Checkliste für optimalen Schutz

In drei Schritten zum sicheren PC

Mit drei Sicherheitsstufen schotten Sie Ihren Rechner optimal gegen Angriffe aus dem Internet ab: richtig konfiguriertes Windows, zuverlässige Anwendungen und schnelles Reparieren im Ernstfall

Gehen Sie mit einem ungesicherten Rechner online, so dauert es nicht lange, und er ist mit Schädlingen verseucht. Laut Sicherheitsspezialist Dshield *(www.dshield.org)* treffen die ersten → Würmer nach durchschnittlich 16 Minuten ein. Im schlimmsten Fall nisten sie sich dauerhaft ein und blockieren die installierte Antiviren-Software und Personal Firewall. So genannte Backdoor-Programme, eine Unterkategorie der → Trojaner, bringen sogar Keylogger und ausgefeilte Analysetechniken mit, die Tastatureingaben und Datenverbindungen nach Passwörtern, PINs, Kreditkarteninformationen oder Software-Schlüsseln durchsuchen und diese Daten über das Internet versenden.

Kaum ein Windows-Rechner ist sicher vor Schädlingen und Attacken aus dem Internet. Erhöhen Sie deshalb Stufe um Stufe das Bollwerk gegen Schädlinge. Im ersten Teilschritt installieren Sie die nötigen Updates und aktivieren die Schutzmechanismen, die Windows bereits an Bord hat. Im zweiten Schritt verabschieden Sie sich von unsicheren Windows-Anwendungen wie dem Internet Explorer oder Outlook Express. Verlässliche Programme übernehmen deren Aufgaben, und Virenwächter sowie Firewall komplettieren den Schutz. Doch kein Sicherheitskonzept ist zu 100 Prozent gefeit vor neuen Gefahren oder schlichten Bedienungsfehlern. Des-

Fotos: Digital Vision, Corbis

halb jagen und eliminieren Sie im dritten Schritt Schädlinge, die sich unbemerkt eingeschlichen haben. Als Lohn Ihres Einsatzes surfen Sie sicher und angstfrei.

Sicherheitsstufe 1: Basisschutz für Windows

In diesem Teil konfigurieren Sie Ihr Betriebssystem optimal. Das Fundament für einen sicheren PC bildet dabei ein aktueller → Patch-Level. Erst wenn Sie die erforderlichen Aktualisierungen für Windows und Office installiert, überflüssige System-Dienste abgestellt und die Zugriffsrechte geregelt haben, erreicht Ihr PC eine Sicherheitsstufe, auf der die meisten Gefahren aus dem Internet effektiv abgeblockt werden.

1. Service Pack 2

Installieren Sie als Anwender von Windows XP das Service Pack 2. Es führt ein zentrales Sicherheitscenter ein, das zeigt, ob automatische Updates sowie Firewall und Virenscanner vorhanden und aktiv sind. Laden Sie das Service Pack 2 von der Microsoft-Website herunter: Öffnen Sie den Internet Explorer und gehen Sie auf *www.microsoft.de*. Klicken Sie im Bereich *Produkt-Ressourcen* auf *Downloads*. Tippen Sie den Begriff **SP2** in das Feld *Stichwörter* ein und klicken Sie auf *Go*. Der Treffer *Windows XP Service Pack 2 für IT-Spezialisten und Entwickler* führt Sie zur Download-Seite für das Service Pack 2. Mit einem Klick auf *Download* laden Sie das 256 Megabyte große Paket für die Netzwerkinstallation auf Ihre Festplatte herunter. Es hat gegenüber der Variante der Expressinstallation den Vorteil, dass Sie die heruntergeladene Service-Pack-Datei auf eine CD brennen und öfter verwenden können.

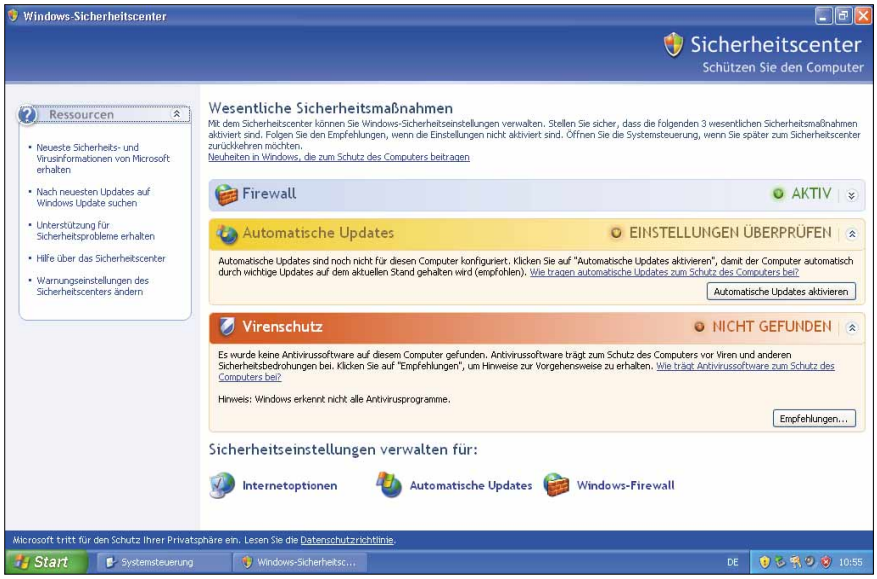
Die Funktionen des Sicherheitscenters reichen nicht aus, um den PC wirksam zu schützen. Die Komponente zeigt nur an, ob ein Virenscanner oder eine Firewall laufen. Sie prüft nicht, ob die Schutzprogramme aktuell sind und die Konfiguration stimmt. Unterhalb der Statusbalken befinden sich drei Schaltflächen, die zum Konfigurieren der *Internetoptionen,* der *Automatischen Updates* und der *Windows-Firewall* dienen. Besonders wichtig ist ▶

Inhalt

Sicherheits-Tools, die jeder braucht

Programm	Beschreibung	Preis	Webadresse	Seite
Sicherheitsstufe 1: Basisschutz für Windows				
Windows-Dienste abschalten	System-Tool, das überflüssige Windows-Dienste deaktiviert	gratis	*www.dingens.org*	91
Fajo XP FSE	Ergänzt Windows XP Home um die fehlende Dateirechteverwaltung	gratis	*www.fajo.de*	92
Sicherheitsstufe 2: Schutz mit Software ausbauen				
Firefox 1.0	Sicherer Open-Source-Browser	gratis	*www.mozilla-europe.org/de*	93
Sygate Personal Firewall 5.5	Firewall gegen Hacker, Virenattacken und Trojanische Pferde	gratis	*www.sygate.de*	94
Acronis True Image 8	Erstellt komfortabel Images Ihrer Festplatten-Partitionen	ca. 50 Euro	*www.acronis.de*	95
Partition Image 3.0	Konsolen-Tool zum Sichern der Festplatten-Partitionen	gratis	*www.toolsandmore.net*	96
Thunderbird 1.0	Das Mozilla-Programm erlaubt sicheres Mailen	gratis	*www.mozilla-europe.org/de*	93
Norton Antivirus 2005	Umfangreiches Schutzprogramm gegen Viren und Trojaner	ca. 50 Euro	*www.symantec.de*	95
Antivir Personal Edition 6.29	Antivir Personal Edition erkennt rund 80.000 Viren und entfernt sie	gratis	*www.free-av.de*	95
Sicherheitsstufe 3: Hilfe im Ernstfall				
Ad-Aware SE Personal	Findet und entfernt Spyware	gratis*	*www.lavasoft.de*	97
Hijack This	Findet und entfernt Spyware-verdächtige Registry-Einträge	gratis	*www.merijn.org*	98
Symantec Removal Tools	Entfernt bestimmte Schädlinge	gratis	*http://securityresponse.symantec.com/avcenter/tools.list.html*	99
Kaspersky Removal Tools	Entfernt bestimmte Schädlinge	gratis	*www.kaspersky.com/de/removaltools*	99
Trend Micro Sysclean	Ein Tool zur Entfernung verschiedener Schädlinge	gratis	*www.trendmicro.com/download/dcs.asp*	97
AVG Vcleaner	Ein Tool zur Entfernung verschiedener Schädlinge	gratis	*www.grisoft.de/ge/ge_remtext.php?id=bagbugnet*	

auf Heft-CD * für Privatnutzer



1. Service Pack 2: Die Balken-Farbe zeigt, ob XP grundlegende Einstellungen als sicher betrachtet

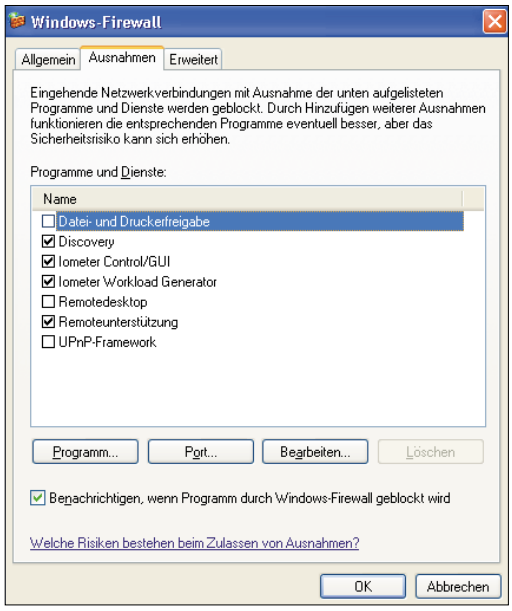
der mittlere Punkt, *Automatische Updates*. Klicken Sie darauf, so haben Sie die Wahl zwischen vier Stufen: Wenn Sie sich für *Automatische Updates Deaktivieren* entscheiden, müssen Sie die essenziellen Sicherheits-Updates in Zukunft manuell über *Start*, *Windows Update* einspielen. Bei der zweiten Stufe *Benachrichtigen* erhalten Sie jedes Mal eine Nachricht, wenn ein neuer Software-Flicken bereitsteht. Stufe 3 lädt jedes neue Update auch gleich herunter, während es bei Stufe 4 sogar automatisch installiert wird. Wir empfehlen, mindestens Stufe 2 zu verwenden.

2. Konfiguration der Windows-Firewall

Die neue Windows-Firewall ist deutlich leistungsfähiger als die nur sehr eingeschränkt konfigurierbare Internet-Verbindungs-Firewall, über die Windows XP bisher verfügte. Im Gegensatz zu handelsüblichen Personal Firewalls bietet sie aber keinen Filter für Anwendungen. Problematisch ist außerdem, dass die Software keine → Prüfsummen speichert und vergleicht. Das bedeutet, dass eine Anwendung, die einmal freigegeben wurde, auch dann noch ungestört Daten senden und empfangen darf, wenn sie nachträglich von einem → Virus oder Wurm manipuliert wurde. Darüber hinaus lässt sich die Firewall von böswilligen Programmen einfach stoppen, wenn Sie mit einem Benutzer-Account arbeiten, der über Administratorrechte verfügt (siehe „6. Eingeschränkte Benutzerkonten“ auf Seite 92).

Setzen Sie daher eine Firewall ein, die auch auf Applikationsebene schützt, wie zum Beispiel die Sygate Personal Firewall. Falls Sie keine Firewall zur Hand haben – etwa weil Sie Ihren Rechner neu installiert und die Schutz-Software noch nicht heruntergeladen haben –, ist eine richtig konfigurierte Windows-Firewall besser als gar kein Schutz.

Starten Sie die Einrichtung der Brandschutzmauer über *Systemsteuerung, Windows-Firewall*. Wählen Sie den Reiter *Ausnahmen* aus und prüfen Sie dort alle Einträge, die mit einem Häkchen versehen sind. Das Häkchen vor einer Anwendung bedeutet, dass sie ungestört Daten senden und empfangen darf. Standardmäßig hat Microsoft die *Datei- und Druckerfreigabe* und die *Remoteunterstützung* erlaubt. Deaktivieren Sie im Firewall-Manager die Option *Datei und Druckerfreigabe,* wenn Sie im Heim-LAN etwa keine Netzlaufwerke einsetzen.



2. Konfiguration der Windows-Firewall: Anwendungen mit Häkchen dürfen ungestört Daten empfangen und senden

Beschränken Sie andernfalls die freigegebenen Laufwerke auf Ihr lokales Netz. Wählen Sie dazu unter *Systemsteuerung, Sicherheitscenter, Windows-Firewall* die *Datei- und Druckerfreigabe* aus und klicken Sie unten auf *Bearbeiten*. Klicken Sie auf *Bereich ändern* und wählen Sie *Nur für eigenes Netzwerk (Subnetz)* aus. Wiederholen Sie den Schritt für alle vier angegebenen TCP-Ports. Wenn Ihr Netzwerk nur aus wenigen Computern besteht, ist es noch sicherer, im Feld *Benutzerdefinierte Liste* die IP-Adressen einzugeben, die Sie verwenden. Lassen Sie die *Remoteunterstützung* nur zu, wenn Sie selbst – oder ein vertrauenswürdiger Bekannter – von außen Zugriff auf Ihren Rechner haben möchten.

Wenn Sie statt der Windows-Firewall eine Personal Firewall einsetzen, deaktivieren Sie die Windows-Software besser. Gehen Sie auf *Start, Systemsteuerung, Sicherheitscenter* und *Windows-Firewall*. Aktivieren Sie die Option *Inaktiv (nicht empfohlen)* und bestätigen Sie die Wahl mit *OK*.

3. Autostarts abschalten

Ein weiterer wichtiger Schritt, Windows XP besser abzusichern, ist das Abschalten von überflüssigen Programmen, die bei jedem Booten des Computers automatisch mitgestartet werden. Klicken Sie dazu auf *Start, Ausführen* und schreiben Sie in das Eingabefenster **`msconfig`**. Nachdem Sie mit *OK* bestätigt haben, startet das Systemkonfigurationsprogramm von Windows. Im Reiter *Systemstart* sehen Sie, welche Programme Ihr Computer automatisch startet.

Nun müssen Sie entscheiden, welche Anwendungen Sie wirklich benötigen und welche nur Ballast oder sogar gefährlich sind. Das Entfernen des kleinen Häkchens links und ein Klick auf *Übernehmen* verhindert den Autostart der jeweiligen Software beim nächsten System-Boot. Auf keinen Fall sollten Sie Anwendungen wie Ihr Antiviren-Programm und Ihre Personal Firewall am automatischen Start hindern.

Suchen Sie bei Google nach einem bestimmten Programm oder einer EXE-Datei, wenn Sie sich unsicher sind, um was für eine Software es sich handelt. Es ist zudem ratsam, immer nur ein Programm zu deaktivieren, das System neu zu starten

Sichern der DFÜ-Verbindung

Im Gegensatz zu den Vorgängern sind die für lokale Netzwerke notwendigen Netbios-Netzwerkdienste bei Windows XP nicht mehr automatisch an DFÜ-Verbindungen gebunden. Auch ohne das Service Pack 2 und die Windows-Firewall können Sie verhindern, dass Ihre Netzwerkfreigaben im Internet zur Verfügung stehen. Prüfen Sie, ob Netbios für DFÜ abgeschaltet ist. Öffnen Sie über *Start, Systemsteuerung, Netzwerk- und Internetverbindungen, Netzwerkverbindungen* die Übersicht über alle Netzwerkverbindungen. Klicken Sie mit der rechten Maustaste auf Ihre DFÜ-Verbindung und wählen Sie den Reiter *Netzwerk* aus. Entfernen Sie gegebenenfalls die Häkchen vor *Datei- und Druckerfreigabe für Microsoft-Netzwerke* und vor *Client für Microsoft-Netzwerke*. Starten Sie Ihren Computer neu. Gehen Sie anschließend wieder in die Eigenschaften Ihrer DFÜ-Verbindung und wählen Sie unter *Netzwerk* den Punkt *Internet-Protokoll (TCP/IP)* aus. Klicken Sie auf *Eigenschaften*, dann auf *Erweitert* und wechseln Sie zum Reiter *WINS*. Wählen Sie dort *NetBIOS über TCP/IP deaktivieren,* bestätigen Sie den Vorgang mit einem Klick auf *OK* und starten Sie den Rechner neu.

Sichern der DFÜ-Verbindung: Deaktivieren Sie die Netbios-Bindung an TCP/IP, um Ihr Netzwerk zu sichern

Wechseln Sie wieder ins Fenster *Netzwerkverbindungen* und wählen Sie unter dem Menüpunkt *Erweitert Erweiterte Einstellungen* aus. Entfernen Sie bei *LAN-Verbindung* und *RAS-Verbindung* alle Bindungen im unteren Fenster. Damit haben Sie die Netbios-Ports 137, 138, 139 und 445 gegenüber dem Internet geschlossen und die Windows-Netzwerkdienste *netbios-ssn, netbios-ns* und *netbios-dgm* deaktiviert.

und zu prüfen, ob der Rechner noch fehlerfrei läuft. Anschließend können Sie die nächste fragliche Software ausschalten. Auch der Speicherort einer Datei, über den der Verzeichnispfad informiert, kann Aufschluss darüber geben, um was für eine Anwendung es sich eigentlich handelt.

4. Unsichere Dienste abschalten

Windows XP lädt bei jedem Systemstart zahlreiche Dienste, die jedoch zum Teil nicht benötigt werden. So braucht beispielsweise ein Anwender, der keinen Scanner einsetzt, den Dienst *Windows-Bilderfassung* nicht. Gleichzeitig stellt jeder gestartete Dienst eine potenzielle Sicherheitslücke dar. Sie können über *Start, Systemsteuerung, Leistung und Wartung, Verwaltung, Dienste* den Dienste-Manager starten und überflüssige Services per Hand deaktivieren. Das ist jedoch sehr mühsam.

Einfacher geht es mit dem Freeware-Tool Windows-Dienste abschalten (gratis, *www.dingens.org*). Das Programm deaktiviert alle nicht benötigten Dienste mit wenigen Mausklicks und reduziert damit das Risiko, im Internet Ziel eines Angriffs zu werden. Ein paar Tipps zum Programm: Ein Maximum an Sicherheit bietet die Option *Einzelner Computer*, die Sie nur dann nicht auswählen sollten, wenn Sie über ein lokales Netzwerk verfügen oder einen Router einsetzen, um ins Internet zu kommen. Wählen Sie in diesem Fall die zweite Option *Computer in einem Netzwerk* aus. Die Änderungen werden erst nach einem Klick auf *OK* und dem Neustart des PCs wirksam. Die getroffenen Modifikationen können Sie mit Hilfe von *Windows-Dienste abschalten* und der Auswahl der Option *Unsicher* wieder vollständig rückgängig machen.

5. NTFS und Zugriffsrechte

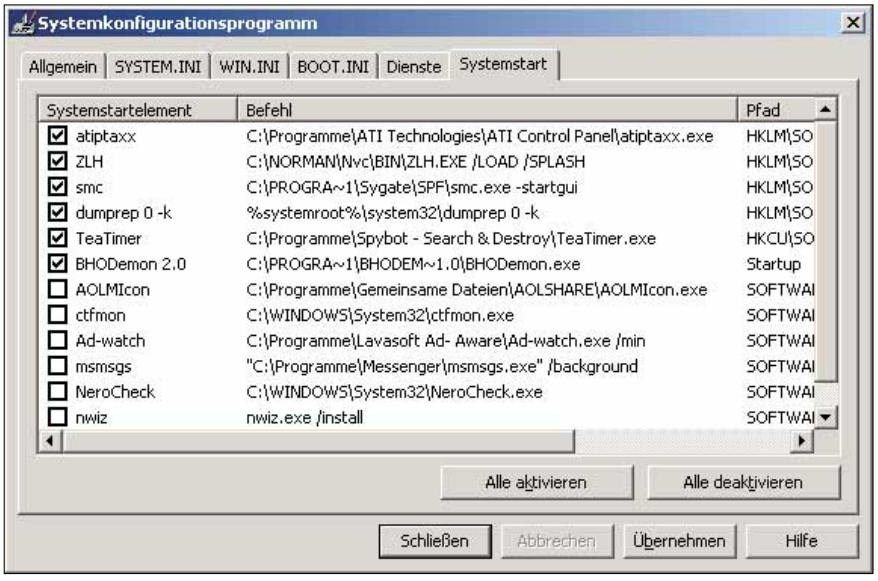
Wer seinen Windows-Rechner noch mit dem FAT32-Dateisystem betreibt, verzichtet auf die zusätzliche Sicherheit, die NTFS dank eingeschränkter Zugriffsrechte bietet. Überschätzen sollte man dieses Dateisystem zwar nicht – mittlerweile gibt es eine ganze Reihe von Tools, die trotz eingeschränkter Zugriffsrechte Dateien auf NTFS-Laufwerken öffnen oder geschützte Verzeichnisse löschen. Solche Manipulationen sind aber nur möglich, wenn jemand direkten Zugang zu Ihrem Computer erhält und beispielsweise Linux mit NTFS-Treibern von CD-ROM oder Diskette bootet.

So wandeln Sie Ihre bestehenden FAT-Partitionen ins NTFS-Format um: Öffnen Sie die Eingabeaufforderung über *Start*, *Ausführen* und das Kommando **cmd**. Geben Sie den Befehl

```
convert c: /fs:ntfs
```

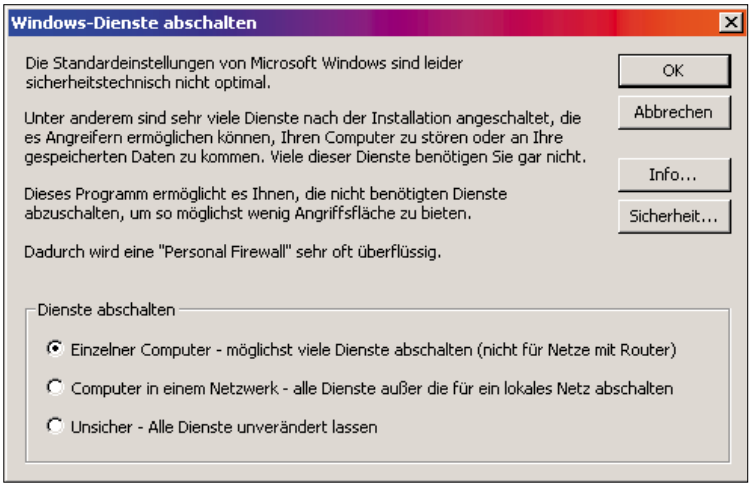
ein. Der Buchstabe **c** bedeutet in diesem Fall, dass die C:-Partition umgewandelt werden soll. Starten Sie den PC neu. Danach beginnt die Umwandlung automatisch.

Mit NTFS stehen Ihnen die so genannten Access Control Lists (ACL) zur Verfügung, mit denen sich genau definieren ▶



3. Autostarts abschalten: Mit dem Tool Msconfig können Sie unerwünschte Autostarts abschalten

lässt, wer auf bestimmte Dateien oder Ordner zugreifen darf und wer nicht. Windows XP Pro bringt bereits eine Verwaltung der ACLs mit, die allerdings nicht standardmäßig eingeschaltet ist. Öffnen Sie den Windows-Explorer und klicken Sie oben auf *Extras, Ordneroptionen*: Entfernen Sie im Reiter *Ansicht* das Häkchen vor *Einfache Dateifreigabe verwenden* und bestätigen Sie die Änderung mit *OK*. Wenn Sie anschließend mit der rechten Maustaste auf eine Datei oder einen Ordner klicken, sehen Sie den zusätzlichen Reiter *Sicherheit*. Dort können Sie detailliert einstellen, wer Vollzugriff hat, wer nur Leserechte hat oder wer gar nicht darauf zugreifen darf. Unter XP Home erreichen Sie dasselbe über das Administratorkonto (siehe in dieser Ausgabe „Windows inoffiziell“, Tipp 19 auf Seite 26) oder auch mit der Freeware Fajo XP FSE, die Sie unter *www.fajo.de* herunterladen können.



4. Unsichere Dienste abschalten: Mit dem Freeware-Tool Windows-Dienste abschalten *(www.dingens.org)* deaktivieren Sie überflüssige Dienste auf Ihrem System

6. Eingeschränkte Benutzerkonten

Die meisten Anwender arbeiten – oft ohne es zu wissen – mit Administratorrechten und riskieren damit, dass Viren und Würmer die vollen Zugriffsrechte auf Dateien und Ordner erhalten und so Schaden anrichten können. Dabei verfügt Windows XP über die Möglichkeit, Benutzerkonten mit eingeschränkten Rechten anzulegen. Damit haben elektronische Schädlinge keine Chance mehr, die Systemdateien von Windows zu infizieren.

Legen Sie zunächst ein neues Konto mit Administratorrechten an. Denn Windows XP verlangt, dass mindestens ein Benutzer mit allen Rechten ausgestattet ist. Der standardmäßig eingerichtete – und bei Windows XP Home versteckte – Administratorzugang zählt dabei nicht. Öffnen Sie über *Start, Systemsteuerung, Benutzerkonten* die Benutzerverwaltung. Klicken Sie auf *Neues Konto erstellen* und geben Sie als Namen **Admin** ein. Als Kontotyp verwenden Sie *Computeradministrator*. Ein Klick auf *Konto erstellen* schließt den Vorgang ab.

5. NTFS und Zugriffsrechte: Mit Access Control Lists (ACL) lässt sich einstellen, wer auf welche Dateien zugreifen darf

Das neue Benutzerkonto ist noch nicht durch ein Passwort geschützt. Klicken Sie in der Übersicht auf das neue Konto, wählen Sie *Kennwort erstellen* aus und folgen Sie dem Assistenten.

Schränken Sie anschließend die Rechte Ihres bisherigen Kontos ein. Klicken Sie im Fenster *Benutzerkonten* Ihr Konto an. Wählen Sie *Kontotyp ändern*. Aktivieren Sie die Option *Eingeschränkt* und klicken Sie auf die Schaltfläche *Kontotyp ändern*. Beachten Sie: Die Änderung wird erst wirksam, wenn Sie sich das nächste Mal mit dem Konto anmelden.

Ab sofort arbeiten Sie deutlich sicherer, wenn Sie sich mit diesem Konto auf Ihrem Computer anmelden. Es kann allerdings zu Problemen mit Programmen kommen, die zum Ausführen Administratorrechte erfordern. Hier gibt es mehrere Möglichkeiten: Probieren Sie zuerst, ob ein Klick mit der rechten Maustaste auf das jeweilige Programm und die Auswahl des Punktes *Ausführen als…* genügt. Wählen Sie unter *Folgender Benutzer* den Benutzernamen *Admin* aus. Per Klick auf *OK* wird das jeweilige Programm mit Administratorrechten gestartet.

Diese Methode hat den Nachteil, dass Sie jedes Mal, wenn Sie das jeweilige Programm starten wollen, wieder das Admin-Konto auswählen und das Passwort eingeben müssen. Auch hier gibt es einen Trick, der jedoch nur unter Windows XP Professional funktioniert: Klicken Sie *Start, Programme* und dann mit der rechten Maustaste auf den Namen der Software. Wählen Sie *Eigenschaften*. Im Feld *Ziel* findet sich zum Beispiel folgender Text:

```
C:\Programme\CSIM\aim.exe
```

Ändern Sie diese Zeile in

```
C:\WINDOWS\system32\runas.exe
/user:Admin /savecred
"C:\Programme\CSIM\aim.exe"
```

Bei dieser Methode werden Sie nur beim ersten Start der Anwendung nach Ihrem Admin-Passwort gefragt.

7. Security-Check

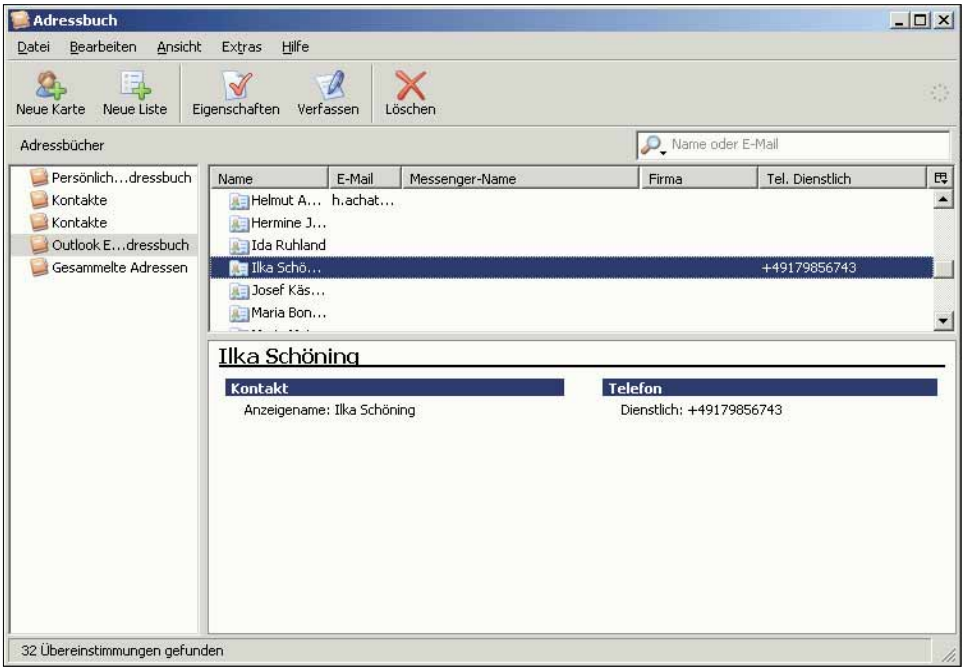
Zuletzt ist ein externer Test auf Sicherheitslücken ratsam. Sygate bietet unter *scan.sygate.com* mehrere Checks, die Ihre Firewall und den eingesetzten Browser auf Herz und Nieren prüfen.

Selbst nach all den oben genannten Schritten ist eine Dosis gesunder Menschenverstand nötig, um einigermaßen sicher vor Viren und anderen Schädlingen zu bleiben: Dazu zählen Vorsicht bei Downloads, Attachments, Mails von unbekannten Absendern und so weiter.

Sicherheitsstufe 2: Schutz mit Software ausbauen

Nachdem Sie Windows mit den gezeigten Konfigurationsschritten die bestmögliche Sicherheit abgerungen haben, erhöhen Sie nun den Schutz mit weiteren Anwen-

dungen: Sichern Sie Ihren Internet- und E-Mail-Zugang gegen unliebsame Überraschungen. Ein gutes Antivirenprogramm ist unverzichtbar, um schädliche Programme abzuwehren. Mit einer Firewall erhalten Sie zusätzlichen Schutz, und falls doch mal etwas schief geht, sollten Sie ein Image Ihrer Festplatte bereithaben.



9. Thunderbird als E-Mail-Client: Das Tool importiert schnell und einfach das Adressbuch anderer Mail-Programme

8. Firefox als Browser

Der Internet Explorer ist dank seiner weiten Verbreitung ein beliebtes Angriffsziel von Hackern, die versuchen, Sicherheitslücken aufzuspüren und auszunutzen. Der Weg zum sicheren Surfen ist unproblematisch und heißt Firefox (gratis, *www.mozilla-europe.org/de)*. Der Browser unterstützt ohne entsprechendes Plug-in keine → ActiveX-Controls und versteht kein → VB-Script, das sind die Hauptangriffsstellen des Internet Explorers. Außerdem verzichtet Firefox auf das schwer zu durchschauende Konzept der Sicherheitszonen.

Am einfachsten installieren Sie Firefox 1.0 von der com!-Heft-CD 1, dort finden Sie ihn unter „Browser". Der Import-Assistent hilft Ihnen beim Umstieg vom Internet Explorer: Beim ersten Start fragt er Sie, ob Sie Einstellungen, Lesezeichen, Chronik, Passwörter und sonstige Daten vom Microsoft-Browser importieren möchten.

Standardmäßig sind Java und Javascript aktiviert, um einen möglichst hohen Surfkomfort zu gewährleisten. Die Gefahren sind gering, aber möchten Sie ganz auf Nummer sicher gehen, können Sie beide Techniken ausschalten. Dazu wechseln Sie über das Menü *Extras* zu den *Einstellungen*. Unter *Web-Features* können Sie nun Java und Javascript deaktivieren. Nach einem Klick auf den Button *Erweitert* lassen sich einzelne Javascript-Aktionen ausschalten, statt ganz auf die Skriptsprache zu verzichten.

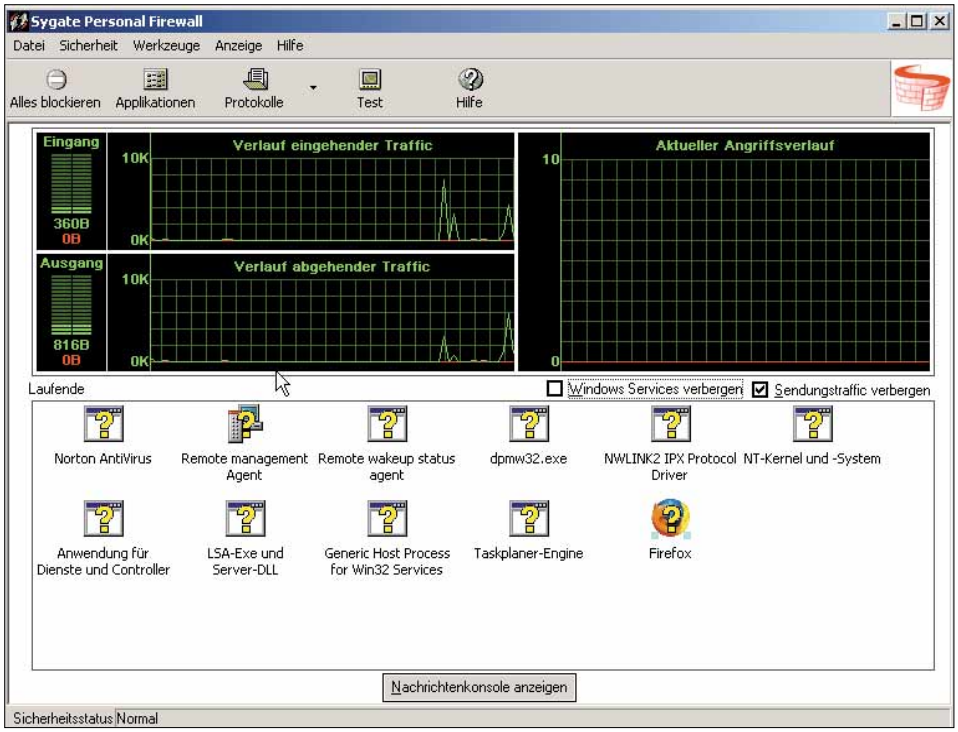
Ebenfalls unter *Einstellungen* finden Sie den Punkt *Datenschutz*. Dort wird alles übersichtlich aufgelistet, was Firefox speichert: Chronik, Passwörter, Cookies und Cache. Eine praktische Funktion: Über den Button *Alles löschen* beseitigen Sie alle gespeicherten Daten mit einem Mausklick.

Wer an noch feineren Rädchen drehen möchte, gibt **`about:config`** in die Adresszeile von Firefox ein. Es erscheint eine lange Liste möglicher Einstellungen, interessant im Hinblick auf Sicherheit sind all jene, die mit „security" beginnen. Die Einstellungen lassen sich mit einem Doppelklick auf eine Zeile ändern. Mehr zu den Konfigurationsmöglichkeiten von Firefox lesen Sie in com! 1/2005 ab Seite 96.

6. Eingeschränkte Benutzerkonten: Als Benutzer mit eingeschränkten Rechten starten Sie widerspenstige Programme mit *Ausführen als ...* und Admin-Rechten

9. Thunderbird als E-Mail-Client

Als Mail-Programm und Newsreader setzen Sie Mozilla Thunderbird 1.0 (gratis, *www.mozilla-europe.org/de)* ein. Es bietet wesentlich mehr Sicherheit als das mit Windows installierte Outlook Express. Zum einen verfügt Thunderbird über einen lernfähigen Spam-Filter, der nach einer Trainingsphase sehr gute Trefferquoten aufweist. Zum anderen unterstützt das Programm die Standardverfahren → S/Mime und → PGP, um E-Mails zu verschlüsseln oder zu signieren. Durch die Installation von → Extensions ergänzen Sie Thunderbird mit zahlreichen Funktionen, beispielsweise mit der → GnuPG-Erweiterung Enigmail ▶



10. Sygate als Personal Firewall: Im Hauptfenster sehen Sie die laufenden Programme und Prozesse

(gratis, *http://enigmail.mozdev.org*), mit deren Hilfe Sie E-Mails mit PGP-Schlüsseln versehen. Ein weiteres Plus: Im Gegensatz zu anderen Mail-Programmen führt Thunderbird Dateianhänge nicht automatisch aus und hemmt auf diese Weise die Verbreitung von Viren. Nicht zuletzt ist Javascript deaktiviert, so dass beim Öffnen einer Mail keine Skripts ausgeführt werden (unter *Extras, Einstellungen, Erweitert, Datenschutz* kann Javascript manuell aktiviert werden).

Die Installation von Thunderbird und Enigmail können Sie direkt von der com!-Heft-CD 1 unter „Internet", „Sicherer PC" starten. Nach dem Willkommensdialog klicken Sie auf *Weiter*, akzeptieren die Lizenzvereinbarungen und klicken erneut *Weiter*. Als Installationsart wählen Sie *Standard*. Sie sehen nun eine Zusammenfassung mit den Einstellungen des Installations-Assistenten und bestätigen diese. Nach erfolgreicher Installation aktivieren Sie das Häkchen bei *Mozilla Thunderbird 1.0 jetzt starten*. Dabei wird Thunderbird von der Default-Sprache Englisch auf Deutsch umgestellt.

Mit dem Konten-Assistenten können Sie Ihr E-Mail-Konto einrichten. Für einen nahtlosen Übergang zum neuen Programm übernehmen Sie die Daten aus Ihrem bisherigen E-Mail-Client – hier am Beispiel von Outlook Express aufgezeigt.

Rufen Sie in Thunderbird *Extras, Importieren* auf. Klicken Sie im Assistenten zunächst auf *Nachrichten* und bestätigen Sie mit *Weiter*. Nun wählen Sie *Outlook Express* aus und klicken erneut auf *Weiter*. Die E-Mails werden jetzt importiert, und Sie schließen den Vorgang mit *Fertigstellen* ab. Thunderbird erstellt für diese Mails ein eigenes Unterverzeichnis in *Lokale Ordner*.

Um auch das Adressbuch einzulesen, gehen Sie in Thunderbird wieder auf *Extras, Importieren*. Aktivieren Sie im Assistenten *Adressbücher* und klicken Sie auf *Weiter*. Wählen Sie als Anwendung erneut *Outlook Express*, bestätigen Sie mit *Weiter* und schließlich mit *Fertigstellen*. In der Liste der Adressbücher hat Thunderbird nun ein eigenes Outlook-Express-Adressbuch angelegt.

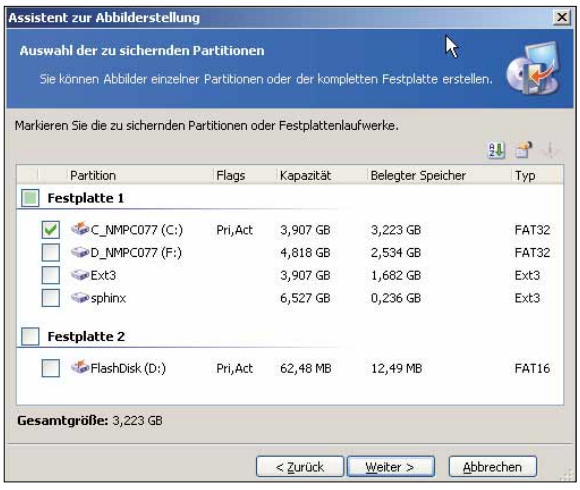
10. Sygate als Personal Firewall

Die Personal Firewall von Sygate (gratis, *www.sygate.de)* schützt Ihren Rechner vor Hackern, Viren- und Trojaner-Attacken sowie vor Passwortdiebstahl. Zunächst installieren Sie die Firewall von der com!-Heft-CD 1. Nach dem Neustart arbeitet die Firewall bereits. Und noch bevor Sie eine Verbindung zum Internet herstellen, tauchen die ersten Warnhinweise auf – ein Zeichen, dass es die Firewall sehr genau nimmt.

Zur Konfiguration klicken Sie doppelt auf das Doppelpfeil-Symbol rechts in der Taskleiste. Klicken Sie auf den Button *Applikationen*. Es erscheint eine Liste der Programme und Prozesse, welche die Firewall derzeit überwacht. Mit einem Klick auf das Kästchen vor der jeweiligen Anwendung ändern Sie den Status zwischen *erlaubt, verboten* und *nachfragen*. Ihrem Browser und E-Mail-Client sollten Sie den Zugang erlauben. Verbieten können Sie *alg.exe* (der Application Layer Gateway Service ist bei XP für die Internet-Verbindungsfreigabe zuständig), *explorer.exe* (Windows-Explorer), *snmp.exe* (Verwaltungsdienst für Netzwerke), *lsass.exe* (die LSA Shell verwaltet die Benutzeranmeldung) und *ntoskrnl.exe* (ein Windows-Kernel-Bestandteil). Diese Angaben lassen sich später jederzeit wieder ändern.

Das Programm fragt Sie bei jeder neuen Verbindung um Ihre Erlaubnis. Soll sich die Firewall Ihre Antwort merken, so aktivieren Sie die Funktion *An meine Antwort erinnern und für diese Applikation nicht weiter Nachfragen*. Sobald Sygate eine Anwendung blockiert, erscheint ein kleines Fenster am rechten unteren Bildschirmrand.

Über *Werkzeuge, Optionen* gelangen Sie zu den Firewall-Einstellungen. Meist ist es sinnvoll, über *Allgemein* einen Passwortschutz gegen unautorisierte Veränderungen der Konfiguration festzulegen. Im Register *Sicherheit* sind viele Optionen aus der kommerziellen Version deaktiviert. Aber auch die Freeware-Version bietet ausreichenden Schutz.



12. True Image für Sicherungen: Hier wählen Sie zu sichernden Partitionen aus. Zur Orientierung wird der belegte Platz angezeigt

Betreiben Sie zu Hause ein LAN, schalten Sie die entsprechenden IP-Adressen frei. Dazu rufen Sie *Werkzeuge, Erweiterte Regeln* auf. Dort klicken Sie auf *Hinzufügen* und aktivieren die Option *Diesen Traffic erlauben*. Wechseln Sie zum Reiter *Hosts* und tragen Sie bei *Subnet* als Subnet-IP-Adresse **192.168.0.0** und als Subnet-Mask **255.255.255.0** ein.

Über diese Regeln können Sie auch einzelne Ports sperren. Um etwa sinnvollerweise den Port 135 für *svchost.exe* zu blockieren, erstellen Sie eine neue Regel und wählen bei *Hosts* die Option *alle Adressen*. Bei *Ports und Protokolle* entscheiden Sie sich für *TCP*, geben in das Feld *Lokal* den Wert **135** ein und wählen als *Traffic-Richtung* den Punkt *Eingang*. Schließlich setzen Sie im Reiter *Applikationen* ein Häkchen beim Eintrag *Generic Host Process …*

11. Norton Antivirus als Virenschutz

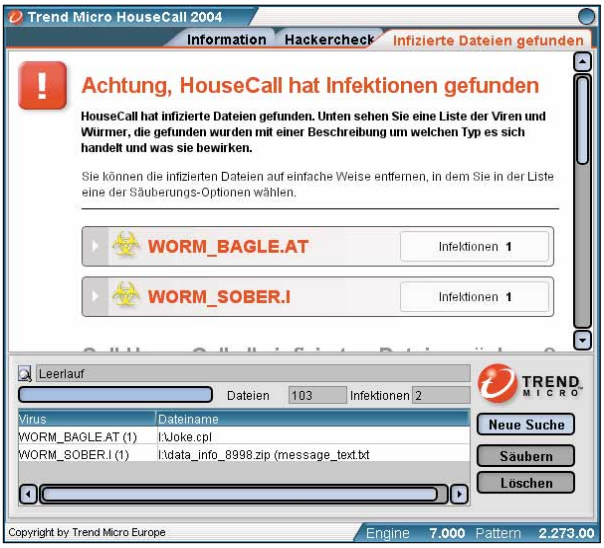
Hundertprozentigen Schutz gegen Schädlinge kann Ihnen kein Programm bieten. Doch Norton Antivirus 2005 (rund 50 Euro, *www.symantec.de)* punktet im Test von neun Antiviren-Programmen (siehe Seite 70 in dieser Ausgabe) mit sehr guten Erkennungsraten in Verbindung mit hoher Funktionalität. Unter anderem prüft und säubert die Software ein- und ausgehende Mails und checkt komprimierte Dateianhänge vor dem Öffnen. Es erkennt und blockt Würmer wie Blaster oder Sasser schon im Eingangsverkehr, bevor sie in den PC eindringen. Auch → Spy- und Adware erfasst das Programm.

Nach der selbsterklärenden Installation klicken Sie doppelt auf das Norton-Antivirus-Symbol auf dem Desktop. Die Voreinstellungen des Programms sorgen für hohe Sicherheit. Unter *Optionen* können Sie diese Einstellungen noch anpassen.

In Norton Antivirus ist die Funktion *Live Update* integriert. Sie stellt unter anderem sicher, dass Sie stets über die aktuellen Virusdefinitionen verfügen. Standardmäßig prüft sie das alle vier Stunden, sofern eine Internet-Verbindung besteht. Sie können die Update-Funktion manuell starten, indem Sie im Hauptfenster auf *Live Update* klicken. Gehen Sie nach dem Willkommensdialog auf *Weiter*. Erscheint die Meldung, dass alle Komponenten auf dem neuesten Stand sind, klicken Sie auf *Fertig stellen*. Wird hingegen angezeigt, dass Aktualisierungen verfügbar sind, klicken Sie auf *Weiter* und nach dem Herunterladen der Aktualisierungen auf *Fertig stellen*.

Mit individuellen Zeitplänen legen Sie selbst fest, wann das Programm seine Virensuche startet. So können Sie beispielsweise einmal wöchentlich den ganzen PC scannen lassen. Wählen Sie dazu im Hauptfenster *Auf Viren prüfen* und klicken Sie auf das Uhrensymbol auf der rechten Seite. Dort können Sie nun Ihren Zeitplan eingeben. Möchten Sie mehrere Zeitpläne für eine Prüfung definieren, etwa bestimmte Uhrzeiten für bestimmte Tage, aktivieren Sie *Mehrfache Zeitpläne anzeigen* und gehen jeweils auf *Neu* für einen neuen Zeitplan. Klicken Sie *OK*.

Als kostenlose Alternative empfiehlt sich Antivir Personal Edition (auf der com!-Heft-CD 1 oder unter *www.free-av.de)*. Im Test kostenloser Antiviren-Tools in com! 10/2004 lieferte der Virenscanner die besten Suchergebnisse.



13. Schädlingsdiagnose: Trend Micro Housecall ist ein effektives Tool zum Identifizieren von Parasiten

12. True Image für Sicherungen

Verabschiedet sich die Festplatte oder zerstört ein Schädling trotz aller Sicherheitsmaßnahmen erfolgreich Ihr System, ist es eine große Erleichterung, wenn ein Image im Schrank liegt. Mit diesem Partitions-Abbild stellen Sie umgehend den Stand der letzten Sicherung komplett wieder her. Eine gute Software ist beispielsweise Acronis True Image 8 (rund 50 Euro, *www.acronis.de)*. Das Pro- ▶

gramm unterstützt CD, DVD, Zip, Jaz und andere Datenträger zur Sicherung.

Nach dem ersten Start ist es empfehlenswert, die Option *Ja, ich möchte die bootfähigen Notfallmedien jetzt erstellen* auszuwählen. Um ein neues Image anzulegen, wählen Sie den Punkt *Abbild erstellen*. Ein Assistent führt Sie durch die weiteren Schritte. Nachdem Sie die zu sichernden Partitionen ausgesucht haben, wählen Sie zwischen einem inkrementellen und einem vollständigen Backup. Ersteres nutzen Sie dann, wenn Sie bereits ein Image erstellt haben und lediglich die Änderungen seit der letzten Sicherung hinzufügen möchten. Ist das Abbild größer als das Speichermedium, teilt True Image die Imagedatei auf Wunsch automatisch auf. Schließlich lässt sich das Abbild noch komprimieren, wobei die Stufe *Normal* völlig ausreicht. Mit einem Klick auf *Fertig stellen* startet die Sicherung.

Wünschen Sie sich ein kostenloses Programm, so greifen Sie zum com!-Tool Partition Image 3.0 (in dieser Ausgabe auf Seite 64). Das Konsolen-Tool zum Sichern der Festplatten-Partitionen kann unabhängig von der zu Grunde liegenden Formatierungsart eingesetzt werden.

Sicherheitsstufe 3: Hilfe im Ernstfall

Trotz aller Sicherheitsmaßnahmen kann es passieren: Auf Ihrem System hat sich ein Wurm, ein Trojaner oder ein anderer Schädling eingenistet. Die gute Nachricht: Ein Rechner, der noch hochfährt, lässt sich fast immer reparieren. Allerdings ist dazu planvolles Vorgehen notwendig. Zuerst führen Sie eine genaue Diagnose durch. Nur wenn Sie wissen, welcher Schädling Ihren Computer befallen hat, können Sie ihn problemlos entfernen. Fast immer werden Sie Viren so los, dass Sie die Attacke glimpflich überstehen. Bei schwierigen Fällen brauchen Sie etliche Tricks, da die normale Reinigungsprozedur nicht ausreicht.

13. Schädlingsdiagnose

Sie können sich einen Schädling völlig unbemerkt auf Grund eines Fehlers in Windows oder über das Ausführen einer infizierten Datei einfangen, die Sie zum

Was ist eigentlich ...?

Abgesicherter Modus: Wird Windows im abgesicherten Modus gestartet, werden die meisten Treiber und Autostart-Programme nicht geladen. Zerschossene Systeme lassen sich im abgesicherten Modus starten und oft wiederbeleben, indem Sie problematische Treiber oder Programme deinstallieren.

ActiveX: Microsoft-Technik für Software-Komponenten, die für die Kommunikation zwischen Programmen eingesetzt wird. Mit ActiveX können Objekte wie Video oder Sound in Dokumente wie etwa Webseiten eingebettet werden.

Adware: siehe Spyware.

DFÜ-Verbindung: DFÜ steht für Datenfernübertragung und bezeichnet eine direkte Verbindung zum Internet über Modem, ISDN oder DSL.

Dienst: Selbst wenn Sie kein Programm starten und nur den Windows-Desktop sehen, laufen im Hintergrund eine Menge Systemprogramme oder Dienste: die Firewall, der Virenscanner, die automatische Netzwerk-Konfiguration, die Fax-Software und vieles mehr.

Extensions: Erweiterungen für Firefox und Thunderbird, die der Anwender nach Bedarf installieren kann.

GnuPG: Gnu Privacy Guard ist ein freies Kryptografie-System zum Verschlüsseln und Signieren von Daten wie E-Mails. Es kann als Ersatz für PGP dienen. GnuPG benutzt nur patentfreie Algorithmen und wird unter der GNU General Public License vertrieben.

NTFS: Das Windows-NT-Filesystem ist sicherer und zuverlässiger, aber auch langsamer als der Vorgänger FAT32.

Online-Virenscanner: Diese Dienste starten per ActiveX oder Java (Letzteres nur bei Trend Micro) einen Virenscanner auf Ihrem Rechner. Sie werden von vielen Scanner-Herstellern kostenlos zur Verfügung gestellt und sind nach einer Infektion hilfreich.

Patch: Ein Patch ist ein kleines Programm, das Fehler in Software repariert. Sie können die Patches von den jeweiligen Hersteller-Websites kostenlos herunterladen. Oft werden Patches auch in die neuen Versionen eines Programms eingebaut.

PGP: Abkürzung für Pretty Good Privacy. Ein weit verbreitetes Programm zum Verschlüsseln von E-Mails.

Prüfsumme: Praktisch eindeutiger digitaler Fingerabdruck einer Programmdatei. Jede auch nur geringfügige Änderung an der Datei – etwa ein paar Bits eines Virus – spiegelt sich in der Prüfsumme wider.

Removal-Tool: Kleines Programm, das genau einen Schädling entfernt. Ersetzt keinen Virenscanner, ist aber höchst nützlich, wenn die Infektion einmal erfolgt ist und der Schädling genau bekannt ist.

S/Mime: Abkürzung für Secure Multipurpose Internet Message Extensions. Verschlüsselungstechnik, die digitale IDs verwendet (bestehend aus einem öffentlichen und einem privaten Schlüssel sowie einer digitalen Signatur) und das Kodierungsverfahren Mime für die Strukturierung der Nachrichten nutzt.

Spyware: Programm, das sich ohne das Wissen des Anwenders installiert und den kommerziellen Interessen des Herstellers dient. Der Name Spyware ist ungenau, weil das Opfer nicht ausspioniert, sondern mit Werbung gequält wird. Deswegen ziehen viele Autoren Adware als Bezeichnung für solche Programme vor.

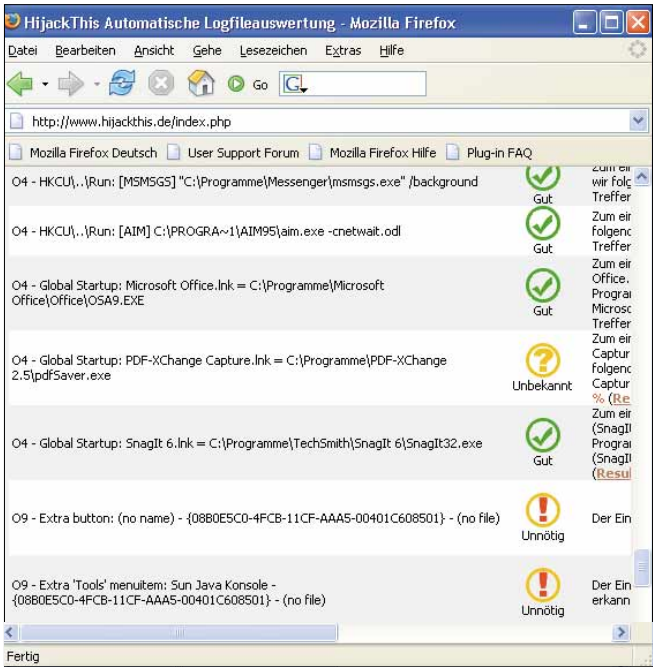
Trojaner: Richtiger: Trojanisches Pferd. So wie die Griechen im Trojanischen Pferd die Stadttore für das erobernde Heer öffneten, macht ein Trojaner eine virtuelle Hintertür im PC auf und erlaubt die Fernsteuerung durch einen kriminellen Remote-Anwender.

VB-Script: Untergruppe der Programmiersprache Visual Basic, die im Internet Explorer implementiert ist und in der Funktionsweise Javascript ähnelt.

Virus: Bösartiges Programm, das sich epidemieartig verbreitet, indem es andere Dateien infiziert, das heißt, es schreibt den eigenen Programmcode in die Wirtsdatei. Aktuelle Schädlinge sind fast ausschließlich Würmer beziehungsweise Trojaner.

Wurm: Bösartiges Programm, das sich über ein Netzwerk verbreitet. Das kann ohne Benutzerinteraktion über Schwachstellen im System geschehen (wie zum Beispiel bei dem Wurm Sasser) oder über fahrlässiges Benutzerverhalten, also das Anklicken unsicherer Dateianhänge von E-Mails (wie zum Beispiel bei Sober).

Beispiel per E-Mail oder Filesharing erhalten haben. Ist eine verseuchte Datei die Ursache der Infektion und haben Sie dieses File noch, dann ist die Diagnose-Erstellung sehr einfach. Besuchen Sie die Webseite *http://virusscan.jotti.dhs.org*, klicken Sie auf den Button *Durchsuchen* und navigieren Sie zur suspekten Datei. Bestätigen Sie mit *Submit*, erhalten Sie sofort Auskunft, ob und mit welchem Schädling die Datei infiziert ist. Diese Website verwendet praktisch alle namhaften Antiviren-Tools parallel. Sie können sich darauf verlassen, dass selbst die neuesten Viren binnen Stunden nach dem ersten Auftauchen dort erkannt werden.

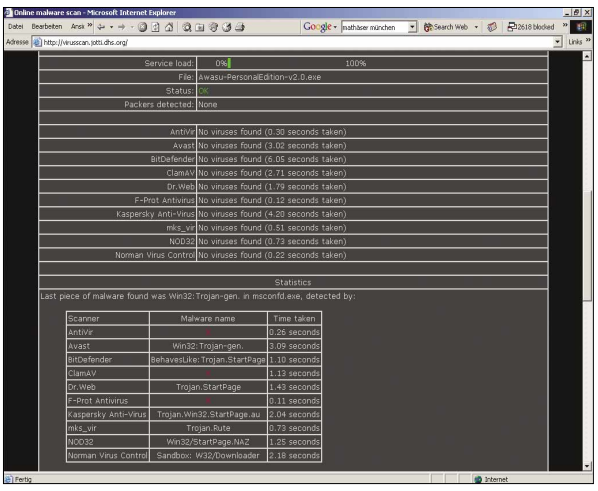


14. Spyware entfernen: Das Besondere an HijackThis ist die genaue Online-Analyse der vom Programm erzeugten Protokolldatei

Etwas schwieriger wird es, wenn Sie zwar ein ungewöhnliches Verhalten Ihres Rechners (häufige Abstürze oder ausgelastete Internet-Verbindung) feststellen, aber nicht wissen, wann Sie sich infiziert haben könnten. Sie müssen dann Ihren PC vollständig überprüfen – den Arbeitsspeicher und den gesamten Festplatteninhalt. Am einfachsten lassen Sie dies von einem der kostenlosen → Online-Virenscanner erledigen. Sie finden auf der Seite *www.scareware.de/virenscanner_3online.html* direkte Links zu solchen Tools.

Einen sehr empfehlenswerten Scanner stellt Trend Micro zur Verfügung, der im Gegensatz zu anderen Produkten auch mit Firefox funktioniert. Voraussetzung ist, dass Sie das Java-Plug-in installiert haben. Um den Online-Scanner direkt aufzurufen, geben Sie als Adresse *http://de.trendmicro-europe.com/conmer/products/housecall_launch.php* ein. Klicken Sie dort dann auf den Button *Meinen PC jetzt prüfen*. Trend Micro Housecall checkt zunächst einmal, ob die Systemvoraussetzungen erfüllt sind. Ist alles in Ordnung, klicken Sie auf *Nächster Schritt*. Es erscheint eine Java-Sicherheitswarnung, in der Sie gefragt werden, ob Sie Trend Micro vertrauen. Klicken Sie auf *Ja*. Nach einer Download-Pause erscheint ein Eingabe-Fenster, in dem Sie die zu durchsuchenden Datenträger markieren können. Klicken Sie danach auf *Suchen*. Der Scanner prüft zunächst den Inhalt des Arbeitsspeichers und danach die ausgewählten Laufwerke.

Werden Infektionen gefunden, bietet Ihnen Housecall zwei Reinigungsoptionen an. Die erste säubert nur Dateien, lässt aber möglicherweise von Viren modifizierte Systemeinstellungen bestehen und wiederholt auch die Virensuche nicht. Empfehlenswerter ist die zweite Option *Säubern & erneute Suche*. Diese Funktion entfernt die Viren, macht Systemänderungen rückgängig und sucht erneut. Klicken Sie also auf den betreffenden Button und dann auf *Automatisch wählen!* Sollte Housecall melden, dass es die Schädlinge nicht entfernen kann – was gar nicht so selten der Fall ist –, dann notieren Sie sich sorgfältig die Namen der Parasiten und lesen Sie unter „15. Infektionen beseitigen“, wie Sie weiter vorgehen.



13. Schädlingsdiagnose: Einzelne Datein lassen Sie online prüfen

14. Spyware entfernen

Virenscanner ignorieren oft → Adware oder Spyware. Das liegt unter anderem daran, dass Spyware-Anbieter großen Wert auf die Feststellung legen, keine Viren zu programmieren. Hersteller von Virenscannern, die Spyware finden und entfernen, werden mitunter aus Wettbewerbsgründen verklagt. Dieses Risiko vermeiden manche Anbieter von Sicherheits-Software, indem sie diese Malware nicht beachten.

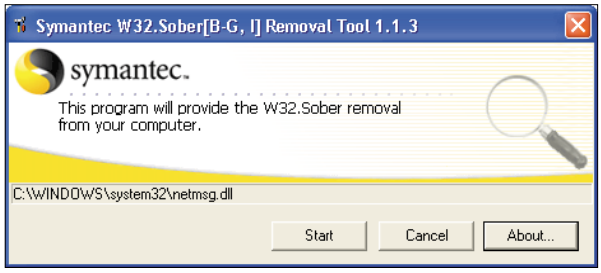
Hier helfen Spezialprogramme. Ein sehr gutes Anti-Spyware-Programm ist Ad-Aware SE Personal (für Privatnutzer kostenlos, *www.lavasoft.de/german/support/download*).

Direkt nach der Installation des Tools wird Ihr System überprüft. Gefundene ▶

Schädlinge markieren Sie, indem Sie einen Haken in das Kontrollkästchen vor ihrem Namen setzen. Mit einem Klick auf *Quarantine* entfernen Sie die Spyware schließlich.

Liefert Ad-Aware kein eindeutiges Ergebnis, hilft Ihnen Hijack This (gratis, *www.merijn.org*) weiter. Das Tool zielt nicht auf spezielle Schädlinge ab, sondern sucht in der Registry nach Hinweisen, dass sich Spyware eingenistet hat. Das dabei entstehende Protokoll ist für Nicht-Spezialisten kaum verständlich. Glücklicherweise finden Sie unter *www.hijackthis.de* eine automatische Auswertung der Protokolldatei. Sollte Ihr Parasit so neu oder ungewöhnlich sein, dass ihn der Online-Dienst nicht kennt, haben Sie immer noch die Möglichkeit, Ihr Protokoll ins Forum dieser Website *(www.hijackthis.de/forum)* zu posten.

Hat die Auswertung Ihres Protokolls mehrere Plagegeister eindeutig identifiziert, müssen Sie Hijack This erneut starten und die Kontrollkästchen aller als gefährlich bewerteten Einträge markieren. Per Klick auf *Fix checked* werden Sie diese



15. Schwere Infektion beseitigen: Die speziell auf einzelne Schädlinge zugeschnittenen Removal-Tools sind sehr einfach zu bedienen

normalerweise los. Falls es auf diesem Weg nicht klappt, können Sie den Vorgang auch noch einmal im abgesicherten Modus versuchen (siehe unter „16. Problematische Fälle“).

15. Schwere Infektion beseitigen

Haben Sie den exakten Namen des Schädlings festgestellt, können Sie sich an das Beseitigen der Infektion begeben. Ein konkretes Beispiel: Ende November oder Anfang Dezember 2004 haben Sie eine Mail von der Universität Mainz mit dem Betreff *Ungültige Zeichen in Ihrer E-Mail -Code: 9801* erhalten und leichtsinnigerweise doppelt auf den Anhang *data_info_1516.pif* geklickt. Eine verdächtige Fehlermeldung erschien, der Computer reagierte langsamer, und gleichzeitig fand eine starke Internet-Aktivität statt, obwohl Sie selbst an diesem Tag gar nicht online waren.

Heute lösen wir den Fall: Wenn Sie entweder *data_info_1516.pif* bei Jotti überprüfen lassen oder einen Voll-Scan bei Trend Micro durchführen, werden Sie schnell feststellen, dass Sie sich einen berüchtigten Schädling eingefangen haben – den erfolgreichsten Wurm-Parasiten in jenen Monaten: die i-Variante von Sober.

Viren tragen leider keine herstellerübergreifenden eindeutigen Namen, denn jeder Antiviren-Hersteller benutzt eine eigene Nomenklatur. Diese Sober-Variante heißt beispielsweise bei Kaspersky I-Worm.Sober.i, bei Symantec dagegen W32.Sober.I@mm. Zum Glück nennen aber viele Hersteller auch die Konkurrenznamen auf ihren Websites, so dass Ihnen im Folgenden eine langwierige Suche erspart bleibt.

Geben Sie im nächsten Schritt bei Google oder einer anderen Suchmaschine

Webseiten zum Thema sicherer PC

Sicherheitsstufe 1: Basisschutz für Windows

- ***www.dingens.org***
  Tipps, Links und Software zum Deaktivieren unsicherer und nutzloser Windows-Dienste – für Windows XP und 2000
- ***http://ntsvcfg.de***
  Hier finden Sie eine Anleitung für eine sichere Konfiguration der Services unter Windows XP und 2000
- ***http://support.microsoft.com/default.aspx?scid=fh;DE;KBHOWTO***
  Knowledge Base von Microsoft

Sicherheitsstufe 2: Schutz mit Software ausbauen

- ***www.mozilla.org/products/firefox/***
  Die offizielle Seite der Entwickler des Open-Source-Browsers Firefox
- ***http://mozilla.bric.de/wiki/index.php/Firefox***
  Das deutsche Mozilla-Wiki hilft Anwendern mit Problemlösungen, Tipps und Tricks
- ***http://firefox.stw.uni-duisburg.de/forum***
  Deutsches Firefox-Forum
- ***www.sygate.de***
  Hier erhalten Sie die verschiedenen Versionen der Sygate Firewall
- ***www.acronis.de***
  Website zu True Image
- ***www.thunderbird-mail.de***
  Thunderbird auf Deutsch zum Herunterladen, Dokumentation und Forum
- ***http://thunderbird.bric.de***
  Deutschsprachige Hilfe-Site zu Thunderbird
- ***http://borumat.de/thunderbird-email-tipps.php***
  Tipps und Tricks zu Thunderbird
- ***www.mozilla.org/products/thunderbird***
  Die offizielle, englischsprachige Thunderbird-Homepage
- ***http://weblogs.mozillazine.org/rumblingedge***
  Für Fortgeschrittene: englischsprachige Infos zu Thunderbird-Nightly-Builds

Sicherheitsstufe 3: Hilfe im Ernstfall

- ***www.dshield.org***
  Nachrichten und Informationen zum Thema Trojaner-Abwehr
- ***www.scareware.de/virenscanner_3online.html***
  Übersicht über Online-Virenscanner
- ***http://virusscan.jotti.dhs.org***
  Online-Virenscanner, der kostenlos eine Datei mit mehreren Scannern prüft
- ***http://de.trendmicro-europe.com/consumer/products/housecall_launch.php***
  Vollfunktionaler Online-Virenscanner; benötigt Java
- ***www.lavasoft.de/german/support***
  Support und Download von Ad-Aware
- ***www.hijackthis.de***
  Automatische Analyse von Hijack-This-Protokollen
- ***www.viruslist.com/en***
  Viren-Informationen von Kaspersky
- ***http://securityresponse.symantec.com***
  Viren-Informationen von Symantec
- ***www.sophos.com/virusinfo/analyses***
  Viren-Informationen von Sophos
- ***www.f-secure.de/v-desk/_new.shtml***
  Viren-Informationen von F-Secure

folgende Suchbegriffe ein: „genauer Virenname“ „removal tool“, also zum Beispiel **`"I-worm.Sober.i" "removal tool"`**. Die Anführungszeichen sind wichtig, um bessere Suchresultate zu erhalten.

Schon der erste Treffer ist eine Symantec Security Response. Dort wird der Wurm exakt beschrieben. Man erfährt über ihn beispielsweise, wie er sich verbreitet und welche Schäden er anzurichten im Stande ist. Außerdem sehen Sie oben rechts den großen Link *To fix this problem, get the removal tool*. Klicken Sie darauf.

Leider reicht es nicht aus, das → Removal-Tool herunterzuladen und einfach nur zu starten. Es ist darüber hinaus unerlässlich, dass Sie die Beschreibung des Removal-Tools auf der Webseite genau lesen und die Anweisungen dort sorgfältig einhalten. Normalerweise müssen Sie zunächst das Tool herunterladen und dann die Internet-Verbindung kappen (am besten Kabel abziehen). Melden Sie sich nun als Administrator an.

Ehe Sie das Removal-Tool ausführen, müssen Sie die Systemwiederherstellung deaktivieren. Das mag paradox klingen, da die Wiederherstellung als Schutz vor Katastrophen gedacht ist. Das Problem ist, dass der Wiederherstellungsordner für das Removal-Tool tabu ist. Es kann Ihnen also passieren, dass das Tool den Virus entfernt, und der scheinbar beseitigte Schädling später von der Systemwiederherstellung wiederbelebt wird. Zum Deaktivieren der Funktion öffnen Sie also die *Eigenschaften* von *Arbeitsplatz* mit der rechten Maustaste. Klicken Sie auf den Reiter *Systemwiederherstellung* und setzen Sie einen Haken bei *Systemwiederherstellung auf allen Laufwerken deaktivieren*. Bestätigen Sie mit *OK*.

Starten Sie erst jetzt das Removal-Tool und folgen Sie exakt seinen Anweisungen. Booten Sie dann den Rechner neu und führen Sie das Removal-Tool wieder aus, um sicherzugehen, dass die Infektion besiegt ist. Vergessen Sie nicht, zum Abschluss die Systemwiederherstellung wieder zu aktivieren.

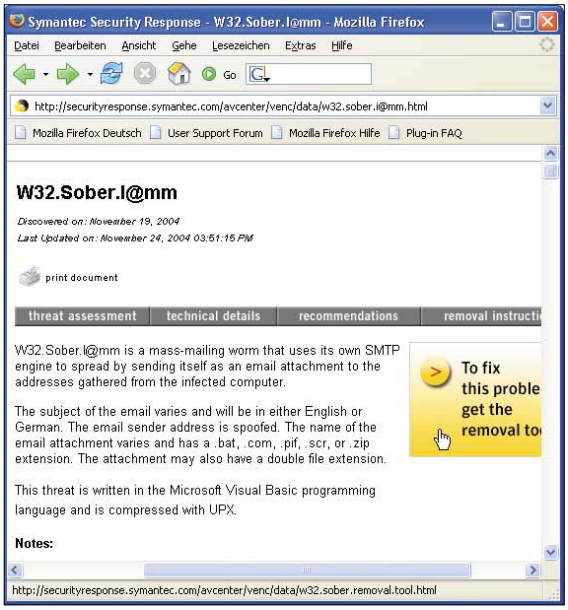
16. Problematische Fälle

Manchmal kann es passieren, dass Sie einen Virenbefall diagnostizieren und die Entfernung des Schädlings streng nach Vorschrift vornehmen – und dann beim abschließenden Test feststellen müssen, dass der Computer immer noch infiziert ist. In solch vertrackten Fällen versuchen Sie zunächst die Entfernung im → abgesicherten Modus. Dieser spezielle Modus von Windows ist zur Fehlerbeseitigung gedacht. Wenn Sie den PC im abgesicherten Modus starten, werden viele Treiber oder Autostartprogramme nicht geladen. Der Nutzen: Der Virus wird nicht aufgerufen und kann sich nicht gegen die Entfernung schützen.

Um Ihren Computer im abgesicherten Modus zu booten, drücken Sie während des Systemstarts die Taste [F8]. Es ist allerdings nicht ganz einfach, den richtigen Moment zu treffen. Betätigen Sie daher sofort nach Erscheinen der ersten Boot-Meldung mehrmals die Taste. Führen Sie dann das Removal-Tool oder den Spyware-Entferner aus und starten Sie den Rechner neu.

Treten Ihre Probleme nach wie vor auf, versuchen Sie das Removal-Tool eines anderen Herstellers, etwa von Kaspersky. AV-Test *(www.av-test.org)* prüfte vor einem Jahr neun Tools gegen eine Sober-Variante – nur drei entfernten den Schädling in allen Umgebungen. Zwar bessern die Antiviren-Hersteller ständig nach, doch bei einer großen akuten Virenattacke haben sie wenig Zeit, um Tools zu programmieren und zu testen. ■

Andreas Dumont/Andreas Th. Fischer/Peter Riedlberger/Ilka Schöning/kpl/hs
internet@com-magazin.de



15. Schwere Infektion beseitigen: Der Link zum Removal-Tool bei Symantec Security Response ist unübersehbar