In diesem Kapitel:

- Kurze Geschichte der Malware
- In the wild – In the zoo
- Artenkunde
- Virenkalender
- Würmer
- Trojaner
- Spyware
- Bots und Botnets
- Vorsichtsmaßnahmen gegen Malware
- Antiviren-Software
- Ausblick auf die weitere Entwicklung

KAPITEL 10
Viren, Würmer und Trojaner

In diesem Kapitel wollen wir uns mit dem großen Thema der schädlichen Programme und Skripten (*Malware*) beschäftigen. Dabei werden wir zuerst die historische Entwicklung betrachten und danach unsere Definitionen aus Kapitel 1, *Gefahren und Akteure im Internet*, vertiefen und genauer auf die Art der verschiedenen Schädlinge eingehen. Besonders eingehend wollen wir uns mit Trojanern, Spyware und Botnets befassen, die zu immer wichtigeren Angriffsmitteln werden. Abschließend werden wir uns den Themen Virenschutz[1] und Antivirensoftware widmen.

Das Jahr 2001 war ein ausgesprochen wichtiges Jahr im Bezug auf Computersicherheit. Die Anzahl und Verbreitung gefährlicher Würmer und Trojaner war überproportional stark, und es zeichneten sich zwei wichtige Paradigmenwechsel ab. Einerseits verschmolzen Würmer und Trojaner zu einem gemeinsamen komplexen Angriffswerkzeug, andererseits begann sich die Crackerszene von Computerfreaks und Pionieren zu organisierten Kriminellen zu wandeln.

Das Jahr 2001 bietet daher weiterhin ausgezeichnete Möglichkeiten, hinter die Kulissen dieser Entwicklungen zu schauen. Aus diesem Grund wollen wir die detaillierten Beschreibungen einiger besonders auffälliger Würmer und Trojaner aus diesem Jahr beibehalten und das Kapitel um zwei neue aus dem Jahr 2004 ergänzen.

1 Die Bezeichnung *Virus* wird häufig als Oberbegriff für schädlichen Code im Allgemeinen benutzt und umfasst in diesem Sinn Würmer und andere Schädlinge. Zwar unterscheiden sich die verschiedenen Arten von Malware zum Teil stark; wo es uns nicht um Details geht, werden wir diesen Sprachgebrauch jedoch übernehmen.

Kurze Geschichte der Malware

Als Erfinder der Computerviren wird im allgemeinen Fred Cohen angesehen. Fred hatte sich im Rahmen seiner Doktorarbeit mit dem Thema »selbstvermehrende Software« befasst und im Laufe seiner Studien (1981-84) auch den ersten echten Virus programmiert. Die Idee der Viren ist jedoch schon viel älter und geht bis in das Jahr 1949 zurück. Erste Umsetzungen von würmer- und virenähnlicher Software gibt es schon seit den 70er Jahren (*Core Wars* war das erste wurmähnliche Programm), wir wollen unseren Überblick aber erst mit den 80ern beginnen.

1982

Jon Hepps und John Shock von Xerox PARC programmierten die ersten bekannt gewordenen Würmer. Diese sollten eigentlich nur intern genutzt werden, um verteilte Berechnungen durchzuführen. Durch einen Programmfehler gerieten sie jedoch außer Kontrolle und vermehrten sich selbstständig. Am Ende mussten daher zahlreiche überlastete Systeme neu gestartet werden.

1986

Der erste PC-Virus wurde entdeckt. Dabei handelte es sich um den so genannten *Brain*-Virus aus Pakistan. Er wurde von zwei Raubkopierern entwickelt und mit deren Kopien verbreitet. Um so erstaunlicher ist es, dass *Brain* nicht nur viel Schaden in Asien, sondern auch in den USA anrichtete. Immerhin muss man bedenken, dass der Virus nicht über das Internet, sondern nur mittels raubkopierter Disketten verbreitet wurde.

1987

Der *Jerusalem*-Virus tauchte als der erste speicherresistente Virus in Israel auf. Er erreichte vor allem deshalb großes Aufsehen, weil er noch jahrelang in verschiedenen, leicht modifizierten Versionen weiterlebte. Bei der *Freitag-der-13.*-Variante kam erstmals eine Zeitkomponente ins Spiel, und das Ausmaß der Schäden steigerte sich von einfachen »Belästigungen« hin zum Beschädigen von *.exe*- und *.com*-Dateien.

Von einem Studenten aus Neuseeland (Universität von Wellington) entwickelt, erschien der *Stoned*-Virus als erster *Master Boot Record*-Virus (MBR). Er erreichte schnell eine große Verbreitung und wurde bereits beim Systemstart aktiv.

1988

Die erste »Antivirensoftware« wurde entwickelt. Aus heutiger Sicht verdient sie zwar diesen Namen noch nicht, wies jedoch den Weg für die zukünftige Entwicklung.

Im November 1988 infizierte der Internetwurm von Robert Morris (damals Doktorand an der Cornell Universität in Ithaca, New York) innerhalb kürzester Zeit über 6.000 Computer und damit etwa 10% aller damals vorhandenen Hosts im Internet. Morris wurde daraufhin verhaftet und zu einer Bewährungs-

strafe von drei Jahren sowie einer Geldstrafe verurteilt. Als Reaktion darauf wurde das CERT (*Computer Emergency Response Team*) ins Leben gerufen.

Ebenfalls 1988 tauchten die ersten *Virus Construction Kits* – zum Beispiel für den Atari ST – auf. Damit war es erstmals möglich, immer neue Computerviren mittels einer einfachen Software zu generieren.

1989

In Israel wurde *Frodo*, der erste Tarnkappenvirus, entdeckt, der sich durch die Infektion von Dateien ausbreitete.

Das legendäre Antivirenprogramm von McAfee erschien in der ersten Version und erkannte die damals unglaubliche Zahl von 44 unterschiedlichen Viren. Die Konkurrenz brachte es zu dieser Zeit gerade mal auf knapp 20.

1990

Aus den USA kamen die ersten Berichte über polymorphe und *Stealth*-Viren, die in der Lage sind, sich selbst zu modifizieren. Das erste Virus Construction Kit für DOS erschien. 1989/90 begannen auch die ersten trojanischen Pferde Fuß zu fassen, damals aber noch bevorzugt auf Macintosh-Systemen.

1991

Die beiden Organisationen EICAR (*European Institute for Computer Anti-Virus Research*) und CARO (*Computer Anti-Virus Research Organisation*) wurden gegründet. Gleichzeitig stieg die Zahl der Viren in »freier Wildbahn« rasant an. Ebenfalls 1991 wurde der berühmte *Michelangelo*-Virus entdeckt; ein Jahr später löste er eine erste Virenhysterie aus. Gleichzeitig wurde Virenprogrammieren zum verbreiteten Hobby, entsprechende Zeitschriften entstanden, und regelrechte Meisterschaften wurden ausgetragen.

1992

Unter dem Pseudonym »Dark Avenger« veröffentlichte ein Programmierer eine *Mutation Engine*, die es von nun an ermöglichte, aus einfachen Viren polymorphe zu machen. In der folgenden Zeit erschienen noch über 60 weitere *Mutation Engines*. Zudem wurden 1992 die ersten Viren entdeckt, die das noch sehr junge MS Windows-Betriebssystem befallen konnten.

1994

Der erste echte Internetvirus (*Kaos5*) tauchte im Usenet auf. Er breitete sich vor allem über die Newsgroup *alt.binaries.pictures.erotica* aus.

1995

Die ersten Viren für Windows 95 erschienen. Das Internet wurde zunehmend zum Hauptverbreitungsmittel für Viren und löste Datenträger wie Disketten o. Ä. schon bald ab. Gleichzeitig erschienen die ersten Makroviren, die im Verlauf der nächsten drei Jahre zu den am häufigsten vorkommenden Virenarten werden sollen. *Concept* gilt als der erste Virus, der diesen Sprung von der Programmdatei zum Dokument geschafft hat.

»Black Baron« (Christopher Pile), einer der berühmtesten Virenprogrammierer, wurde verhaftet und bekannte sich der Computerkriminalität in elf Fällen für schuldig.

1996

Mit *XM.Laroux* erblickte der erste Excel-Virus das Tageslicht. Die MS-Makrosprache im *Office*-Paket erlaubte nun auch das Erstellen gefährlicher Viren ohne die dazu bisher nötigen Assembler- oder C-Programmierkenntnisse. 1996 wurde die Zahl existierender Viren auf 10.000 geschätzt. Dabei zeichnete sich auch schon der Trend in Richtung Windows-Viren deutlich ab. Während sichere Betriebssysteme wie Unix weiterhin nur mit wenigen Viren konfrontiert wurden, stieg die Zahl der Windows-Viren erheblich. Zeitweise verschwanden Unix-Viren sogar fast ganz.

1997

Der erste Linux-Virus wurde von McAfee entdeckt. Böse Zungen behaupteten, dass seine Entstehung mit der Markteinführung des McAfee-Virenscanners für Linux in Verbindung stand. Zudem erweiterten sich die Ausbreitungsmöglichkeiten nochmals, so dass sich auch ein erster Virus über das Internet-Chatsystem IRC vermehrte.

1998

Spätestens seit 1998 verbreiten sich Viren blitzschnell über das Internet und richten so erheblichen Schaden an. Die Zahl der Schädlinge und ernsthaften Vorfälle hat so stark zugenommen, dass wir im Folgenden nur noch einen kleinen Auszug der wichtigsten Meilensteine betrachten können.

NetBus wurde von Carl-Fredrik Neikter veröffentlicht und verbreitete sich als einer der mächtigsten Trojaner schnell im Internet. Mittels *NetBus* kann man infizierte Computer fernsteuern. Einige Monate später veröffentlichte der »Cult of the Dead Cow« den berühmtesten aller Trojaner namens *Back Orifice*. Damit war die Tür für die größten Angriffe der Zukunft offen, und von nun an wurde *Back Orifice* zusammen mit dem später erschienenen *SubSeven* zum wichtigsten Angriffswerkzeug auf Windows-Clientsysteme.

Mit *VBS.Rabbit* erschien der erste Skript-Virus, der in Visual Basic Script geschrieben wurde.

Mit dem *CIH*-Virus entstand der bis dahin gefährlichste Virus. Er versuchte, das BIOS des befallenen Computers zu überschreiben und richtete damit erstmals Schäden an der Hardware an. Glücklicherweise verbreitete er sich nicht so schnell und stark wie befürchtet. Am 26. April 1999 richtete er in Asien jedoch erheblichen Schaden an. Auch hier war der Programmierer ein Student (Chen Ing-Hau).

1999

Der *Melissa*-Wurm wurde entdeckt. Er breitete sich über E-Mails aus und verschickte sich an bis zu 50 weitere Personen aus dem Adressbuch des Infizierten. Da er nur Outlook-Benutzer angreifen konnte, wurde starke Kritik an Micro-

softs Skriptpolitik geübt. Erstmals wurde in vollem Umfang klar, wie gefährlich die Monokultur unter den Mail-Clients wirklich sein kann. *Melissa* breitete sich so schnell aus, dass zahlreiche Mailserver unter der Last zusammenbrachen und das Internet stellenweise deutlich verlangsamt wurde. David L. Smith wurde als Programmierer des Virus verhaftet.

Unerklärlicherweise schafften es aber noch zwei weitere Viren, unter Verwendung von Outlook erheblichen Schaden anzurichten. Dazu zählte einerseits *ExploreZip*, der Dateien mit der Endung *.doc*, *.xls* und *.ppt* zerstörte, und andererseits *VBS.BubbleBoy*. Dieser ist besonders interessant, da er bereits beim Lesen einer E-Mail gestartet wurde. Das Öffnen eines Attachments war also nicht mehr nötig.

2000

Der *I LOVE YOU*-Wurm brach aus und verbreitete sich viel stärker und schneller als je ein Schädling vor ihm. Trotz der immer wiederholten Warnung, keine unbekannten oder unerwarteten Attachments zu öffnen, befiel *I LOVE YOU* mehrere hunderttausend Hosts und richtete vor allem bei größeren Unternehmen erheblichen Schaden an. Zahlreiche Mailserver im Internet brachen unter der Nachrichtenlast zusammen. Der Erfolg des Virus ist umso erstaunlicher, wenn man weiß, dass er im Prinzip dem *Melissa*-Virus sehr ähnlich ist. Zahlreiche Viren versuchten daraufhin, auf den VBS-Outlook-Zug aufzuspringen, teilweise auch mit Erfolg.

2000 erschien auch der erste Virus für PDAs.

Im Frühjahr 2000 fanden zudem die ersten großen DDoS-Angriffe gegen große Internetanbieter wie Yahoo, Amazon und eBay statt. Wir zählen sie hier unter der Geschichte der Viren, Würmer und Trojaner auf, da diese verteilten Überlastungsangriffe mittels vieler hundert durch Trojaner ferngelenkter PCs stattfanden (während deren Benutzer meist nichts davon wussten). Seither finden jedes Jahr zahlreiche solcher Angriffe statt und legen Internetangebote teils über Tage komplett lahm.

2001

Das Jahr 2001 stellte in jeder Hinsicht neue Rekorde bezüglich der gefährlichsten und am weitesten verbreiteten Würmer auf. Zudem läutete es eine Trendwende in der Entwicklung der Würmer ein, indem zunehmend eigene Serverdienste und Hintertüren in den Code integriert wurden und daher die Grenze zwischen Würmern und Trojanern immer mehr verschwand. Die Würmer aus dem Jahr 2001 sind wahre Alleskönner. Das beste Beispiel hierfür sind wohl *SirCam* und *Nimda*, aber auch andere weisen eine unglaubliche Fülle an Funktionen auf. Zugleich wurden auch die Grenzen der Betriebssysteme überwunden, so dass es inzwischen Viren und Würmer gibt, die Linux und Windows gleichermaßen befallen. Es entstanden sogar Würmer, die andere Würmer suchen und eliminieren, auch diese »guten« Würmer bergen aber gewisse Gefahren in sich. Zugleich tauchten die ersten Würmer auf, die Chat

und Instant Messenger heimsuchten. Auch Dialer, mit denen wir uns in Kapitel 11, *Angriffsszenarien*, genauer befassen werden, sorgen für massiven finanziellen Schaden. Ganz neu unter den Schädlingen ist auch die uns aus dem Kapitel 3, *Sicherheitsbewusstsein,* bekannte Spyware.

Für *CodeRed* und ähnliche Würmer wurde der Begriff der *fileless worms*[2] geprägt. Er bezeichnet Schädlinge, die sich über Datenpakete statt anklickbare Dateien verbreiten (der Begriff setzte sich jedoch nicht durch).

Aus dem Auftauchen von *Nimda* lässt sich einiges über die weitere Entwicklung im Bereich der Malware folgern, daher werden wir uns später die vier bekanntesten Schädlinge dieses Jahres etwas genauer anschauen.

2002

Nach dem vorläufigen Höhepunkt 2001 wurde es 2002 deutlich ruhiger. Das Sicherheitsbewusstsein der Anwender und vor allem Unternehmer hatte spürbar zugenommen. Das bedeutet jedoch nicht, dass es weniger Würmer gab, sie erreichten nur keine so große Verbreitung wie in den Jahren zuvor. Ein dennoch sehr erfolgreicher Wurm, der in verschiedensten Variationen sogar bis 2005 überdauerte, war der *Benjamin*-Wurm, der das populäre KazaA-Netz befiel und zehntausende Computer von Tauschbörsennutzern infizierte. Erwähnt werden soll noch, dass *CodeRed* (ebenfalls in verschiedenen Versionen) sich auch 2002 immer noch ausbreiten konnte.

Viel interessanter als die verschiedenen Würmer und Trojaner des Jahres 2002 ist jedoch der allmählich spürbare Wandel innerhalb der Virenschreiber-Community. Je populärer und allgegenwärtiger das Internet wurde, desto mehr begannen auch politische und soziale Themen eine Rolle bei den Crackern zu spielen. So griffen beispielsweise indische Cracker mit dem *Yaha.E*-Wurm und dem daran gekoppelten DoS-Tool die Internetseite der pakistanischen Regierung an. Der *Bugbear*-Wurm dagegen interessierte sich für Kreditkartennummern und Passwörter.

2003

Das Jahr 2003 begann mit einem großen Paukenschlag, der zeigen sollte, dass sich an der typsichen Windows-Sicherheitsproblematik in all den Jahren kaum etwas getan hatte. Gleich zwei Würmer legten das Internet im Januar 2003 stellenweise komplett lahm oder verzögerten Zugriffe massiv. Der *Sobig*-Wurm erreichte eine erhebliche Verbreitung, obwohl er nach dem immer gleichen Schema funktionierte, in dem man eine merkwürdige E-Mail öffnen und eine Anlage eigenständig per Doppelklick ausführen muss. Auf den Erfolg von *Sobig* folgten zahlreiche verwandte Würmer (auch aus Deutschland).

Viel gefährlicher war jedoch *SQLSlammer*, ein Wurm, der den Microsoft SQL-Server und Windows-Installationen mit Microsoft Desktop Engine 2000 befiel

2 Was man etwa mit »dateilose« oder »dateifreie« Würmer übersetzen könnte.

und damit viele zehntausend Server im Internet lahm legte. Dabei enthielt der Wurm nicht einmal einen Schad-Code im üblichen Sinn, sondern nutzte einfach die gesamte Bandbreite der befallenen Server, um sich mittels eines einzigen UDP-Datenpaketes (der Wurm war klein genug, um dort komplett hineinzupassen) weiterzuverbreiten. In den USA fielen sogar mehr als 10.000 Bankautomaten aus, und selbst die Rechner bei Microsoft waren massiv betroffen. Zwar konnten Provider den Wurm durch das Blockieren des UDP-Paketes an Port 1434 schnell unschädlich machen, zeitweise waren aber über 300.000 Rechner befallen und ganze Bereiche des Internets komplett ausgefallen.

Ebenso darf der *LoveSAN/W32.Blaster*-Wurm nicht unerwähnt bleiben. Dieser nistete sich auf hunderttausenden von PCs ein und versuchte, eine DDoS-Attacke gegen den Updateserver von Microsoft zu starten.[3]

2004

Während in der Vergangenheit Würmer zunächst Windows, später auch Linux, Serverdienste und Internetapplikationen (z.B. Messenger, Tauschbörsen) befielen, erweiterte sich die Palette der Angriffsziele zunehmend auch um weit verbreitete Webseitenapplikationen. So befiel 2004 der Wurm *Santy* etwa 40.000 Internetforen, die mit der beliebten Open Source-Software *phpBB* betrieben wurden.

Unter den zahlreichen Würmern des Jahres sind *Sasser* und *Phatbot*[4] interessant. Dabei handelt es sich um zwei Schädlinge, die unterschiedlicher nicht sein könnten und dennoch erst zusammen zu einer echten Gefahr wurden. Beide infizierten Schätzungen zufolge mehr als eine Million PCs und richteten auf sehr unterschiedliche Weise Schäden in Millionenhöhe an. Wir wollen daher später genauer auf beide eingehen.

Seit 2003/2004 bekriegen sich die verschiedenen Virenschreibergruppen teils auch gegenseitig und hinterlassen Nachrichten im Quell-Code der eigenen Schädlinge. Zudem versuchen die entsprechenden Würmer, die Konkurrenz auf den befallenen PCs auszuschalten. Besonders deutlich wurde dies 2004 bei *Netsky* und *MyDoom*, die gegenseitig versuchten, sich von befallenen PCs zu entfernen. Dies mag auf den ersten Blick absurd erscheinen, macht aber plötzlich Sinn, wenn wir uns in einem späteren Abschnitt mit so genannten *Botnets* beschäftigen.

---

3 Etwas später folgten neben etlichen Varianten auch ein Wurm namens *W32.Welchia.Worm* (der Name stammt von Symantec, andere AV-Experten benannten den Wurm teils anders, z.B. *W32/Nachi.worm*, der in Computer einbrach, um dort den *LoveSAN/W31.Blaster*-Wurm (auch hier geht der Doppelname auf die unterschiedliche Benennung durch verschiedene Experten zurück) zu entfernen.

4 Der (deutsche) Enwickler von Phatbot war außerdem anscheinend am spektakulären Raub des Quell-Codes zu Halflife2 beteiligt. Dabei drangen Angreifer in das Computernetzwerk des Spieleherstellers Valve ein, erbeuteten den Programm-Code des lang erwarteten Halflife2 und stellten diesen anschließend frei ins Internet. Der Schaden, der dadurch entstand (unter anderem erschien das Spiel erst viele Monate später), wird auf mehrere Millionen Euro beziffert.

2005

Wie beschrieben befindet sich die Virenschreiber- und Crackerszene seit einigen Jahren in einem Wandel weg von lose operierenden Gruppen von Computerenthusiasten und leichtsinnigen Jugendlichen zu einer organisierten kriminellen Szene, in der es vor allem um (sehr viel) Geld geht. 2005 spiegelt diese Entwicklung wie kein anderes Jahr. Die Würmer tragen längst Trojaner mit sich, die entweder Botnets aufbauen, Kreditkartennummern und TANs erbeuten oder Spam in gigantischen Ausmaßen verteilen.

Lion-Wurm (Linux)

Der *Lion*-Wurm drang im März 2001 über eine bekannte Sicherheitslücke in Linux-Server ein. Er verschickte das Root-Passwort verschlüsselt ins Internet und installierte zusätzlich einige so genannte *Backdoors* (Hintertüren), mit denen Cracker anschließend leicht Zugriff auf das befallene System erhalten. Das verschlüsselte Passwort konnte nachher leicht entschlüsselt sowie zum Eindringen benutzt werden. Besonders gefährlich war der Wurm jedoch, weil er sich nicht ohne Weiteres deinstallieren ließ. Das SANS-Institut veröffentlichte zwar ein Tool zum Entdecken, nicht aber zum Entfernen von *Lion*. So blieb einem nichts anderes übrig, als den gesamten Server neu zu installieren.

Zwei Monate später erschien ein neuer Linux-Wurm mit dem Namen *Cheese*. Dieser suchte auf Linux-Systemen nach dem Port 10.008, jenem Port, auf dem *Lion* seine Hintertüren installiert hatte. Wurde der Wurm fündig, schloss er die Backdoor auf dem System und versuchte von dort aus, weitere infizierte Hosts zu finden. Da die Aktivität von *Cheese* durch die Anzahl der gemessenen Portscans ermittelt werden konnte, wird davon ausgegangen, dass es eine große Anzahl an mit *Lion* infizierten Systemen gegeben haben muss. Wie bereits erwähnt, sollte ein »guter« Wurm wie *Cheese* aber nicht im Gegensatz zu den schädlichen Würmern positiv hervorgehoben werden, denn immerhin dringt auch dieser ungebeten in andere Systeme ein.

SirCam-Wurm (Windows)

Der *SirCam*-Wurm tauchte im Juli 2001 auf und landete innerhalb von wenigen Tagen ganz weit oben auf der Top-10-Liste der gefährlichsten und am weitesten verbreiteten Schädlingen überhaupt. Der angerichtete Schaden wird im Rückblick auf etwa ein bis anderthalb Milliarden US-Dollar bei etwa zwei Millionen infizierten Rechnern beziffert.[5]

5 Damit ist der Schaden, den *SirCam* verursacht hat, vergleichsweise gering, einige Würmer haben bereits die Zehnmilliardengrenze gesprengt.

Wir wollen uns daher vor allem mit der Wirkungsweise dieses außergewöhnlichen Wurms beschäftigen. Zunächst einmal installiert sich der Wurm in einigen Systemverzeichnissen, darunter auch dem Windows-Papierkorb. Anschließend versucht er, persönliche Dateien aus dem Ordner *Eigene Dateien* per E-Mail zu versenden. Besonders trickreich ist *SirCam* deswegen, weil er über einen eigenen, eingebauten SMTP-Server verfügt (dies war 2001 revolutionär und ist inzwischen zu einem festen Standard geworden) und so unabhängig von Mailtools ist. Die Zieladressen kann *SirCam* aus fast allen Mailprogrammen lesen, daher stellt er nicht nur für Outlook-Benutzer eine Gefahr dar. Auch das einfache Herausfiltern der Würmer mit Hilfe der Filterfunktion von Mail-Clients ist bei *SirCam* nicht mehr möglich, da sich die Betreffzeile der E-Mail abhängig vom als Attachment versendeten Dokument ändert. Öffnet ein Benutzer das Attachment, installiert sich der Wurm auch bei ihm. Allen infizierten Mails ist allerdings gemeinsam, dass sie im Nachrichteninhalt die Zeile »Hi! How are you?« oder »Hola, como estas?« enthalten. Neben dem Weg per E-Mail breitet sich der Wurm auch im lokalen Netz aus, indem er die freigegebenen Ordner durchsucht und sich dort einnistet.

Doch damit nicht genug, zusätzlich gibt es eine 1:20-Wahrscheinlichkeit, mit der *SirCam* am 16. Oktober alle Daten von Ihrer Festplatte löscht, wenn diese infiziert ist. Insgesamt scheint es so, als haben die Antivirenspezialisten den Wurm zuerst als eine Variante der ewig wiederkehrenden *I LOVE YOU*-Würmer angesehen und daher unterschätzt. Zwar breitete sich *SirCam* zuerst eher langsam aus, doch letztendlich erreichte er einen kritischen Punkt, ab dem seine Verbreitung sprunghaft zunahm und er zu einem der am weitesten verbreiteten Würmer der Malwaregeschichte wurde.

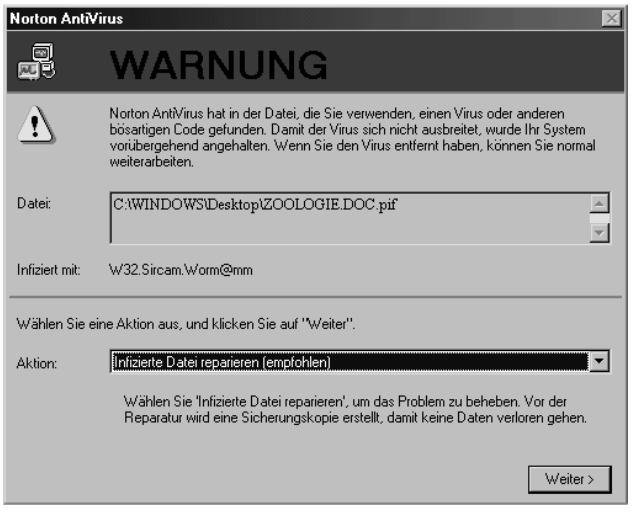

Abbildung 10-1: Norton AntiVirus blockt den SirCam-Wurm ab.

CodeRed-Wurm (Windows/IIS)

Obwohl CodeRed schon 2001 auftauchte, gab es 2003 sogar noch mehr infizierte Server im Internet als damals. Der Schaden wird auf etwa drei Milliarden US-Dollar beziffert. Der *CodeRed*-Wurm befiel ausschließlich Windows-Systeme mit dem installierten *Internet Information Server* (IIS, der Standard-Webserver von Microsoft) in den Versionen 4 und 5. Dabei nutzte er eine schon seit längerem bekannte Sicherheitslücke, um das System zu unterminieren. Anschließend veränderte er die Startseite in den Schriftzug »Hacked by Chinese!«. Besonders tückisch war *CodeRed* dadurch, dass er sich zu keiner Zeit auf die Festplatte schreibt, sondern im Hauptspeicher des Servers verblieb. Dadurch war er für alle gängigen Virenscanner praktisch unsichtbar. Diese unangenehme Tatsache hat aber auch einen Vorteil: Der Wurm ließ sich mittels eines Patches von Microsoft und durch simples Neustarten des Servers entfernen.

Neben den regelmäßigen Verbreitungswellen, bei denen *CodeRed* versuchte, weitere Server zu befallen, gab es noch eine weitere Routine, bei der alle infizierten Server versuchten, gleichzeitig die Webseite des Weißen Hauses in Washington D.C. durch eine DDoS-Attacke lahmzulegen. Neben dieser Variante existierte ein weiterer Typ von *CodeRed*, der die Startseite des befallenen Wirtes nicht veränderte und so länger unentdeckt blieb.

Seit Anfang August 2001 vermehrte sich noch eine dritte Variante (*CodeRed II*) schnell im Internet, die sich vor allem in der Verbreitungsroutine von ihren Vorgängern unterschied und daher gefährlicher für lokale Netze war (zur Ausbreitungstechnik von *CodeRed II* siehe den Abschnitt »Würmer« weiter unten in diesem Kapitel). Zudem installierte *CodeRed II* Backdoors, durch die ein Cracker anschließend freien Zugriff auf das System erhielt. Es ist anzunehmen, dass es sich bei *CodeRed II* nicht wirklich um eine Variante, sondern um einen komplett neuen Wurm handelte, darüber sind sich die Experten aber nicht einig.

Die erste Welle des *CodeRed*-Wurms schaffte es innerhalb weniger Tage, mehr als 200.000 Server zu infizieren. Da *CodeRed* von jedem System aus nur eine weitere Befallswelle auslöste, ist es umso erstaunlicher, dass die zweite Welle Anfang August nochmals 600.000 Windows-Server befallen konnte. Besonders erschreckend ist, dass es auch den Server *www.windowsupdate.microsoft.com* erwischte.

Nimda-Wurm (Windows/IIS)

Nimda sorgte Mitte September 2001 für einen enormen Schaden und befiel Schätzungen zufolge drei bis fünf Millionen PCs und Server (damit dürfte er wohl weiterhin der erfolgreichste Wurm der Geschichte sein).[6] Der Wurm war ein ganz besonders interessantes Exemplar, da er zum einen ein klassischer Trittbrettfahrer

6 Solche Zahlen schwanken grundsätzlich stark, sind bei *Nimda* aber anscheinend besonders ungenau.

war, der die Vorarbeit anderer Schädlinge ausnutzte, und zum anderen den Beweis für eine trotz ihres langen Bestehens als eher theoretisch eingestufte Gefahr erbrachte. Im Prinzip war *Nimda* eine Verschmelzung der beiden Windows-Würmer *SirCam* und *CodeRed*. Er verfügte also über einen eigenen SMTP-Server und befiel Microsoft IIS-Server sowie sämtliche Windows-Clients. Auch der Ausbreitungsmechanismus erinnerte stark an die von *CodeRed II* bekannte Vorgehensweise.

Um zu erkennen, was an *Nimda* so besonders war, müssen wir einen Blick auf die Wirkungsweise des Wurms werfen. Er suchte zunächst nach nicht-gepatchten IIS-Servern oder nach solchen, auf denen *CodeRed II* eine Backdoor hinterlassen hatte. Im Folgenden befiel er den Server und lud eine Datei namens *admin.dll* nach. Anschließend manipulierte der Wurm alle auf dem Server gefundenen *.html-*, *.htm-* und *.asp*-Dateien so, dass sie einige bösartige Zeilen JavaScript enthielten. Rief ein ahnungsloser Surfer nun mit seinem Internet Explorer die befallenen Internetseiten auf, wurde der darin eingefügte JavaScript-Code ausgeführt, die Datei *readme.eml* wurde auf den Client geladen und anschließend sofort gestartet. Damit war auch dieser Computer infiziert. Es war also erstmals möglich, sich durch bloßes Surfen zu infizieren.

Doch *Nimda* verbreitete sich darüber hinaus auch per E-Mail. Dazu wurde der Nachricht eine Datei mit dem Namen *readme.exe* als Attachment beigefügt. Das Besondere daran war, dass der Empfänger die E-Mail nicht aktiv öffnen und damit die befallene *.exe*-Datei starten musste. Bereits die Mailvorschau reichte aus, um den Mechanismus in Gang zu setzen. Sowohl der Fehler im Mailtool als auch der im Browser rührten von derselben, nicht einmal neuen Sicherheitslücke mit dem Namen *Automatic Execution of Embedded MIME Types* her.

Als dritten Verbreitungsweg suchte *Nimda* im lokalen Netz nach freigegebenen Ordnern und versuchte dort, *.exe*-Files zu infizieren. Technische Details über den Verbreitungsmechanismus und die genaue Wirkung des Wurms finden Sie bei Interesse unter *http://www.incidents.org/react/nimda.pdf*.

Sasser und Phatbot (Windows)

Diese beiden Schädlinge aus dem Jahre 2004 zählen sicherlich zu den spektakulärsten ihrer Art und waren darüber hinaus teilweise aneinander gekoppelt. Wir wollen daher zunächst auf *Sasser* eingehen und später beschreiben, wie *Phatbot* von ihm profitierte.

Sasser gilt als ein sehr unsauber und schlecht programmierter Wurm, doch offensichtlich trug dies massiv zu seiner Verbreitung bei. Besonders gefährlich war *Sasser* vor allem wegen seiner enormen Ausbreitungsgeschwindigkeit und der mit dem Wurm einhergehenden Systemabstürze. Um sich mit *Sasser* anzustecken, war es nicht nötig, eine E-Mail zu öffnen oder bestimmte Internetseiten aufzurufen, sondern es reichte schlicht und einfach aus online zu sein. Da ein immer größerer Teil

der Nutzer über schnelle und dauerhafte Anbindungen zum Internet verfügt, war dies eine fatale Mischung. Der *Sasser*-Wurm drang dabei über die einige Wochen zuvor bekannt gewordene Schwachstelle im *Local Security Authority Subsystem Service (LSASS)* ein und installierte anschließend einen kleinen FTP-Server, mit dem es möglich war, Daten von dem infizierten PC zu erbeuten. Dieser FTP-Dienst war jedoch nicht sonderlich professionell programmiert und enthielt seinerseits eine Sicherheitslücke, über die neue Würmer (z.B. *Dabber*) in infizierte Systeme eindringen und häufig noch mehr Schaden verursachen konnten.

Viel gefährlicher war jedoch, dass die Infektion (oder der Infektionsversuch) sehr häufig zum Absturz des LSA-Dienstes unter Windows führte. Dies wiederum zog einen automatischen Neustart nach sich, so dass die Rechner in zahlreichen Firmen ständig hoch- und runterfuhren. Kaum war der Rechner neu gestartet und wieder online, wurde er von *Sasser* infiziert und stürzte wieder ab. Gerade zu Anfang hatten Benutzer oftmals nicht die Chance, den Virenscanner oder die Firewall per Update auf den neuesten Stand zu bringen oder das entsprechende Patch bei Micorosoft herunterzuladen, da ihr PC inzwischen wieder neu gestartet wurde.

Abbildung 10-2 zeigt die dabei erscheinende Fehlermeldung. Nach insgesamt 60 Sekunden, in denen der Benutzer eventuell geöffnete Dokumente sichern sollte, erfolgte der automatische Neustart. Um diesen zu verhindern, war es nötig, unter START → AUSFÜHREN `shutdown -a` einzugeben und so das Herunterfahren abzubrechen. Anschließend war es möglich, weiter im Netz zu surfen und entsprechende Updates zu installieren. Verständlicherweise dauerte es jedoch einige Tage, bis sich diese Information herumgesprochen hatte. War der eigene PC befallen, versuchte sich der Wurm an andere Rechner weiterzusenden.

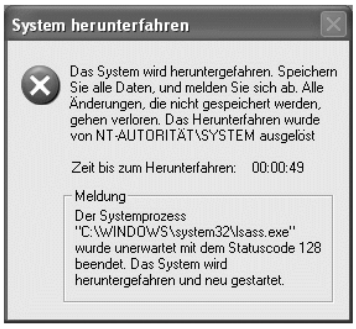

Abbildung 10-2: Durch Sasser ausgelöster Neustart des Systems

Halten wir also fest, dass *Sasser* ein sehr kompakter kleiner Wurm war, der sich vor allem rasend schnell ausbreiten konnte und zwar ohne das Zutun des Anwenders. Phatbot hingegen (der teilweise auch unter Linux lief) war ein wirkliches Schwergewicht und gehörte zu den wohl aufwändigsten und anspruchsvollsten Schädlingen,

die je entwickelt wurden. Seine Funktionsfülle war so groß, dass man damit ein komplettes Kapitel füllen könnte, und er war zudem stark konfigurierbar und somit flexibel. *Phatbot* benutzte bekannte Sicherheitslücken in Windows oder Hintertüren, die von anderen Schädlingen angelegt wurden (z.B. von *MyDoom*), um in das System einzudringen, welches er anschließend vollständig übernehmen konnte. Tauchten neue Sicherheitslücken auf, war es dem Angreifer möglich, *Phatbot* aus der Ferne auf den neuesten Stand zu bringen und eine neue Angriffswelle zu starten. Der so befallene Computer konnte also als *Bot* (auch *Zombie* genannt) vom Angreifer ferngesteuert werden. Doch dies war längst nicht alles: *Phatbot* durchsuchte den geknackten PC nach verschiedenen nützlichen Informationen wie etwa Zugangsdaten oder Schlüsseln für Computerspiele.

All dies ist schon Furcht einflößend genug, hinzu kam jedoch, dass der komplette (wenn auch leicht veränderte und somit nicht direkt nutzbare) Quell-Code des Schädlings frei im Internet verbreitet wurde. Es war somit ein Leichtes, ihn anzupassen und als Basis für eigene Entwicklungen zu nutzen.

Der Grund dafür, dass wir die beiden Schädlinge *Sasser* und *Phatbot* in einem gemeinsamen Abschnitt beschreiben ist jedoch der, dass *Phatbot* sich *Sasser* zunutze machte. Während es bis dahin schon als sehr fortschrittlich gegolten hatte, die von anderen Würmern angelegten Hintertüren zu nutzen, ging *Phatbot* noch einen entscheidenden Schritt weiter. Während der Schädling nach dem Befall die Hintertüren anderer Würmer löschte, um von nun an allein über das System zu herrschen, nutzte er *Sasser* geschickt zu seiner Verbreitung aus. Dazu löschte er *Sasser* nicht etwa, sondern folgte dessen Spuren und konnte so geschickt die Systeme infizieren, in die *Sasser* vom betreffenden System aus bereits eingedrungen war.

Viele Anwender bekamen es daher gleich mit zwei Würmern zu tun, von denen der eine das komplette System in seine Gewalt brachte. Da solch installierte Schädlinge im Verborgenen arbeiten, ist weiterhin davon auszugehen, dass es viele tausend von *Phatbot* befallene Rechner gibt, deren Benutzer nichts davon ahnen. Wir werden uns im weiteren Verlauf dieses Kapitels noch weiter mit den daraus resultierenden Bots und Botnets befassen und einen kurzen Blick in die entsprechende Szene werfen.

In the wild – In the zoo

Schätzungen zufolge gibt es zurzeit über 100.000 Computerschädlinge; warum werden aber nur die wenigsten von ihnen bekannt? Zum einen muss man die genannte Zahl in Frage stellen, denn es gibt weder ein einheitliches Zählverfahren noch eine Nomenklatur für Computerviren, und so sind Mehrfachnennungen sehr wahrscheinlich. Desweiteren gibt es von fast jedem Schädling dutzende Subtypen und Varianten, die sich nur durch Kleinigkeiten unterscheiden. Außerdem muss man zwischen so genannten *In-the-zoo*- und *In-the-wild*-Schädlingen unterscheiden.

Bei den erstgenannten handelt es sich um Viren und Würmer, die nur zu Forschungszwecken im Labor gehalten werden, also keine wirkliche Gefahr darstellen. Dazu zählt man teilweise auch die ausgestorbenen oder nie verbreiteten Schädlinge. Die In-the-wild-Viren und -Würmer hingegen sind diejenigen, denen Sie als Nutzer auch tatsächlich begegnen können. Sie befinden sich also in »freier Wildbahn«. Dies trifft nur auf 3%, allerhöchstens 5% der Schädlinge zu. In konkreten Zahlen schwanken die Angaben zwischen 2500 und 5000. Interessanterweise sind auch von den In-the-wild-Schädlingen immer nur einige wenige wirklich verbreitet, während sich der Rest eher marginaler Ausbreitung erfreut. Sie können also davon ausgehen, dass eine reelle Gefahr von etwa 50-100 Schädlingen pro Jahr ausgeht. Dies liegt wohl zum einen daran, dass sich gerade in der Vergangenheit solch präsente Viren oder Würmer wie *I LOVE YOU* nach ihrer Hochphase kaum noch ausbreiteten, und dass zum anderen Schädlinge, die sich einer Sicherheitslücke bedienen, nur so lange existieren können, wie diese Lücke nicht bei der Mehrzahl der Nutzer durch einen Patch geschlossen ist.

Für einen Überblick über die aktuellen In-the-wild-Viren empfiehlt sich ein Blick auf die Seite von *WildList* (*http://www.wildlist.org*) Dort finden Sie auch aktuelle Listen über alle gefundenen und gemeldeten Schädlinge eines bestimmten Monats. Zwar stammen fast alle dort aufgelisteten Schädlinge aus den Jahren 2003 bis 2005, es ist aber erschreckend, dass dort auch Viren aus dem letzten Jahrtausend zu finden sind.

Artenkunde

Oftmals wird zwischen Viren und Würmern nicht genau differenziert, tatsächlich aber weisen sie einige Unterschiede auf. Im Gegensatz zu den klassischen Viren handelt es sich bei Würmern um eigenständige Programme, die nicht dafür programmiert wurden, einzelne Applikationen oder Dokumente zu befallen, sondern das System an sich zu unterminieren. Sie verbreiten sich also nicht von Datei zu Datei, sondern von Host zu Host. Ein weiterer Unterschied zu den Viren besteht darin, dass die Würmer, einmal auf den Weg gebracht, nicht auf die Interaktion mit dem Benutzer angewiesen sind und sich so viel schneller ausbreiten können als Viren. Neben der eigentlichen Ausbreitungsroutine verfügen viele Würmer noch über Schadensroutinen, die virenähnliche Schäden anrichten können. Während die Viren früher eindeutig in der Überzahl waren, hat sich das Verhältnis nun zugunsten der Würmer verlagert. Seit diese (etwa ab 2001) zusammen mit Trojanischen Pferden oder ähnlichen Funktionen auftreten, stellen sie über 80% aller Schädlinge dar.[7] Um zu verstehen, wie Viren und Würmer funktionieren und welche Gefahren von den verschiedenen Typen ausgehen, muss man sich zunächst ein Bild darüber

7 In der Literatur tauchen oft Werte von über 90% auf, diese vernachlässigen dann jedoch Spyware, die ich auch zu den Schädlingen zähle.

machen, welche Arten von Schädlingen man unterscheiden kann. Daher wollen wir uns im Folgenden die wichtigsten Virentypen anschauen und kurz besprechen. Gerade im Bereich der Würmer und Trojaner könnte man viele weitere Subtypen unterscheiden, darauf wollen wir hier jedoch verzichten.

ActiveX-Viren, Java-Viren und VBScript-Viren

In einigen Beschreibungen der gängigen Virentypen tauchen auch diese drei Arten auf. Die zugrundeliegenden Techniken haben wir bereits in Kapitel 4, *World Wide Web*, eingehend besprochen. Daher brauchen wir sie hier nur noch von den anderen Viren abzugrenzen bzw. zu charakterisieren.

Wie alle Viren sind auch diese sehr stark auf das Internet angewiesen oder kommen sogar nur dort zum Tragen. Ein typisches Beispiel wäre ein ActiveX-Virus, der eine Sicherheitslücke im Browser nutzt, um seine Schadenswirkung zu entfalten. Allerdings muss zu dieser Definition einschränkend gesagt werden, dass die VBS-Programmiersprache auch durch den Windows Scripting Host direkt auf das Windows-Betriebssystem wirken und so unabhängig vom Internet werden kann.

Boot-Viren

Diese Art von Viren nistet sich im Boot-Sektor von Disketten oder im *Master Boot Record* (MBR) von Festplatten ein und wird dadurch schon beim ersten Zugriff auf den Datenträger aktiv. Ein Virus im MBR erwacht also schon beim Starten des Computers zum Leben und ist daher nicht ohne Weiteres von der Betriebssystemebene aus zu entfernen.

Companion-Viren

Gewöhnlich versucht ein Virus, sich in eine Programmdatei einzunisten und sich dann weiter zu verbreiten oder seine Schadensroutine auszuführen, sobald das Programm gestartet wird. Companion-Viren hingegen lassen das eigentliche Programm völlig unberührt und erschaffen stattdessen ein neues Programm, das den bösartigen Code enthält und jedes Mal vor dem Ausführen der Applikation gestartet wird. Ist der Code abgearbeitet, startet der Virus das eigentlich vom Benutzer gewünschte Programm. Dadurch bemerkt dieser nicht, dass im Hintergrund noch andere Dinge vor sich gehen, und schöpft keinen Verdacht. In der Vergangenheit sind auch zahlreiche Virenscanner auf diesen Trick hereingefallen.

Dateilose Würmer

Diese Würmer legen keinerlei Dateien auf dem befallenen System an, sondern verbleiben die ganze Zeit über im Speicher des Rechners. Startet man diesen neu, verschwinden Sie daher wieder. Dies scheint zwar auf den ersten Blick von Nachteil zu sein, jedoch werden diese Würmer für Virenscanner so sehr schwer auffindbar und umgehen Zugriffsbeschränkungen auf Dateien. Zudem werden Serversysteme nur sehr selten neu gestartet, weshalb der Wurm dort lange verweilen und sich entsprechend verbreiten kann. Nach einem Neustart kann er

das System von einem fremden Host aus erneut befallen (sofern kein entsprechender Patch installiert wurde). Sauber entwickelte dateilose Würmer legen auch für die integrierten Schadensroutinen keine Dateien an, sondern belassen ebenfalls diese Komponente im Speicher des Systems.

Dropper

Dropper sind eigentlich keine Viren, sondern ganz »gewöhnliche« Programme. Daher fallen Sie den meisten Antivirenprogrammen auch nicht weiter auf. Führt man aber so ein vermeintlich harmloses Programm aus, installiert es einen Virus auf dem System. Dropper kapseln also quasi Viren und schützen sie so vor der Erkennung.

Hoax

Fälschlicherweise werden oft auch die uns aus Kapitel 6, *E-Mail – wer liest mit?*, bekannten Hoaxes zu den Viren gezählt. Da die Unterschiede hier aber gegenüber den Ähnlichkeiten bei Weitem überwiegen, ist von einer solchen Klassifizierung abzuraten. Weder vermehren sich Hoaxes selbstständig, noch befallen Sie Programme, Dokumente, Boot-Sektoren oder ganze Systeme. Auch eine Schadensroutine wird man bei ihnen vergeblich suchen.

Hybridviren

Eigentlich definiert man als Hybridviren diejenigen, die sowohl Programme als auch Boot-Sektoren befallen. In Zukunft könnte man diese Definition aber auch ausweiten und alle Arten von Mischvarianten dazu zählen.

Logische Bomben

Die logischen Bomben sind zwischen den Viren und den trojanischen Pferden angesiedelt, passen aber in keines der beiden Konzepte richtig hinein. Eine solche Bombe besteht immer aus zwei festen Bestandteilen: dem Auslöser (*Trigger*) und einer Schadensroutine (*Payload*). Dabei versteckt sich die Bombe in einem anderen Programm und überprüft nach jedem Start die Trigger-Bedingung. Trifft diese nicht zu, verhält sich die ausgeführte Applikation wie gewöhnlich. Im anderen Fall »explodiert« die logische Bombe, indem die Schadensroutine ausgeführt wird.

Da Schädlinge immer nur dann einfach zu identifizieren sind, wenn es eine direkte Verbindung zwischen Ursache und Wirkung gibt, sind solche Bomben nur sehr schwer zu erkennen. Möglicherweise startet ein Benutzer die befallene Applikation tagtäglich, ohne dass sich daraus irgendwelche Konsequenzen ergeben. Wenn dann anscheinend urplötzlich die Schadensroutine zur Wirkung kommt, ist nicht mehr genau nachzuvollziehen, von wo aus oder aus welchem Grund die Bombe explodiert ist. So könnte man sich z. B. als einfachen Trigger einen Counter vorstellen, der bei jedem Start des Programms herunterzählt; die meisten Auslöser sind jedoch wesentlich komplizierter aufgebaut.

Makroviren

Diese Schädlinge gehören zu der Kategorie der Dokumentviren, befallen also keine ausführbaren Dateien, sondern beispielsweise Word-Dokumente. Wie

der Name bereits verrät, sind die Viren in den jeweiligen Makro-Programmiersprachen der gängigen Office-Pakete programmiert und kommen nur dann zur Anwendung, wenn solche Applikationen gestartet werden. In aller Regel verbreiten sie sich durch die Infektion der Standardvorlage und verdrehen dann Standardkommandos oder führen kleinere Veränderungen am Dokument durch, bis es schließlich unbrauchbar wird.

Der Benutzer erhält z. B. per Diskette oder E-Mail ein Word-Dokument und öffnet es in seiner Applikation. Daraufhin wird der bösartige Code (*Makro*) aktiv und speichert sich als Erstes in der Standardvorlage *Normal.dot* ab. Wenn der Benutzer später ein neues Dokument anlegt, wird dadurch auch immer der Virus automatisch aktiviert. Eine mögliche Funktion wäre z.B., dass der Schädling die Speicherfunktion so manipuliert, dass vor jedem Abspeichern alle Vokale in dem Dokument in jeweils den alphabetisch nächsten getauscht werden.

Polymorphe Viren

Diese Virenart entzieht sich der Erkennung durch Virenscanner, indem Sie bei jeder Verbreitung mutiert. Der Virus kann also eigenständig seinen Programm-Code umschreiben, so dass später keine Bytefolge mehr dem Original gleicht. Besonders ausgefeilte Exemplare können mehrere Milliarden Mutationen erzeugen, ohne dass Parallelen zwischen den einzelnen Individuen zu erkennen sind. Dadurch sind polymorphe Viren nur schwer oder gar nicht von Scannern zu erkennen.

Spyware

Die rechtliche Lage bei Spyware ist etwas verworren, es handelt sich dabei um Programme, die mehr oder weniger heimlich mit anderen Applikationen zusammen auf die eigene Festplatte geraten und dort das Verhalten des Surfers ausspionieren und ihm immer wieder Werbung unterschieben. Mitunter verändern sie auch die Anzeige von Internetseiten. Da es hier um viel Geld geht, versuchen die Hersteller Spyware vom Schädlingsimage zu befreien, was wir jedoch für falsch halten. Diese Programme dienen der Bereicherung Dritter, sind unerwünscht auf den eigenen PC gekommen und richten zudem teilweise Schaden an.

Stealth- oder Tarnkappenviren

Diese Art von Viren ist immer speicherresistent, d. h., die Viren verbleiben im Hauptspeicher und erlangen dadurch Kontrolle über das gesamte System. Tarnkappenviren versuchen mit verschiedenen Tricks, die eigene Identität zu verschlüsseln. Dazu manipuliert der Virus das Betriebssystem so, dass er zum Beispiel Dateizugriffe abfängt und so verändert, dass nichts mehr auf seine Anwesenheit hindeutet. Greift beispielweise ein Virenscanner auf eine Datei zu, um diese auf Unregelmäßigkeiten zu prüfen, erkennt der Tarnkappenvirus diesen Zugriff und extrahiert sich selbst aus der befallenen Datei. Bei dem anschließenden Scan findet die Antiviren-Software also eine unbefallene Datei vor und schöpft keinen Verdacht.

Trojanische Pferde
: Da die Trojaner eine besondere Stellung innerhalb der Malware einnehmen, werden wir diese gesondert in einem eigenen Abschnitt betrachten und daher hier nicht weiter auf sie eingehen.

Virenkalender

Zahlreiche Hersteller von Antiviren-Software bieten auf ihren Webseiten so genannte *Virenkalender* an, anhand derer man feststellen kann, wann ein Virus aktiv wird. Dies funktioniert natürlich nur bei Schädlingen, die eine Zeitroutine eingebaut haben, ist in diesen Fällen jedoch äußerst informativ. Auffällig bei solchen Kalendern ist vor allem, dass an bestimmten historischen Daten sowie am Monatsanfang und -ende die Zahl der aktiven Viren erheblich zunimmt. Ein Beispiel hierfür ist der 1. Januar, an dem sogar zwölf bekannte Virenarten zuschlagen, oder der 31. Dezember mit immerhin noch zehn verschiedenen Typen.

Besonders empfehlenswert ist der Virenkalender der Firma Symantec (*http://www.symantec.com/avcenter/calendar/*). Allerdings scheint der Trend bei der Malware weg von kalendarischen Eigenschaften zu gehen oder sie sind, wie bei *SirCam,* nur noch ein Randaspekt.

Würmer

Da wir uns auf den vorigen Seiten ausführlich mit den verschiedenen Arten und Wirkungsweisen von Schädlingen befasst haben, wollen wir nun einmal genauer darauf eingehen, wie ein solches Programm technisch überhaupt funktioniert. Als Anschauungsmodell soll uns hierfür der bereits beschriebene *CodeRed*-Wurm aus dem Jahr 2001 in der Version 3 dienen. Er ist deshalb als Beispiel gut geeignet, weil er zum einen eine ganz klassische Sicherheitslücke ausnutzt und zum anderen inzwischen sehr gut dokumentiert ist.

Buffer Overflow

Bei einem *Buffer Overflow* (Pufferüberlauf) handelt es sich um die wohl häufigste Sicherheitslücke in Software, die sich neben anderen Schädlingen auch der *CodeRed*-Wurm zunutze macht. Bei der Programmierung werden für bestimmte Variablen Speicherbereiche reserviert. Diese haben je nach Wahl der Entwickler eine bestimmte Größe im Gesamtspeicher. Solange der Inhalt in den Speicherbereich passt, kommt es zu keinem Problem; ist der Inhalt aber zu lang, wird er nicht einfach am Ende des Bereichs abgeschnitten, sondern überschreibt die nachfolgenden Speicherpositionen. In den meisten Fällen kommt es dadurch zum Absturz des Programms oder zu nicht reproduzierbaren Fehlern (Fehler deren Ursache nicht zu ergründen ist, weil sie sich nicht reproduzieren lassen), je nachdem, was sich ursprünglich in den nunmehr überschriebenen Bereichen befand.

Wenn man nun beispielsweise den Buffer durch eine lange Kette von sinnlosen Buchstaben überlaufen lässt, mag das eine gute DoS-Attacke sein, einen Wurm kann man auf diese Weise aber noch nicht in das System schleusen. Wirklich interessant wird ein Buffer Overflow erst dann, wenn man genau ausmachen kann, ab welchem Zeichen der Kette der Puffer überläuft, und anschließend mittels Assembler-Code direkt ausführbare Befehle in den Speicherbereich schreibt. Da diese anschließend ausgeführt werden, erlangt man unter Umständen Zugriff auf systeminterne Programmroutinen und kann auf diese Weise das System kompromittieren. Der folgende HTTP-Request zeigt die Anfrage eines von *CodeRed II* infizierten IIS-Systems auf den Port 80 eines anderen Webservers (Testsystem).

```
1: Incoming call...
< GET /default.
ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u
8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
< Content-type: text/xml
< Content-length: 3379
1: Closed.
```

Die angefragte `default.ida` ist Teil des *Microsoft Indexing Services* und enthält die eigentliche Sicherheitslücke (*ldq.dll*), auf die der Angriff erfolgt. War der Buffer Overflow erfolgreich, wird der bösartige Code ausgeführt.

Der Code

Einmal in den Speicherbereich gelangt, wird der Quelltext von *CodeRed* ausgeführt und ruft die für seine Zwecke benötigten Routinen auf. Dazu lädt sich der Wurm erst einmal selbst und anschließend eine Reihe von Windows-Bibliotheken (*.dll*s), die ihm Zugriff auf verschiedenen Teile der Webserversoftware und des Betriebssystems verschaffen. Anschließend bootet der Wurm den Host neu und überprüft die Spracheinstellung des Betriebssystems. Wenn es sich um eine chinesische oder taiwanesische Version handelt, erschafft er 600 neue Threads (unabhängige Routinen, die eine bestimmte Aufgabe autonom bewältigen können), anderenfalls sind es »nur« 300 Stück. Diese Threads sorgen im Folgenden für eine weitere Verbreitung des Wurms. Der Haupt-Thread des Schädlings verändert währenddessen Einträge in der System-Registry (einer Art Konfigurationszentrale für MS-Betriebssysteme) und kopiert die *cmd.exe* in das Verzeichnis *\inetpub\Scripts\Root.exe*. Bei dieser Datei handelt es sich um den Windows-Befehlsinterpreter, mit dem man das System, wenn auch nur umständlich, zu großen Teilen bedienen kann.[8] Danach schläft der

8 Ein Befehlsinterpreter ist auf jedem Windows-Betriebssystem enthalten und erlaubt es, Grundfunktionen über ein Textfenster einzugeben. So kann man zum Beispiel Dateien verstecken, löschen oder kopieren, aber auch Netzwerkfunktionen nutzen. Die Eingabe von `del *.doc` löscht zum Beispiel alle Word-Dokumente im aktuellen Ordner, während man mit dem Befehl `net view` alle verfügbaren Netzressourcen angezeigt bekommt. Unter Windows erreichen Sie den Interpreter wenn Sie unter START → AUSFÜHREN `cmd` eintippen.

Haupt-Thread für 48 bzw. 24 Stunden ein, bootet anschließend das System neu und steht von nun an für neue *CodeRed*-Infektionen offen.

Die Hintertür

Nachdem der Wurm die *cmd.exe* in das *Scripts*-Verzeichnis des Webordners *inetpub* kopiert und einige Veränderungen in der Registry vorgenommen hat, ist der Windows-Befehlsinterpreter aus dem Web erreichbar, da das *inetpub*-Verzeichnis den Wurzelordner für den im Web sichtbaren Bereich des Servers darstellt. Jeder Angreifer kann nun mit einem HTTP-Request vollständigen Zugriff auf das System erlangen. Zudem stellte Symantec fest, dass *CodeRed* noch einen Trojaner namens *VisualRoot* in sich trägt und versucht, diesen auf dem System zu installieren.[9] Mit Hilfe dieses Trojaners ist dann zusätzlich zur Schadensroutine des Wurms das Fernsteuern des befallenen Servers möglich.

Die Verbreitungsroutine

Bisher haben sich Würmer oft dadurch verbreitet, dass sie von der befallenen Plattform aus versucht haben, mittels automatisch generierter IP-Adressen andere Server zu befallen. Auch Version 3 von *CodeRed* geht im Prinzip genauso vor, nutzt aber ein optimiertes Verfahren. Anstatt nur blind Adressen zu generieren und sie auf Befallsmöglichkeiten zu prüfen, agiert der Wurm unter der Annahme, dass sich in einem Netz meist ähnliche, gleich aktuelle Systeme befinden. Die Wahrscheinlichkeit, einen angreifbaren IIS-Server dort zu finden, wo bereits einer war, ist also größer.

Um dieser Idee Rechnung zu tragen, generiert der Wurm nur 1/8 der IP-Adressen beliebig, 3/8 stammen aus dem gleichen B-Netz (z.B. 192.168.x.y) und 4/8 aus dem gleichen A-Netz (z.B. 192.x.y.z) des befallenen Servers. Auf diese Weise ist die Wahrscheinlichkeit, dass der Wurm sich im lokalen Netz ausbreitet, wesentlich größer als bei den anderen Würmern.

Wie Sie an dem Beispiel *CodeRed* sehen konnten, sind die Methoden, mit denen die Schädlinge vorgehen, sehr komplex und werden immer komplexer, werden dadurch aber auch immer systemspezifischer. Der hier vorgestellte *CodeRed II* kann seine Wirkung nur auf einem nicht gepatchten ISS-Server unter Windows 2000 voll entfalten. Zwar befällt er auch Windows NT 4.0 und einige Cisco-Produkte, kann dort aber nur einen Teil seiner Funktionsvielfalt ausspielen.

9 Der Trick mit dem Einschleusen der *cmd.exe* in einen öffentlich zugänglichen Bereich ist keineswegs neu und wird oft bei Attacken über ungesicherte FTP-Server genutzt. Dabei erlangt der Angreifer Zugriff auf einen Gast-Account oder ein anonymes Konto auf dem Webserver, versucht, in das besagte *Scripts*-Verzeichnis zu gelangen und hofft, in dieses die *cmd.exe* seines eigenen Computers hochladen zu können. Nach ein paar weiteren Kniffen stellt sich die Situation genau wie beim *CodeRed*-Wurm dar.

Trojaner

Im Folgenden wollen wir uns mit dem großen Arsenal der trojanischen Pferde – kurz: Trojaner – beschäftigen. Dazu werden wir zunächst klären, was sich überhaupt hinter dem Begriff verbirgt, und anschließend eines der drei berühmtesten Exemplare etwas genauer unter die Lupe nehmen. Zum Ende des Kapitels hin werden wir uns dann noch anschauen, welche Rolle die Trojaner in naher Zukunft einnehmen werden.

Wirkungsweise

Während der Fokus bei Viren und Würmern eher auf der Verbreitung und der automatischen Schädigung von Systemen liegt, spielt bei den trojanischen Pferden der Gedanke der Kontrolle über ein einzelnes System oder ein Netzwerk die wichtigste Rolle.[10] Daher enthalten Trojaner im Allgemeinen auch keine Verbreitungsmechanismen, sondern verstecken sich in vermeintlich harmloser Software. Wird das Programm vom Benutzer gestartet oder installiert, erwacht auch der darin enthaltene Trojaner zum Leben und versucht, möglichst viele Informationen über das Verhalten des Users zu sammeln.

Typische Aufgaben solcher Malware sind zum Beispiel das vollständige Überwachen der Tastatureingaben, der gestarteten Applikationen und/oder des gesamten Systems. Durch diese Fähigkeiten sind die Trojaner in der Lage, Ihr Verhalten in Echtzeit zu belauschen und zu protokollieren. Dies wird insbesondere beim Eingeben von Passwörtern, Kreditkartendaten oder Home-Banking-TANs und iTANs zu einem ernsten Problem.

Neben diesen Lauschfunktionen haben die meisten größeren Trojaner noch eine ganz andere Aufgabe: Sie sollen es dem Angreifer ermöglichen, Zugang zu Ihrem System zu erlangen und es aus der Ferne zu bedienen. Dazu wartet der einmal gestartete Trojaner so lange im Hintergrund, bis Sie eine Verbindung ins Internet aufbauen, und verschickt dann seine Logdateien per E-Mail an den Angreifer, oder aber er lauscht an einem dafür vorgesehenen Port, bis sich der Cracker anmeldet, um den befallenen PC von nun an fernzusteuern. Dies bedeutet aber auch, dass der Angreifer nur Macht über Ihr System hat, solange Sie online sind. Lange Online-Sitzungen bergen daher, wie in Kapitel 3, *Sicherheitsbewusstsein*, beschrieben, immer ein gewisses Risiko.

Aus dem beschriebenen Spektrum an Funktionen, das moderne Trojaner mit sich bringen, lassen sich die entstehenden Gefahren gut abwägen. Als Erstes wäre der häufig unterschätzte Aspekt des Verlusts der Privatsphäre zu nennen. Daneben entstehen finanzielle Gefahren durch den Missbrauch von Kreditkarteninformationen

10 Wie bereits mehrfach angesprochen, bricht diese Unterscheidung aber zunehmend weg.

oder Passwörtern. Auch die Ihnen aus dem Kapitel 6, *E-Mail – wer liest mit?*, bekannten Social Engineering-Angriffe werden durch Trojaner stark begünstigt. Wenn z.B. ein installierter Trojaner die Account-Daten Ihres E-Mail-Anschlusses mitliest, kann ein Angreifer quasi in Ihrem Namen Nachrichten an Bekannte oder Kollegen verschicken. Auch aus dem Bereich der Instant Messenger sind solche Attacken bereits bekannt geworden. Neben solchen Angriffen, die vor allem Sie oder Ihren näheren Umkreis betreffen, sind auch DDoS-Angriffe auf das Wirken von trojanischen Pferden zurückzuführen. Der von einem Trojaner gekaperte Computer wird dabei zum ferngesteuerten Angreifer. Mit diesen so genannten Bots und Botnets werden wir uns weiter unten ausführlicher beschäftigen.

Kommen wir zuletzt noch auf die Verbreitungsmöglichkeiten dieser Art von Malware zu sprechen. Wie eingangs erwähnt, vermehren sich Trojaner nicht selbst, sondern werden aktiv, wenn sie, auch unbewusst, vom Benutzer installiert werden. Der häufigste Weg einer Infektion verläuft dabei über Downloads oder per E-Mail-Attachments. Als Köderprogramme sind insbesondere kostenlose Tools zur Systembeschleunigung oder -verbesserung sowie Bildschirmschoner und Spiele beliebt, aber auch andere Typen von Software können mit Trojanern infiziert sein. Trojaner, die Teil des Schadprogramms von Würmern sind, vermehren sich jedoch sehr wohl und können ohne Zutun des Anwenders aktiv werden!

Stellvertretend für die wichtigsten Trojaner wollen wir uns im Folgenden *Back Orifice* anschauen und anhand dieses Tools auch den grundsätzlichen Aufbau solcher Programme kennenlernen.

Back Orifice

Das Tool *Back Orifice* wurde 1998 von der Gruppe »Cult of the Dead Cow« entwickelt und ein Jahr später in der Version *Back Orifice 2000* (BO2K) stark erweitert. Laut Webseite und Produktbeschreibung handelt es sich dabei natürlich nur um ein *Remote Administration Tool* (RAT). Remote Administration ist mittlerweile zu einem wichtigen Steuerungsmittel in der Systemverwaltung geworden, weshalb solche Tools ihre Berechtigung haben. Da es aber durchaus Sinn macht, ein Produkt nach seinem hauptsächlichen Einsatzgebiet zu klassifizieren, können wir im Fall von *Back Orifice* ruhig von einem klassischen trojanischen Pferd sprechen. Man käme auch ziemlich ins Schwitzen, wollte man zahlreiche für die Administration unnötige Funktionen erklären, wie beispielweise die Tarnvorrichtung oder das Mitprotokollieren jeder Tastatureingabe.

Da das gesamte Tool im Quell-Code frei verfügbar ist, existieren zudem Plugins, die den Funktionsumfang von BO2K noch einmal deutlich erweitern. Dazu zählt beispielsweise eine Erweiterung, die den BO-Datenverkehr für Antivirensoftware unsichtbar macht, und eine Erweiterung, die dem Angreifer mittels *ICQ* die IP-Adresse des befallenen Hosts mitteilt.

Das eigentliche Tool besteht, wie andere Trojaner oder RATs auch, aus drei unterschiedlichen Komponenten: dem Server, der auf dem fremden System laufen soll, dem Konfigurationstool, mit dem der Server konfiguriert wird, und dem Client, der auf dem Rechner des »Fernadministrators« läuft und über den er die Aktivitäten des Servers steuern kann. Eine genaue Beschreibung des Programms würde hier zu weit führen und soll daher den einschlägigen Tutorials (z.B. unter *http://www.bo2k.de*) überlassen bleiben. Wir wollen uns hingegen an dieser Stelle detaillierter dem Funktionsumfang von *Back Orifice* widmen und einige interessante Funktionen aufzählen, um einschätzen zu können, welche Gefahren von einem solchen Tool ausgehen können.

Get System Info
: Da es für einen Angreifer immer sehr wichtig ist, möglichst viele Informationen über das befallene System zu erhalten, kann er sich mit diesem Befehl Informationen über den Namen des Computers, den Belegungszustand der Festplatte und weitere systembezogene Daten anzeigen lassen.

GUI Commands
: Hier findet sich die Option zum Erzeugen eines Dialogfelds auf dem Server, mit dem der Angreifer Informationen an den ahnungslosen Benutzer übermitteln kann.

Keylogging
: Mittels Keylogging zeichnet der BO2K-Server alle Tastatureingaben auf und schreibt sie in eine frei wählbare Datei. Um eine bessere Rekonstruktion der eingetippten Daten zu ermöglichen, wird zudem immer das Fenster, in dem die Eingabe getätigt wurde, mitprotokolliert.

MS Networking
: Unter diesem Begriff sind zahlreiche Funktionen zusammengefasst, mit denen man die Dateifreigabe unter Windows manipulieren kann. So erlaubt das Kommando ADD SHARE beispielsweise, eine neue Freigabe hinzuzufügen und so die dort enthaltenen Daten dem ganzen Netzwerk zur Verfügung zu stellen. Andere Funktionen wie LIST SHARES ON LAN zeigen die bereits bestehenden Freigaben der Netzwerkumgebung an und helfen dem Eindringling somit auch, an Daten von nicht befallenen Computern im gleichen Netz zu gelangen.

Process Control
: Sollte der Angreifer einmal das Verlangen haben, beliebige Programme auf dem Server zu starten oder zu stoppen, kann er auf die Befehle aus diesem Bereich zurückgreifen. Damit wäre es beispielsweise auch möglich, einen Virenscanner oder eine Firewall kurzerhand auszuschalten oder weitere Software nachzuinstallieren.

Registry
: Die Registry ist einer der Kernbestandteile eines jeden Windows-Betriebssystems. Vereinfachend kann man sagen, dass es sich um ein zentrales Konfigura-

tions- und Verwaltungstool handelt. Beispielsweise kann in der Registry geregelt werden, welche Programme mit welchen Optionen schon beim Systemstart geladen werden oder ob Benutzerpasswörter im Klartext übertragen werden sollen. Die Fähigkeit von *Back Orifice*, Einträge zur Registry hinzuzufügen, zu ändern oder neu einzufügen, verschafft dem Tool im System sehr weit gehende Eingriffsmöglichkeiten. So könnten beispielsweise Einträge so manipuliert werden, dass ein Virenscanner nicht mehr ordnungsgemäß arbeitet oder andere Schutzsoftware deaktiviert wird.

System Commands
: Unter diese Rubrik fallen die Befehle zum Neustart des befallenen Systems (z. B. um Konfigurationsänderungen wirksam werden zu lassen), zum Einfrieren des Systems ähnlich wie bei einem Systemabsturz (um z. B. einen Benutzer davon zu überzeugen, dass sein Betriebssystem sich aufgehängt hat und der Rechner neu gestartet werden muss) oder zum Auslesen gespeicherter Passwörter z. B. aus dem Internet Explorer.

TCP/IP Commands
: In dieser Rubrik finden sich zahlreiche nützliche Netzwerkfunktionen wie zum Beispiel das Umleiten eines bestimmten Ports auf eine andere IP-Adresse oder das Verschicken von Dokumenten vom Server an den Client. Sogar an eine Art eingebauten HTTP-Server hat man gedacht, mit dessen Hilfe man das fremde Dateisystem bequem im eigenen Webbrowser durchsuchen kann. Dieses Funktionspaket kann als besonders leistungsstark angesehen werden, da es dem BO2K-Client erlaubt, unbemerkt beliebige Dokumente vom Server zu stehlen.

Neben den hier vorgestellten Befehlen gibt es auch noch zahlreiche weitere Funktionen (zum Beispiel durch Plugins). Anhand dieser kurzen Übersicht sollten Sie sich aber bereits ein Bild über die Konsequenzen eines heimlich im Hintergrund laufenden *Back Orifice*-Servers machen können. Neben der beeindruckenden Komplexität fällt vor allem die Kommunikationsfreude des Trojaners auf. Bisher war es für einen Angreifer immer problematisch, schnell herauszufinden, bei welcher IP-Adresse sich sein Schädling gerade befindet und ob er überhaupt online ist. Dies liegt daran, dass die meisten Computer nur über Wählleitungen mit dem Internet verbunden sind und bei jeder Online-Sitzung eine neue IP-Adresse zugeordnet bekommen. Mittels eines Plugins kann der Trojaner nun, sobald er online ist, seine IP-Adresse per Instant Messaging weiterleiten und den Angreifer so darüber informieren, dass er auf dessen Instruktionen wartet.

Schutz vor Trojanern

Wie der Name schon andeutet, liegt das Wesen eines trojanischen Pferdes darin, unentdeckt zu bleiben und somit dem Angreifer eine längerfristige und zuverlässige Hintertür zum befallenen System zu verschaffen. Gerade diese Eigenschaft macht aber die Gefährlichkeit der Programme aus, denn Sie verweilen meist unbemerkt

Monate oder sogar Jahre auf Ihrem System. Einen wirksamen Schutz gegen Trojaner bieten daher entweder Virenscanner und Personal Firewalls oder aber spezielle Tools, die sich auf das Erkennen verdächtiger Aktivitäten spezialisiert haben.

Gerade die weit verbreiteten Virenscanner zeigen deutliche Schwächen beim Umgang und Auffinden von Trojanern und Hintertüren im Allgemeinen. Hier empfiehlt sich beispielsweise die kostenlose Version des Bitdefenders (siehe Abbildung 10-3) als Zweitscanner[11] oder F-Secure Anti-Virus. Die angesprochenen Spezialtools bieten meist nicht viel mehr Funktionen als die integrierten Pakete oder richten sich vor allem an fortgeschrittene User.

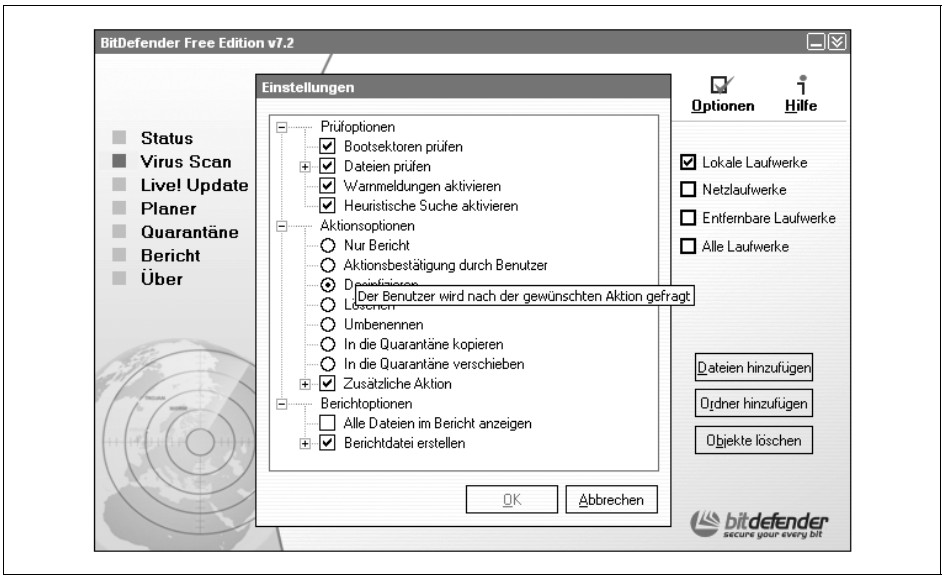

Abbildung 10-3: Das Suchfenster von Bitdefender mit geöffnetem Einstellungsmenü

Sehr nützlich sind auch Produkte, die einen genaueren Blick auf die Systemkonfiguration, die beim Systemstart geladenen Programme und die Prozesse, die sich im Speicher befinden, zulassen. Diese Tools eignen sich jedoch durch die Bank weniger für Einsteiger – ihr Einsatz ist bei Verdacht sehr sinnvoll, soll hier jedoch nicht genauer besprochen werden. Als Tipp sei das kostenlose *a-squared HiJackFree* genannt (das sie unter *http://www.hijackfree.de/de/* herunterladen können). Ähnliche Funktionen wie HiJackFree (siehe Abbildung 10-4) bietet im Prinzip auch Microsoft mit dem integrierten *msconfig* an, das Sie über START → AUSFÜHREN erreichen. Der Funktionsumfang und Informationsgehalt sind jedoch deutlich geringer.

11 Besonders empfehlenswert ist die erweiterte Version *Professional Plus* für knapp 50 Euro. Beide sind über *http://www.bitdefender.de* zu beziehen.

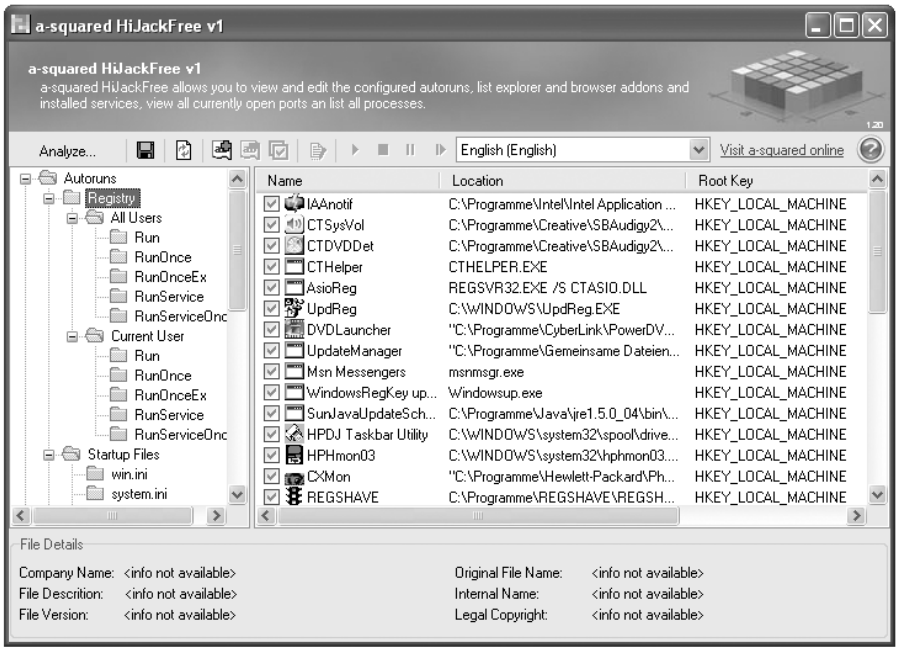

Abbildung 10-4: HiJackFree zeigt die Programme, die beim Systemstart geladen werden.

Spyware

Wir haben bereits mehrfach das Thema Adware, Spyware und unerwünschte Programme oder Programmfunktionen angesprochen. In diesem Abschnitt wollen wir daher nur kurz die Brücke zwischen Würmern und Spyware schlagen, um die Vernetzung innerhalb der verschiedenen Szenen zu zeigen.

Wie erwähnt, befindet sich die globale Community der Schädlingsentwickler und Cracker seit einigen Jahren in einem Wandel hin zu zunehmender Kriminialisierung. Einige Erfinder von Würmern und Trojanern leben schon von ihrer Arbeit und programmieren auf Anfrage oder verkaufen Zugänge zu den erbeuteten Rechnern.

Bei den Entwicklern von Spyware handelt es sich hingegen meist nicht um Einzelpersonen oder verschworene Gemeinschaften, sondern um Unternehmen im klassischen Sinn. Etwas vereinfacht dargestellt, entwickelt der Spyware-Hersteller ein Programm, das möglichst unbemerkt im Hintergrund arbeitet und zwei Aufgaben erfüllt: Erstens protokolliert es sämtliche Surfgewohnheiten des Benutzers (besuchte Online-Shops, erworbene Produkte etc.), und zweitens setzt es Links in Internetseiten ein, auf denen der Surfer sich gerade befindet. Diese Links führen zu Online-Shops oder weiteren Angeboten, die den Surfer an einen anderen (nicht vertrauenswürdigen) Shop weiterleiten.

Spyware-Hersteller verdienen ihr Geld also gleich mit zweierlei Dingen: mit der Erstellung und dem Verkauf von Benutzerprofilen auf der einen Seite und mit Vermittelungsprämien an dubiose Online-Shops auf der anderen. Dazu haben Spyware-Hersteller Verträge mit zahlreichen Online-Shops geschlossen und bekommen für jeden angeklickten Link oder jedes verkaufte Produkt eine Provision.

Bleibt nur noch die Frage, wie die Spyware verbreitet wird. Es ist ein mühseliges Geschäft, Spyware auf fremden Rechnern zu platzieren, so dass sich Hersteller dieser Art von Software unterschiedlicher Kniffe bedienen. Eine weit verbreitete Möglichkeit, Spyware unter die Leute zu bringen, besteht darin, ein Softwareprodukt zu entwickeln, diesem die Spyware beizufügen und das Produkt möglichst vielen Internetnutzern schmackhaft zu machen. Um möglichst viele Surfer dazu zu bewegen, über die Links der Spyware einen Online-Shop zu betreten, wird das Provisionssystem, das zwischen Online-Shop und Spyware-Hersteller existiert, auf die Endkunden ausgeweitet. Der Spyware-Hersteller gibt also gewissermaßen einen Teil des Rabatts, den mit seinen Online-Shop-Partnern vereinbart hat, an den Käufer eines Produkts weiter. Dieser Teil des Geschäftsmodells ist absolut legal, aber es birgt auch die Möglichkeit, für illegale Machenschaften genutzt zu werden. So können sich Cracker beim Spyware-Hersteller als Nutzer der Software registrieren und sich einen Account geben lassen, über den die Vergünstigungen bei den Online-Shops abgerechnet werden. Anschließend integrieren sie die Spyware oder Teile davon in einen eigens dafür programmierten Trojaner und verbreiten die Software so über tausende PCs. Die Spyware wird dort aktiv und schiebt den ahnungslosen Internetnutzern Links zu besagten Online-Shops unter. Klickt ein Surfer auf so einen Link zu einem Online-Shop und kauft er dort etwas ein, stünde ihm eigentlich ein bestimmter Rabatt zu. Davon weiß der Käufer allerdings nichts, denn die Spyware, an die die Vergünstigung gekoppelt ist, wurde ohne sein Wissen auf seinem Rechner installiert. Deshalb kann der Preisnachlass dem Cracker gutgeschrieben werden. Damit das geschieht, sorgt der Trojaner dafür, dass der Account des Crackers bei der Erstattung der Vergütung angegeben wird. Dass die dabei zustande kommenden Summen nicht unerheblich sind, haben einige Fälle 2005 deutlich gezeigt. Hersteller von Spyware verdienen daran natürlich gut mit und müssen ihrerseits die Kontakte zu Schädlingsschreibern nur so locker halten, dass ihnen die Unternehmung weiterhin als echter Mehrwert für den Kunden erscheint.[12]

Ein gutes Beispiel für einen Spyware-Angriff ist der im September 2005 aufgetauchte Google-Wurm *P2Load.A*, der nach der Infektion Google-Anfragen eines Nutzers an Werbeseiten umleitet und sich dazu einer gefälschten Host-Datei bedient. Einen solchen Angriff werden wir im nächsten Kapitel ausführlich besprechen.

Als Tool zum Auffinden und Entdecken von Spyware eignet sich beispielsweise (die kostenlose Version von) Ad-aware, die Sie unter *http://www.lavasoftusa.com/german/*

12 Solche »echten« Kunden hat der Unternehmer in der Regel jedoch nur sehr wenige.

software/adaware/ aus dem Internet herunterladen können. Beachten Sie auch hier, dass die Software nur zuverlässig arbeitet, wenn sie regelmäßig per Update auf den neuesten Stand gebracht wird.

Bots und Botnets

Wir besprechen das Thema Botnets bewusst erst an dieser Stelle und separat von den Trojanern, um die verschiedenen Arten von Schädlingen und die Verknüpfungen unter diesen getrennt beurteilen zu können. Botnets sind nun quasi der Grund für den ganzen Aufwand, den bösartige Programmierer treiben, und somit der Schlüssel zum Verständnis des zuvor Gelesenen.

Als Bots bezeichnet man Programme, die weitgehend selbstständig bestimmte Aufgaben übernehmen, mit denen eine menschlich gesteuerte Software überfordert wäre. Der klassischste aller Bots ist dabei sicherlich der IRC-Bot. *Der Internet Relay Chat* ist das größte weltumspannende Chatsystem im Internet und verfügt zu jederzeit über hunderttausende einzelner Chaträume. Dabei kann jeder Benutzer (von zahlreichen Betriebsystemen aus) einen Chatroom eröffnen, nach Belieben benennen und sogar per Passwort schützen. Der eröffnende Benutzer wird zugleich Chat-Operator für den betreffenden Raum und kann somit unerwünschte Gäste aussperren und weitere administrative Funktionen wahrnehmen. Verlässt der letzte Benutzer den Chatroom, hört dieser auf zu existieren. Bestimmte Namen für Chatrooms können nicht dauerhaft reserviert werden.

Da zahlreiche Communities aber genau dies möchten, wurden Chat-Bots erfunden. Dabei handelt es sich um kleine Prograämmchen, die auf einem Server laufen und nichts anderes tun, als rund um die Uhr in dem jeweiligen Chatroom zu sein und dort Operatorfunktionen innezuhaben. Betritt dann der Betreiber des Bots den Raum, kann er sich die Rechte von diesem übertragen lassen und wird selbst zum Operator. Bots können aber auch andere Funktionen einnehmen, wie etwa Chats zu protokollieren oder Hilfefunktionen für neue Benutzer anzubieten.

Bots an sich sind also weder gut noch schlecht. Die Bots aber, von denen wir im Folgenden sprechen werden (die auch Zombies genannt werden), wurden für bösartige Zwecke erschaffen. Diese Bots sind nichts anderes als von Trojanern infizierte Endbenutzer-PCs. Wenn ein Angreifer einen Wurm-Trojaner-Mix im Internet verbreitet, so tut er das oft, um möglichst viele solcher Bots für sich zu gewinnen. Der Wurm dringt in das System ein, hinterlässt dort das Bot-Programm und versucht sich anschließend auf weitere PCs auszubreiten. Das Programm meldet sich sogleich an einem bestimmten IRC-Channel (Chatroom) an, dessen Zugangspasswort es kennt, und wartet dort auf Befehle des Crackers. Dieser kann sich nun wiederum selbst im Chatroom anmelden und Befehle an die einzelnen Bots verteilen und somit die befallenen Systeme fernlenken.

Neben diesen bösartigen IRC-Bots gibt es weitere Bot-Arten, die jedoch alle nach demselben Prinzip funktionieren. Die Bots laufen im Verborgenen auf den kompromittierten Rechnern und warten dort auf die Befehle eines Master-Bots, der vom Angreifer gelenkt wird. Wir wollen uns hier jedoch nur mit IRC-Botnets beschäftigen.

Die Summe aller Bots, die in einem Chatroom auf die Befehle des Angreifers warten, nennt man *Botnet*. Natürlich kommen ständig neue Bots hinzu und andere verschwinden wieder. Dies kann einerseits daran liegen, dass der PC-Benutzer mittels eines Scanners den Befall entdeckt und den Bot entfernt hat. Viel wahrscheinlicher aber ist es, dass der befallene PC gerade ausgeschaltet oder nicht mit dem Internet verbunden ist. Diese Schwankungen sind teils erheblich und hängen auch von der Zeitzone ab, in der der Angreifer sitzt. Hat er beispielsweise vor allen Dingen Rechner aus den USA unter seiner Kontrolle, stehen ihm tagsüber (nordamerikanischer Zeit) viel mehr Bots zur Verfügung als nachts.

Das bisher größte beobachtete IRC-Botnet (im Jahr 2003) bestand aus über 100.000 einzelnen Rechnern! Diese Zahl ist unvorstellbar groß und der Schaden, den man mit einem solchen Zombienetz anrichten könnte, ist immens. Der Aufbau und die Pflege eines solchen Netzes sind jedoch extrem aufwändig und gefährlich, und ein Cracker prahlt zwar sehr gerne mit der Größe seines Botnets, würde es aber niemals unnötig aufs Spiel setzen. Benutzt er das Netz beispielsweise dazu, von zehntausenden Rechnern gleichzeitig Datenmüll an einen bestimmten Online-Shop zu schicken, wird dieser unter der Last zusammenbrechen und nicht mehr erreichbar sein. Der Angreifer riskiert aber, dass zahlreiche seiner Bots auffliegen oder er sogar selbst gefasst wird. Leider ist es jedoch extrem schwierig, herauszufinden wer eine solche verteilte Attacke lenkte und die meisten Täter fühlen sich daher zurecht sehr sicher.

Geschickte Cracker nutzen Ihre Botnets daher nicht für spektakuläre Angriffe aus,[13] sondern verkaufen Dienstleistungen mittels dieser Bots. Vielleicht haben Sie sich schon einmal gefragt, wer eigentlich in der Lage ist, so viel Spam im Internet zu verteilen, dass nur jede vierte Nachricht, die in der durchnittlichen Mailbox eines Benutzers landet, wirklich erwünscht ist. Stündlich werden also mehrere Millionen Spam-Nachrichten verschickt. Kein Server dieser Welt, und sei er noch so teuer, verfügt über ausreichend Rechenkapazität und Leitungsbandbreite, um hunderttausende Nachrichten pro Minute zu verschicken. Selbst wenn es einen solchen Rechner geben sollte, wäre es für die Behörden und Internetorganisationen ein Leichtes, diesen zentralen Rechner stillzulegen und somit das Problem Spam aus der Welt zu schaffen. Professionelle Spammer mieten daher ganze Botnetze von Cracker-Gruppen an und nutzen die in den Bots enthaltenen SMTP-Server zum mas-

13 Es sei denn es geht darum, damit einen anderen Cracker oder Cracker-Ring anzugreifen, denn bei diesen ist sicher, dass sie sich nicht an die Polizei wenden. Solche Bot-Kriege unter rivalisierenden Gruppen finden täglich statt.

senhaften Mailen (*SirCam* war hier wirklich richtungweisend). Diese Art von Spam kann nicht blockiert werden, denn jeder Bot hat nur eine dynamische Anbindung zum Internet und wechselt daher pro Einwahl seine Internetadresse. Selbst wenn man die einzelnen Bots stilllegte, würde man damit einzig und allein die ahnungslosen PC-Besitzer treffen. Der Vermietungspreis für ein Botnet beträgt übrigens oftmals mehrere tausend, teils zehntausend Dollar.

Die Fälle, in denen Botnets für DDoS-Angriffe gegen einzelne Internetseiten oder Netze herangezogen werden, sind spektakulär. Grundsätzlich sollte man hier zwischen den einzelnen DDos-Attacken genau unterscheiden. Insgesamt ist davon auszugehen, dass jährlich zehntausende dieser Angriffe stattfinden und neben befeindeten Crackergruppen täglich auch Online-Shops, Communities und Infoportale betroffen sind und zum Erliegen gebracht werden. Einen beträchtlichen finanziellen Schaden oder Imageverlust richtet jedoch nur ein relativ geringer Teil dieser Angriffe an. So versuchten Cracker 2005 beispielsweise ein Online-Wettbüro zu erpressen und forderten 40.000 Euro für die Einstellung eines DDos-Angriffs. Besonderes Augenmerk verdient sicherlich auch der Angriff auf die Webseiten des heise-Verlags (*www.heise.de*). Im Februar 2005 gelang es immer noch unbekannten Angreifern, die komplette Webpräsenz des heise-Verlags so massiv anzugreifen, dass die Seite über drei Tage kaum oder gar nicht zu erreichen war. Dabei reagierten die Angreifer immer wieder auf Änderungen der heise-Administratoren und konnten den Angriff so über lange Zeit erfolgreich durchführen. Der heise-Verlag und vor allem der heise-Newsticker zählt zu den wichtigsten deutschen IT-Informationsquellen und genießt in großen Kreisen (auch der Crackerszene) sehr hohes Ansehen. Ausgerechnet diesen Server lahm zu legen, ist aus Crackerperspektive ein großer Erfolg und kann, zumindest in Deutschland, kaum noch übertroffen werden. Auf lange Sicht sind daher die Chancen, die Täter zu fassen, nicht schlecht, denn früher oder später wird jemand zu laut mit diesem Angriffserfolg prahlen.

Die mehreren hundert Botnets, die rund um die Welt aktiv sind, bestehen aus einigen hundert bis zehntausend Rechnern, und viele davon sind groß genug, um empfindliche Teile des Internets lahm zu legen und Schaden in Höhe vieler Milliarden Euro zu verursachen.

Vorsichtsmaßnahmen gegen Malware

Den wichtigsten Schutz vor einer Infektion durch Malware stellen Antiviren-Programme dar. Da diese aber in der Regel nur bekannte Schädlinge ausmachen können, ist der Schutz durch solche Software keineswegs vollständig. Zwar preisen die Hersteller ihre Software häufig mit dem Vermerk an, sie könne auch unbekannte Viren erkennen, dieser Funktion ist aber nur bedingt zu trauen. Richtig ist zwar, dass die Produkte bei Zugriffen oder Situationen, die ihnen ungewöhnlich erscheinen, Alarm schlagen, dies bedeutet jedoch noch lange nicht, dass neue Viren zuverlässig erkannt werden. So konnte sich beispielsweise der *SirCam*-Wurm auf dem

System des Benutzers austoben, ohne dass irgendein Virenscanner eine Gefahr gemeldet hätte.

Weitere Einzelheiten zu den Scannern und ihren Funktionen wollen wir in einem späteren Abschnitt thematisieren und uns an dieser Stelle insbesondere mit den Maßnahmen befassen, die Sie als User bewusst treffen müssen, um die Gefahr eines Befalls zu reduzieren. Weiterhin fällt der Schutz vor einigen Würmern immer mehr in den Aufgabenbereich der so genannten Firewalls, die wir im nächsten Kapitel ausführlich besprechen wollen.

Datenträger, Dokumente und Downloads scannen

Die klassischen Viren verbreiten sich entweder über Dateien oder über Datenträger, daher sollten Sie niemals Software von unbeschrifteten Datenträgern installieren, deren Quelle Sie nicht eindeutig ausmachen können. Dies gilt für Disketten, die Sie auf Ihrem Arbeitstisch finden, wie auch für selbst gebrannte CDs von einem Nachbarn oder Freund.

Wenn Sie dennoch einmal Dateien von einem fremden Datenträger benötigen, sollten Sie diesen unbedingt vorher mit Ihrer Antivirensoftware scannen und so schon von vornherein Infektionen vorbeugen.[14] Da Sie sich aber niemals sicher sein können, wie es um das Sicherheitsbewusstsein von Kollegen oder Freunden bestellt ist, sollten Sie nach Möglichkeit auch augenscheinlich vertrauenswürdige Datenträger scannen. Unter keinen Umständen sollten Sie Ihren Rechner von fremden Datenträgern booten. Legen Sie solche CDs und Disketten daher erst dann ein, wenn Sie diese auch tatsächlich benötigen.

Während in der Zeit fortgeschrittener Vernetzung und des Internets immer seltener Datenträger zum Informationsaustausch benutzt werden, verhält es sich mit zugeschickten Dokumenten oder Downloads umgekehrt. Um auch hier keine unnötigen Risiken einzugehen, empfiehlt es sich, die im Kapitel 3, *Sicherheitsbewusstsein*, empfohlenen Maßnahmen zu ergreifen und beispielsweise nur von seriösen Quellen Downloads vorzunehmen.

Bevor Sie auch auf den ersten Blick vertrauenswürdige Office-Dokumente öffnen, sollten Sie die Einstellungen in Ihrem Office-Paket so ändern, dass Makros nicht mehr automatisch ausgeführt werden können. Sollten dann tatsächlich Makros in einem Dokument enthalten sein, fragt die Applikation vorher nach, ob diese ausgeführt werden dürfen. Grundsätzlich empfiehlt es sich, dies zunächst einmal abzulehnen und Rücksprache mit dem Absender zu halten, ob er bewusst Makros integriert hat und wenn ja, zu welchem Zweck. Erst dann sollten Sie die Makros, falls zwingend nötig, aktivieren.

14 Zahlreiche Virenscanner bieten dazu einen Beim-Zugriff-Scan, der automatisch alle Dateien untersucht, auf die der Benutzer zugreifen möchte.

Mail-Attachments mit Bedacht prüfen

Immer häufiger breiten sich Viren und Würmer durch E-Mail-Anhänge aus. Daher gilt es hier inzwischen, besondere Maßnahmen zu ergreifen. Im einfachsten Fall erhalten Sie eine Mail samt Attachment von einem *fremden* Empfänger. Solche Nachrichten gehören direkt in den Papierkorb und sollten unter keinen Umständen geöffnet werden. Da die meisten Würmer sich mit der Quelladresse des Opfers verschicken, reicht diese einfache Unterscheidung leider nicht aus.

Ein zweites Kriterium, das als sehr sicher erachtet werden kann, ist entweder der Betreff oder der Mail-Body. Sollten diese in englischer, spanischer oder sonst einer Sprache verfasst sein, in der der angebliche Absender mit Sicherheit nicht mit Ihnen sprechen würde, ist Vorsicht angebracht. Spätestens wenn Ihnen ein Arbeitskollege plötzlich eine Mail samt Attachment auf Englisch schickt, sollten Sie diese nicht öffnen, sondern erst einmal telefonisch Rücksprache halten.

Einige Würmer wie z. B. *SirCam* sind bereits so clever und benennen die Betreffzeile nach dem Namen des Attachments, so dass man hier verschärft auf den Nachrichten-Body schauen muss.

Ein weiterer wichtiger Hinweis auf Würmer in Attachments sind die so genannten *doppelten Extensions*. Diese erkennen Sie daran, dass nicht wie im Normalfall nur eine Dateiendung, sondern zwei enthalten sind. Ein solches Dokument könnte beispielsweise den Namen *wichtig.doc.vbs* im Falle einer als *Word*-Dokument getarnten Visual Basic Script-Datei tragen oder *bild.jpg.exe* im Falle eines ausführbaren Programms, das sich als Bild zu tarnen versucht. Genaueres hierzu finden Sie in Kapitel 3, *Sicherheitsbewusstsein*.

Auch wenn keines dieser Kriterien zutrifft und der Adressat Ihnen sogar bewusst ein Attachment geschickt hat, bedeutet dies jedoch keineswegs, dass das Dokument virenfrei ist.

Bitte beachten Sie, dass im Falle von Outlook und Outlook Express besondere Vorsicht geboten ist, hier reicht es teilweise aus, eine E-Mail anzuklicken (zu lesen), um sich zu infizieren. Deaktivieren Sie daher bei diesen Produkten immer die so genannte Vorschaufunktion. So bleibt Ihnen wenigstens die Möglichkeit verdächtige E-Mails zu löschen, ohne dass diese Schaden anrichten können.

Mehrere E-Mail-Konten nutzen

Je mehr Menschen im Besitz Ihrer E-Mail-Adresse sind, desto größer ist die Wahrscheinlichkeit, dass Sie früher oder später einen Wurm zugeschickt bekommen. Es empfiehlt sich daher immer, mindestens zwei Konten zu führen: eines für einen engeren Personenkreis samt Arbeitskollegen und Bekanntschaft und ein weiteres für den Rest der Welt. Während Sie Attachments aus dem zweiten Konto grundsätzlich nicht oder nur in besonderen Fällen öffnen sollten, bleibt die Gefahr für Ihr erstes

Konto kleiner. Sie behalten leichter den Überblick, wer eigentlich an dieses Konto schreibt und welche Nachrichten verdächtig sind. Dennoch ist natürlich auch hier weiterhin Vorsicht geboten: Wenn Sie ein verdächtiges Attachment erhalten, öffnen Sie es erst, wenn Ihnen der Absender bestätigt hat, dass es wirklich von ihm ist.

Benutzen Sie für das zweite Konto keinen Account auf Ihrer Festplatte, sondern einen Freemail-Dienst. So können Sie überdies sicher sein, dass auch eine schädliche Mail ohne Attachment ihre Wirkung nicht auf dem lokalen System entfalten kann. Zwar gibt es auch in einem solchen Fall Ausnahmen von der Regel, 100-prozentigen Schutz kann Ihnen aber ohnehin kein Dienst bieten.

Zugriffsrechte im lokalen Netz begrenzen

Immer mehr Würmer nutzen nicht nur das Internet als Träger von Host zu Host, sondern versuchen – einmal in ein Netz eingedrungen –, sich auch lokal in diesem zu vermehren. In den meisten Fällen sucht der Schädling nach freigegebenen Ordnern und infiziert die dort zugreifbaren Dateien. Daher sollten Sie sowohl in Ihrem privaten Heimnetzwerk als auch am Arbeitsplatz niemals unnötig Verzeichnisse freigeben. Sollte dies aus irgendwelchen Gründen unbedingt erforderlich sein, ist darauf zu achten, dass nur Leserechte vergeben werden. Wer jedoch glaubt, dass dies ausreicht, um die Würmer an der Verbreitung zu hindern, ist auf dem Holzweg.

Ein einfaches Beispiel soll dies demonstrieren: Ein neuartiger Wurm gelangt über einen E-Mail-Anhang auf ein System in Ihrem Netzwerk. Der Schädling durchsucht daraufhin den Host und pflanzt ein Makro in die gefundenen Word-Dokumente in einem Netzwerkordner. Zwar können die Benutzer, die auf ihn zugreifen, nur lesen und nicht darin schreiben, diese Einschränkung gilt jedoch nicht für das lokale System, auf dem sich die Dokumente befinden. Öffnet nun ein anderer Benutzer die bereits infizierte Datei, wird das Makro auch bei ihm ausgeführt, und das System ist unterminiert und kann nun weitere Hosts anstecken. Zwar war es in der Vergangenheit nur selten der Fall, dass ein Wurm solche Schadensroutinen mitbrachte, der Fall von *SirCam* und *Phatbot* illustriert jedoch eindrucksvoll, dass wir in dieser Richtung noch viel erleben werden.

Netzdienste sparsam einsetzen

Um auf ein System zu gelangen, müssen die Würmer sich einen offenen Dienst zunutze machen. Dabei kann es sich um einen E-Mail-Client, einen Dateifreigabedienst oder auch, wie im Fall von *CodeRed*, um einen HTTP-Dienst handeln. Ein System ohne lauschende Dienste ist also schwierig oder nur über Umwege angreifbar. Daher gilt auch hier die Regel, dass weniger mehr ist. Als Privatperson sollten Sie daher keinen Webserver auf Ihrem eigenen System betreiben oder diesen nur bei Bedarf starten; Gleiches gilt für Serverfunktionen bei Online-Spielen und vor allem

für so anfällige Dienste wie FTP oder Telnet. Öffnen Sie daher, auch ins lokale Netz, nur so viele Türen, wie unbedingt nötig sind.

Antiviren-Software

Die ersten Antiviren-Produkte waren eher an Administratoren und Firmenkunden als an Privatpersonen gerichtet. Heutzutage gibt es aber gerade für den Heimmarkt eine große Menge interessanter und leistungsfähiger Produkte. Während man den Einsatz solcher Software früher als nützlich, aber nicht essenziell ansehen konnte, hat sich dies heute grundsätzlich geändert. Ein aktueller Virenscanner ist auf jedem an ein Netzwerk oder das Internet angeschlossenen Computer Pflicht. Der Verzicht auf solche Software gefährdet nicht nur Ihre Daten und die Sicherheit Ihres eigenen Systems, sondern auch in immer größerem Maße andere Hosts. Während man früher also nur eine Gefahr für sich selbst darstellte, muss man heutzutage auch Verantwortung für andere Benutzer und Systeme mittragen. Schließlich erwarten Sie auch von Ihren Kollegen oder Freunden, dass deren Dokumente virenfrei sind und Sie diese ohne Gefahr öffnen können.

Mit dem Kauf eines Virenscanners beginnt jedoch erst der stete Kampf gegen die Schädlinge, denn bei täglich neu erscheinenden Viren ist ein frisch gekaufter Scanner schon nach wenigen Wochen nicht mehr aktuell. Zwar erkennen einige Scanner auch unbekannte Schädlinge, indem sie nach verdächtigen Zugriffen und Routinen suchen, zuverlässig ist dieser Schutz jedoch keineswegs. Daher sollten Sie beim Kauf der Antiviren-Software darauf achten, dass der Hersteller regelmäßig neue Viren-Updates zur Verfügung stellt. Besonders die großen Hersteller wie McAfee oder Symantec bringen ihre Updates mindestens im wöchentlichen Zyklus heraus und reagieren auf neue, gefährliche Würmer und Viren sogar innerhalb weniger Stunden. Wichtig für Sie als Benutzer ist es daher, dieses Angebot auch wahrzunehmen und in regelmäßigen Abständen die aktuellen Virusdefinitionen aufzuspielen. Besonders elegant funktioniert das, wenn der jeweilige Scanner automatisch im Internet nach Updates suchen und diese installieren kann.[15] Da der Hersteller nicht nur mit dem eigentlichen Produkt, sondern auch mit seinen Updates Geld verdienen möchte, gilt das Update-Recht meist nur für die ersten sechs oder zwölf Monate nach der Installation. Wer danach noch aktuelle Definitionen beziehen möchte, wird, glücklicherweise nur in geringem Umfang, zur Kasse gebeten.

Da die Vorstellung einzelner Produkte mit ihrer Vielzahl an Optionen und Einstellungsmöglichkeiten den Rahmen des Buchs sprengen würde, wollen wir uns hier auf die drei Vertreter konzentrieren, die in Deutschland am häufigsten anzutreffen

15 An anderer Stelle haben wir davon abgeraten, Programmen den automatischen Zugriff aufs Internet zu erlauben. Im Prinzip sollte das auch für Virenscanner gelten. Da Virenschutz aber in zunehmendem Maß wichtig wird und ein regelmäßiges Updaten auf keinen Fall vergessen werden sollte, machen wir hier eine Ausnahme von dieser Regel.

sind, und diese im Folgenden kurz vorstellen. Es soll jedoch nicht unerwähnt bleiben, dass es mit Bitdefender, AntiVirenKit und F-Secure Anti-Virus und vielen mehr weitere ausgezeichnete Produkte auf dem Markt gibt. In jedem Fall aber sollten Sie darauf achten, dass das Programm einen Beim-Zugriff-Scanner (*On-Access*) besitzt und nicht nur einen On-Demand-Scanner, den sie regelmäßig selber nach Viren suchen lassen müssen. Bitdefender gibt es beispielsweise in zwei Versionen von denen die kostenlose nur über einen On-Demand-Scanner verfügt – dennoch lohnt dieser als Zweitscanner, da der Hersteller täglich Updates zur Verfügung stellt, wobei selbst die große Konkurrenz nicht mithalten kann.

AntiVir Personal Edition

AntiVir Personal Edition stellt die Lightversion des großen *Professional*-Scanners der Firma H+BEDV dar. Er ist für den privaten, nicht kommerziellen Gebrauch kostenlos unter *http://www.free-av.de* erhältlich und gerade mal 7 MByte groß.[16] Zwar verfügt die Personal Edition noch längst nicht über die Vielzahl an Optionen und die Netzwerkfähigkeit des großen Bruders, sie reicht für den Gebrauch zu Hause jedoch völlig aus.[17]

Bereits während der Installation führt *AntiVir* einen ersten kurzen oder nach Wunsch auch einen vollständigen Scan des Systems durch. Wie auch das restliche Programm wirkt das eigentliche Scantool, das auf den amüsanten Namen *Luke Filewalker* hört, grafisch etwas angestaubt. Dafür fallen aber die Geschwindigkeit und der geringe Verbrauch von Speicherressourcen positiv auf.

Wichtigste Kriterien sind bei einer Antivirensoftware neben der Erkennungsrate auch die Update-Fähigkeit und der Takt, in dem neue Virusdefinitionen erscheinen. Auch in dieser Hinsicht braucht sich die Personal Edition nicht vor kommerziellen Produkten zu verstecken, auch an ein Internet-Update direkt aus dem Programm heraus und einen Scheduler (für das Programmieren regelmäßiger automatischer Scans) haben die Entwickler gedacht.

Gerade da AntiVir nicht nur kostenlos und somit weit verbreitet ist, sondern auch qualitativ überzeugt,[18] ist es zum Hauptangriffsziel zahlreicher Würmer und Trojaner geworden (Ähnliches gilt für die ZoneLabs-Firewall, die Sie in Kapitel 12, *Firewalls und erweiterte Sicherheitssysteme*, kennen lernen). Zahlreiche Schädlinge sorgen also dafür, dass AntiVir nicht mehr sauber arbeiten kann. Wenn nach der Installation der Software das Regenschirmsymbol in der Taskleiste geschlossen bleibt und es nicht gelingt, AntiVir zu aktivieren, wird der Prozess durch einen

16 Neben der kostenlosen Version gibt es die AntiVir Personal Edition Premium für 20 Euro pro Jahr.

17 Neben einer Version für Windows gibt es auch Editionen für Linux und weitere Unix-Derivate (FreeBSD, Solaris, etc.).

18 Dabei muss dennoch erwähnt werden, dass AntiVir in der Personal Edition mit den Virenscannern von Symantec und McAfee nicht mehr ganz mithalten kann. Dies gilt leider auch für die Erkennungsrate.

Schädling geblockt. Wie man in solchen Fällen dennoch zum Ziel kommt, erklärt das Kapitel 13, *Erste Hilfe*. Achten Sie daher stets darauf, dass das Regenschirmsymbol geöffnet und die Software auf dem akuellen Stand ist.

Norton AntiVirus

Zwar besteht die Norton-Reihe noch aus einer ganzen Palette anderer Produkte, die Antivirensoftware gehört aber mit Sicherheit zu einer der berühmtesten Applikationen aus dem Hause Symantec.[19] Allerdings empfiehlt es sich, diese nicht einzeln, sondern als Teil eines Pakets zu kaufen. Möchte man beispielsweise die Firewall gleich miterwerben (siehe dazu Kapitel 12, *Firewalls und erweiterte Sicherheitssysteme*), spart man im Paket nicht nur Geld, sondern erhält dafür eine sauber integrierte Version beider Programme, die gut miteinander harmonieren. Mit seinen zahlreichen Funktionen, zum Beispiel der »Impfung« von Dateien und einer sehr umfassenden Routine zum Erkennen noch unbekannter Schädlinge, gehört Norton AntiVirus zu den leistungsfähigsten Scannern auf dem Markt. Ein Scheduler und das automatische Updaten der Virusdefinitionen und sogar der eigentlichen Software gehören hier schon seit früheren Versionen zum Standard.

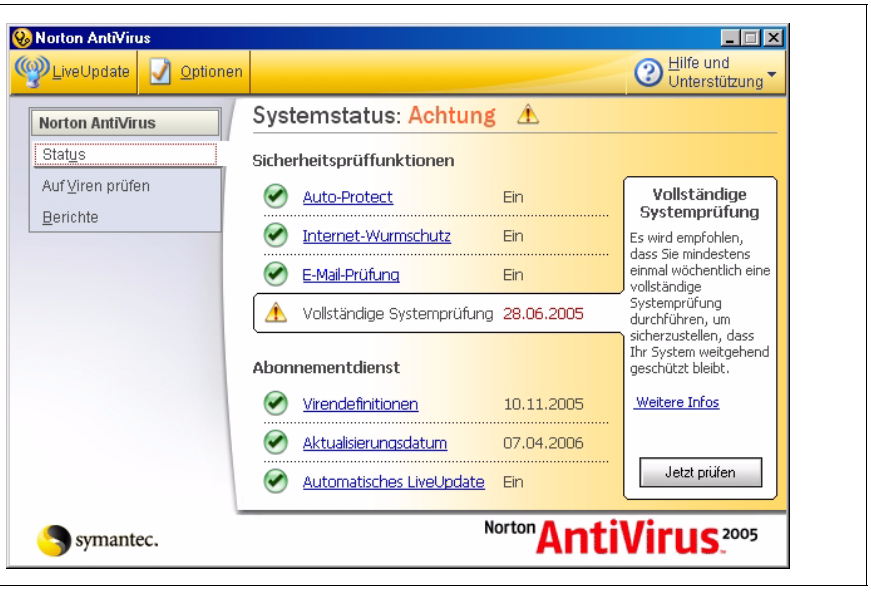

Abbildung 10-5: Aufgeräumt und übersichtlich: Norton AntiVirus 2005

19 Norton AntiVirus 2006 ist für ca. 45 Euro pro Jahr zu haben, Sie können ältere Versionen jedoch gegen eine geringe Gebühr aktuell halten.

Nennenswert ist auch der E-Mail-Schutz. Dabei verändert Norton AntiVirus die Einstellungen in Ihrem Mail-Client automatisch so, dass der Verkehr erst über einen dazugehörigen POP-Proxy fließt und so die Attachments schon im Vorfeld auf mögliche Gefahren gescannt werden können. Das mag zwar nicht jedermanns Sache sein, funktioniert aber erstaunlich gut. Schade ist nur, dass es dabei teilweise zu Verzögerungen oder langsamen Übertragungsraten kommen kann.

McAfee VirusScan

Ebenso wie den Norton-Scanner können Sie das McAfee-Produkt im Paket kaufen und so eine voll integrierte Sicherheitslösung erhalten. Im Leistungsumfang und der Qualität unterscheiden sich die Scanner von McAfee und Symantec kaum, auch wenn dem erstgenannten eine schnellere Scan-Engine nachgesagt wird. Festzuhalten bleibt jedoch, dass McAfee deutlich detailliertere Einstellungsmöglichkeiten bietet und sich eher an fortgeschrittene oder ambitionierte Benutzer richtet. Hingegen kann er in puncto Benutzerfreundlichkeit weniger punkten, da viele zusätzliche Informationen nur auf Englisch vorliegen. Abbildung 10-6 zeigt eine von VirusScan gefundene Hintertür auf einem System. Diese hatte der Konkurrent AntiVir Personal übrigens im Testlauf übersehen. Dies liegt aber nicht daran, dass AntiVir in diesem konkreten Fall schlechter wäre als der McAfee Scanner, sondern schlicht und einfach daran, dass McAfee den AntiVir Scanner als Schädling erkennt. Dies ist ein bekanntes Problem, das hier jedoch nicht weiter besprochen werden soll. Installieren Sie also unbedingt nur einen On-Access-Scanner auf Ihrem Computer.

Abbildung 10-6: VirusScan findet eine Hintertür auf dem System.

Zuverlässigkeit von Virenscannern

Auch wenn die Produkte heutzutage sehr ausgreift sind und die größeren Hersteller schon auf Erfahrung vieler Jahre zurückgreifen können, zeigen sich doch auch immer wieder einige spezifische Schwächen.

So funktioniert zum einen das Erkennen unbekannter Schädlinge nur sehr unzuverlässig, zum anderen hapert es immer wieder bei der Beseitigung von Viren und Würmern. Das Entdecken und Anzeigen eines Virenbefalls ist zwar der erste wichtige Schritt, bringt allein aber noch nichts, wenn der Virus gar nicht, nur teilweise oder falsch entfernt wird. Regelmäßig liest man in Foren und Newsgroups Berichte von zerstörten Dateien oder gar ganzen Betriebssystemen, die nach einer »erfolgreichen« Bekämpfung eines Virus den Geist aufgegeben haben. Daher sollten Sie trotz Virenscanner immer auf das regelmäßige Anfertigen von (noch nicht infizierten) Backups achten.

Auch vor dem Entfernen eines Schädlings sollte nach Möglichkeit eine Sicherungskopie angefertigt werden. Diese ist zwar dann mit dem Virus infiziert; gelingt es dem jeweiligen Antiviren-Programm jedoch nicht, das betreffende Dokument ordentlich zu restaurieren, kann man es anschließend mit einem Produkt der Konkurrenz noch einmal versuchen oder beim Support um Rat fragen.

Ein weiterer Fehler der meisten Produkte ist besonders erstaunlich: So sind diese zwar wahre Meister darin, Sie vor bösartigen Programmen zu schützen, der Eigenschutz wird dabei aber oft komplett vernachlässigt. Wie die Zeitschrift *c't* berichtete, speicherte eines der bekannteren Produkte zum Beispiel die Liste der zu scannenden Dateitypen in einer unverschlüsselten Textdatei ab. Ein nicht sofort erkannter, ganz neuer Schädling könnte ganz einfach diese Datei so umschreiben, dass beispielsweise statt *.doc* oder *.ppt*-Dokumenten nur *.do1* und *.pp1* gescannt würden. Während weder der Benutzer noch der Scanner etwas davon mitbekommen würden, könnte der Virus in aller Ruhe Word- und Powerpoint-Dateien befallen, da diese ja dann nicht mehr auf der Liste der zu untersuchenden Dokumente stünden.

Ausblick auf die weitere Entwicklung

Bei der rasanten Entwicklung der verschiedenen Schädlinge in den letzten vier Jahren ist es natürlich nur schwer möglich, einen zuverlässigen Blick in die Zukunft zu werfen. Einige Tendenzen können wir dennoch festhalten.

Als Hauptgrund für die starke Verbreitung der Würmer ist sicherlich der immer stärker werdende Einfluss des Internets zu nennen. Bei zurzeit schätzungsweise 500 Millionen Internetnutzern ist es nicht weiter verwunderlich, dass ein Schädling, der genau diese Technologie zur Vermehrung nutzt, eine perfekte Reproduktionsgrundlage vorfindet. Zur weiteren Verbesserung der Lebensgrundlage der Würmer hat aber auch die starke Microsoft-Monokultur erheblich beigetragen, die es Würmern

erlaubt, immer genügend Opfersysteme ausfindig zu machen, die sich mit der gleichen Methode befallen lassen. Hinzu kommt noch, dass Microsoft-Betriebssysteme von Haus aus anfällig gegen solche Angriffe sind, die durch den Einsatz unsicherer Skriptsprachen noch gefördert werden. Den momentanen Höhepunkt dieser Entwicklung stellt sicher *Sasser* dar, der es fertig brachte, Rechner völlig ohne aktives Zutun der Benutzer zu infizieren. Es reichte vollkommen aus, mit einem Windows-System online zu gehen, um befallen zu werden.

Angenommen, jeder durch Sasser befallene Host (immerhin über eine Million) würde nicht nur abstürzen oder Bandbreite verbrauchen, sondern eine Liste der wichtigsten DNS-Server auf der Ebene der Top-Level-Domains mit einer DoS-Attacke angreifen: Teile der Infrastruktur des Internets würden innerhalb kürzester Zeit ausfallen.

Vor einem solchen Zusammenbruch wird übrigens seit Jahren gewarnt, und es scheint nur eine Frage der Zeit zu sein, dass sich ein Angreifer findet, der leichtsinnig genug ist, sein Botnet gegen zentrale Ziele zu lenken. Dass einige Schädlinge sogar Bankautomaten zum Abstürzen bringen und auch mit den Stromausfällen in den USA in Zusammenhang gebracht werden,[20] zeigt, wie gefährlich die weltweite Vernetzung möglicherweise sein kann.

Die jüngste Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI) prangert immer noch fehlendes Sicherheitsbewusstsein als einen der Hauptgründe für die Ausbreitung von Computerschädlingen an. Dies gilt sowohl für die Endanwender als auch für die Softwareindustie. Zwar muss man einräumen, dass Microsoft inzwischen anfängt, das Thema Sicherheit wirklich ernst zu nehmen, doch angesichts der gigantischen finanziellen Mittel, die diesem Konzern zur Verfügung stehen, der enormen Bedrohung und der über 60 Milliarden[21] US-Dollar Schäden, die jährlich entstehen, fragt man sich, ob es nicht auch möglich wäre, im Vorhinein typische Programmierfehler zu vermeiden, anstatt im Nachhinein wöchentlich Patches anzubieten.

Natürlich ist Software niemals völlig frei von Fehlern, und auch andere Betriebssysteme und Produkte leiden unter massiven Sicherheitslücken, doch das enschuldigt die groben und z.T. fahrlässigen Versäumnisse von Microsoft keineswegs.

Software sauber zu spezifizieren und zu entwickeln, ist sehr kostspielig, aber dass die meisten Unternehmen auf Kosten der Benutzer sparen, ist inakzeptabel. Die Schuld nur bei den großen Softwarehäusern zu suchen, wäre jedoch zu einfach gedacht, denn unsere eigene »Geiz-ist-Geil«-Mentalität spielt mindestens eine

20 Glücklicherweise können wir einige dieser Thesen eher als moderne Horrormärchen ansehen.

21 Grundsätzlich sollte man bei diesen offiziellen Zahlen sehr skeptisch sein und sie eher deutlich niedriger – wenn auch auf hohem Niveau – ansiedeln.

genauso große Rolle. Wenn der Preisdruck auf die Hersteller zu groß wird, leidet die Qualität.

Wenn die Verflechtung zwischen Würmern, Tojanern, Spyware und geschäftlichen Interessen weiter zunimmt, steigt das Risiko für den einzelnen PC-Benutzer in Zukunft deutlich an. Eine erste Konsequenz daraus werden wir in Kapitel 11, *Angriffsszenarien*, eingehender beleuchten. Die Abbildung 10-7 zeigt jedoch schon sehr deutlich, wohin die Reise geht: Unter den Top-Ten-Schädlingen finden sich inzwischen regelmäßig auch Spyware-Produkte mit kommerziellem Hintergrund.

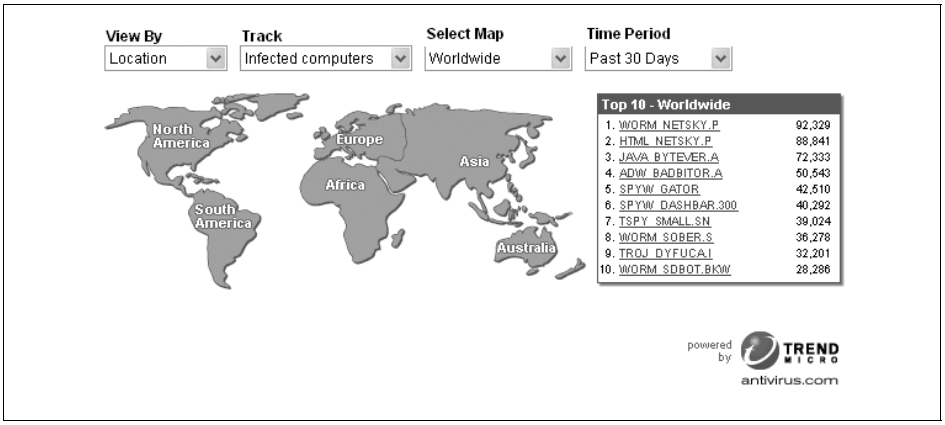

Abbildung 10-7: TrendMicro-Statistik für August 2005

Ein weiteres Problem versteckt sich hinter dem eigentlich positiv besetzten Begriff der *Usability*, also der Benutzbarkeit. Betriebssysteme und Programme versuchen, den Benutzer immer weiter vom eigentlichen System fern zu halten und ihn durch Assistenten zu unterstützen. Das führt jedoch gleichzeitig dazu, dass wir erstens immer weniger verstehen, was eigentlich in unseren Computern passiert, und dass uns zweitens zunehmend die Kontrolle entzogen wird. Wenn Sie beispielsweise zum ersten Mal eine Personal Firewall installieren, werden Sie überrascht feststellen, wie viele Programme völlig ohne Grund »nach Hause telefonieren«. Je mehr Funktionen ohne Rücksprache mit dem Benutzer auf unserem System arbeiten, desto größer ist die Gefahr, dass wir uns gegen Fehler in diesen Funktionen nicht wehren können.

Um dieses Kapitel jedoch nicht mit einem so düsteren Ausblick enden zu lassen, sei ebenso erwähnt, dass das Thema Computersicherheit so zentral geworden ist, dass sich nicht nur Unternehmen, sondern auch offene Communities und sogar Behörden damit auseinander setzen. Mit einem kostenlosen Virenscanner und fünf Minuten Installationsarbeit haben Sie schon einen ersten Schritt in eine sicherere Internetwelt getan. Und man wird Ihnen bei vielen Sicherheitsfragen in zahlreichen Internetforen gern mit Rat und Tat zur Seite stehen, wenn es einmal klemmt oder der eigene PC befallen ist.