In diesem Kapitel:
- Windows installieren
- Im Ernstfall

KAPITEL 13

Erste Hilfe

In diesem Kapitel wollen wir uns mit der sicheren Installation von Windows und dem Vorgehen im Falle eines erfolgreichen Einbruchs in Ihr System beschäftigen. Wir behandeln diese Themen bewusst erst an dieser Stelle, da sie ein grundlegendes Verständnis für die potenziellen Gefahren und Angriffstechniken voraussetzen.

Windows installieren

Wie Sie gelesen haben, ist es oberstes Ziel eines jeden Angriffs, zunächst einmal die Abwehrmaßnamen des Opfers zu kompromittieren. Daher sind Virenscanner, Firewalls und Updatesysteme in der Regel zuerst betroffen. Ist der PC erst einmal ohne Schutz, kann der Angreifer beliebig schalten und walten. Dieses Vorgehen ist dabei völlig unabhängig davon, ob es sich um einen menschlichen Angreifer oder dessen automatisiertes Werkzeug in Form eines Wurms oder Trojaners handelt.

Das Hauptproblem bei der Neuinstallation von Windows ist es daher, so lange zu »überleben«, bis man die nötigen Sicherheitsmaßnahmen ergriffen hat. Ist der Angreifer schneller, wird der zu spät installierte Virenscanner gar nicht erst zum Zuge kommen, da er keine Updates starten kann oder überhaupt nicht geladen wird.

Um die folgende Anleitung nicht auf den Benutzerkreis einer bestimmten Betriebssystemversion (wie etwa Windows XP Service Pack 2) zu beschränken, werden wir versuchen, sie so allgemein wie möglich zu halten und unabhängig davon, ob Sie Windows 2000, XP Home oder XP Professional benutzen.

Survival Time

Um die aktuelle Gefahrensituation im Internet zu messen und mit früheren Zeitpunkten zu vergleichen, bedienen sich Sicherheitsspezialisten zahlreicher Analysemethoden. Für Windows-Systeme ist dabei vor allem die *Survival Time* ein

aussagekräftiger Indikator. Dabei wird gemessen, wie lange ein Computer mit ungepatchtem Betriebssystem online überleben kann, wie lange es also im Durchschnitt dauert, bis der PC befallen ist. Dieser Test funktioniert natürlich nicht nur für Windows, sondern wird auch für Unix-Systeme oder bestimmte Applikationen gemessen (etwa ungepatchte HTTP-Server). Das Besondere an diesem Test ist, dass er über die Jahre hinweg einen kontinuierlichen Einblick in die Sicherheitslage des Internet gibt und die Testergebnisse miteinander vergleichbar sind. So lässt sich beispielsweise ersehen, ob die Sicherheit eines bestimmten Betriebssystems im Verhältnis zum Gefahrenpotenzial zu- oder auch abnimmt und wie erfolgreich (auf lange Sicht gesehen) bestimmte Sicherungsmaßnahmen und Updates ausfallen. Dies wird dadurch möglich, dass für eine solche Analyse die zum Testzeitpunkt aktuellen und verbreiteten Betriebssysteme herangezogen werden. Ältere Systeme sollten, falls möglich, proporzional zu ihrer aktuellen Verbreitung einbezogen werden.

Den wohl bekanntesten und zudem öffentlich zugänglichen Survival Time-Test finden Sie auf der Webseite des Internet Storm Center unter *http://isc.sans.org/survivalhistory.php*. Dort ist belegt, dass die Überlebenszeit eines ungepatchten Windows-Systems innerhalb der zweiten Jahreshälfte 2005 noch einmal spürbar abgenommen hat und derzeit bei unter 20 Minuten liegt. Im Vergleich dazu sind die knapp 1.000 Minuten bei Unix-Systemen noch ein akzeptabler Wert.

Spätestens mit dem Unterschreiten der 20-Minuten-Marke ist aber eine wichtige Messlatte gefallen, denn es dauert in der Regel deutlich länger, nach der Installation von Windows auf dem heimischen PC alle nötigen Updates herunterzuladen und die Sicherheitslösung (allen voran Firewall und Virenscanner) auf den neuesten Stand zu bringen. Die Konsequenz haben wir weiter oben bereits angesprochen. Noch bevor Sie sich gegen Angriffe zur Wehr setzen können, sind Sie meist schon zum Opfer geworden. Der Versuch, das System anschließend wieder zu säubern, stellt sich als viel zeitaufwändiger und gefährlicher heraus, als es einfach noch einmal – und diesmal richtig – neu zu installieren.

Natürlich muss man bedenken, dass diese 20 Minuten die *durchschnittliche* Zeit bis zum Befall darstellen. Es ist also ohne Weiteres möglich, dass Ihr System die ersten 30 oder 60 Minuten überlebt. Genauso kommt es aber vor, dass ein Computer bereits fünf Minuten nach der ersten Online-Verbindung befallen ist. Wie Sie im Laufe dieses Buchs bemerkt haben, zieht ein erster erfolgreicher Angriff meist einen ganzen Strom neuer Angriffe nach sich. So nutzen Würmer die Hintertüren bereits installierter Schädlinge, öffnen ihrerseits neue und installieren Spyware oder im schlimmsten Fall sogar Keylogger auf Ihrem System. Alle Passwörter, die Sie dann auf Ihrem scheinbar taufrischen System eingeben, landen anschließend in fremden Händen.

Vor der Installation

Wir gehen in diesem und den folgenden Abschnitten davon aus, dass Sie Windows eigenhändig auf dem (neuen) System installieren. Sollte es bereits vom Hersteller vorinstalliert worden sein, ist das Vorgehen, von wenigen Ausnahmen abgesehen, analog.

Zunächst einmal gilt es zu schauen, wie alt das Installationsmedium eigentlich ist. Microsoft presst zwar regelmäßig die neuesten Betriebssystemversionen auf CD; bis diese aber beim Händler und anschließend bei Ihnen ankommen, vergehen in der Regel viele Wochen. Dies liegt nicht zuletzt daran, dass der Händler hohe Stückzahlen ordert und diese erst einmal verkauft, bevor er die nächste Bestellung tätigt. So kommt es durchaus vor, dass selbst einem neu gekauften PC veraltete Windowsversionen beiliegen. Wenn Sie das Betriebssystem separat gekauft haben oder seit Monaten im Schreibtisch aufbewahren (z.B. von Ihrem letzten PC), sieht die Lage meist noch schlimmer aus. Es ist wichtig zu wissen, dass es nicht von der Betriebssystemversion abhängt, ob das System aktuell ist oder nicht. Wenn Sie also eine Windows XP Professional CD in den Händen halten, muss diese keineswegs aktuell sein.

Viel entscheidender ist die Version des enthaltenen Service Packs (SP), die man entweder auf der CD oder der Verpackung ablesen kann. Solche Service Packs kann man sich am besten als die Zusammenfassung zahlreicher einzelner Updates vorstellen. Microsoft gibt wöchentlich einzelne Updates heraus und werkelt nebenbei an weiteren Funktionen. Sind erst einmal genug dieser Verbesserungen zusammengekommen, werden sie gemeinsam mit erweiterten Optionen und teils auch größeren Betriebssystemänderungen in einem Service Pack veröffentlicht. Dennoch sollte man natürlich keineswegs mit dem Updaten auf ein Service Pack warten, denn diese erscheinen nur in unregelmäßigen Abständen, während Sicherheitslücken innerhalb weniger Tage oder Wochen ausgenutzt werden. Im Gegensatz zu einzelnen Patches, die meist deutlich kleiner als zehn MByte sind, fallen Service Packs entsprechend groß aus und sprengen oft die 100-MByte-Grenze. Daher dauert es mitunter eine halbe Stunde oder länger, bis das Service Pack auf Ihrer Festplatte ist – genau die Zeit, die Sie nicht haben.

Vor der Installation Ihres Betriebssystems gilt es daher zu prüfen, ob das Service Pack auf dem Installationsmedium aktuell ist. (Vorsicht: Keine Service Pack-Angabe bedeutet meistens, dass noch gar keines auf der CD enthalten ist!) Sollte dies nicht der Fall sein, empfiehlt es sich, das benötigte Service Pack (Sie brauchen jeweils nur das letzte) bei einem Bekannten oder im Internetcafe aus dem Netz zu laden und auf CD zu brennen. Alternativ hilft auch der Computerhändler um die Ecke weiter. Beim Herunterladen ist unbedingt darauf zu achten, das eigentliche Service Pack und nicht nur den Netz-Installer herunterzuladen.

Als Nächstes sollten Sie sich für ein Sicherheitspaket aus Firewall und Antivirenprogramm entscheiden und dieses vor der Installation des Systems erwerben oder herunterladen. Sollten Sie noch unschlüssig sein, können Sie mit der Kerio-Firewall und AntiVir Personal Edition einen guten Anfang machen. Unabhängig davon müssen Sie sicherstellen, dass Sie die Software von einer sicheren Quelle herunterladen (am besten direkt vom Hersteller) und keinesfalls etwa über eine Tauschbörse. Als Letztes sollten Sie noch einen Browser herunterladen oder eine der zahlreichen Computerzeitschriften beigefügten CDs nutzen. Es empfiehlt sich entweder Firefox oder Opera.

Wenn Sie die Software aus dem Internet laden, können Sie zudem davon ausgehen, dass die Version relativ aktuell ist.

Während der Installation

Während der Installation des eigentlichen Betriebssystems gilt es vor allem auf Folgendes zu achten: Zunächst einmal sollten Sie bei der Installation der Netzwerkkomponenten den benutzerdefinierten, manuellen Weg einschlagen und unbedingt den CLIENT FÜR MICROSOFT-NETZWERKE sowie die DATEI- UND DRUCKERFREIGABE FÜR MICROSOFT-NETZWERKE deaktivieren. Sollten Sie beides für das Heimnetzwerk brauchen, können Sie die Optionen zu einem späteren Zeitpunkt bequem wieder aktivieren. Anschließend wird Windows wahrscheinlich nach dem Internetzugang fragen und anbieten, diesen direkt bei der Installation einzurichten. Wenn Sie hier Ihre Zugangsdaten eingeben und zum Beispiel DSL-Nutzer sind, kann es Ihnen später passieren, dass Windows unmittelbar nach der Installation eine Verbindung zum Internet herstellt. Da das System zu diesem Zeitpunkt aber keineswegs sicher ist, sollten Sie genau das verhindern. Wenn Ihr PC über einen Router und DHCP direkt ins Internet gelangen könnte, so sollten Sie das Netzwerkkabel entfernen.

Je nach Windows-Version werden Sie dazu aufgefordert, ein Administratorpasswort einzugeben. Wählen Sie dieses mit Bedacht und achten Sie dabei auf eine alphanumerische Zusammensetzung. Anschließend sollten Sie nur einen weiteren Benutzer-Account anlegen und die restlichen erst später manuell ausstöpseln.

Unter Windows XP Home werden Sie eventuell nicht nach einem Administratorpasswort gefragt, denn bei dieser Version legt Windows das Konto automatisch ohne Passwort an. Das ist natürlich eine dramatische Sicherheitslücke, und Sie sollten nach der Installation in der Kommandozeile `net user Administrator` **`Ihr Kennwort`** eingeben, um ein eigenes Kennwort zu setzen.

Nachdem sich das Betriebssystem nun auf der Festplatte befindet, sollten Sie das aktuelle Service Pack von CD einspielen. Nach dem erforderlichen Neustart installieren Sie Firewall, Browser und Virenscanner. Im Fall von Windows XP Service Pack 2 reicht für den Anfang auch die enthaltene Windows-Firewall.

Nun ist ein gewisser Grundschutz hergestellt, und Sie können Ihre Internetverbindung einrichten und das erste Mal online gehen.

Nach der Installation

Zuerst sollten Sie den Virenscanner und die Firewall per Internet-Update auf den neuesten Stand bringen. Benutzen Sie dazu den zuvor von CD installierten Browser und laden Sie anschließend eventuell benötigte Browser-Updates nach. Öffnen Sie nun den Internet Explorer – das muss sein, denn der Download von Windows-Updates funktioniert leider nur mit Microsofts hauseigenem Browser. Stellen Sie zunächst die Sicherheit in allen Zonen auf HOCH. Fügen Sie nun die Microsoft-Updateseite (*www.windowsupdate.microsoft.com*) den vertrauenswürdigen Seiten hinzu und wählen daraufhin für diese Zone die Sicherheitseinstellung MITTEL. Starten Sie nun über START → PROGRAMME → WINDOWS UPDATE die Suche nach benötigten Patches und Erweiterungen. Laden Sie alle – auf jeden Fall alle kritischen – Updates herunter und warten, bis Windows diese installiert hat. Unter Umständen sind dazu gleich mehrere Neustarts nötig. Manchmal kann es passieren, dass Windows ein einzelnes Patch, zum Beispiel für den Internet Explorer, separat herunterladen und installieren muss. Führen Sie daher nach dem Herunterladen der benötigten Dateien gleich noch einmal das Windows Update aus, um wirklich sicherzustellen, dass alle Komponenten auf dem neuesten Stand sind.

Installieren Sie nun weitere Kernsoftware wie etwa das Office-Paket oder den E-Mail-Client und laden Sie die entsprechenden Updates herunter. Falls Sie über ein Programm zum erstellen von (Disk-)Images verfügen (z.B. Norton Ghost), wäre nun ein guter Zeitpunkt, ein solches Image anzulegen und sich für die Zukunft viel Arbeit zu sparen.

Bevor Sie nun weitere Software, vor allem solche, die nicht zu hundert Prozent vertrauenswürdig ist (beispielsweise Shareware aus dem Internet), herunterladen und installieren, sollten Sie dem eingerichteten Benutzer-Account, unter dem Sie derzeit arbeiten, die Administratorrechte entziehen. Die während der Windows-Installation eingerichteten Accounts verfügen über Rechte, die Sie im Alltag nicht brauchen, die den Schädlingen aber Tür und Tor öffnen (da diese nur innerhalb der Rechte des aktuellen Benutzers schalten und walten können). Dazu öffnen Sie unter START → SYSTEMSTEUERUNG die Rubrik BENUTZERKONTEN und wählen dort Ihren Account aus. Anschließend ändern Sie dort die Benutzergruppe, der Sie angehören, auf HAUPTBENUTZER (EIGENEN KONTENTYP ÄNDERN) und entfernen Ihren Account aus der Gruppe der Administratoren (siehe Abbildung 13-1). Stellen Sie hier zudem sicher, dass der Gast-Account komplett deaktiviert ist.

Der Sinn dieses Vorgehens ist es, den eigentlichen Administrator-Account für alle Systembelange und grundsätzlichen Einstellungen zu benutzen und ansonsten nur

mit einem weniger mächtigen Benutzer-Account zu arbeiten. Sie reduzieren Ihr persönliches Risiko damit erheblich!

Nachdem Sie nun auf der sicheren Seite sind, können Sie mit der Installation weiterer Software und mit dem Arbeiten mit Ihrem neuen PC beginnen.

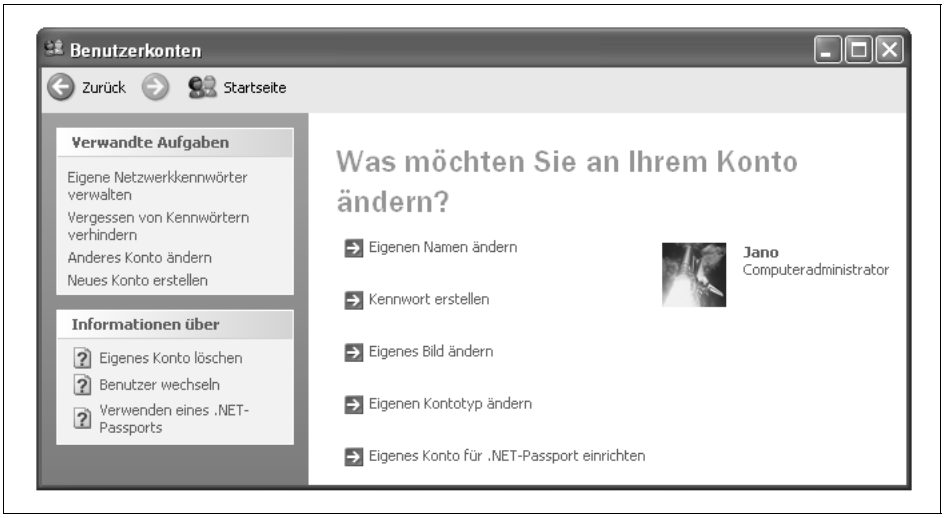

Abbildung 13-1: Die Benutzerverwaltung in Windows XP

Im Ernstfall

In diesem Abschnitt wollen wir uns nun damit befassen, was zu tun ist, wenn das eigene System trotz aller Vorsichtsmaßnahmen befallen wurde.

Infektionen erkennen

Zunächst einmal stellt sich natürlich die Frage, woran man überhaupt erkennt, dass der eigene PC infiziert ist. Tatsächlich ist es nicht einfach, hierfür eine klare Definition zu finden, ohne dass es auf eine schwammige Antwort wie etwa »wenn sich Ihr PC komisch verhält« hinauslaufen würde. Jede Angriffstaktik und jeder Wurm wirkt sich schließlich anders aus; zudem versuchen viele Schädlinge, z.B. Trojaner, unbemerkt zu bleiben. Es gibt jedoch einige Anzeichen, die zumindest den Verdacht erwecken, dass etwas im Argen liegt.

Den einfachsten und offensichtlichsten Fall findet man häufig bei Spyware: Tauchen innerhalb besuchter Webseiten plötzlich Links oder gar Werbeeinblendungen zu Online-Shops oder unseriösen Angeboten auf, ist dies ein stichhaltiges Indiz. Diese Werbung lässt sich übrigens relativ gut von den echten Werbeeinblendungen der ursprünglichen Webseite unterscheiden. Einerseits sind solche Spyware-Pro-

gramme in den allermeisten Fällen für den amerikanischen Raum konzipiert und die Werbung führt daher in englischer Sprache auf englischsprachige Angebote (und es ist kaum davon auszugehen, dass eine in Deutsch verfasste Webseite ihre Werbung auf Englisch verfasst), zum anderen betten Spyware-Hersteller die Links gerne in den Webseitentext ein. Wenn Sie also eine Webseite besuchen, bei der von typischen Produkt- und Artikelbezeichnungen aus Links zu Online-Shops führen, so ist dies zumindest ungewöhnlich. Dies gilt umso mehr, wenn Sie sich dabei bereits auf der Webseite eines Online-Shops Ihrer Wahl befinden. Kein Anbieter würde auf der eigenen Seite Links zur Konkurrenz unterhalten. Ebenso können Sie davon ausgehen, dass auch der Hersteller, wie beispielsweise Sony, keine direkten Links auf externe Shops setzen wird.

Natürlich gibt es aber auch Arten von Spyware, die sich nicht so auffällig verhalten. Da der Hersteller mit dem Schädling aber letztendlich Geld verdienen will, werden seine Motive früher oder später sichtbar.

Bei Würmern und Trojanern sieht es hingegen schon deutlich schwieriger aus. Ein sicheres Zeichen, das aber nicht für sich allein gesehen werden darf, sind plötzliche Abstürze des gesamten Systems oder einzelner Systemkomponenten. Als Beispiel für ein solches Szenario haben wir den *Sasser*-Wurm kennen gelernt. Oft führen Programmierfehler innerhalb des Wurms oder Trojaners zu solchen Problemen. Dies liegt aber meistens nicht am mangelnden Talent der Angreifer, sondern daran, dass die Konfiguration und Softwareausstattung jedes einzelnen Systems sehr unterschiedlich ist, was selbst großen Softwareschmieden Probleme bereitet. Zudem können die Angreifer oft nur Vermutungen über die Funktionsweise bestimmter Systemkomponenten anstellen, da Microsoft den Quellcode nicht freigibt und Funktionen teilweise nur unzureichend dokumentiert (und diese Dokumentationen wiederum nur bestimmten Entwicklern zur Verfügung stellt).

Häufig bremsen Schädlinge das eigene System stark aus und verbrauchen vor allem viel Internetbandbreite. Wenn Sie also im Web surfen, ohne etwas herunterzuladen, und Ihr PC plötzlich anfängt, größere Datenmengen ins Netz zu senden, stimmt oft etwas nicht.

Oft wird behauptet, dass man Schädlinge an ungewöhnlichen Einträgen in der Registry, in Konfigurationsdateien und im Taskmanager ausfindig machen könnte. Dies ist zwar völlig richtig und ein ausgesprochen zuverlässiger Weg (obwohl sich zahlreiche Trojaner auch hier geschickt zu tarnen wissen), für den Einsteiger ist es jedoch völlig aussichtslos, einen Schädling auf diese Weise ausfindig zu machen. Natürlich kann es aber nicht schaden, nach dem Namen merkwürdiger Prozesse im Web zu suchen (am besten bedient man sich hier zunächst des bereits besprochenen HiJackFree).

Das sicherste und deutlichste Indiz ist jedoch, dass Ihr Virenscanner und Ihre Firewall entweder komplett deaktiviert sind oder sich nicht mehr auf den neusten Stand

bringen lassen. Das Gleiche gilt natürlich auch für den Zugriff auf das Windows-Update.

Wenn Bekannte oder Kollegen sich beschweren, dass sie virenverseuchte Nachrichten von Ihrer E-Mail-Adresse bekommen haben, ist dies zwar ein möglicher Hinweis, dem man nachgehen sollte, aber noch kein stichhaltiges Indiz. Würmer benutzen bewusst alle Absenderadressen, die sie bei Ihrem Opfer finden können, und so kann es ebenso gut der Fall sein, dass nicht Sie befallen sind, sondern eine Person, die Ihre E-Mail-Adresse auf dem Rechner hat (z.B. im Adressbuch des Mailprogramms).

Gegenmaßnahmen

Wenn Sie erst einmal sicher sind, dass sich Malware auf Ihrem System befindet, gilt es, nicht übertrieben hastig zu reagieren. Als erster wichtiger Schritt sollten Sie die Internetverbindung trennen, am besten durch herausziehen des entsprechenden Steckers. Wenn Ihr Computer Teil eines Netzwerks ist, sollten Sie auch diese Verbindung kappen (um nicht andere Rechner in Gefahr zu bringen). Ansonsten kann es im schlimmsten Fall zu einem Ping-Pong-Effekt kommen, bei dem sich die Rechner immer wieder gegenseitig infizieren.

Von wenigen Ausnahmen abgesehen richten weder Würmer, Spyware noch Trojaner Schäden an Ihren persönlichen Dateien an. Hat der Angreifer aber erst einmal volle Kontrolle über Ihr System, mag es durchaus sein, dass er auch Dokumente und Bilder manipulieren, löschen oder sogar öffentlich ins Internet laden wird. Daher sollten Sie als erste Handlung eine Sicherung sämtlicher persönlicher Daten auf CD brennen und unbedingt auf dieser vermerken, dass die Daten eventuell infiziert sind.

Als nächsten Schritt starten Sie Ihren Virenscanner und weisen ihn an, einen kompletten Systemcheck durchzuführen. Anschließend sollten Sie zudem einen Spyware-Scanner über Ihr System laufen lassen. Löschen Sie alle Inhalte, die von den Scannern als potenziell gefährlich eingestuft werden. Sie brauchen sich dabei dank der Sicherungs-CD keine Sorgen um Datenverlust zu machen. Notieren Sie sich während des Scans unbedingt die Namen der gefundenen Schädlinge. Nachdem das System nun wieder sauber ist, sollten Sie sich mit dem Internet verbinden und Ihre Scanner schnell auf den neusten Stand bringen. Nun gilt es, mehr über die gefundenen Schädlinge zu erfahren. Nutzen diese Sicherheitslücken in Windows, dem Browser oder dem Mailtool aus? Wenn ja, sollten Sie als Nächstes die entsprechenden Updates herunterladen. Als gute Informationsquelle eignen sich die im Virenkapitel genannten Seiten von Symantec (*http://www.symantec.de/*) und McAfee (*http://www.mcafee.com/de/*) oder die der Kaspersky Labs (*http://www.kaspersky.com/de/*). Dort finden Sie zudem spezielle Removal-Tools für die meisten weit verbreiteten Viren und Würmer. Mit diesen Tools können Sie (unabhängig davon, ob Sie Kunde eines der beiden Unternehmen sind) Ihre Festplatte auch ohne eigenen Scanner reinigen. Obwohl Ihr PC jetzt scheinbar frei von Schädlingen ist, sollten Sie die Soft-

ware herunterladen und zur Sicherheit ausführen. Gerade zu den Hauptverbreitungszeiten fängt man sich denselben Wurm im Minutentakt immer wieder ein, bevor der Virenscanner auf den neuesten Stand gebracht ist. Diese Tools laufen zudem selbst dann noch, wenn der Virenscanner durch den Schädling außer Funktion gesetzt wurde.

Ist das System sauber, können Sie bei Bedarf eventuell gelöschte Daten wieder von der Sicherungs-CD auf Ihren Computer überführen. Vergessen Sie jedoch zuvor nicht, den Datenträger mit dem Virenscanner zu untersuchen.

Das oben beschriebene Szenario geht davon aus, dass Ihr Virenscanner noch in Betrieb ist und zudem den Schädling erkennen kann, also über die entsprechenden Updates verfügt. Wenn dies nicht der Fall ist, sollten Sie gleich zum passenden Removal-Tool greifen. Um herauszufinden, welcher Wurm Ihr System befallen hat, müssen Sie in diesem Fall jedoch von Hand auf den entsprechenden Seiten nach potenziell in Frage kommenden Schädlingen suchen und anschließend lieber ein Tool zu viel als zu wenig herunterladen. Blockiert der Angreifer jedoch den Zugriff auf diese Seiten, hilft Ihnen meist der örtliche Computerhändler oder ein Bekannter weiter. Die Removal-Tools sind in der Regel so klein, dass sie auf einer Diskette Platz finden. Meist sind nur wenige Würmer auf einmal so weit verbreitet, dass es zu ernsthaften Problemen kommt – Sie müssen sich also nicht zwischen hunderten potenzieller Schädlinge und den entsprechenden Tools entscheiden.

Für den seltenen Fall, dass auch das automatische Tool versagt, bleibt Ihnen noch die Möglichkeit, Anleitungen zum manuellen Löschen des Schädlings auszuprobieren. Diese Anleitungen finden sich schon kurze Zeit nach dem Auftauchen des Schädlings auf zahlreichen IT-Portalen (trauen Sie hier nur Seiten, die Sie bereits kennen).

Eine andere Möglichkeit ist auch ein Online-Virenscanner, da dieser nicht lokal auf ihrem System installiert werden muss. Die meisten lassen sich aber nur mit dem Internet Explorer und der mittleren Sicherheitsstufe benutzen. Eine Auflistung aktueller Online-Scanner finden Sie unter *http://www.tu-berlin.de/www/software/antivirus.shtml* im gleichnamigen Abschnitt.

Um die eigene Sicherheit nochmals deutlich zu steigern, empfiehlt es sich unter Umständen, einen zweiten Virenscanner auf dem System parat zu haben. Dieser zweite Scanner darf jedoch nicht im Wächtermodus (On-Access-Modus) arbeiten. Als solcher On-Demand-Scanner eignet sich beispielsweise die kostenlose Version des Bitdefenders (*http://www.bitdefender.de*). Zum einen ist die Wahrscheinlichkeit, dass der Schädling beide Scanner entdeckt und deaktiviert, deutlich niedriger (vor allem bei On-Demand-Scannern) und zum anderen ist im Gegenzug die Wahrscheinlichkeit, dass der neue Schädling bei beiden Scan-Durchläufen unbemerkt bleibt, gering. Da sich moderne Virenscanner automatisch per Online-Update auf dem neuesten Stand halten, gibt es praktisch keinen Mehraufwand für Sie als Benutzer.

Auf meinem Rechner verrichtet eine Kombination aus McAfee-Scanner und Bitdefender ihren Dienst. Dabei ist es der Bitdefender, der wöchentlich einen Komplettscan des Systems und aller Laufwerke durchführt.