der Internetseite von O'Reilly.[10] Dieses kleine Experiment mag auf den ersten Blick wenig eindrucksvoll erscheinen, wenn

10 Wenn Sie nicht mehr ganz sicher sind, weshalb dem so ist, können Sie dies noch einmal im Kapitel 2, *Technische Hintergründe*, nachschlagen.

Sie aber auf die Statusleiste Ihres Browsers (oder der Abbildung 12-12) blicken, werden Sie feststellen, dass der Browser alle weiterführenden Links ebenfalls mit falschem Namen auslöst. Hätte ein Angreifer Sie nun nicht auf O'Reilly sondern auf einen exakten Nachbau von eBay gelotst, wären Sie völlig chancenlos. Im Falle des klassischen Phishing wird immer wieder als Tipp genannt, niemals Links aus E-Mails anzuklicken, sondern die Webadresse selber einzutippen, aber gerade dies funktioniert hier nicht. Sie können die Adresse per Hand eingeben oder aus Ihren Bookmarks auswählen, in jedem Fall landen Sie auf der gefälschten Seite. Genauso gut könnte man so auch die Update-Anfragen von Sicherheitstools oder anderen Programmen umleiten und Schad-Code unterschieben.

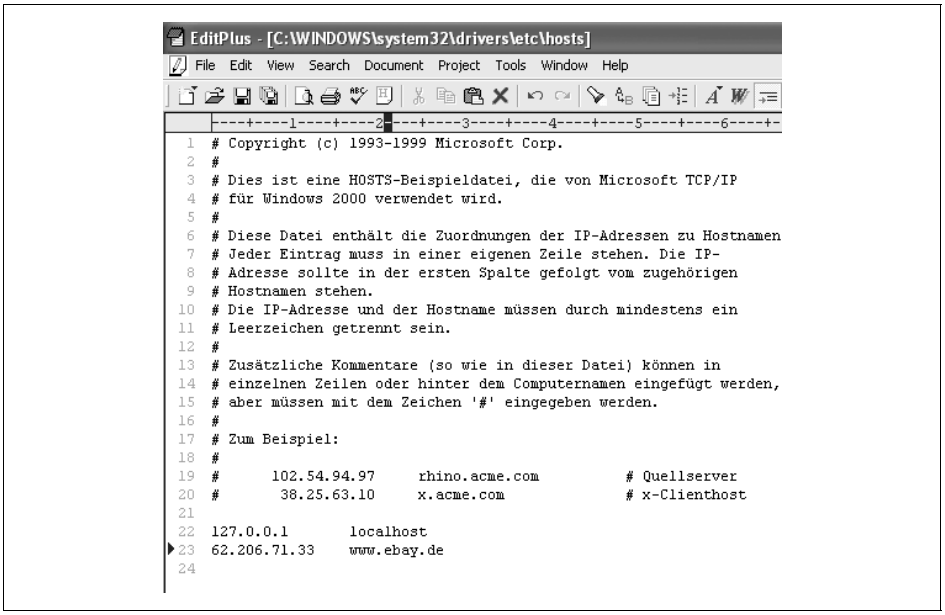

Abbildung 12-13: Die manipulierte hosts-Datei

Fatal daran ist, dass die meisten Personal Firewalls die *hosts*-Datei nicht beachten. Dabei wäre es ein Leichtes, per eigener DNS-Anfrage gegenzuprüfen, ob die IP tatsächlich stimmt, oder einfach Änderungen in der Datei mit einem Warnfenster absichern. In ZoneAlarm hingegen können Sie die *hosts*-Datei schützen. Ist diese Option aktiviert, haben andere Programme keinen Schreibzugriff und können daher keinerlei Änderungen durchführen. Bisher sind wenige Angriffe dieser Art bekannt geworden, jedoch wird sich die fehlende Sorgfalt zahlreicher Sicherheitslösungen schnell herumsprechen. Hat ein Trojaner dann erst einmal die Datei verändert, stört es den Angreifer nicht weiter, wenn sein Werkzeug später von einem Virenscanner erkannt und entfernt wird, die Umleitungen aus der *hosts*-Datei bleiben weiterhin aktiv. Einen Wurm, der diesen Angriff nutzt, haben wir bereits im vorigen Kapitel besprochen, weitere werden mit Sicherheit folgen.

Wer darf ins Netz?

In diesem Abschnitt wollen wir uns anhand von ZoneAlarm ein weit verbreitetes Problem der Personal Firewalls im Allgemeinen anschauen. Werfen wir dazu noch einmal einen Blick auf die Abbildung 12-2. Die Meldung besagt, dass *opera.exe* versucht, auf den DNS-Dienst des lokalen Rechners *192.168.1.1* zuzugreifen. Wollen Sie das erlauben? Um das wirklich einschätzen zu können, müssen Sie in der Lage sein zu beurteilen, was *opera.exe* ist, welcher Rechner *192.168.1.1* ist und ob besagtes *opera.exe* eine DNS-Abfrage an diesen richten darf. Wie bereits erwähnt, ist ZoneAlarm etwas übervorsichtig mit dem lokalen Netz. Das ist zwar grundsätzlich sinnvoll, denn viele Angreifer kommen entweder von innerhalb des eigenen Netzes oder vermögen ihre tatsächliche IP-Adresse hinter einer fremden (z.B. lokalen) Adresse zu tarnen, aber diese Vorsicht bewirkt letztendlich, dass der Benutzer abstumpft und Meldungen im Schnelldurchgang wegklickt.

Der Rechner, den *opera.exe* hier anfragt, ist ein (WLAN-)Router, der die Anfragen mehrerer Rechner über einen gemeinsamen DSL-Anschluss ins Netz leitet. Solche Router senden regelmäßig Verwaltungsnachrichten an die angeschlossenen Computer, auch hier springt jedes mal ein ZoneAlarm-Warnfenster auf. Wie Sie bereits wissen, ist Opera ein Browser, der somit zwangsläufig DNS-Abfragen starten muss, um die IP-Adresse des gesuchten Servers herauszufinden. Somit können wir hier ohne Bedenken auf ZULASSEN klicken, richtig? Scheinbar ja, in Wirklichkeit habe ich jedoch ein winzig kleines Programm geschrieben und es schlicht und einfach *opera.exe* genannt, noch dazu sendet es zwar Daten an den Port 53 (DNS), dabei handelt es sich jedoch um keine echten DNS-Anfragen, sondern um kurze Zeichenketten, die etwa Passwörter sein könnten. Die allermeisten Personal Firewalls achten nur auf die Portnummern oder einige Verbindungsdetails – was letztendlich übertragen wird, ist also unklar. Selbst für den Fall, dass die Firewall das DNS-Protokoll wirklich verstehen könnte, bliebe einem Angreifer immer noch die Möglichkeit, Anfragen wie etwa *www.daserbeutetepasswort.de* an einen Server seiner Wahl zu schicken.

Um wirklich sicherzustellen, dass Sie nicht gerade einem Trojaner Tür und Tor öffnen, brauchen Sie neben dem reinen Programmnamen weitere Eckdaten. Zahlreiche Personal Firewalls bieten Ihnen dazu weiter gehende Informationen wie den Namen des Herstellers, die Versionsnummer und den Pfad (also das Verzeichnis), in dem sich das Programm befindet. Theoretisch lassen sich auch diese Informationen fälschen, das ist jedoch schon um ein Vielfaches komplizierter, und es geht uns ja darum, kein einfaches Ziel zu sein. Klicken Sie die Meldungen der Firewall daher niemals sorglos weg, sondern nutzen Sie alle gebotenen Informationsmöglichkeiten und Hilfsfunktionen. Leider macht es Ihnen Windows zusätzlich kompliziert, indem es kryptische Namen verwendet. Wenn Sie eine Personal Firewall auf ihrem PC betreiben, werden Programme wie *rundll32*, *lsass* oder *svchost* früher oder später versuchen, auf das Internet zuzugreifen. Dabei handelt es sich um Windows-Kom-

ponenten, weshalb der Zugriff zugelassen werden sollte. Unglücklicherweise benennen sich zahlreiche Trojaner analog zu diesen Programmen, so handelt es sich bei *rundll16* oder *svhost* um bösartige Software, der Sie unter keinen Umständen das »Nach-Hause-Telefonieren« erlauben sollten. Um die Situation noch verzwickter zu machen, nisten sich diese Programme im Windows-Verzeichnis ein, so dass der Programmpfad trügerisch sein kann.

Im Internet gibt es zahlreiche Seiten, die über die meisten harmlosen und gefährlichen Prozessnamen Buch führen und zahlreiche Informationen zu möglichen Gefahren bieten. Da man Ihnen dort häufig das eigene Sicherheitsprodukt verkaufen möchte, verzichten wir hier auf einen Weblink.[11] Generell können Sie aber nach folgender Taktik vorgehen: Versucht ein Programm, bei dem sie nicht hundertprozentig sicher sind, auf das Internet zuzugreifen, verbieten Sie den Zugriff zunächst; arbeitet dann alles so weiter, wie Sie wünschen, ist das Programm entweder nicht nötig gewesen oder ein Schädling. Sehr viele kommerzielle Produkte versuchen, sich mit dem Server des Herstellers zu verbinden, um nach Updates zu suchen oder sich aus anderen (weniger erwünschten) Gründen beim Hersteller zu melden. Verbieten Sie diesen Programmen den Zugriff, ärgert sich zwar der Hersteller, für Sie hat dies jedoch keinerlei Konsequenzen. Sollte hingegen nach dem Zugriffsverbot eine Software nicht ordentlich arbeiten oder die Updatefunktion blockiert sein, können Sie die Software manuell in der Personal Firewall freischalten. Wenn sich die Firewall zu häufig meldet und Ihren Arbeitsfluss stört, sollten Sie den Meldelevel (nicht den Sicherheitslevel!) herunterschrauben.

Fazit

Insgesamt lässt sich den Personal Firewalls ein positives Gesamturteil ausstellen. Negativ fällt bei einigen Produkten eine teilweise deutlich spürbare Geschwindigkeitsverzögerung auf. Zudem haben viele Firewalls anscheinend Probleme mit dem lokalen Netz. So kann es beispielsweise zu Störungen in der Kommunikation der lokalen Systeme untereinander kommen. Häufig wird berichtet, dass einzelne Computer im Netzwerk nicht mehr sichtbar sind oder der Zugriff generell blockiert wird. Zwar bieten die meisten Produkte für genau solche Fälle die Möglichkeit an, weniger restriktive Regeln für das lokale Netz zu verwenden, dennoch kann es gerade bei ansonsten schnellen Netzverbindungen zu Verzögerungen beim Öffnen von Dokumenten aus dem Netzwerk kommen. Daher sollten die Produkte nur bei Einzelplatz-PCs oder kleinen Hausnetzwerken zum Einsatz kommen.

Ein weiteres Problem ergibt sich aus der Struktur der Personal Firewalls: Während professionelle Firewalls immer auf einem eigenen Rechnersystem laufen, sind Perso-

11 Die meisten dieser Seiten sind dennoch informativ und empfehlenswert. Geben Sie einfach »rundll32« oder »Task Manager Prozesse« in Ihre Internetsuchmaschine ein.

nal Firewalls zwangsläufig auf demselben System installiert wie die Benutzerdaten und sämtliche Software. Dadurch ergeben sich für Trojaner und Würmer interessante Angriffsmöglichkeiten, die auch schon in einigen Fällen dazu geführt haben, dass die Firewall einfach umgangen oder vorher schlicht und ergreifend vom Trojaner deaktiviert wird. Der Vorsprung, den man sich gegen mögliche Angreifer erkämpft hat, ist also nicht so groß wie vielleicht erhofft. Daher kann der Einsatz dieser Produkte nur als eine zusätzliche Maßnahme aufgefasst werden und nicht als alleinige Lösung.

Es sei jedoch deutlich darauf hingewiesen, dass eine Personal Firewall inzwischen zur absoluten Grundausrüstung gehören sollte; entscheidet man sich gegen ein kostenpflichtiges Paket, sollte man wenigstens die Lösung von Microsoft oder ZoneAlarm benutzen. Neben den hier vorgestellten Firewall-Produkten gibt es noch eine Vielzahl kostenloser und kostenpflichtiger Produkte, die einen genaueren Blick wert sind.