NEU! PC-WELT-SPEZIAL ALLES ZUM THEMA SICHERHEIT AM PC

PC WELT
02/2002

PC WELT SPEZIAL

Deutschland € 9,95 | Österreich € 10,95 | Schweiz sfr 19,90 | Luxemburg € 11,45
www.pcwelt.de | AOL-Stichwort pcwelt

Neue Tipps und Tools gegen 0190-Dialer

100 SICHERHEITS-TOOLS AUF CD

▸ Basis-Ausstattung

Diese Sicherheits-Tools müssen unbedingt auf Ihren Rechner

▸ Sicherheits-Add-ons

0190 Alarm 3.00 · Ad-Aware 5.83 · Anti-Trojan 5.5 · AntiVir Personal Edition 6.14 · Autostartmanager 1.42 · Back it Up 1.23 b · Backup Xpress Pro 2.72 · Cookie Crusher 3.0.4.35 · Das Schließfach 2.0 · Drive Crypt 3.0.3a · E-Safe Desktop 3.1 · McAfee VirusScan 6.02 · Ontrack Easy Recovery 6.0 Trial · Outpost Firewall Free 1.01 · Password Recovery Toolkit · Pegasus Mail 4.01 · Pop Up Cop 1.2 · Pretty Good Privacy 7.03 · Safersurf 2.0 · Security 1.2 · Steganos Online Shield 1.51 · The Cleaner 3.5 · Tiny Trojan Trap 3.0 · Trojan Check 5 · WebWasher 3.0 · Win-Dietrich 2.00 · WinPatrol 4.0 · XP-AntiSpy 3.51 · YAW 3.01 · Zone Alarm Free 3.1.291 und noch viel mehr Free- & Shareware

4 195895 809954 02

Alles sicher!

0190-DIALER So wehren Sie sich effektiv!
Tools: Der beste Schutz gegen die 0190-Abzocker

VIREN So arbeitet Ihr Viren-Scanner optimal!
Test: 15 Antiviren-Programme auf dem Prüfstand

TROJANER So schalten Sie die Gefahr aus!
Tipps: Firewall Zone Alarm problemlos einrichten

SPIONAGE So machen Sie Windows dicht!
Tricks: Spyware in Gratis-Programmen beseitigen

PLUS: Schritt für Schritt zum bombensicheren PC

ALLES DRIN: HACKER, PASSWORT-CRACKER, BROWSER-LECKS, VERSCHLÜSSELUNG

PC-WELT Spezial 2/2002: Sicherheit

Alles sicher!

Täglich gibt es neue Viren, erfolgreiche Dialer-Attacken und Datendiebstähle. Die PC-WELT stellt alle wichtigen und wirksamen Schutzmechanismen vor.

Das komplette Sicherheits-Paket

Für die Heft-CD haben wir über 100 Programme und Utilities zusammengetragen, die auch in den Artikeln vorgestellt werden. Die Software, die wir auf CD gepackt haben, ist im Heft mit dem Logo ◉ auf Heft-CD gekennzeichnet. Eine Auflistung dieser Programme und Utilities in alphabetischer Reihenfolge finden Sie auf der CD-Hülle (▷ Seite 5).

Auf unserer Heft-CD finden Sie immer die Programmversion, auf die wir im Heft Bezug nehmen, auch wenn im Internet inzwischen nur noch eine andere Version verfügbar ist.

Keine Angst vor Viren: Bevor die PC-WELT-CDs die Redaktion verlassen, prüfen wir sie gründlich mit mehreren Antiviren-Programmen. Wenn Sie sich selbst davon überzeugen wollen: Die Logdatei eines der Virenscanner finden Sie im Hauptverzeichnis der Heft-CD unter der Bezeichnung NOVIRUS.TXT.

Grundlagen PC-Sicherheit: Erst wenn Sie wissen, wie Viren, Dialer oder Hacker arbeiten und womit sie Angriffe auf Ihren PC initiieren, können Sie sich wirksam gegen sie schützen. Denn meist sind Windows-PCs offen wie ein Scheunentor und laden Angreifer geradezu ein. Mit der richtigen Abwehrstrategie und einigen unentbehrlichen Programmen sichern Sie Ihren Windows-PC wirkungsvoll ab. Und: Viele bekannte Sicherheitslücken lassen sich bereits mit Windows-Bordmitteln oder durch Updates schließen.

Viren und Trojaner: Viren sind die mit Abstand größte Plage für alle PC-Besitzer. Als unauffällige E-Mail-Datei-Anhänge getarnt oder als infizierte Dateien, die Sie aus dem Internet laden, richten sie enormen Schaden an und verbreiten sich selbsttätig weiter. In einem Vergleichstest haben wir 15 Virenscanner unter die Lupe genommen. Außerdem stellen wir Ihnen neun Spezialprogramme zur Trojanerabwehr vor. Lesen Sie zudem, welche Gefahren Ihnen beim Einsatz eines Instant Messengers drohen und was es mit den Spionage-Aktivitäten von Adware auf sich hat.

0190-Dialer: Wer im Netz surft, wird immer wieder abgezockt. Zwei Klicks zu viel – und schon läuft die Internet-Verbindung über eine teure 0190er-Nummer. Dreiste Anbieter haben schon bis zu 300 Euro abkassiert, seriöse Anbieter verlangen beispielsweise knapp 1,80 Euro pro Minute. Da die Dialer immer raffinierter zu Werke gehen, bedarf es besonderer Vorsicht und eines Schutzprogramms wie Yaw, dessen Konfiguration und Arbeitsweise wir in einem Workshop beschreiben.

Sicher im Netz: Sowohl im Internet als auch im lokalen Netzwerk ist Ihr Windows-PC ständigen Gefahren ausgesetzt. Lesen Sie, was für Aufgaben eine Firewall übernimmt und wie sie funktioniert. Ein Workshop zum wohl populärsten Gratisprogramm Zone Alarm hilft Ihnen bei der Einrichtung und zeigt, welche Einstellungen für höchstmöglichen Schutz sorgen. Auch das Thema Browser-Sicherheit kommt nicht zu kurz – so erfahren Sie etwa, was sich hinter den Sicherheitsoptionen verbirgt. All das sorgt für mehr Sicherheit beim Surfen und sperrt Angreifer aus.

Verschlüsselung: Um sensible Daten vor den Blicken Neugieriger zu schützen, setzen Profis auf eine Verschlüsselung: Nur Absender und Empfänger können dann die Nachrichten einsehen. Wir geben einen Überblick über die Verfahren und sagen Ihnen, wie sich die Programme in Bezug auf Sicherheit und Handhabung unterscheiden. In einem Workshop erfahren Sie, wie einfach Sie Mails mit der populären Software Pretty Good Privacy (PGP) verschlüsseln. Dazu gibt es noch die besten Tools für Passwortsicherheit.

▸Abwehrstrategien für Windows

▸Netzwerk- und Online-Sicherheit

▸Trojaner, Viren und Spyware stoppen

Fortsetzung Seite 9

Abwehrstrategien für Windows

Persönliche Daten können Ihren PC ohne Ihre Genehmigung verlassen. Wir zeigen Ihnen die potenziellen Schwachstellen und sagen, was Sie dagegen tun können.

ab Seite 12

Netzwerk- und Online-Sicherheit

Sie schützen Ihren PC mit Passwörtern für Bios, Bildschirmschoner und Freigaben? Die vermeintliche Sicherheit ist in Sekunden dahin. Wir sagen, auf was Sie achten müssen.

ab Seite 44

Trojaner, Viren und Spyware stoppen

Zur Verbreitung gefährlicher Software haben Programmierer ausgebuffte Möglichkeiten ersonnen, hinterhältige Programme auf Ihren PC zu schmuggeln.

ab Seite 76

Gebührenfalle 0190-Dialer

Kaum ein Tag vergeht, an dem nicht neue Abzockereien mittels 0190-Dialer ans Tageslicht kommen. Wir zeigen, wie Sie sich davor schützen können.

ab Seite 110

Vertrauliche Daten verbergen

Angesichts der vielen Verschlüsselungsmethoden hängt die Auswahl von drei Faktoren ab: Sicherheit, Verschlüsselungsgeschwindigkeit und Einsatzgebiet.

ab Seite 120

▸Trojaner, Viren und Spyware stoppen

▸Gebührenfalle 0190-Dialer

▸Vertrauliche Daten verbergen

Rubriken

Gefahrenquelle Internet

Hacker greifen an

Persönliche Daten können Ihren PC ohne Ihre Genehmigung verlassen. Wir zeigen Ihnen die potenziellen Schwachstellen Ihres Rechners und sagen, was Sie dagegen tun können.

Das Internet steckt voller Gefahren. Hacker verwenden Abhörprogramme zum Ausspionieren Ihres PCs, setzen bösartige Trojaner, Würmer und Viren ein, um Ihren PC lahm zu legen, oder starten heimlich Fernsteuerungsprogramme, über die sie die Kontrolle über Ihren PC übernehmen wollen. Abzocker jubeln Ihnen beim Surfen Dialogfenster unter in der Hoffnung, dass Sie diese vorschnell akzeptieren und sich dabei einen 0190-Dialer einfangen, der Ihre Telefonrechnung in die Höhe treibt. Bei der Entwicklung neuer Anwendungsprogramme und Utilities vernachlässigen viele Hersteller die Sicherheit zugunsten von Benutzerfreundlichkeit und Funktionsfülle – ein nicht unerhebliches Risiko für die Sicherheit Ihrer Daten. Ungesicherte Online-Schnittstellen und unverschlüsselte Kennwortübermittlungen im Klartext sind an der Tagesordnung. Aber auch ohne Online-Anbindung sind Ihre Daten Risiken ausgesetzt. So werfen neugierige Kollegen möglicherweise in Ihrer Abwesenheit schon einmal einen Blick auf Ihre Dokumente, manipulieren Ihre Daten oder knacken Ihre Passwörter.

Das für Netzwerke offene Windows XP wurde zwar viel sicherheitsbewusster als seine Vorgänger konzipiert, und viele Sicherheitslecks wurden bereits entdeckt. Dennoch ticken noch zahlreiche Zeitbomben in dem Betriebssystem. Dass besonders häufig Microsoft-Produkte Ziel von Angriffen sind, liegt vor allem an der großen Verbreitung. Die Schwächen der Produkte sind bekannt, und das für zielgerichtete Angriffe erforderliche Wissen gibt es im Internet.

Sicherheitslücken: Nicht nur Windows ist betroffen

Auch andere populäre Betriebssysteme wie Linux sind betroffen. Die Schwachstellen laden Hacker und Datenspione geradezu ein, in Ihr System einzudringen. Zudem macht es eine Reihe von Anwendern den Crackern sehr leicht. Viele PC-Nutzer haben nur geringe Kenntnisse über Sicherheit und über die Gefahren, denen sie ihre Daten aussetzen. Welche Verhaltensregeln Sie unbedingt beachten sollten, lesen Sie ab ▷ Seite 14.

Info: PC-Attacken

Die vernetzte Internet-Welt hat ihren Preis: Die Sicherheit gespeicherter PC-Daten und persönlicher Informationen sind durch Angriffe von außen gefährdet. Die meisten Schlupflöcher lassen sich aber abdichten.

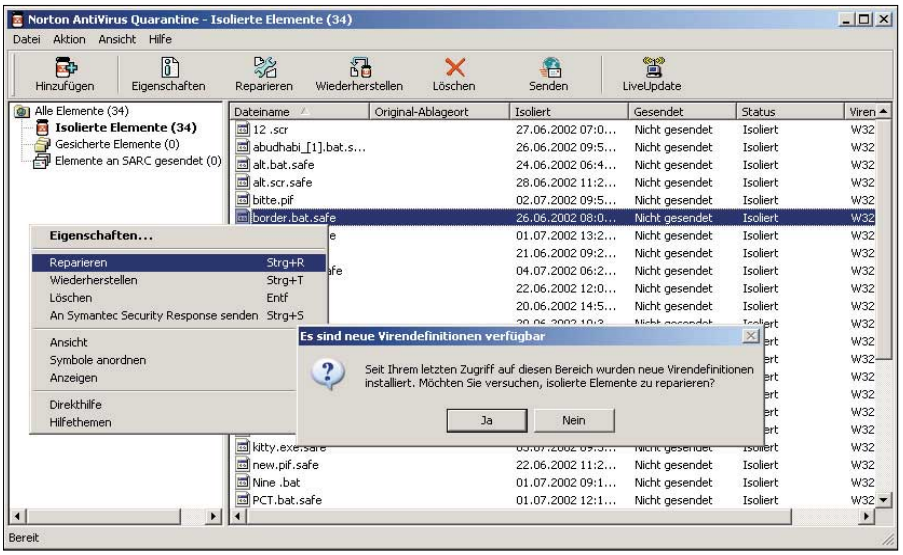
Hackerangriffe über das Internet: Inzwischen die Regel

Um das eingesetzte Betriebssystem und die Anwendungs-Software gegen die immer häufigeren Attacken zu schützen, stellen fast alle Hersteller kostenlose Updates und Software-Patches zur Verfügung. Durch das Einspielen der Patches schließen Sie die Lücken, durch die Angreifer die Gewalt über Ihren Rechner erlangen können.

Dass Hackereinbrüche überhaupt gelingen können, liegt aber nur zu einem geringen Teil an dem verwendeten Betriebssystem und der eingesetzten Software. Ganz wesentlich tragen auch die Unkenntnis und Gleichgültigkeit von PC-Anwendern dazu bei. Nur sehr wenige Angriffe von außen haben ohne Zutun des Anwenders Erfolg. Mit einem Portscanner bewaffnet können Angreifer zwar systematisch nach offenen Ports suchen und so mögliche Angriffsziele ausmachen. Da für Hacker interessante Ports aber normalerweise erst durch einen Trojaner geöffnet werden, muss dieser zunächst einmal auf Ihren PC gelangen.

Auf der Festplatte: Angriff von Viren und Trojanern

Die meisten Gefahren gehen von Viren und Trojanern aus, die die Anwender selbst aktivieren. Weil Sie die aus dem Internet hereinkommenden Datenpakete unmöglich von Hand auf gefährliche Inhalte überprüfen können, setzen Sie dazu einen Virenscanner ein. Er schützt Sie gleich in mehrfacher Hinsicht: Durch die Integration in Ihr Mailprogramm scannt die Antiviren-Software alle empfangenen Nachrichten, noch bevor Sie die Mails angezeigt bekommen, und sortiert verseuchte Mitteilungen aus. Auch aus dem Internet geladene Dateien laufen vor dem Speichern auf Festplatte durch den permanent aktiven Virenscanner und werden im Falle eines Schädlingsbefalls erst gar nicht auf dem lokalen Datenträger abgelegt. Gute Antiviren-Programme prüfen zudem auch von Ihnen in Richtung Internet gesendete Daten, damit Ihr PC nicht als Replikationsstation dient, sollte sich ein Virus auf Ihrem System befinden. Wie Sie den passenden Virenscanner finden und worauf Sie achten müssen, lesen Sie ab ▷ Seite 76.



Täuschen und tricksen: Beim Verpacken von Viren und Trojanern in scheinbar harmlose Mails, Filesharing-Tauschangebote und Downloads lassen sich Hacker immer wieder neue Dateinamen einfallen

Besonders heimtückisch sind Angriffe mit angeblichen Software-Updates. Sie werden von Hackern gezielt per Mail verschickt und enthalten im Anhang eine verseuchte Datei, über die sich Dritte Zugang zu Ihrem PC verschaffen oder über die Sie beim Starten des Anhangs einen Virus aktivieren. Sehr beliebt sind gefälschte Windows-XP-Patches, Virenkiller und Spiele. Auch als Bilder oder Textdokumente getarnte VB-Scriptdateien stellen eine erhebliche Bedrohung dar. Wie Sie Windows mit Bordmitteln optimal sichern, lesen Sie ab ▷ Seite 44.

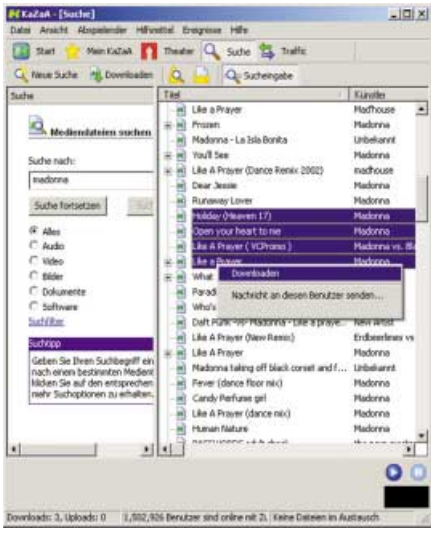
Hacker-Attacken: Das können Sie dagegen tun

Die Motive von Hackern sind vielfältig und nicht immer vom Gedanken getragen, Daten zu vernichten. Oft steckt auch nur die Neugier dahinter, einmal ein fremdes System zu knacken. Aber Sie können rechtzeitig erkennen, wenn jemand versucht, in Ihr System einzudringen, und ihn dann am Datendiebstahl hindern. Dabei bildet eine Desktop-Firewall eine Schutzmauer zwischen dem Internet und Ihrem PC. Zwar kann eine Firewall weder den Befall mit Trojanern noch das Aktivwerden eines per Mail eingeschleusten Fernsteuerungsprogramms verhindern. Sobald die bösartige Software jedoch versucht, Daten von Ihrem PC an einen unbekannten Server im Internet zu senden oder Infos online von einer Gegenstelle abzurufen, schlägt der Software-Wachhund Alarm. In unserem Vergleichstest ab ▷ Seite 50 sagen wir Ihnen, welche Personal Firewalls empfehlenswert sind. Tipps dazu gibt's ab ▷ Seite 61.

Dauerhafte Sicherheit: Nicht allein per Software

Sicherheit gibt es nicht umsonst, und Sicherheit macht Arbeit – das bedeutet, dass Sie sich fortlaufend um die Sicherheit Ihres PCs kümmern müssen. Eine Antiviren-Software ist nur so gut, wie ihr letztes Update. Desktop-Firewall und Zusatz-Tools können nur dann Sicherheit bieten, wenn der Anwender über das erforderliche Hintergrundwissen verfügt. Das Know-how und die passende Software liefert dieses PC-WELT Spezial.

Christoph Metzger



Riskante Tauschbörsen: Die Programme öffnen Ports, über die Dritte Zugang zum PC erhalten

Sicherheit fängt beim Anwenderverhalten an

Vorsorgeuntersuchung

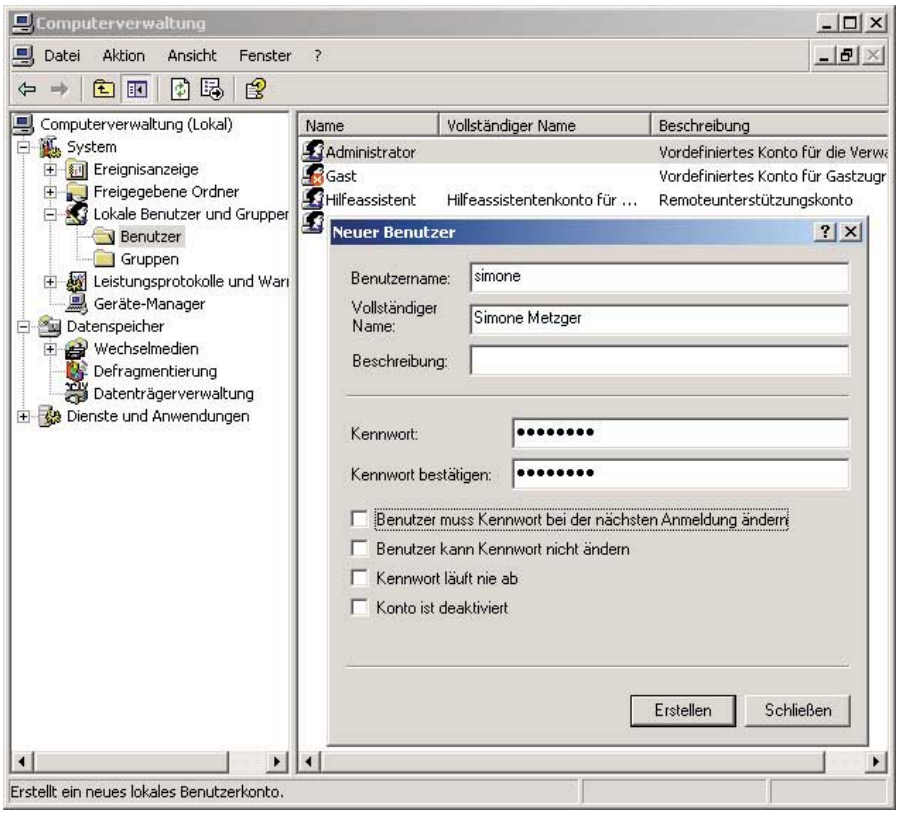
Unachtsame Anwender geraten schnell in die Fänge von Datenspionen und geben ihre Privatsphäre preis. Doch schon mit ein paar einfachen Verhaltensregeln minimieren Sie die Gefahr.

▸Fast jeder Anwender hat eine Menge Daten auf seinem PC, deren Verlust beziehungsweise die dadurch notwendige Neuerstellung ein Vielfaches der PC-Anschaffungskosten ausmachen würde. Sicherheit am PC beginnt bei elementaren Überlegungen zur Datensicherung und geht über die Sicherung des Rechners gegen unbefugte Nutzung bis hin zur geschützten Kommunikation via Internet.

Regelmäßige Datensicherung ist die wichtigste Schutzregel

Um ein Backup zumindest Ihrer Dokumente und der wichtigsten Dateien kommen Sie nicht herum. Für die Sicherung dieser persönlichen Ordner und Dateien, die häufig im Verzeichnis „Eigene Dateien“ auf Laufwerk C: abgelegt sind, genügt in der Regel die Speicherkapazität eines CD-Rohlings. Auch eine Sicherung Ihrer Datenpartition über ein Image-Programm wie Drive Image 2002 (**www.powerquest.com**; 65 Euro) oder Norton Ghost 2002 (**www.symantec.de**; 45 Euro) schützt Sie gegen Datenverlust.

Damit Unbefugte keinen Zugang zu Ihrem PC haben, aktivieren Sie das Anmeldepasswort von Win XP oder der Vorgängerversionen. Win XP erlaubt es bei der Installation, auf ein Kennwort zu verzichten, so dass das Betriebssystem ohne Passwortabfrage hochfährt – eine eklatante Sicherheitslücke. Außerdem sollten Sie im PC-Alltag keinesfalls als Administrator arbeiten, sondern über „Systemsteuerung, Verwaltung, Lokale Benutzer und Gruppen“ ein zusätzliches Benutzerkonto einrichten, das nicht der Gruppe „Administratoren“ angehört. Dadurch sind wichtige Systemeinstellungen vor unbeabsichtigten Änderungen geschützt. Zusätzlich aktivieren Sie das Bios-Passwort, um ein Booten des Systems mittels Startdiskette oder Boot-CD zu verhindern, über das alle auf der Platte gespeicherten Daten zugänglich sind. Das gilt auch bei Verwendung des Dateisystems NTFS, das sich mit geeigneten Spezialtreibern aushebeln lässt.



Nie als Administrator: Richten Sie sich eine zusätzliche Benutzerkennung ohne Administratorenrechte ein, die nur eingeschränkt Änderungen an den Windows-Einstellungen vornehmen kann

Diese Schutzmaßnahmen halten Neugierige ab

Wichtige und sensible Daten verschlüsseln Sie entweder über den Passwortschutz der jeweiligen Software oder besser über eine zusätzliches, leistungsfähiges Verschlüsselungsprogramm, das sichere Algorithmen wie den aktuellen Krypto-Standard AES verwendet. Tipps dazu lesen Sie ab ▷ Seite 120. Besonders einfach in der Handhabung sind Krypto-Programme, die mit verschlüsselten virtuellen Laufwerken arbeiten. Diese werden als zusätzliche Laufwerksbuchstaben in Windows eingebunden und stehen in allen Anwendungen und im Windows-Explorer

Info: Sicherheitsregeln

Das größte Sicherheitsproblem ist und bleibt der Anwender, der durch Leichtsinn und Unwissenheit den Datenhackern die Türen öffnet. Bei Beachtung einiger weniger Vorbeugemaßnahmen sind Sie aber auf der sicheren Seite.

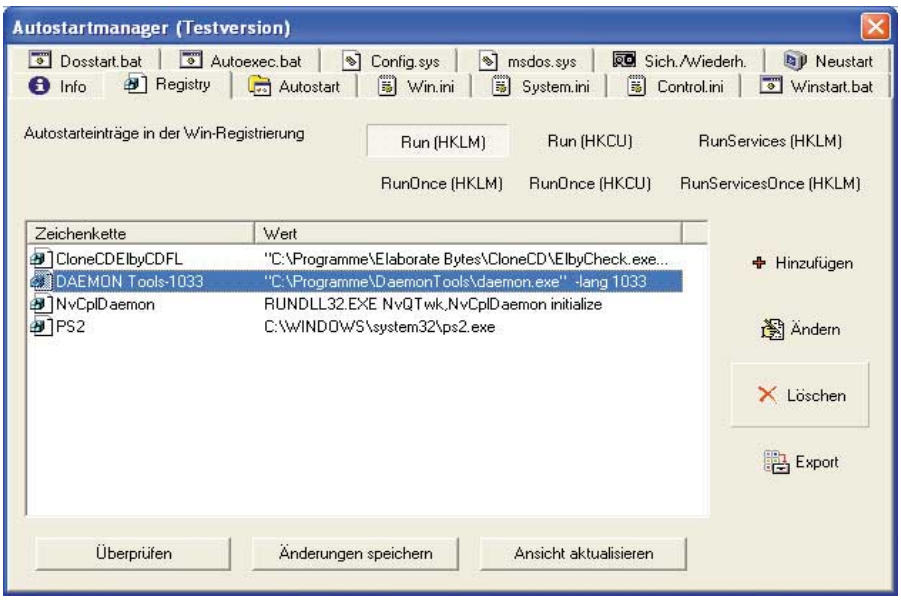
wie physikalische Laufwerke zum Lesen und Schreiben zur Verfügung. Alle Daten sind durch Verschlüsselung geschützt, und die Datei, die das virtuelle Laufwerk enthält, kann zu Sicherungszwecken beispielsweise auf CD gebrannt werden. Haben Sie keine Lust, jedes Mal ein langes und kompliziertes Passwort zum Zugriff auf das geschützte Laufwerk einzugeben, entscheiden Sie sich für eine Verschlüsselungs-Software, die Unterstützung für externe Hardware-Schlüssel, etwa einen portablen USB-Stecker bietet. Dabei wird Ihre Zugangskennung auf dem elektronischen Schlüssel gespeichert. Zur Anmeldung stecken Sie den Stecker einfach in einen USB-Anschluss Ihres PCs.

Generelle Sorgfalt walten lassen sollten Sie insbesondere bei der Auswahl Ihrer Kennwörter. Tabu sind alle Begriffe, die von Dritten leicht zu erraten sind. Verwenden Sie stets unterschiedliche Passwörter, besonders wenn Sie sich im Internet auf verschiedenen Websites anmelden. Ansonsten genügt es, Ihr Kennwort einmal abzufangen, um alle Passwortanfragen zu umgehen. Benutzen Sie Passwörter, die mindestens acht Zeichen lang sind und Klein- und Großschreibung sowie Ziffern enthalten. Benutzen Sie nie Wörter, die einen Sinn ergeben. Ein regelmäßiger Wechsel der verwendeten Kennwörter, beispielsweise alle zwei bis drei Monate, erhöht Ihre Sicherheit. Auf das Notieren Ihrer Passwörter auf Papier sollten Sie besser verzichten. Können Sie sich Ihre Kennungen einfach nicht merken, verwenden Sie eine Passwortverwaltung, die selbst mit einem sicheren Kennwort geschützt ist. Alternativ schreiben Sie Ihre Passwörter unauffällig zusammen mit anderem Text auf ein Blatt Papier und verwahren dieses räumlich getrennt vom Computer auf.

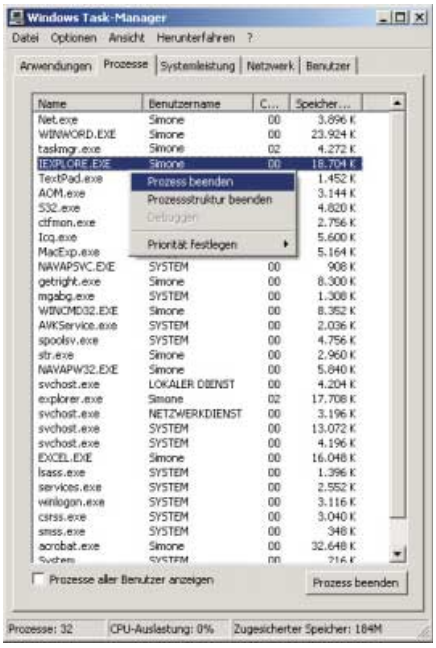
So zeigen Sie Schnüfflern die Rote Karte

Nutzen Sie zum Surfen im Internet möglichst einen aktuellen Browser, um bekannt gewordene Sicherheitslöcher älterer Versionen zu schließen. Allerdings ist es nicht ratsam, einen neuen Browser bei einem Versionssprung gleich in den ersten Tagen nach seiner Veröffentlichung zu installieren sowie Beta-Software einzusetzen. In solchen Fällen sind grobe Programmierfehler wahrscheinlich, die noch nicht erkannt und beseitigt worden sind.

Öffnen Sie nie Anhänge von Mails eines fremden Absenders, bei bekannten Absendern sollten Sie Anhänge vor dem Öffnen stets mit einem Virenscanner überprüfen. Auch bei Chats oder beim Instant Messaging sollten Sie keine Dateitransfers akzeptieren, wenn Sie die Dateien nicht explizit angefordert haben. Zum Schutz Ihrer Privatsphäre ist es empfehlenswert, Cookies und Browser-Cache regelmäßig zu löschen. Lassen Sie keine Software wie Filesharing-Programme, Web- oder FTP-Server oder Fernsteuerungsprogramme im Hintergrund laufen, die Schnittstellen ins Internet offen halten. Virenscanner und Firewall sollten Sie immer auf dem neuesten Stand halten und die verfügbaren Sicherheits-Updates für Windows einspielen.



Start unter Kontrolle: Mit der deutschsprachigen Freeware Autostartmanager 1.42 (330 KB, **www.wt-rate.de**, auf Heft-CD) verhindern Sie, dass Programme beim Systemstart automatisch aktiv werden



Ein jähes Ende: Über den Taskmanager können Sie alle verdächtigen Programme beenden

Installieren Sie keine Software aus unbekannten Quellen

Bei der Installation von Software sollten Sie darauf achten, dass Sie die gewünschten Programme nur aus authentischen Quellen beziehen. Bei Free- und Shareware, die Sie aus dem Internet herunterladen, sollten Sie zum Download die Hersteller-Website besuchen, auch wenn Sie an anderer Stelle auf das jeweilige Programm aufmerksam geworden sind. Seien Sie auch bei der Installation von Software von CD, DVD und Disketten skeptisch, wenn Sie nicht genau wissen, woher die Programme stammen. Für permanenten Schutz sorgt hierbei ein Hintergrund-Virenscanner.

Ein ganz erhebliches Risiko geht von 0190-Dialer-Programmen aus, die zu horrenden Einwahlgebühren auf das Internet zugreifen. Lesen Sie die Dialoge sorgfältig durch, brechen Sie unaufgeforderte Downloads sofort ab, und lassen Sie spezielle Programme nach installierten Dialern suchen. Wenn Sie diese Sicherheitsaspekte berücksichtigen, wird es für Spione und Saboteure erheblich schwerer, in Ihren PC einzudringen.

Christoph Metzger

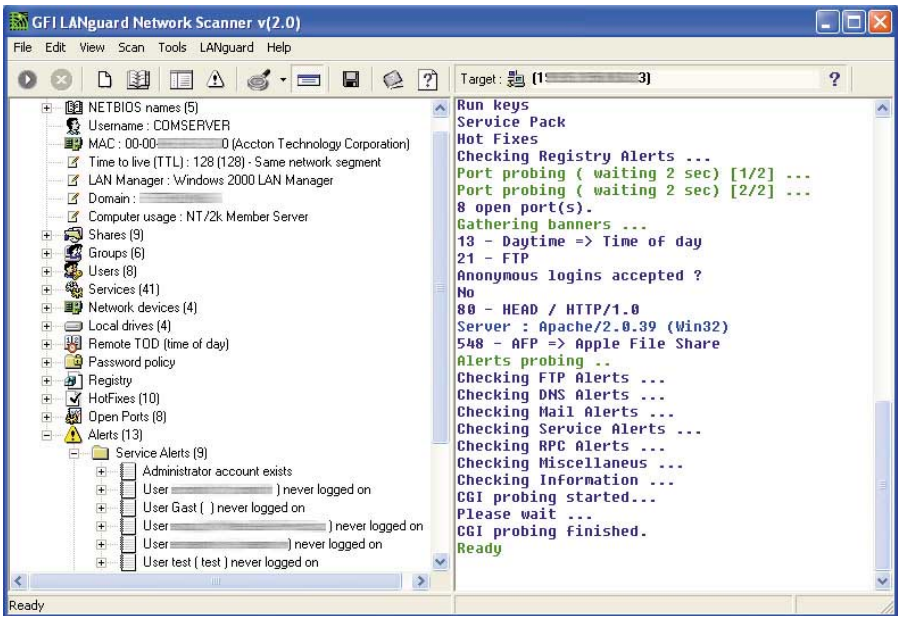
Professioneller Systemschutz durch Hilfsmittel

Der bombensichere PC

Bei jeder Internet-Sitzung geben Sie eine Reihe persönlicher Infos preis, die Angreifer für Attacken nutzen können. Das muss nicht sein – Sie können sich auch unerkannt im Web bewegen.

▸Ob Ihr PC von einem Dateivirus, einem lästigen Mailwurm oder einem Spionageprogramm befallen ist oder nicht, können Sie ohne entsprechende Software kaum feststellen. Oft merken Sie es nur, wenn der Eindringling gerade seinen heimtückischen Auftrag erfüllt – dann ist es aber meistens schon zu spät.

Der erste Schritt zu mehr Sicherheit: Hinterfragen Sie Ihre Surfgewohnheiten, kontrollieren Sie Ihre Systemkonfiguration, und überdenken Sie die Zugangskontrollen zu Ihrem Rechner. Bei der Absicherung von Windows helfen spezielle Security-Utilities, mit denen Sie die Netzaktivitäten des Betriebssystems schützen und Gefahren von Ihrem PC fernhalten. Die hier vorgestellten Hilfsprogramme und Dienste bieten verschiedene Varianten, den individuellen Schutzgrad Ihres Rechners gegen Schadprogramme zu erhöhen.



Systematischer Check: Der Languard Network Scanner sucht nach potenziellen Sicherheitslücken auf Rechnern im Netzwerk, damit Sie Sicherheitslecks schließen können

Lokale Windows-Sicherheit kontrollieren

Viele kleine Sicherheitsschwächen oder für Dritte nutzbare, aber nicht vorgesehene Zugangsmöglichkeiten zu Ihrem PC fallen den Programmierern von Betriebssystemen gar nicht auf, weil sich viele Lücken erst im täglichen Betrieb offenbaren. Dem Internet sei dank, werden diese Lücken sehr schnell veröffentlicht und die Software-Hersteller können mit kleinen Programm-Updates reagieren, die diese Sicherheitslücken alsbald schließen. Das ist besonders bei schwerwiegenden Sicherheitslecks wichtig, weil Saboteure ansonsten diese Lücken nutzen können, um Ihren PC lahm zu legen. Doch was tun, wenn Sie überhaupt nicht sicher sind, ob auf Ihrem PC eine Sicherheitslücke vorhanden ist? Erste Hilfe bei der Kontrolle der eigenen Integrität bieten Sicherheits-Scanner.

Languard Network Scanner 2.0

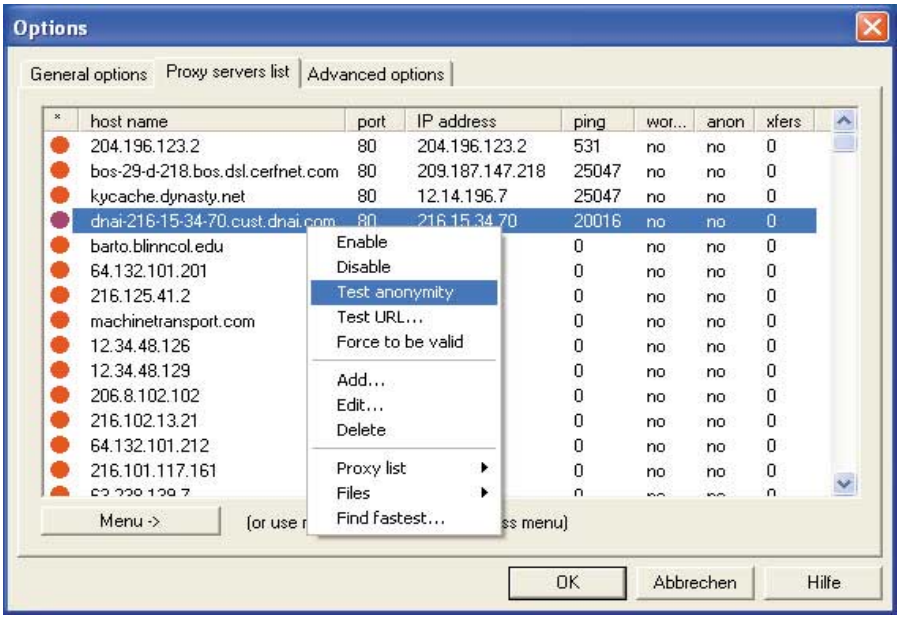
Der Languard Network Security Scanner 2.0 von GFI (6,3 MB, Download unter **www.gfisoftware.com**) durchsucht das lokale Netz nach vorhandenen PCs und untersucht die gefundenen Arbeitsstationen auf bekannte Sicherheitslücken und Falschkonfigurationen. Das funktioniert auch auf Einzelplatz-PCs, die mit TCP/IP arbeiten, was bei PCs mit Internet-Anschluss fast immer der Fall ist. Dabei greift die englischsprachige Software auf eine umfangreiche Datenbank bekannter Schwachstellen zurück. Die Software läuft auf PCs mit Windows 95/98/ME, NT 4 und XP, durchleuchtet über das Netzwerk aber auch Rechner mit anderen Betriebssystemen wie Apple Mac-OS oder Linux. Sogar Router und Switches mit eigener IP-Adresse werden überprüft.

Bei der Durchführung der Sicherheitstests scannt Languard das Netz stationsweise und liefert unzählige Informationen über mögliche Sicherheitsrisiken der kontrollierten Stationen. In der Auflistung der Resultate finden sich Netbios-Daten, detaillierte Angaben über freigegebene Laufwerke, Host- und Benutzernamen, MAC-Adressen vorhandener Netzwerkadapter, unsichere Passwörter auf Windows-95- und -98-Arbeitsstationen und vieles andere mehr.

Info: Schutz-Tools

Das Angebot an Datenschutz-Tools und -diensten im Internet ist riesig, doch Klasse geht hier vor Masse. Viele der angebotenen Hilfsprogramme funktionieren nicht richtig. Wir stellen Ihnen Helfer vor, die uns überzeugt haben.

Eine Überprüfung der eigenen PC-Sicherheit mit Languard ist deshalb besonders empfehlenswert, da ein Großteil der Online-Angriffe über aus Unachtsamkeit offen gelassene Ports erfolgt, die bei der Installation von Programmen freigeschalten wurden. Der Sicherheits-Scanner überprüft Windows-PCs dazu auf bekannte Verwundbarkeiten und versucht, Schwächen in Bereichen wie HTTP-, FTP- und SMTP-Dienste zu erkennen. Weitere Sicherheitstests erfolgen anhand einer Sammlung allgemein verbreiteter Passwörter und ICMP-Nachrichten (Echo, Timestamp und Information Requests).



Wechselnde Adressen: Mit Utilities wie Multiproxy surfen Sie unter ständig wechselnden IP-Adressen und verwirren so die Protokoll-Software, die auf vielen Websites vorhanden ist

Die Sicherheitsprüfung zeigt gravierende Lücken auf

Nach dem Programmstart und der Eingabe des gewünschten Prüfbereichs sehen Sie die in Ihrem Netzwerk vorhandenen Stationen als Baumansicht in der linken Fensterhälfte des Network Scanners. Rechts daneben zeigt die Software den Fortschritt der momentanen Sicherheitsprüfung an. Alle gesammelten Angaben zu den Arbeitsstationen sowie Informationen über potenzielle Sicherheitsmängel fügt Languard in die Baumstruktur ein. Sobald der Scan abgeschlossen ist, sollten Sie sich an die Analyse der Resultate machen. Dazu klicken Sie sich durch die Baumansicht, sichten die vom Scanner ermittelten Löcher und korrigieren die Konfiguration der betroffenen Arbeitsstationen im Netz. Ein erneuter Scan-Durchlauf zeigt die Wirksamkeit der getroffenen Sicherungsmaßnahmen.

Das Security-Programm ist in einer zur reinen Privatnutzung kostenfreien Version sowie einer kommerziellen Ausgabe zum Preis von 99 US-Dollar erhältlich.

In geheimer Mission: Unerkannt unterwegs mit Anonet

Das deutschsprachige Gratis-Tool Anonet 1.07 (493 KB, für Win 95/98/ME, NT 4, 2000 und XP, Download unter **www.onlinetimer.de** oder ◉ auf Heft-CD) sorgt für Anonymität Ihres Browsers beim Surfen und damit auch Ihrer eigenen Person gegenüber den Servern, die Sie besuchen. Dies geschieht über die Codierung von Internet-Adressen über Online-Proxy-Dienste, so dass alle Informationen, die Rückschlüsse auf Sie zulassen, herausgefiltert werden.

Software installieren

Die Installation verläuft ohne Besonderheiten. Sie müssen nur das gewünschte Zielverzeichnis angeben. Das Setup richtet einen zusätzlichen Start-Menüeintrag für einen „Netiquette-Guide“ mit Verhaltensregeln für das Internet ein.

Serverliste aktualisieren

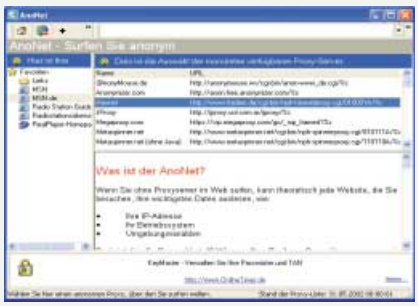
Der erste Schritt nach dem Programmstart besteht darin, die vorgegebenen Proxies über das Internet zu aktualisieren. Das Datum der letzten Aktualisierung der Proxy-Liste zeigt Anonet in einer Statuszeile am unteren Fensterrand an. Am oberen Fensterrand befindet sich eine Symbolleiste, über die Sie die wichtigsten Programmfunktionen steuern. Klicken Sie zur Aktualisierung auf das zweite Icon von links (Weltkugel mit abgehendem Pfeil). Nach einem Hinweis, den Sie mit einem Mausklick bestätigen müssen, holt sich Anonet eine aktuelle Liste frei zugänglicher Proxy-Server. Die Übertragung dauert nur wenige Sekunden.

Geschützt browsen

Sobald die Aktualisierung der Proxy-Dienste abgeschlossen ist, zeigt die Software die verfügbaren Server in der rechten Fensterhälfte an. Um einen Server auszuwählen, markieren Sie ihn. Anschließend geben Sie die gewünschte Adresse, die Sie anonym ansurfen möchten, in das Eingabefeld innerhalb der Symbolleiste ein und drücken die ‹Return›-Taste oder klicken auf den grünen Pfeil daneben. Anschließend öffnet Anonet Ihren Standard-Browser, beispielsweise den Internet Explorer, mit der gewählten Adresse. Abhängig von der Geschwindigkeit des Proxy-Servers treten beim Surfen auf der Website gelegentliche Verzögerungen auf.

Anonymität überprüfen

Um sicherzugehen, dass Sie auch tatsächlich unerkannt unterwegs sind, lassen Sie sich Ihre neu zugewiesene IP-Adresse unter **http://privacy.net/analyze/** anzeigen.



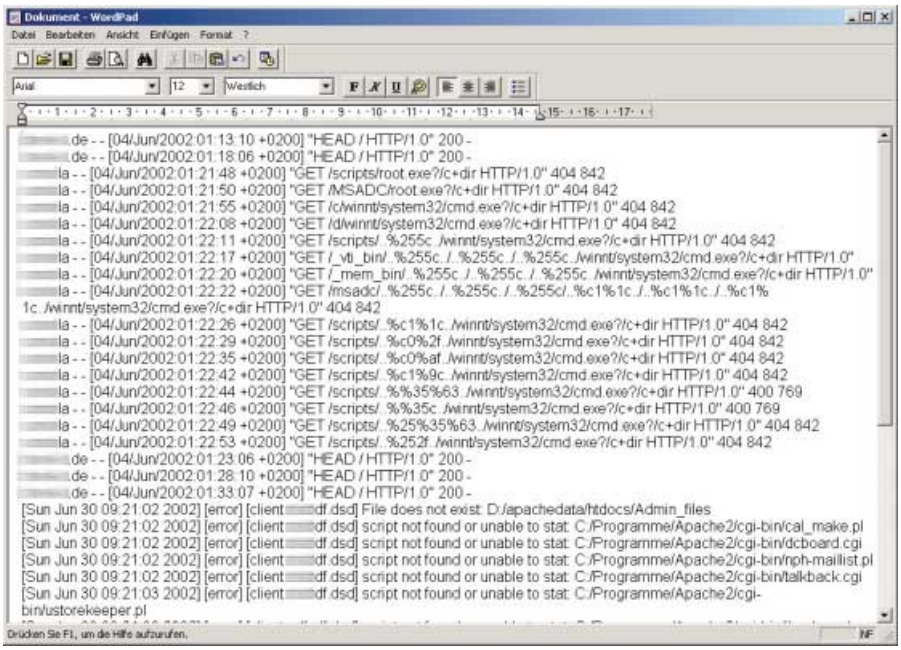
Proxy vorgeschaltet: Trotzdem kann man sich im Internet nicht 100-prozentig sicher fühlen

Letztere beinhaltet eine für Administratoren hilfreiche Funktion zum Vergleich zweier Scanvorgänge. Hierdurch lassen sich Netzwerkveränderungen – beispielsweise neu installierte Dienste, hinzugefügte Anwender oder neue Ports – schnell identifizieren.

Anonym surfen reduziert die Sicherheitsrisiken

Angenommen, Sie ziehen in eine fremde Stadt um. Würden Sie Ihre neue Anschrift jedem anvertrauen, der Ihnen auf der Straße begegnet? Würden Sie jeden zu sich nach Hause einladen, der Ihnen über den Weg läuft? Wohl kaum. Was für die reale Welt abstrus wirkt, ist im Internet jedoch Realität, denn das Netz birgt im Hinblick auf Ihre Privatsphäre große Gefahren. Das Internet ist ein Paradies für professionelle Datenschnüffler, die jeden Surfer zu einem gläsernen Anwender machen wollen und jeden Ihrer Schritte mitprotokollieren. Es liegt aber zum Großteil in Ihrer Hand, wie sicher Ihre persönlichen Daten sind.

Durch den Einsatz spezieller Utilities ist es möglich, Ihre Online-Aktivitäten zu verschleiern und eine Verfolgung Ihrer Surfgewohnheiten erheblich zu erschweren. So kommen Sie im einen Moment augenscheinlich aus England und sind im nächsten Moment für einen Serverbetreiber ein Besucher aus den USA. Dazu ist aber eine Umgewöhnung erforderlich, da das anonyme Surfen bei weitem nicht so komfortabel ist und zudem den Umgang mit Zusatzprogrammen erfordert.



Anonym im Netz: Jeder Besuch im Internet offenbart Ihre IP-Adresse – Web-Anbieter der von Ihnen besuchten Seiten können daraus auf Ihren Standort schließen. Das verhindern Anonymisierungs-Tools

Sobald Sie eine Website besuchen, wird Ihre IP-Adresse im Protokoll des Servers gespeichert, Ihr Aufenthalt somit penibel genau schriftlich festgehalten. Und nicht einmal die bei den meisten Verbindungen über DSL oder ISDN übliche dynamische IP-Vergabe, bei der Ihnen bei jeder Einwahl eine andere, vorübergehende IP-

Online-Sicherheit: Internet-Services bieten Schutz (I)

Haben Sie keine Lust, sich ständig um den Schutz Ihres PCs zu kümmern und wollen Sie dennoch sicher online sein? Dann können Sie auf den neuartigen Online-Schutz Safersurf (**www.safersurf.de**) des Anbieters Nutzwerk (**www.nutzwerk.de**) zurückgreifen. Der Service arbeitet als Proxy-Dienst, und die Einrichtung ist in wenigen Minuten ohne Installation von Software nur durch das Eintragen der Proxy-Server von Safersurf in Mailprogramm und Browser erledigt.

Virenschutz extern: Bevor Mails auf Ihren PC wandern, laufen die Daten über Safersurf

Aus einzelnen Sicherheitsmodulen stellen Sie sich ein Paket zusammen, das auf Ihre individuellen Sicherheitsbedürfnisse zugeschnitten ist. Bezahlt wird monatlich, die Kosten richten sich nach den in Anspruch genommenen Modulen. Zur Auswahl stehen Werbebannerblocker (0,50 Euro), Virenschutz für Internet-Daten (1 Euro), Virenschutz und Anti-Spam für Mails in einem Postfach (2 Euro), 0190-Dialer-Abwehr (1 Euro). Im Angebot sind 300 MB Transfervolumen für Ihre Daten pro Monat enthalten, alle Module zusammen kosten 3,90 Euro im Monat. Jedes zusätzliche Mailpostfach schlägt mit 0,50 Euro zu Buche, 300 MB zusätzliches Transfervolumen kosten 1 Euro. Für DSL-Nutzer gibt es ein Zusatzpaket mit 1 GB Transfervolumen zum Preis von 2 Euro monatlich.

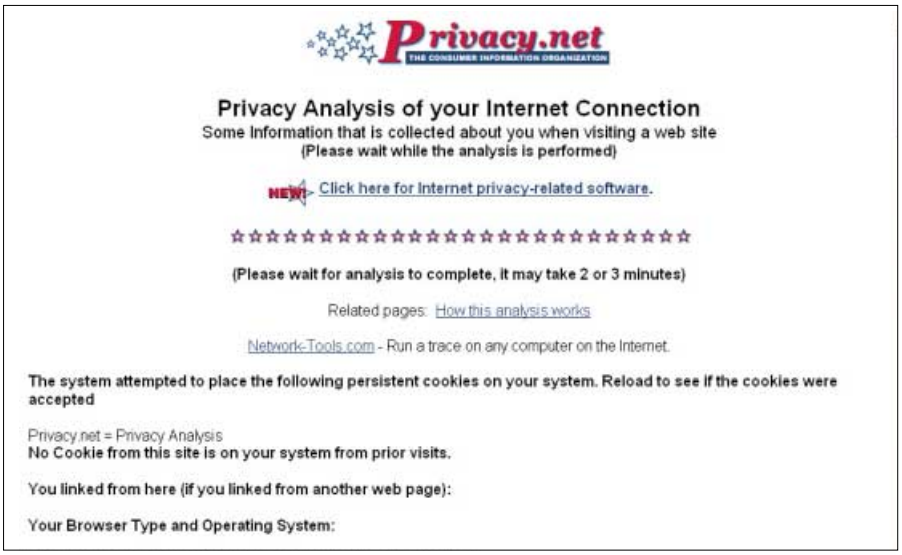
Dabei verlagern Sie die Prüfung der von Ihnen aus dem Internet empfangenen und an das Internet gesendeten Daten zu einem Dienstleister. Dieser verfügt über die erforderliche Hard- und Software sowie das passende Know-how, alle durchlaufenden Daten auf Virenbefall, Trojaner und anderen bösartigen Code zu scannen und kritische Inhalte aus dem Datenstrom auszufiltern, bevor er auf Ihren PC gelangt. Um die Aktualisierung einer Personal Firewall, das Einspielen neuer Virensignaturen oder die Pflege von Spam-Absenderlisten müssen Sie sich nicht mehr kümmern, denn diese Aufgabe erledigt der Service-Anbieter. Allerdings begeben Sie sich damit in die Hände eines Dritten, der Ihre gesamten Daten im Klartext mitlesen kann. Im Hinblick auf die eigene Privatsphäre ist das ein nicht zu unterschätzendes Risiko.

Auch traditionelle Software-Anbieter schwenken um

Auch der durch Virenscanner bekannt gewordene Hersteller McAfee wirbt mit einem

Adresse zugeteilt wird, bietet hier Schutz vor einer Rückverfolgung.

Aus der Verbindung aus Server-Protokolldateien und den Einwahlaufzeichnungen Ihres Providers können zum Beispiel Ermittlungsbehörden Ihre Identität ermitteln und Schritt für Schritt nachvollziehen, welche Seiten Sie besucht haben. Natürlich ist dieser Kreuzvergleich nur bei besonders schweren Vergehen und in der Regel nur nach einer richterlichen Anordnung möglich, doch Sie selbst können ja nicht nachvollziehen, wann und wer Ihre Daten auswertet. Daher sollten Sie die Möglichkeiten kennen, Ihre verräterische IP-Adresse zu tarnen.



Was andere über Sie wissen: Die Online-Sicherheitsanalyse von Privacy.net zeigt Ihnen, welche Informationen Sie beim Surfen durch das Internet nach außen tragen

Anonymity 4 Proxy 2.52

Geht Ihnen dieses Nachspionieren zu sehr in Richtung gläserner Anwender, setzen Sie besser Anonymity 4 Proxy 2.52 (1 MB, Download unter **www.a4proxy.com** oder ◉ auf Heft-CD, Vollversion 35 US-Dollar) als Tarnschild ein. Die englischsprachige Software für Win 95/98/ME, NT 4, 2000 und XP arbeitet als so genannter Proxy-Manager und leitet jeden Request über einen der zahlreichen im Internet beheimateten Proxy-Server um. Auf die meisten dieser Dienste können Sie kostenlos zugreifen – eine Registrierung ist nicht erforderlich. Über das Menü „Options, Language, German" stellen Sie die Bedienerführung auf Deutsch um.

Steganos Internet Anonym 2.05

Auch die Steganos-Software wendet sich an Internet-Nutzer, die nicht länger persönliche Informationen auf Webservern hinterlassen möchten, die sie besucht haben. Wie Anonymity 4 Proxy greift Steganos Internet Anonym 2.05 für Win 95/98/ME, NT 4, 2000 und XP (2,2 MB, Download unter **www.steganos.de** oder ◉ auf Heft-CD, Registriergebühr: 25 Euro) auf im Internet frei verfügbare Anonymisierungsdienste in Form von Proxy-Servern zurück, um Ihre Privatsphäre zu schützen und für Anonymität zu sorgen.

Ihre eigene IP-Adresse bleibt den Betreibern von Websites verborgen, denn

Online-Sicherheit: Internet-Services bieten Schutz (II)

Online-Schutzpaket um die Gunst der Anwender. Über die Adresse **www.mcafee.com** gelangen Sie zum Sicherheitsdienst McAfee Security Center, das einen Sicherheitsindex und ein Echtzeit-Sicherheitsbenachrichtigungssystem enthält. McAfee.com ist ein reiner ASP-Anbieter, die Software arbeitet also ausschließlich über das Internet und ist im Gegensatz zu herkömmlichen McAfee-Produkten nicht auf CD erhältlich.

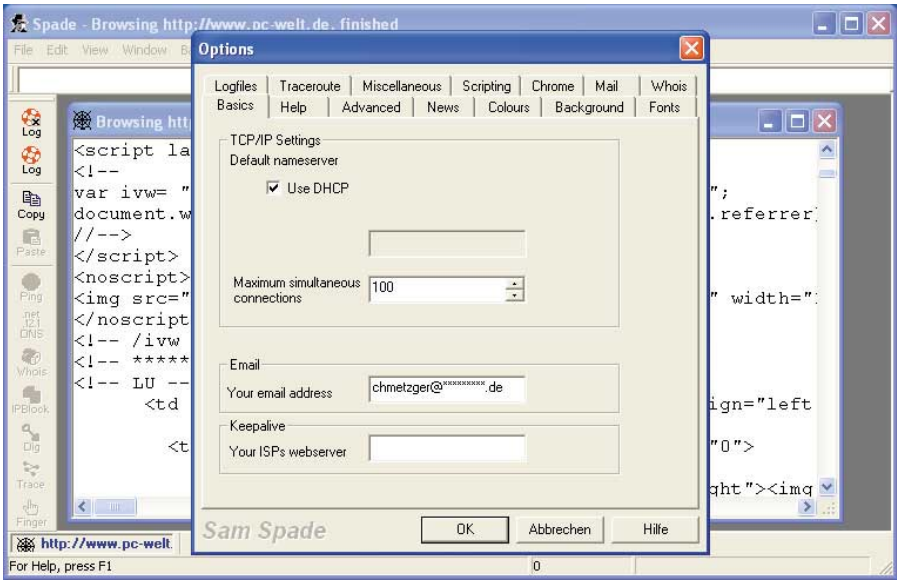
Die Dienste ermitteln Internet-basierte Sicherheitslücken auf Ihrem PC und benachrichtigen Sie, falls eine Schwachstelle gefunden wurde. Der Index bewertet mit Werten von 0 (einige Sicherheitslücken vorhanden) bis 10 (hoher Schutz) die Risiken, mögliches Opfer einer Hackerattacke zu werden. Anschließend erhalten Sie Ratschläge, wie Sie sich mit dem Online-Virenschutzsystem Virusscan Online, Personal Firewall und Privacy Service schützen. Um die Dienste zu nutzen, müssen Sie ein Abonnement für ein Jahr (33,95 Euro je Dienst) oder zwei Jahre (57,95 Euro je Dienst) abschließen, das alle Updates enthält. Virusscan Online schützt Ihren PC vor Viren- und Wurmbefall, die Personal Firewall bildet eine Durchgangskontrolle zwischen dem Internet und Ihrem PC, und der Privacy Service filtert Inhalte. Damit kontrollieren Eltern den Internet-Zugriff nach Altersstufen und blockieren Websites mit jugendgefährdenden Inhalten.

Mit Gnutella-Technik geht die Filter-Software von Spamnet (**www.cloudmark.com/products/spamnet/**) gegen unerwünschte Werbezusendungen per Mail vor. Das kostenlose Outlook-Plug-in für Outlook 2000 und XP ordnet jeder vom Benutzer als Spam identifizierten und in einen speziellen Ordner verschobenen Nachricht eine eindeutige ID zu und veröffentlicht diese in einem Online-Katalog. Über die von Napster und Kollegen bekannte Peer-to-Peer-Technik gleichen sich die Datenbanken untereinander automatisch ab und das Outlook-Zusatzprogramm repliziert den Katalog wiederum auf den eigenen PC. Dadurch bleibt Ihr Posteingangsordner von allen Werbebotschaften verschont, die andere Spamnet-Nutzer bereits erhalten haben. Jeder Teilnehmer von Spamnet trägt so ein klein wenig zur Verringerung der Werbeflut per Mail bei.

Noch Beta: Spamnet für Outlook 2000/XP sammelt Adressen von Werbeversendern

Sie erscheinen unter ständig wechselnden Tarnadressen, über die Sie nur mit viel Aufwand identifiziert werden können. Einstellen müssen Sie dazu nichts – das Tool arbeitet automatisch und richtet auch Ihren Browser ein. Sie können die Anonymisierung lediglich an- oder abschalten.

Der Clou: Die Software ändert Ihre IP-Adresse automatisch im Abstand weniger Sekunden und verwirrt damit mögliche Auswertungsprogramme der Gegenstelle. Allerdings können langsame Proxy-Server das Surftempo stark reduzieren. Daher entfernt Steganos Internet Anonym nach einiger Zeit langsame Server aus der internen Serverdatenbank.



Mit Sam Spade das Netz durchsuchen: Mit dem zur Bekämpfung von Werbemail konzipierten Tool sammeln Sie Informationen über Spammer. Die Software bietet einige Internet-Diagnosewerkzeuge

Multiproxy 1.2a

Auch Multiproxy 1.2a hilft beim Verwischen Ihrer Identität und erschwert eine Verfolgung. Das englischsprachige Gratisprogramm für Win 95/98/ME, NT 4, 2000 und XP (170 KB, Download unter **www.multiproxy.org** oder ◉ auf Heft-CD) erleichtert die Suche eines passenden und vor allem schnellen Proxy-Dienstes. Dazu testet die Software eine Liste mit über 100 vorgegebenen Proxies auf Verfügbarkeit, Geschwindigkeit und Anonymität. Proxy-Server, die keine ausreichende Anonymisierung erzielen, schließt das Tool aus. Die Proxy-Datenbank können Sie bei Bedarf online aktualisieren und in der neuesten Fassung direkt auf der Website **www.multiproxy.org** einsehen.

Damit die Anfragen Ihres Browsers von Multiproxy zu einem Proxy-Dienst umgeleitet werden, müssen Sie in Ihrem Webbrowser die Proxy-Adresse „127.0.0.1:8088“ eintragen. Anschließend kümmert sich Multiproxy um die Auswahl eines passenden Servers und den automatischen Wechsel des Proxy-Dienstes in regelmäßigen Abständen. Offiziell erhalten Sie dann die Identität des jeweils aktiven Proxy-Servers. Auf der Website

Zusätzliche Mailadresse: Mit Postfächern arbeiten

Die Zeit der anonymen Mailanbieter ist vorbei. Seriöse Dienstleister wie Web.de Freemail, GMX oder E-Post verlangen bei der Anmeldung persönliche Angaben wie Name, Anschrift und Geburtsdatum, die anschließend auch überprüft werden. Erst nach einem positiven Check wird ein neues Postfach in vollem Umfang aktiviert. Anders verhält es sich bei verschiedenen im amerikanischen und asiatischen Raum angesiedelten Maildienstleistern. Hier können Sie in der Regel falsche Angaben machen. Bei kostenpflichtigen Diensten benötigen Sie lediglich eine Kreditkarte. Eine Verifizierung Ihrer Angaben findet nur zur Zahlungsabwicklung statt, weitere Kontaktdaten gibt der Betreiber Dritten in der Regel nicht preis. Anonym sind Sie dadurch jedoch auch nicht, denn über Ihre Kreditkartennummer ist ein Rückschluss möglich.

Trotzdem leisten reine Mail-Provider gute Dienste, denn damit haben Sie es in der Hand, wem Sie im Internet welche Ihrer Kontaktadressen preisgeben. Das ist besonders für Registrierformulare auf Internet-Seiten wichtig, wenn Sie Spam-Mails unterbinden möchten.

Anbieter	Hotmail	GMX	E-Post	Web.de
Adresse	www.hotmail.com	www.gmx.de	www.epost.de	www.freemail.de
Mailadresse	name@hotmail.com	name@gmx.de	name@epost.de	name@web.de
Anmeldungsprozedur	schnell	recht schnell	schnell	schnell
POP3/IMAP/WAP	ja/nein/nein	ja/ja/ja	ja/nein/ja	ja/ja/ja
Sicherheit	dreistufig einstellbar	dreistufig einstellbar	Verschlüsselung	digitale Unterschrift und Verschlüsselung
Adressbuch	ja	ja	ja	ja
Mitgliederverzeichnis	ja	ja	nein	nein
Mailverwaltung	ja	ja	ja	ja
Filterfunktionen	ja	ja	ja	ja
Speicherplatz	2 MB	10 MB	9 MB	8 MB
Sonstiges	Signaturen, Abfrage anderer POP3-Konten, Posteingangsschutz	Signaturen, Mailweiterleitung, Urlaubsbenachrichtigung, Ausschlusslisten, Senden von SMS	Abfrage anderer POP3-Konten, Urlaubsbenachrichtigung	Unified Messaging Services, Mailinglisten, Urlaubsbenachrichtigung, Abfrage anderer POP3-Konten

von Multiproxy steht unter dem Menüpunkt „Anonymity Checker“ ein Online-Test zur Anzeige Ihrer aktuellen IP-Adresse bereit.

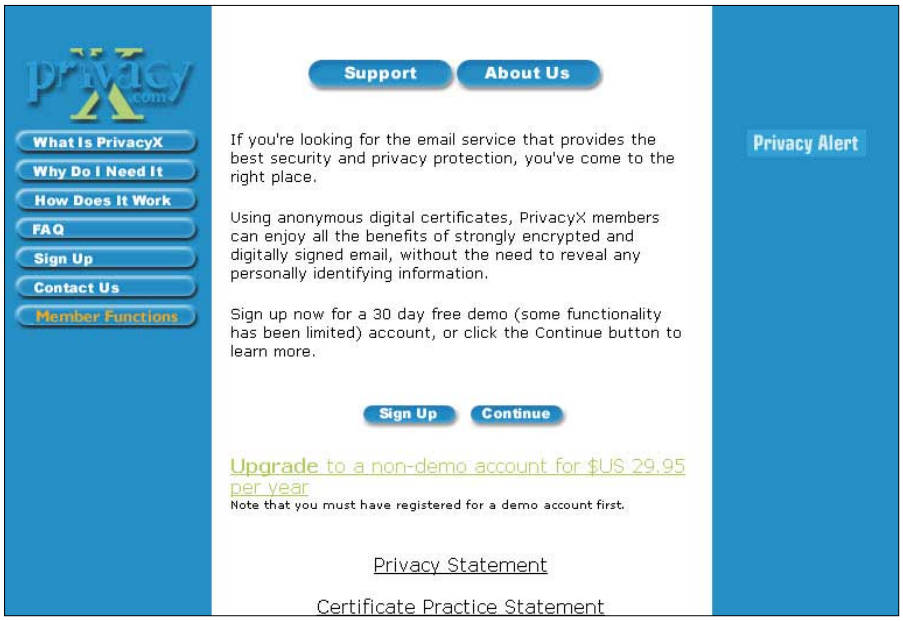
Online-Check: Was Anbieter im Netz von Ihnen sehen

Wollen Sie wissen, was fremde Server so alles aus Ihrem PC auslesen können, führen Sie einen Online-Test durch. Informationen zu den Daten, die während eines Besuchs auf einer Web-Seite weitergegeben werden können, gibt Ihnen der englischsprachige Sicherheits-Check Privacy.net (**http://privacy.net/analyze/**). Angefangen von Systeminfos (Prozessortyp, Auflösung, installiert Plug-ins), über Sicherheitseinstellungen Ihres Browsers und aktueller IP-Adresse bis hin zur Information, von welcher Web-Seite Sie gekommen sind (so genannter Referrer) – alles ist für Dritte sicht- und speicherbar.

Weiter geht der deutschsprachige Test von Logosec (**www.logosec.de/userinfo.htm**). Neben der Anzeige verschiedener Systemeinstellungen versendet die Website zu Demozwecken auch zufällig generierte Benutzerdaten per Mail an den Betreiber der Seite. Dazu müssen Sie lediglich einen Button drücken, um ein unsichtbares Formular zu starten – schon geht die Nachricht einschließlich Ihrer Mailadresse und Ihres Namens auf die Reise. So eine Routine kann theoretisch ganz unscheinbar hinter einer Schaltfläche auf einer Website platziert werden und beim Anklicken Ihre Identität preisgeben. Kommerzielle Werbeanbieter nutzen diese und weitaus raffiniertere Verfahren, um an Ihre Kontaktdaten zu kommen und Ihnen ungefragt Werbung zukommen zu lassen.

Informationen über Angreifer sammeln

Angriffe in einem TCP/IP-basierten Netz wie dem Internet müssen grundsätzlich unter einer bestimmten IP-Adresse erfolgen. Zwar betreiben erfahrene Hacker einigen Aufwand, ihre echte IP-Adresse vor Ihnen zu verbergen, dennoch ist es einen Versucht wert, bei Bedarf mehr Informationen über eine bestimmte Adresse oder Domäne herauszufinden. Dazu setzen Sie ein so genanntes Whois-Tool ein, das die im Internet verfügbaren Betreiber- und



E-Mail-Tarnkappe: Der Anbieter Privacy-X ermöglicht den Versand von Nachrichten ohne direkte Rückschlussmöglichkeit auf den Absender. Wirklich anonym sind Sie aber nicht

Kontaktinfos auflistet. Zwar sind über den Browser auch manuelle Whois-Abfragen möglich, allerdings müssen Sie dazu wissen, bei welchem Whois-Server Sie für welchen Adressbereich anfragen müssen. Außerdem benötigen Sie mehrere Abfragen, um alle Details zu einer IP-Adresse oder Domäne zu bekommen.

Sam Spade 1.14

Diese Nachteile vermeidet die englischsprachige Freeware Sam Spade 1.14 für Win 95/98/ME, NT 4, 2000 und XP (1 MB, Download unter **www.samspade.org** oder ◉ auf Heft-CD). Das Utility sucht sich nicht nur automatisch den richtigen Whois-Server heraus, sondern sammelt auch gleich alle relevanten Infos. So startet es etwa eine gruppenweise Whois-Abfrage für einen IP-Adressblock.

Darüber hinaus bietet Sam Spade eine Reihe weiterer Internet-Diagnosewerkzeuge, darunter Ping und Traceroute zur Auflistung zwischengeschalteter Internet-Stationen, Nslookup und Dig für DNS-Abfragen sowie Finger für Benutzeranfragen. Über eine am linken Fensterrand positionierte Symbolleiste wählen Sie die angebotenen Funktionen aus und öffnen ein Fenster zur Anzeige der Resultate.

Christoph Metzger

Mit SSL verschlüsselt mailen: Maildienste wie Freenet bieten weitreichende Möglichkeiten zum Abruf von Nachrichten aus anderen Postfächern und zur Weiterleitung

Schnüffelprogramme und Aktivitätsmonitore bekämpfen

Großer Lauschangriff

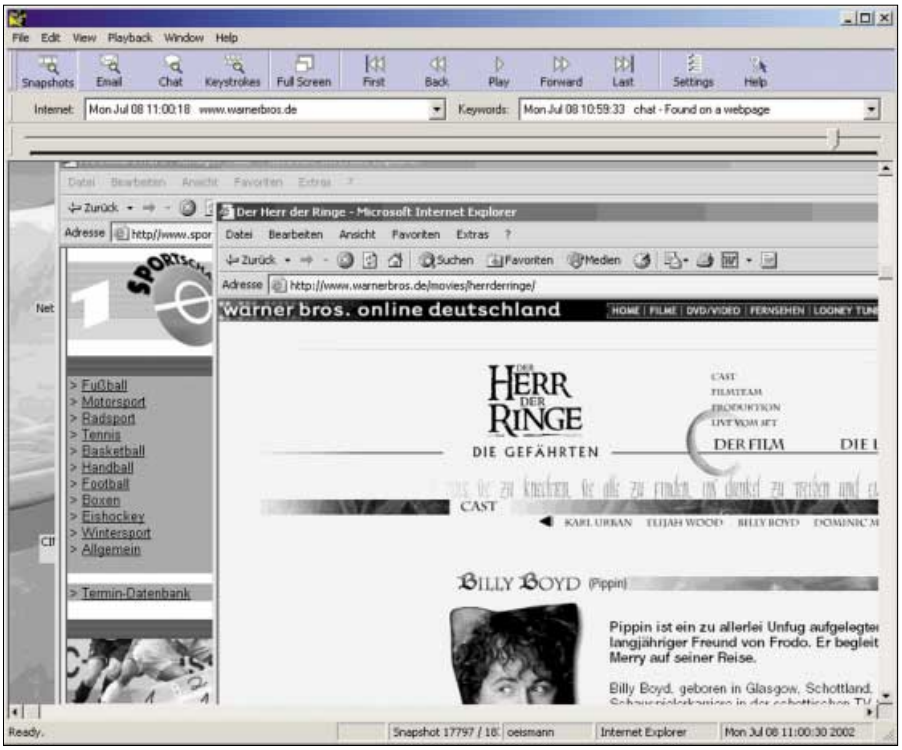
Wird Ihnen heimlich eine Überwachungs-Software untergeschoben, können Neugierige jeden Ihrer Arbeitsschritte genau nachvollziehen. Wir sagen Ihnen, wie Sie sich dagegen schützen.

▸Tastaturschnüffler – auch Keylogger genannt – gehören zu jener Gruppe kleiner System-Tools, die sich unbemerkt in Ihr Betriebssystem einnisten und fortan jede Ihrer Aktivitäten am PC beobachten und fein säuberlich in einer Protokolldatei mitschreiben. Dabei spielt es keine Rolle, ob Sie gerade einen Brief in Word tippen, Homebanking erledigen, im Internet surfen oder ein paar Zahlen in einem Tabellenprogramm berechnen – das Schnüffelprogramm sieht alles und registriert sämtliche Tastaturanschläge. Aus der Welt der Geheimdienste entsprungen, sind Bespitzelungsprogramme mittlerweile für jedermann erhältlich, einige der Programme werden sogar in Deutschland entwickelt.

Die Wächterprogramme laufen unbemerkt im Hintergrund und speichern regelmäßig detaillierte Berichte über alle PC-Aktivitäten oder versenden diese per Mail oder über eine direkte TCP/IP-Verbindung. Besonders tückisch: Nach der Installation arbeiten Keylogger selbständig und spähen Daten aus. Über Einträge im Autostart-Ordner, in der Datei WIN.INI und in der Registry sorgen Keylogger für ihre automatische Ausführung beim Systemstart. Einmal installiert, führen sie ihre Tätigkeit vollautomatisch und ohne weitere Benutzereingriffe durch. Dabei tarnen sich die Programme so geschickt, dass sie kaum zu identifizieren sind.

Info: Keylogger

Keylogger sind Programme zur Überwachung und Protokollierung aller Computeraktivitäten. Die Programme können Sie völlig unsichtbar ausspionieren, ohne die Arbeit zu stören. Grund genug, diese Tools von Ihrem PC zu verbannen.



PC-Privatnutzung im Visier: Mit spezieller Überwachungs-Software spähen Unternehmen ihre Arbeitnehmer aus und bringen – teilweise unerlaubt – in Erfahrung, wie viel Zeit wofür benötigt wurde

Protokoll-Software spioniert Sie systematisch aus

Einen Schritt weiter gehen Backdoors, die nicht nur ein Protokoll aller Tastatureingaben erstellen und sämtliche Anwenderaktionen aufzeichnen, sondern darüber hinaus auch einen Fernzugriff von außen erlauben. Die Aufzeichnung umfasst alle PC- und Internet-Aktivitäten und arbeitet textbasiert durch das Extrahieren aller auf dem Desktop vorhandenen Textinformationen oder grafisch wie ein herkömmlicher Videorecorder. Das Nutzerprotokoll umfasst Angaben über geöffnete Anwendungen, besuchte Web-Seiten, Chatunterhaltungen, Tastenanschläge, geladene Bilder, Mails und Computerspiele. Sogar eine vollständige Fernsteuerung des Rechners ist mitunter vorgesehen. Aufgrund ihrer Funktionsweise sind diese Programme ein heimtückisches Werkzeug zur Informationsbeschaffung durch Bespitzelung.

Neben Aufnahmen des Monitors bieten Spionageprogramme der aktuellen Generation einen Recorder für die auf Internet-Seiten eingegebenen Formulardaten, eine Benutzerverwaltung, die die Protokollierung gezielt bei bestimmten Anwendern aktiviert, sowie eine Pausenfunktion zur automatischen Unterbrechung und Wiederaufnahme der Aufnahme. Über die Erkennung von Schlüsselwörtern und eine daran gekoppelte Alarmfunktion verschicken Schnüffelprogramme unbemerkt Kurzmitteilungen, falls der Anwender eine Seite

aufruft oder ein Dokument bearbeitet, das einen bestimmten Begriff enthält. Dadurch kann der Angreifer unbemerkt einschreiten, beispielsweise durch einen Online-Fernzugriff auf den PC.

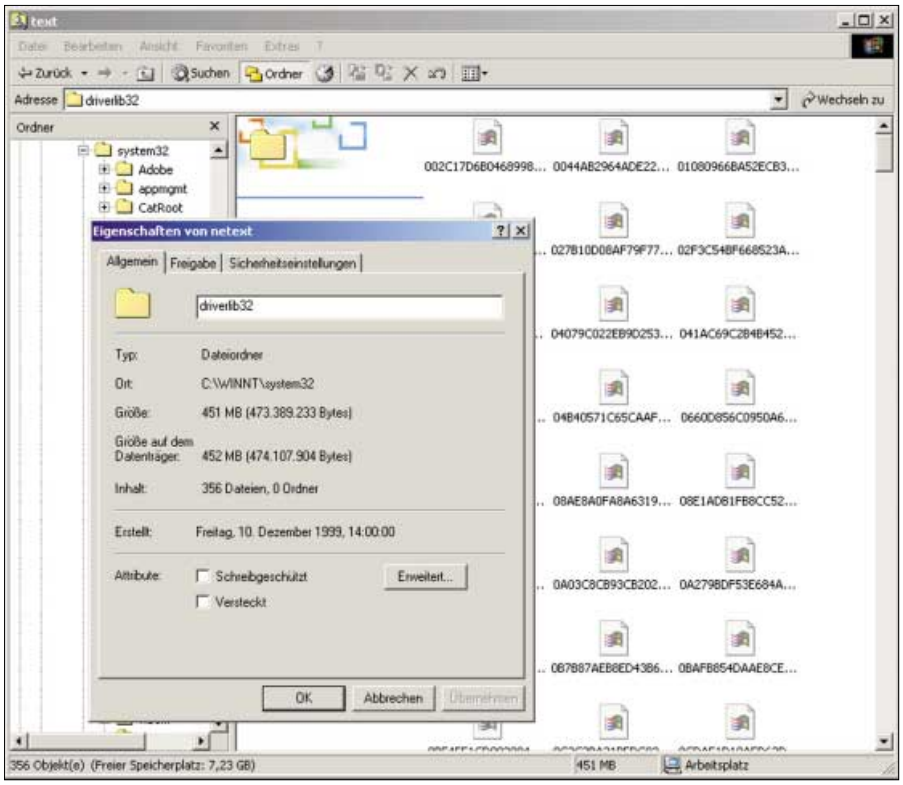
Gratwanderung zwischen Risiko und Nutzen

Es existiert aber auch eine Reihe sinnvoller Einsatzmöglichkeiten für Schnüffel-Software. So stellen Sie mit Hilfe einer Überwachungs-Software etwa fest, wer Ihren PC in Ihrer Abwesenheit benutzt hat und auf welche Dateien zugegriffen wurde. Die Aufdeckung von Computermissbrauch in Unternehmen ist ein weiteres Szenario für Protokollprogramme, um etwa Wirtschaftsspionage oder Mobbing zu entlarven. Im Fortbildungsbereich lassen sich Benutzer beaufsichtigen und deren Kenntnisse gezielt verbessern. Eltern haben mit Aktivitätsmonitoren eine Kontrolle über den PC-Gebrauch ihrer Kinder.

Betrachtet man die von Keyloggern eingesetzten Mechanismen zur Tarnung und Spionage von Benutzerdaten, zeigt sich eine starke Ähnlichkeit mit herkömmlichen Trojanern. So verwundert es kaum, dass sich unter den in den vergangenen Monaten neu aufgetretenen Trojanern auch Eindringlinge wie der Mailwurm „Bad Trans“ befinden, die als klassische Keylogger arbeiten.

So erkennen und beseitigen Sie Schnüffel-Software

Wer sich nicht sicher ist, ob möglicherweise Keylogger, Fernsteuerungs-Tools oder Protokoll-Software auf dem eigenen Rechner aktiv sind, sollte sein System genau inspizieren. Hinweise zum generellen Schutz vor Viren und Würmern finden Sie ab ▷ Seite 78. Die in diesem Beitrag vorgestellten Tipps & Tricks gelten auch für die Vorbeugung vor Keyloggern. Erster Ansatzpunkt sind die zahlreichen Bildschirmfotos und Protokolldateien, die irgendwo auf der Festplatte abgelegt werden müssen und eine beachtliche Größe annehmen können. Bei einer Bildschirmauflösung von 1280 x 1024 Punkten kommen bei einem Screenshot alle 15 Sekunden abhängig von der verwendeten Komprimierung schnell zwischen 450 und 700 MB an Daten zusammen. Häufig muss als Speicherort das Windows-Verzeichnis herhalten, denn dort befinden sich unzählige Dateien und Ordner mit nichts sagenden Dateinamen. Suchen Sie daher nach Dateien und Ordnern, die besonders viele Dateien ähnlicher Größe aufweisen und deren Namen eine Regelmäßigkeit erkennen lassen.



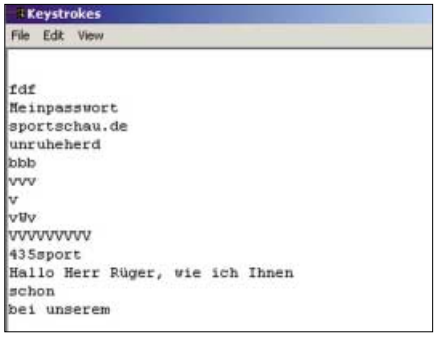
Als Systemdatei getarnt: Bei den in diesem Ordner abgelegten Dateien (rund 450 MB) scheint es sich um Treiber zu handeln – es sind jedoch die verschleierten Protokolle des Schnüffel-Tools Spector

Autostart unterbinden durch Startup-Kontrolle

Damit der Spionagemonitor beim Systemstart aktiv wird, muss dieser dafür sorgen, dass der Monitor beim Hochfahren automatisch geladen wird. Ein Start über den Autostart-Ordner ist in den seltensten Fällen wahrscheinlich – er wäre zu leicht von Ihnen zu entdecken. Einige der Überwachungsprogramme erzeugen zum Start einen Registry-Eintrag im Schlüssel „Hkey_Local_Machine/Software/Microsoft/Windows/CurrentVersion/Run“. Ein hilfreiches Tool zum Überprüfen Ihrer Autostart-Programme ohne mühsame Suche in der Registry ist die englischsprachige Freeware Startup Manager 1.5.2.25 (613 KB, **www.freewarenetz.de**) für Windows 95/98/ME, NT 4, 2000 und XP. Damit können Sie unerwünschte Einträge vorübergehend deaktivieren oder löschen. Trojaner und Schnüffelprogramme sind in der Regel besonders hartnäckig und kontrollieren die Autostart-Einstellungen bei jedem Programmlauf.

Verdeckte Hintergrundprozesse aufdecken

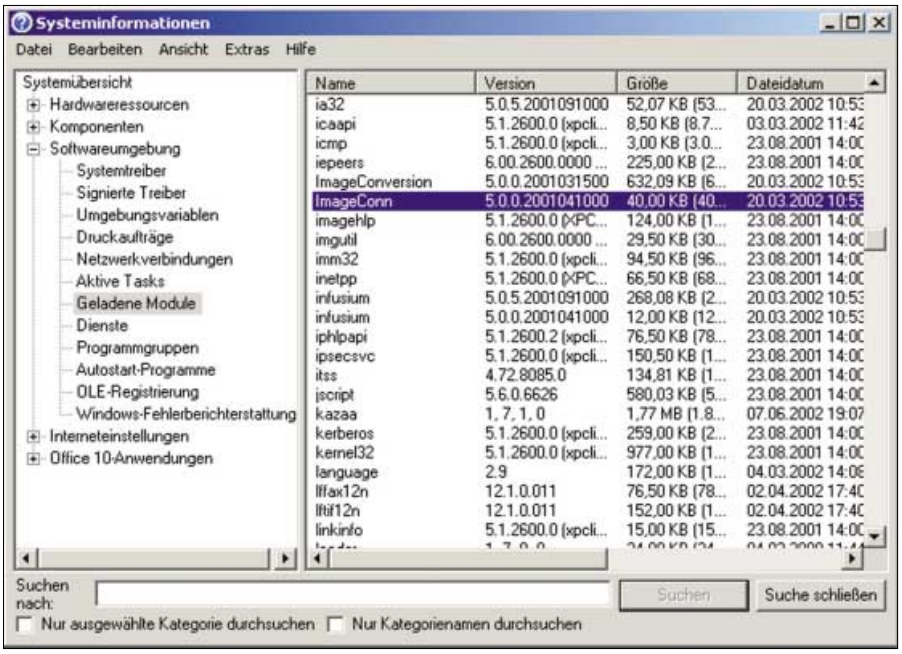
Schnüffelprogramme laufen mit wenigen Ausnahmen als Hintergrundprozess, den Sie mit Hilfe eines erweiterten Taskmanagers aufspüren können. Mit dem Taskmanager von Windows kommen Sie hier nicht weiter, denn einige der Spione schleichen sich an ihm vorbei. Besser verwenden Sie das englischsprachige Tool DLL-Show 2000 4.9 (147 KB, **www.gregory**



Ordentlich vermerkt: Spector späht die Adressen aufgerufener Internet-Seiten aus und führt Listen

braun.com und ◉ auf Heft-CD, Registriergebühr: 25 US-Dollar), das auch solche Prozesse anzeigt, die der Windows-Taskmanager nicht auflistet. Spionage-Software, die als Systemtreiber läuft, können Sie allerdings auch mit DLL-Show nicht aufspüren.

Ein weiterer Ansatzpunkt bei der Suche sind Software-Module, die während der Überwachung geladen werden. Im Startmenü unter „Programme, Zubehör, Systemprogramme“ finden Sie das Utility „Systeminformationen“. Wenn Sie hier unter „Softwareumgebung, Geladene 32-Bit Module“ nachsehen, können Sie auch die von der Kontroll-Software genutzten DLL-Dateien erkennen. Neuere Lauschprogramme mit Tarnkappenfunktion (Stealth-Modus) sind jedoch mit keiner der beiden Methoden auffindbar.



Im Überblick: Die Systeminformationen von Windows leisten bei der Identifizierung von Schnüffelprogrammen anhand der verwendeten Bibliotheksdateien gute Dienste

Kommunikation unterbrechen durch Desktop Firewalls

Zur Erkennung von Keyloggern und Protokoll-Software, die Daten über das Netzwerk verschicken, eignen sich auch Desktop Firewalls. Firewalls bieten zwar keinen generellen Schutz davor, dass Sie sich ein bösartiges Programm einfangen, blockieren aber die Kommunikationswege. Dieser Schutz greift auch dann, wenn

Big Brother: Diese Protokoll-Software kann jedermann erwerben

Überwachungs-Tools gibt es in vielen Variationen. Angeboten wird sogar externe Zusatz-Hardware in Form eines Miniatursteckers (Hersteller Key Ghost, **www.keyghost.com**), der unauffällig zwischen Tastaturkabel und PS/2-Tastaturanschluss platziert wird und alle Tastenanschläge in einen nichtflüchtigen Speicher schreibt. Standard bei der PC- und Internet-Überwachung ist jedoch Zusatz-Software. Wir geben einen Überblick über die wichtigsten Vertreter, damit Sie sich ein Bild vom Einsatzzweck wie auch vom möglichen Missbrauch der einzelnen Tools machen können.

Spector Pro 3.1

Wie eine Kamera macht Spector (**www.spectorsoft.de**) Aufnahmen von dem, was der Anwender auf seinem Monitor sieht. Spector kann mehrere Hundert Aufnahmen pro Stunde versteckt auf der Festplatte ablegen. In den Programmoptionen stellt der Administrator ein, wie häufig und detailliert (Farbe oder Schwarzweiß, hohe oder niedrige Qualität) Spector aufnehmen soll. Zum Abspielen blendet das Tool Videorecorder-Bedienelemente ein. Die sofortige Mailbenachrichtigung informiert den Administrator, sobald der PC unbefugt benutzt wird oder wenn zuvor definierte Schlüsselwörter erkannt werden.

Orvell Monitoring 2002

Orvell (**www.orvell.com**) ist mit einer umfangreichen Überwachungstechnik für Bildschirmaufnahmen, Tastenanschläge und Web-Adressen ausgestattet und arbeitet transparent im Hintergrund. Positiv: Als einer der wenigen Observationsmonitore kann Orvell beim Programmstart einen frei wählbaren Warntext ausgeben, etwa „Achtung, die Aktivitäten dieses PCs werden videoüberwacht“. Für die Aufzeichnung von Bildschirminhalten legt Orvell Screenshots in frei wählbaren Zeitabständen an. Der Hersteller gibt als Festplattenspeicherbedarf für ein Bild alle 30 Sekunden rund 25 MB pro Tag an. Sobald die im Programm eingestellte Vorhaltezeit in Tagen erreicht ist, überschreibt die Software die ältesten Aufnahmen. Bei der Angabe des Speicherpfads für die Bildschirmfotos sind auch Netzwerkfreigaben zulässig, um die Bilder zentral abzulegen. Die Wiedergabe der Aufnahmen erfolgt als Zeitrafferfilm, wie dies auch bei herkömmlichen Videoüberwachungskameras üblich ist.

Visual Time Analyzer 1.3

Um sich von reiner Überwachungs-Software abzuheben, verzichtet Visual Time Analyzer (**www.neuber.com**) auf die Aufzeichnung von Tastaturanschlägen und Passwörtern – Web-Adressen werden notiert. Die PC-Protokollierung erfasst jedoch minutengenau, wann welche Programme verwendet werden und erzeugt eine statistische Auswertung für beliebige Zeiträume.

Orvell Monitoring 2002: Protokoll-Software mit umfangreichen Funktionen

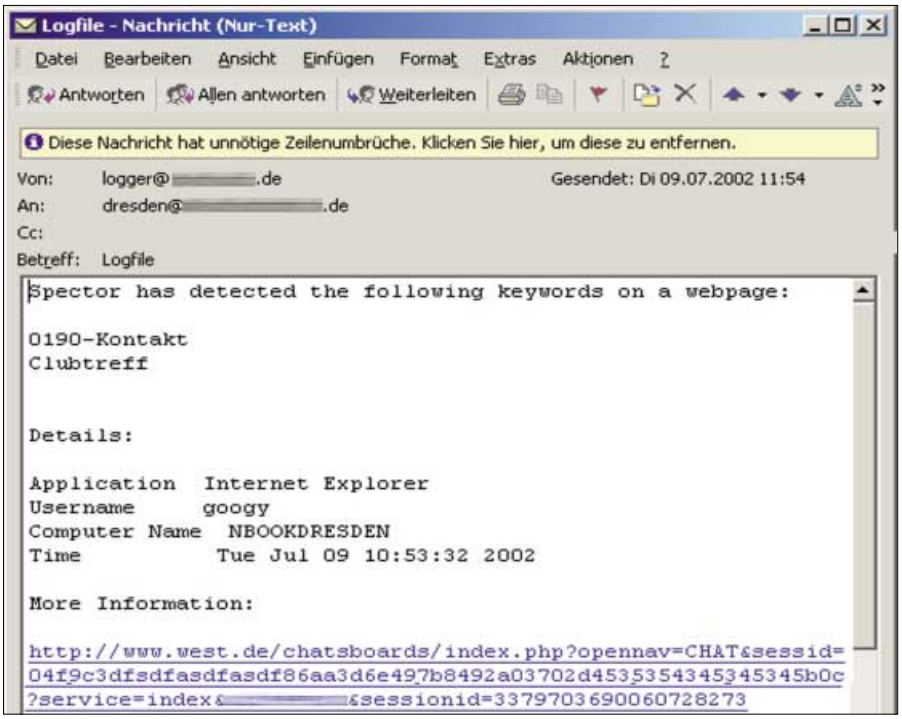
das lokalen Netzwerk als sichere Zone eingetragen ist, wie dies beim Einsatz von Personal Firewalls in einem Netzwerk normalerweise konfiguriert wird.

Jedes Programm, das etwas nach draußen senden möchte und dazu Ports auf Basis von TCP/IP benutzt, muss die Firewall passieren. Das gilt auch für die umgekehrte Richtung, wenn beispielsweise eine Fernsteuerungs-Software auf Ihren PC angesetzt wird. Handelt es sich dabei um eine Software, die Sie überhaupt nicht wissentlich gestartet haben, sollten Sie die Kommunikation verbieten.

Sie sollten die Liste derjenigen Programme, denen Sie innerhalb der Firewall eine Erlaubnis zur Datenkommunikation im lokalen Netzwerk oder über das Internet erteilt haben, von Zeit zu Zeit kontrollieren und alle Programmnamen aus der Befugnisliste löschen, deren Bedeutung Ihnen nicht ganz klar ist. Handelt es sich dabei beispielsweise um ein Mailprogramm oder einen Instant Messenger, den Sie versehentlich entfernt haben, aber tatsächlich benötigen, müssen Sie die Netzwerkkommunikation beim nächsten Programmstart bei der Nachfrage durch die Desktop Firewall einfach wieder freischalten.

Im laufenden Betrieb sollten Sie jedes Programm, das etwas versenden möchte, genauestens kontrollieren. In unregelmäßigen Abständen auftauchende Firewall-Meldungen über einen Versuch des Windows-Explorers, des Internet Explorers oder einer kryptische Systemdatei, eine Verbindung über das Internet aufzubauen, sind typische Alarmzeichen für Spionage-Software. Doch auch wenn Sie einen versteckten Keylogger finden, bedeutet das noch nicht unbedingt den Super-GAU. Klemmen Sie in diesem Fall Ihren PC vorübergehend vom Netz ab, löschen Sie alle verdächtigen Dateien, Autostart-Einträge und Registry-Einträge, starten Sie Ihren PC neu, und ändern Sie alle verwendeten Kennwörter.

Stefan Forster



Immer heimlich informiert: Schnüffelprogramme scannen den gesamten Bildschirminhalt ab und versenden augenblicklich eine Mail, sobald ein Suchbegriff auf dem Desktop vorhanden ist

Problematisch: Einsatz von Keyloggern in Unternehmen

Welcher Vorgesetzte möchte nicht gerne wissen, welche Internet-Seiten seine Mitarbeiter am Arbeitsplatz besuchen? Zwar lassen sich Web-Seiten beispielsweise mit pornographischem oder radikalem Inhalt in einem Firmennetzwerk von vorneherein blockieren, doch eine Überwachung lässt sich so kaum realisieren.

Auch zur Administration und als Helpdesk-Lösung setzen größere Unternehmen häufig zentrale Verwaltungswerkzeuge wie Microsoft SMS (System Management Server) ein, die eine Fernaufschaltung auf einzelne Arbeitsplätze erlauben. Damit ist ebenfalls ein Belauschen des einzelnen Anwenders möglich.

Achtung: Die Verwendung von Überwachungs-Software greift in die Rechte der Mitarbeiter ein und ist grundsätzlich unzulässig, es sei denn, ein Gesetz oder eine Rechtsvorschrift erlauben dies, es liegen besondere Gründe vor oder der Mitarbeiter hat seine Zustimmung erteilt.

Die detaillierte Aufzeichnung der Computernutzung eines oder aller Anwender stellt einen Umgang mit personenbezogenen Daten dar, der den Reglementierungen des Bundesdatenschutzgesetzes unterliegt, das auf die Landesdatenschutzgesetze verweist. Besondere Gründe können unter Umständen vorliegen, wenn der Arbeitgeber gegenüber einem einzelnen Arbeitnehmer ein berechtigtes Interesse nachweisen kann und ein schutzwürdiges Interesse des Betroffenen nicht entgegensteht. Das kann zum Beispiel zur Aufdeckung von Betrug der Fall sein, wenn ein durch Tatsachen begründeter Verdacht gegen einen Mitarbeiter vorliegt und die Überwachung zur Aufklärung beitragen kann.

Auch eine Protokollierung aller Eingaben aus einer betrieblichen Erfordernis heraus ist zulässig. Eine betriebliche Erfordernis könnte beispielsweise die Aufzeichnung zu Schulungszwecken oder das Speichern aller Eingaben für die vertragsgemäße Erfüllung von Verpflichtungen gegenüber Kunden des Unternehmens sein. Über diesen Umstand muss der Arbeitnehmer jedoch gesondert informiert werden.

Auch Betriebsvereinbarungen können ein Aufzeichnen aller Computeraktivitäten innerhalb eines Unternehmens regeln – es bedarf jedoch generell der Einbeziehung des Betriebsrats, sofern ein solcher existiert. Außerdem muss der Mitarbeiter gesondert und im Vorfeld auf die Protokollierung hingewiesen worden sein. Unzulässig gewonnene Daten dürfen übrigens nicht als Beweismittel herangezogen werden.

Systemdienste unter Windows NT 4, 2000 und XP

Dienste mit Vollmacht

Systemdienste arbeiten unbemerkt im Hintergrund und haben weitreichende Zugriffsrechte auf Windows. Wir sagen Ihnen, wie Sie Maßnahmen zur Sicherung des PCs ergreifen.

▸Wer von Windows 95/98/ME auf Windows 2000/XP umsteigt, wird mit einer ganzen Reihe von Neuerungen bei der Systemsicherheit konfrontiert. Dazu gehören vor allem die im Hintergrund laufenden Dienste, die viele Windows-Funktionen übernehmen, sowie Konten, die das Fundament der Betriebssystemsicherheit darstellen. Sowohl Systemdienste als auch Konten können von Schadprogrammen missbraucht werden. Der folgende Überblick gibt einige Hintergrundinfos sowie Empfehlungen zur Erhöhung der Systemsicherheit bei Windows-2000/XP-Workstations.

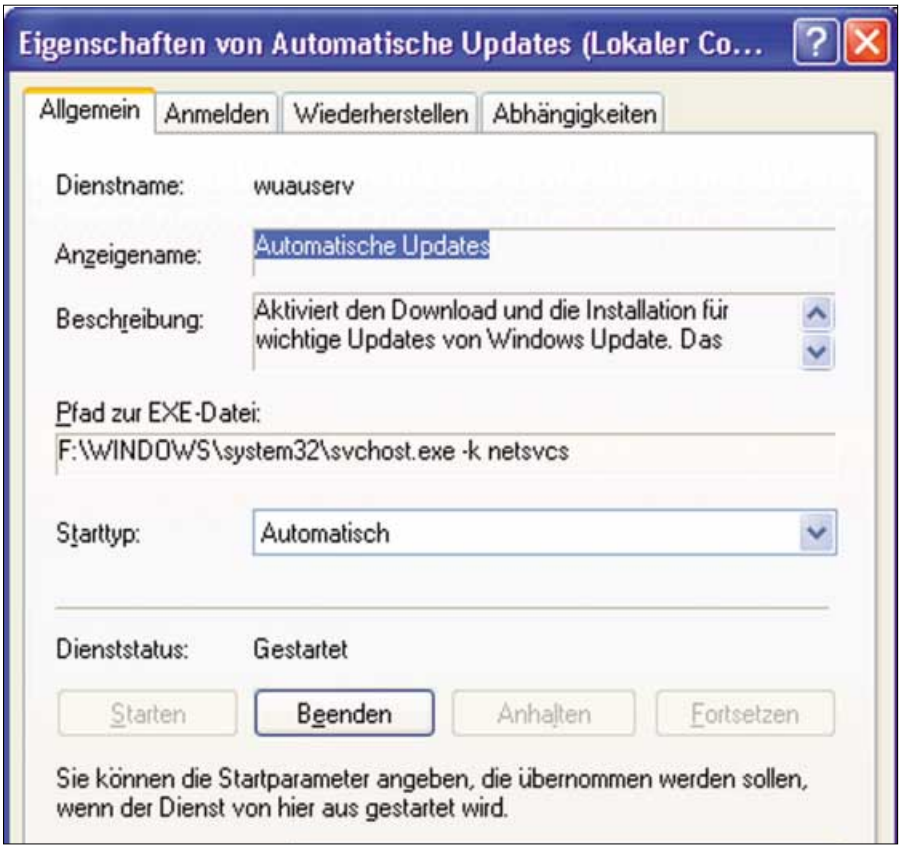
Dienste: Automatische Funktionen im Hintergrund

Windows 2000 und XP sowie deren Vorgänger Windows NT 4 verwenden im Gegensatz zu den kleinen Windows-Versionen 95/98 und ME ein ausgefeiltes, komplexes Dienstkonzept. Dienste sind mit gewöhnlichen Programmen vergleichbar, bieten jedoch einige Vorzüge:

- Sie werden automatisch mit Windows gestartet;
- sie laufen im Hintergrund;
- sie laufen unter einem Benutzerkonto.

Viele lebenswichtige Windows-Funktionen sind in Diensten verpackt und werden automatisch beim Hochfahren von Windows gestartet. Der Dienst „Sicherheitskontenverwaltung“ kümmert sich zum Beispiel um alles, was mit der Sicherheit lokaler Benutzerkonten zu tun hat. Diese systemrelevanten Dienste laufen, ohne dass sich ein Benutzer am System anmelden muss: Bootet Windows also bis zum Anmeldedialog, ist kein Benutzereingriff nötig, um die Funktionsweise des Systems sicherzustellen. Weitere typische Anwendungen für Dienste sind jede Art eines Serverbetriebs wie Web- oder FTP-Server, aber auch Antiviren-Programme und so genannte Live-Updates installieren sich als Dienst im System. Spy- oder Adware, Trojaner und jede Art von Schadprogrammen können sich ebenfalls als Dienst einrichten und werden unbemerkt ausgeführt.

Dienste benötigen Ressourcen wie Arbeitsspeicher und Prozessorzeit. In der Voreinstellung laufen auf einem Windows-PC bereits über 30 Dienste, insgesamt gibt es über 100. Das ist einer der Gründe für den hohen Bedarf an Arbeitsspeicher – 64 MB ist das absolute Minimum für eine Windows-XP-Installation. Deshalb kann es sinnvoll sein, nicht benötigte Dienste abzuschalten oder so zu konfigurieren, dass sie erst bei Bedarf gestartet werden.



Schaltzentrale: Im Eigenschaften-Dialog sind im Register „Allgemein“ alle wichtigen Informationen, darunter auch der Speicherort und die Startvariante eines Dienstes, aufgelistet

Info: Systemdienste

Unter Win NT 4, 2000 und XP werden bei jedem Start über 30 Dienste unbemerkt im Hintergrund geladen. Da sich aber auch Trojaner und Spyware-Komponenten als Dienst einnisten können, empfiehlt sich ein Blick in die Einstellungen.

Die Konfiguration der Dienste erfolgt in der Computerverwaltung, die Sie mit einem rechten Mausklick auf das „Arbeitsplatz“-Icon erreichen. Im Abschnitt „Dienste“ befinden sich alle installierten Systemdienste mit einer Kurzbeschreibung. In den Eigenschaften der Dienste befindet sich im Register „Allgemein“ unter anderem der Pfad zur ausführbaren Datei. Anwendungen wie etwa LSASS.EXE sind für die Sicherheitskontenverwaltung oder SVCHOST.EXE für eine ganze Reihe von Netzwerkaufgaben verantwortlich. Die meisten dieser Dateien befinden sich im Windows-System32-Verzeichnis.

Ob und welche Dienste laufen, lässt sich am schnellsten mit dem Taskmanager feststellen: Im Register „Prozesse“ sind alle aktuell laufenden sichtbaren Dienste mit ihrem derzeitigen Ressourcenbedarf aufgelistet.

Dienste-Start: Automatisch oder bei Bedarf

Ob ein Dienst mit Windows zusammen startet, lässt sich ebenfalls in seinen Eigenschaften beeinflussen: Zur Verfügung stehen manuell, automatisch oder deaktiviert. „Automatisch“ bedeutet, dass Windows diesen Dienst beim Booten aktiviert. Bei „manuell“ wird der Dienst nicht gestartet, kann aber vom Benutzer oder einem anderen Dienst aktiviert werden. Bei „deaktiviert“ lässt sich dieser Dienst nicht verwenden – weder vom System noch vom Benutzer.

Die Deaktivierung von Diensten ist grundsätzlich mit einem Verlust an Funktionen verbunden. Sinnvoll kann das Abschalten der Windows-Update-Funktion oder auch das Deaktivieren des Indexdienstes sein.

Das Gruppenkonto der lokalen Administratoren: Hier sollten keine unbekannten Einträge stehen

Schadprogramme können sich theoretisch ebenfalls als Dienst im System verankern. Dazu sind allerdings administrative Rechte erforderlich – es muss also ein Administrator-Account zugänglich gemacht werden. Der übliche Weg ist allerdings der, dass der Anwender selbst (als Administrator) Dienste – vielleicht sogar unwissentlich – installiert und aktiviert.

Accounts: Auf das Konto kommt es an

Diese Überlegungen führen zum Konzept der Benutzerkonten, das eine effektive Systemsicherheit erst ermöglicht. Dienste laufen grundsätzlich unter einem Konto und verfügen über Rechte, zum Beispiel über das Recht zur lokalen Anmeldung oder das Recht zur Sicherung von Systemdateien. Den Rechten werden Konten zugewiesen. Davon zu unterscheiden sind Berechtigungen – diese werden Objekten wie zum Beispiel einer Datei oder einem Ordner zugewiesen.

Windows enthält bereits eine Reihe vordefinierter Konten für Benutzer und Gruppen. Sie lassen sich in der Computerverwaltung im Abschnitt „Lokale Benutzer und Gruppen“ einsehen. Für eine effektive Verwaltung werden Rechte nicht an einzelne Konten vergeben, sondern an Gruppenkonten. Anwender, die ein bestimmtes Recht erhalten sollen, werden in die Gruppe aufgenommen, die über dieses Recht verfügt. Sollen einem Konto Rechte zugeteilt werden, ist das Modul „Lokale Sicherheitseinstellungen“ über die Eingabe von „secpol.msc“ in der Kommandozeile zu starten.

Das wichtigste Konto ist das Administrator-Konto. Es ist Mitglied der lokalen Gruppe der Administratoren. Um zu prüfen, ob sich ein Anwender unberechtigt Administratorrechte verschafft hat, öffnen Sie einfach die Eigenschaften des lokale Gruppenkontos der Administratoren. Dort sind alle Mitglieder aufgelistet.

Die Kontenverwaltung ist eng mit dem Gruppenkonzept von Windows verbunden, das bei einer lokalen Workstation noch übersichtlich ist, in einer Domäne mit vielen verschachtelten Gruppen jedoch schnell unübersichtlich werden kann. Der Einstieg in diese Materie wird zudem durch so genannte Systemkonten etwas unübersichtlich – diese sind fest vorkonfiguriert und lassen sich nicht ändern. Im Dienste-Modul finden sich zum Beispiel diese Konten:

Übersichtlich: In den Kontoeinstellungen können Benutzer- oder Gruppenkonten zugeteilt werden

- NT AUTHORITY\LocalService
- NT AUTHORITY\NetworkService

Unter diesen Konten werden Dutzende von Diensten ausgeführt, zum Beispiel der viel diskutierte Generic Host Process for Win32-Services (SVCHOST.EXE). Näheres dazu finden Sie in unserem Workshop zu Zone Alarm ab ▷ Seite 64.

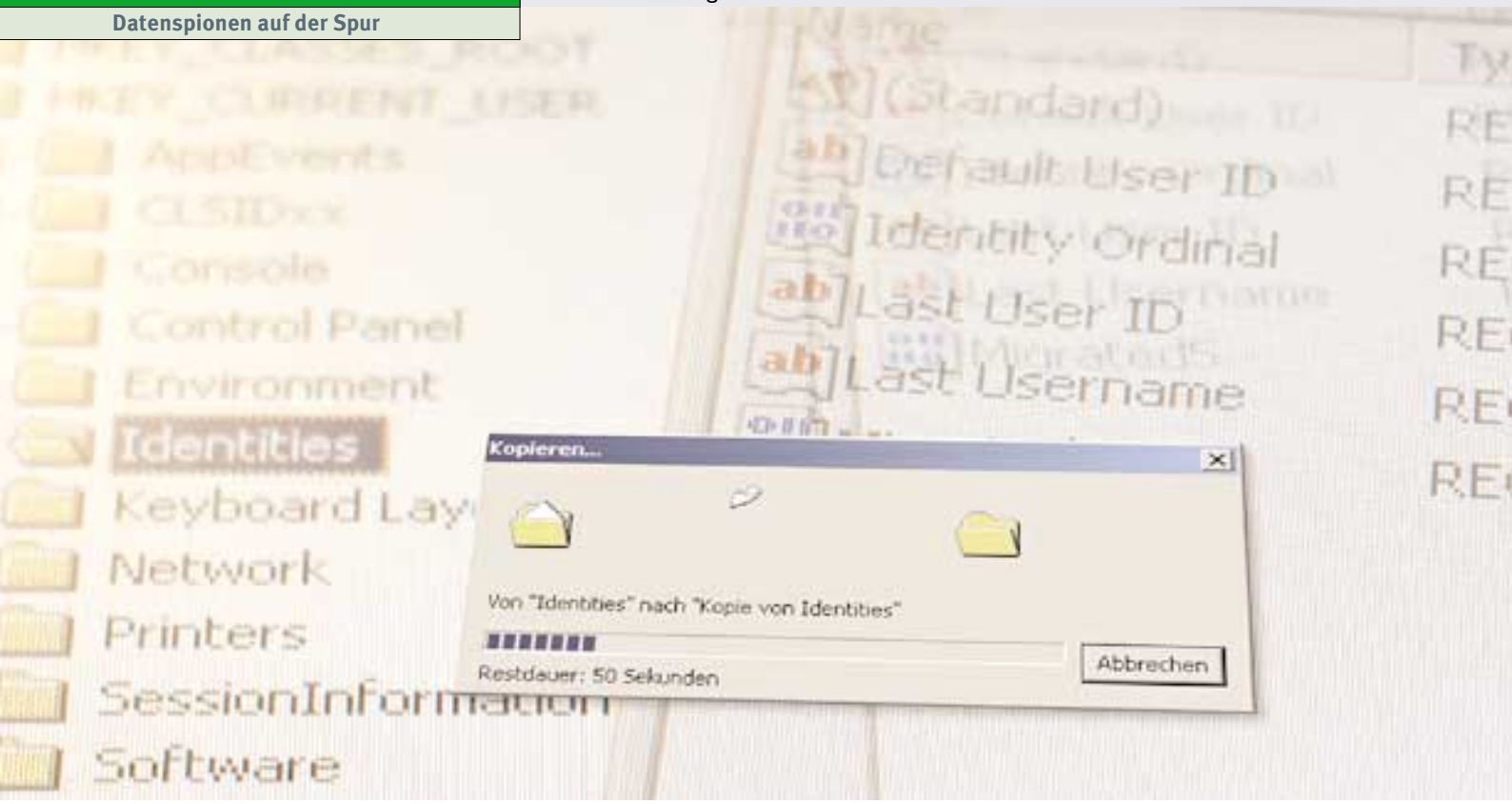
Empfehlungen: Worauf der Anwender achten muss

Um Ihr System dauerhaft „sauber“ zu halten, müssen Sie alle Systemprozesse, alle Konten und alle Mitglieder der Konten kennen und regelmäßig überprüfen. Folgende Aufgaben sind daher bei einem Verdacht durchzuführen:

- Überprüfen der Konten auf unbekannte Mitgliedschaften;
- Überprüfen auf unbekannte Prozesse im Taskmanager.

Werden Prozesse im Taskmanager beendet, kann das System instabil werden. Gleiches gilt für das Abschalten von Diensten, da viele Dienste wiederum von anderen Diensten benötigt werden. Bevor Sie Änderungen an Diensten vornehmen, sollten Sie eine Sicherung der gesamten Partition durchführen. Zusätzlich ist die Registry zu sichern. Hier sollten Sie einen Export des Schlüssels „Hkey_Local_Machine\System\CurrentControlSet\Services“ durchführen. Viele Schädlinge wie Trojaner oder Ad- und Spyware lassen sich mit Trojaner-Scannern erkennen und eliminieren. Allerdings besteht hier immer die Gefahr, dass Programme anschließend nicht mehr funktionieren.

Burkhard Müller



Unbemerkte Informationsübermittlung durch Windows XP

Das weiß Microsoft

Die Kombination aus Internet-Zugang und Microsoft-Betriebssystem lässt Böses erahnen. Spioniert der Software-Riese die Anwender aber wirklich aus und sammelt verfängliche Daten?

Seit Windows XP auf dem Markt ist, gibt es immer mehr Gerüchte über die so genannten „Phone-Home"-Aktivitäten dieses Produkts. „Phone-Home" bedeutet, dass die Software bei verschiedenen Gelegenheiten unbemerkt über das Internet „nach Hause telefoniert", also Kontakt zu einem Server des Herstellers aufnimmt und Daten übermittelt. Mittlerweile beschäftigen sich auch unzählige private Homepages mit der möglichen Anwenderbelauschung der Windows-Benutzer durch Microsoft. Fast immer ist dabei nur die Rede von einem „Verdacht", exakte Aussagen gibt es kaum. Die PC-WELT liefert Fakten: Nach Lektüre dieses Beitrags können Sie — bewaffnet mit den richtigen Tools — selber prüfen, ob, wann und in fast allen Fällen auch was an Microsoft gesendet wird.

Info: PC-Spionage

Neben zigtausend bekannten Spyware-Programmen steht auch Microsoft im Verdacht der Spionage. An den Vorwürfen der Datenschützer ist zwar wenig dran. Technisch ist Microsoft jedoch dazu schon jetzt in der Lage.

Auflösung: Warum ist das Spionieren so gefährlich?

Die schlimmsten Spekulationen befürchten das Senden persönlicher Informationen wie Passwörter, Systemeinstellungen, Mails oder Informationen über installierte und möglicherweise raubkopierte Software direkt an Microsoft. Der Windows Media Player soll Informationen über sämtliche Multimedia-Dateien, die Sie abspielen, an wen auch immer versenden, damit Sie dann gezielt Werbung bekommen oder gar eine Anzeige wegen unerlaubter Nutzung von urheberrechtlich geschützten Songs und Videos erhalten. Eins vorweg: Das ist alles Unsinn. Die zahlreichen Verbindungen, die Windows XP von sich aus ins Internet herstellt, sind derzeit weitgehend harmlos, abgesehen von einigen Ausnahmen, wie Sie auf den nächsten Seiten lesen werden.

Weil bloße Spionage-Behauptungen keinen tatsächlichen Nutzen bringen und nur der allgemeinen Panikmache dienen, ist es besser, die im Internet kursierenden Meldungen selbst zu überprüfen. Mit wenig Aufwand machen Sie sich selbst ein Bild davon, welche Daten von Ihrem PC übertragen werden, und finden so heraus, welche Anwendung zu welchem Zeitpunkt an wen ins Internet sendet. Das ist nicht schwer: Mit einem Sniffer machen Sie alle Daten, die der eigene

PC ins Internet sendet, in einer so genannten Paketanalyse sichtbar. Es bleibt Ihnen dabei wirklich nichts verborgen. Wie Sie mit einem Sniffer arbeiten, lesen Sie im Kasten „Paket-Analyse: Daten sichtbar machen mit Sniffern“ auf ▷ Seite 32. Wir haben Ihnen die Arbeit abgenommen und schildern im Folgenden die möglichen Spionage-Aktivitäten der wichtigsten Win-XP-Komponenten.

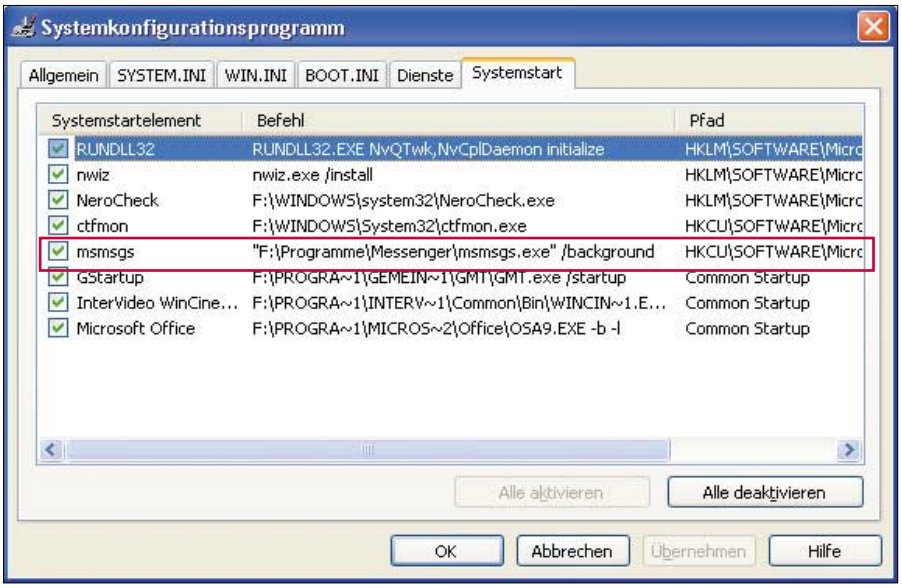
Internet Explorer: Technisch ist eine Spionage möglich

Webbrowser wie der Internet Explorer arbeiten mit dem Http-Protokoll, das – wie in den letzten Monaten gezeigt wurde – getunnelt werden kann. Mit Tunneln ist das Einbetten beliebiger Daten in das Http-Protokoll gemeint, die damit unbemerkt von einer aktiven Firewall in das Internet übertragen oder aus diesem eingeschleust werden. Und das ist das Problem: Die Firewall lässt sich damit überlisten. Testprogramme zum Tunnel-Verhalten sind unter dem Namen „Leaktest“ bekannt geworden. Populär ist der Online-Test von Steve Gibson (**http://grc.com**), inzwischen gibt es aber eine Reihe weiterer Leaktest-Programme, die alle nur eins zeigen sollen: Eine Firewall bietet keinen perfekten Schutz. Eine Suche mit Google nach „leak test“ fördert etliche interessante Seiten zu diesem Problem zu Tage.

Als Schlussfolgerung bleibt festzuhalten: Was der Browser darf, lässt sich in besseren Firewalls per Regel zumindest teilweise festlegen. Sicher ist das jedoch keinesfalls. Wie Sie Ihren Browser absichern und damit sicher unterwegs sind, lesen Sie ab ▷ Seite 70.

Spyware wie Alexa, die in älteren Versionen des Internet Explorers fest eingebaut war, findet sich in Windows XP zum Glück nicht mehr. Über die so genannten „verwandten Links“ hat diese Software das Surfverhalten ausspioniert und teilweise private Daten an verschiedene Dienste im Internet gesendet. Ältere Versionen des Internet Explorers als 6.0 sollten daher nicht mehr verwendet werden. Ansonsten sind dem nackten Internet Explorer keine Spionagefunktionen nachzuweisen.

Frei erhältliche Suchmaschinen-Toolbars für Browser stellen sich ebenfalls häufig als Spionage-Software (Spyware) heraus. Sicherheitsbewusste Anwender



Chat dauerhaft abschalten: Mit dem Deaktivieren dieser Option verhindern Sie den automatischen Start des Microsoft Messengers beim Hochfahren von Windows

verzichten auf derartige Zusätze. Spyware lässt sich am einfachsten mit dem Programm Ad-Aware (◉ auf Heft-CD oder unter **www.lavasoftusa.com**, englischsprachige Version für Windows 95/98/ME, 2000 und XP, 871 KB) entfernen, allerdings ist die Spyware-Problematik komplex wie alle Sicherheitsthemen: Nach dem Entfernen der Spyware läuft das verseuchte Programm womöglich nicht mehr. Ein unschönes Beispiel dafür ist der Divx 5.02 Pro Video-Codec (**www.divx.org**, werbefinanziert oder 30 Dollar Registriergebühr, für Windows 95/98/ME, 2000 und XP). Aber es gibt noch viele tausend weiterer verseuchter Programme, die als Spyware entlarvt wurden. Mehr dazu lesen Sie ab ▷ Seite 104.

MSN Messenger: Garantiert keine Privatsphäre

Beim in Windows XP fest verankerten MSN Messenger interessiert, ob zum Beispiel eine Chat-Verbindung über die Microsoft-Server läuft oder Daten nur direkt zwischen den Verbindungspartnern ausgetauscht werden. Interessant ist diese Frage auch in Bezug auf die Windows-eigene Fernsteuerungs-Software Remote Desktop. Zunächst betrachten wir den Ablauf der Anmeldung.

Wer den XP-Messenger nutzt, benötigt zwingend einen kostenlosen Hotmail/Passport-Zugang (**www.hotmail.de**). Die Anmeldung verläuft über verschiedene Microsoft-Server, unter anderem auch über einen der MSN-Server, was die Verquickung der verschiedenen Microsoft-Dienste unterstreicht. Dabei wird der Benutzername des Hotmail-Kontos mehrfach in den Http-Headern im Klartext übertragen, das zugehörige Passwort ist mit SSLv3 verschlüsselt. Die Ablaufverfolgung zeigt mehrere SSL-verschlüsselte Pakete zu verschiedenen Servern. Diese Daten lassen sich jedoch nicht einfach im Klartext sichtbar machen — dazu müsste die SSL-Verschlüsselung geknackt werden. Auf jeden Fall wird nicht nur das reine Passport-Passwort übertragen, dazu sind die verschlüsselten Datenmengen mit einigen tausend Zeichen schlicht zu groß. Zu sehen ist ebenfalls, dass Cookies gelöscht und gesetzt werden.

Die SSL-Verschlüsselung ist bei der Anmeldung an passwortgeschützten Systemen mehr als sinnvoll, hat jedoch den Nachteil, dass der Anwender nicht feststellen kann, welche Daten genau übertragen werden. Positiv ist, dass dies eine der wenigen verschlüsselten Übertragungen von Windows XP ist.

Chat: Microsoft hört auch hier ein wenig mit

Führen Sie eine Ablaufverfolgung eines Messenger-Chats durch, so ist sofort erkennbar, dass alle ausgetauschten Texte ausschließlich über den Server Msgr-sb58.msgr.hotmail.com laufen — natürlich im Klartext. Der genannte Server ist einer von mehreren Microsoft-Messenger-

Servern. Solche Chats sind also alles andere als privat. Auch andere Messenger-Clients wie Jabber (**www.jabber.org**) senden — wenn sie mit dem XP-Messenger kommunizieren — alle Daten zuerst an Microsoft, von dort gelangen diese dann zum Verbindungspartner. Die Microsoft-Server erhalten allerdings keine verschlüsselten Daten von den PCs der Chat-Teilnehmer, so dass das heimliche Versenden von Angaben zu Anwender oder Systemumgebung hier ausgeschlossen werden kann.

Etwas anders verhält es sich beim Remote Desktop: Hier sind die Microsoft-Server nur zur initialen Kontaktaufnahme notwendig, die Remote-Sitzung verläuft direkt zwischen den beiden Verbindungspartnern. Während der Sitzung werden größere Mengen binärer Daten über das spezielle Remote Desktop Protokoll zwischen den Partnern ausgetauscht, deren Sinn hier nicht entschlüsselt werden kann. Allerdings findet auch hier offensichtlich kein verschlüsselter Datenaustausch mit Microsoft-Servern statt.

Bei zentralen Messenger-Systemen laufen die Daten immer über die Messenger-Server des Anbieters — das sollten Sie wissen, wenn Sie sich in einer vermeintlich privaten Unterhaltung befinden. Das Senden von Passwörtern und anderen sensiblen Informationen sollten Sie daher unbedingt vermeiden. Wenn Sie den Messenger ganz abschalten möchten, starten Sie das Systemkonfigurationsprogramm MSCONFIG.EXE über die Eingabeaufforderung und deaktivieren im Register „Systemstart“ das Kontrollkästchen vor „msmsgs“.

Media Player: Was hören Sie denn heute?

Auch der Windows Media Player ist in Verruf gekommen. Gerüchten zufolge besteht die Gefahr, dass er Informationen über abgespielte Audio-CDs, Videofilme und andere Multimedia-Daten an Microsoft sendet.

Sobald der Media Player gestartet wird, sendet er ein Cookie an den Host Windowsmedia.com, sofern es auf dem PC des Anwenders vorhanden ist, sonst wird es von diesem Host im Cookie-Verzeichnis angelegt. Das Cookie ist nur für diese eine Sitzung gültig. Die Cookie-Informationen ändern sich nicht, wenn eine Audio-CD eingelegt oder eine andere Multimedia-Datei abgespielt wird. Möglich wäre hier die Übertragung von Dateinamen oder Seriennummern der Audio-CDs.

Deutlich sichtbar: Hier sendet der Anwender-PC unverschlüsselte Partitions-Infos an Microsoft

Allerdings wird mehrfach eine so genannte GUID (Global Unique Identifier) an Windowsmedia.com gesendet. Sie ist

Meta-Informationen: Was Office-Dokumente verraten

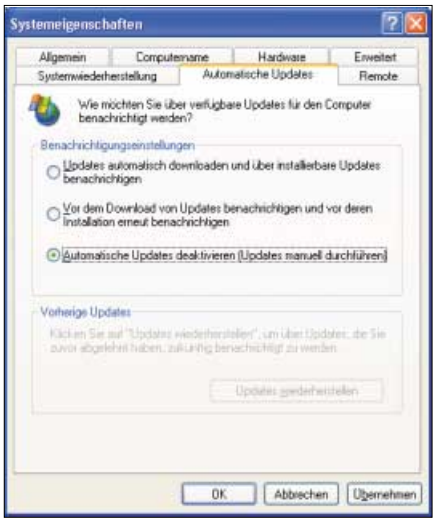
Ein bekanntes, aber häufig wenig beachtetes Sicherheitsproblem stellen moderne Office-Dokumente dar, wie sie zum Beispiel von Microsoft Office, aber auch von anderen Produkten erzeugt werden. Diese enthalten außer dem eigentlichen Text und Formatierungsanweisungen für das Layout auch so genannte Meta-Informationen wie den Benutzernamen oder die PC-Kennung aller Anwender, die das Dokument bearbeitet haben. Insbesondere bei eingeschalteter Ablaufverfolgung (etwa dem Überarbeiten-Modus von Word XP, den Sie über „Extras, Änderungen nachverfolgen“ aktivieren) lässt sich nachvollziehen, welche Änderungen von welchen Personen durchgeführt wurden. So ist zum Beispiel der Weg eines Dokuments innerhalb einer Firma nachvollziehbar — vom Ersteller über verschiedene Zwischenstufen bis zu dem Anwender, der die letzten Änderungen vorgenommen hat. Da sich in solchen Dokumenten auch Namen von PCs befinden können, etwa „Buchhaltung01“, bekommen Dritte durch Sichtbarmachen dieser Informationen auch Einblicke in die Struktur eine Firma.

Innerhalb eines Unternehmens oder einer geschlossenen Benutzergruppe mögen diese Infos wenig brisant sein, werden solche Dokumente aber als Mail versendet oder zum Beispiel im Web veröffentlicht, können Fremde die eingebetteten Meta-Informationen missbrauchen. Meta-Informationen sind ohne Hilfsmittel oft nicht vollständig sichtbar. Es ist aber einfach, sie mit einem Hex-Editor anzuzeigen – das kann jeder. Hex-Editoren zeigen jedes Byte einer Datei, auch die versteckten Informationen.

Ein weiteres Problem stellen eingebettete Makro-Viren dar sowie die Informationen, die Sie bei Word zum Beispiel unter „Datei, Eigenschaften“ finden. Sie verraten bereits einiges über den Ersteller des Dokuments.

Abhilfe schafft zum Beispiel die Konvertierung eines Dokuments in eine reine Textdatei (Ascii), wobei aber das Layout verloren geht. Auch Textformate wie RTF oder besonders PDF geben weniger Informationen preis, allerdings sind auch in solchen Dokumenten teilweise Zusatzinformationen enthalten. Gut geeignet ist ein reines, einfaches HTML, wie es von vielen Web-Editoren erzeugt wird. Allerdings müssen Sie dann bei den Layout-Funktionen Abstriche machen und auf spezielle Formatierungen verzichten oder diese manuell ersetzen. Die HTML-Exportfunktionen der Office-Pakete erzeugen dagegen ein unübersichtliches, aufgeblähtes HTML.

Wenn Sie also nicht möchten, dass die versteckten Informationen Ihrer Dokumente von anderen ausgewertet werden, sollten Sie sich überlegen, ob Sie nicht eine Konvertierung zum Beispiel in das PDF-Format vornehmen. PDF-Exportfilter gibt es über Zusatzprogramme für nahezu alle Office-Anwendungen — der dazugehörige Acrobat Reader ist kostenlos. Dieser kleine zusätzliche Arbeitsschritt kann die Datensicherheit ganz wesentlich erhöhen.



Nie mehr automatisch: In diesem Register schalten Sie die Windows-Update-Funktion endgültig ab

von der Form „D5BA4CB9C98C4BDDBC8862CF29018948“ und ändert sich nicht während der Übertragungen. Was sie genau bedeutet, lässt sich nicht vollständig klären, jedoch ist sicher, dass sie nicht mit Multimedia-Titeln in Zusammenhang steht. Im Zusammenhang mit Videodateien lädt der Media Player nach Übermittlung der Codec-Informationen lediglich zur Wiedergabe erforderliche, aber auf dem lokalen PC nicht vorhandene Codecs vom Microsoft-Server. Damit steht fest: Der Media Player sendet keine persönlichen Angaben über abgespielte Multimediadateien wie Audio-CDs, MP3- oder Videodateien.

Zwei Einstellungen sollten Sie beim Media Player dennoch in Erwägung ziehen: Deaktivieren Sie im Register „Player“ der Optionen die beiden Kontrollkästchen „Identifikation des Players durch Internet Sites zulassen“ und „Lizenzen automatisch erwerben“, sofern Sie sich überhaupt mit Microsofts Multimedia-Formaten abgeben, die ein Rechte-Management integriert haben.

Windows Update: Feature oder Spionage-Tool?

Die Windows-Update-Funktion, die Sie über das Start-Menü oder über das „Hilfe- und Support-Center“ aufrufen, untersucht Ihren Computer nach installierten Komponenten, um eventuell vorhandene Updates, Treiber und Patches anzubieten. Diese lassen sich dann auf Wunsch von den Microsoft-Servern laden und lokal installieren.

Den Dialog zwischen Ihrem eigenen PC und dem Microsoft-Server können Sie sehr schön mit dem im Kasten auf ▷ Seite 32 vorgestellten Gratis-Sniffer Ethereal (◉ auf Heft-CD oder unter **www.etherreal.com**, englischsprachige Version für Win 95/98/ME, 2000 und XP, 7,1 MB) sichtbar machen: Im ersten Schritt werden zunächst einige allgemeine Daten abgefragt:

- ▷ die Art des Betriebssystems mit Versions- und Build-Nummer;
- ▷ die Versionsnummer des Microsoft Internet Explorers;
- ▷ die Anzahl installierter Festplatten mit Laufwerksbuchstaben und freiem Speicherplatz.

Gegen die Übertragung dieser Informationen ist zunächst wenig einzuwenden. Interessanter wird es im nächsten Schritt: Der Update-Server sendet Registry-Schlüssel, deren Inhalt das Update zurücksendet. Es handelt sich dabei um die Informationen in „Hkey_Local_Machine\Software\Microsoft\Active Setup\Installed Components\“.

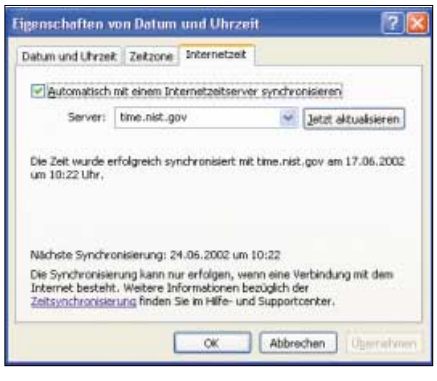
Unterhalb dieses Schlüssels befinden sich Informationen zu installierten Windows-Komponenten wie Netmeeting, Media Player, Outlook Express und anderen Windows-Zubehörprogrammen. Die Update-Funktion erfährt damit, ob eine bestimmte Komponente installiert ist und falls ja, mit welcher Versionsnummer. An diesem Punkt interessiert vor allem die Frage, ob Informationen über Microsoft-fremde Produkte übertragen werden – das war im Test nicht der Fall.

Der weitere Informationsaustausch läuft immer nach dem gleichen Schema ab: Der Server fordert im Dialog gezielt einzelne Informationshäppchen an, die der eigene Rechner liefert. Er holt nicht zum Rundumschlag aus und fordert zum Beispiel eine komplette Liste aller installierten Programme an, was für ihn ein Leichtes wäre. Auch Seriennummern, Benutzernamen, Passwörter und andere sensible Informationen werden nach diesen Untersuchungen mit der momentan aktuellen Version des Windows-Update-Programms nicht an Microsoft übertragen, auch nicht die Seriennummer von Windows. Mit einer automatischen Online-Aktualisierung der Update-Software kann Microsoft dieses Verhalten jedoch jederzeit ändern.

Nach den Daten über die Windows-Komponenten werden einige Versionsnummern installierter Treiber übertragen. Danach überprüft die Update-Funktion die installierte Hardware. Wieder fragt der Server detailliert nach Informationen wie Prozessortyp und installierten Laufwerken inklusive Herstellername und exakter Typbezeichnung. Diese Informationen sind notwendig, da das Windows-Update auch Treiber installiert und dafür wissen muss, welche Treiber in welchen Versionen bereits installiert sind. Damit ist die Kommunikation zu Ende. Kurze Zeit später bietet der Server die gefundenen Updates zum Download an.

Die gesamte Kommunikation erfolgt im Klartext. Lediglich zu Beginn des Datenaustauschs sendet der Update-Server binäre Daten, die wahrscheinlich ein Active-X-Control darstellen. Innerhalb dieser Binärdaten finden sich lesbare Copyright-Hinweise von Microsoft und Verisign, die die Active-X-Controls von Microsoft zertifiziert. Damit ist es offensichtlich, dass ausführbarer Code geladen wird, der im Prinzip mit dem System beliebige Dinge anstellen kann. Entscheidend aber sind die Antworten des eigenen PCs: Und die gehen unverschlüsselt im Klartext über das Internet. Damit spioniert die Update-Funktion in der zum Redaktionsschluss gültigen Fassung den Benutzer nicht aus.

Das Windows-Update läuft automatisch im Hintergrund und meldet sich, falls Updates vorhanden sind. Wer das nicht möchte und die genannten Informationen nicht an Microsoft senden will, schaltet die Update-Funktion aus: Öffnen Sie dazu in der Systemsteuerung das Element „System“, und wählen Sie im Register „Automatische Updates“ die Option „Automatische Updates deaktivieren (Updates manuell durchführen)“. Grundsätz-



Völlig harmlos: Time Server aus dem Internet synchronisieren die interne Computer-Uhr

lich sollten Sie aber auf die Update-Funktion nicht verzichten. Denn Microsoft hat gerade in letzter Zeit eine Vielzahl von Sicherheits-Patches zur Verfügung gestellt, die den Windows-Rechner gegen Hackerattacken aus dem Internet schützen sollen.

Time Server: Wirklich nur ein automatischer Zeitabgleich?

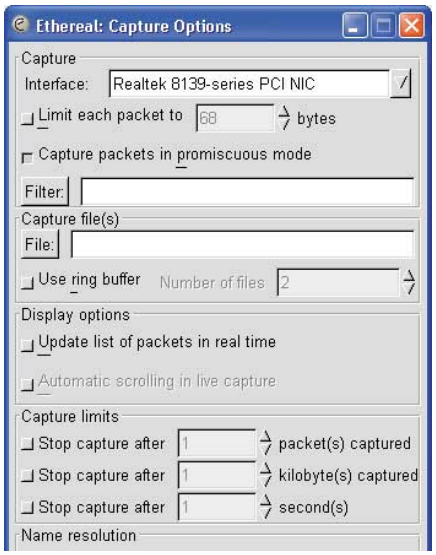
Windows XP kann die Systemzeit mit einem Atomuhr-Zeitserver im Internet automatisch abgleichen. Auf diese Weise ist eine einheitliche Zeit auf allen Systemen sichergestellt. Diese nützliche Funktion sehen Sie in den „Eigenschaften von Datum und Uhrzeit“, wenn Sie doppelt auf die Uhr in der Taskleiste klicken. Im Register „Internetzeit“ lässt sich der Zeit-Server eintragen und die Aktualisierung durchführen. Dabei wird genau ein Paket an den Timer Server gesendet, und dieser sendet genau ein Paket mit der aktuellen Zeit für die Zeitzone. Das dafür verwendete Sntp (Simple Network Time Protocol) ist sehr einfach im Kommunikationsmitschnitt des Sniffers zu erkennen und auszuwerten. Es werden keinerlei weitere Daten gesendet. Abschalten lässt sich diese Funktion, wenn Sie das Kontrollkästchen „Automatisch mit einem Internetzeitserver synchronisieren“ deaktivieren.

Privatsphäre schützen: Tools aus dem Internet helfen

Viele der beschriebenen Einstellungen lassen sich mit zwei Tools aus dem Internet bequem vornehmen: Das Freeware-Programm XP-Antispy (auf Heft-CD oder Download unter **www.xp-antispy.de**) und die Shareware XP-Manager (850 KB, Download unter **www.softwareedition.de/download.htm**, Registriergebühr: 10 Euro) nehmen Ihnen die Arbeit ab, sich durch die zahllosen Einstellungen zu klicken. Auf beiden Websites finden Sie übrigens gut gepflegte Diskussionsforen mit weiteren Informationen.

Microsofts Produktaktivierung: Scheinbar geklärt

Die Aktivierung von Windows XP soll verhindern, dass Gelegenheitskopierer Raubkopien herstellen, hat aber auch dazu geführt, dass sich viele Anwender illegal eine „Corporate Edition (Unternehmenslizenz)“ von Windows XP Professional „besorgt“ haben, die ohne Produktaktivierung auskommt. Noch vor der endgültigen Freigabe von Windows XP sind Details zur Produktaktivierung bekannt geworden. Sie stand ebenfalls in Verdacht, persönliche Anwender-Informationen an Microsoft zu senden.



Mitlesen von Daten: Hier wird die Schnittstelle ausgewählt, die Etherreal überwachen soll

Paket-Analyse: Daten sichtbar machen mit Sniffern

Um den Datenverkehr zwischen dem eigenen PC und Rechnern im Internet sichtbar zu machen, eignet sich ein Sniffer wie Ethereal (auf Heft-CD). Er fängt alle Datenpakete ab und stellt ihren Inhalt nach Protokollen aufgeschlüsselt dar. Das Abfangen der Datenpakete, die bei einer Online-Sitzung übertragen werden, wird als Ablaufverfolgung (Packet Trace) bezeichnet.

Vor der Installation von Ethereal müssen Sie den Paket-Treiber Winpcap (auf Heft-CD) installieren. Das Sniffen starten Sie über „Capture, Start“. Im folgenden Dialog wählen Sie bei „Interface“ die Netzwerkkarte aus, deren Daten Sie mitlesen möchten. Mit den Einstellungen „Update list of packets in real time“ und „Automatic scrolling in live capture.“ werden die ausgetauschten Pakete in Echtzeit angezeigt. Wer nicht über DSL online ist, stellt den Modem- oder ISDN-Treiber ein. Welche Pakete genau angezeigt werden, hängt von der verwendeten PC-Konfiguration ab. Bei Einzelplatz-PCs sind alle Pakete interessant. Sniffen Sie in einem nicht geswitchten lokalen Netzwerk und befindet sich die Netzwerkkarte im so genannten Promiscous Mode, werden alle Pakete abgefangen, auch diejenigen von anderen Clients im gleichen Segment. Beachten Sie, dass das Ausspähen von Datenpaketen Dritter nicht erlaubt ist. Die Unterscheidung der Pakete erfolgt leicht über die IP-Adresse — interessant sind hier nur die Pakete, die von der eigenen IP-Adresse abgehen oder dort ankommen. In geswitchten Netzen ist es einfacher: Hier sieht der Sniffer nur die Pakete, die zwischen dem eigenen Rechner und dem Router ausgetauscht werden.

Packet Traces (Kommunikationsprotokolle) lassen sich in diversen binären Formaten für eine spätere Analyse abspeichern. Für unsere einfachen Zwecke eignet sich das Speichern als TXT-Datei. Unter „File, Print“ geben Sie einen Dateinamen für die Textdatei an. Für unsere Zwecke interessieren die Protokolle weniger, wichtig sind die übertragenen Daten — und die werden jeweils am Ende eines Pakets angezeigt. Es gibt nur zwei Möglichkeiten: Entweder die Daten lassen sich im Klartext lesen, oder es tauchen merkwürdige, scheinbar sinnlose Zeichen auf — dann werden binäre Daten übertragen. Taucht im Paket das SSL-Protokoll auf, sind die Daten verschlüsselt und mit einfachen Mitteln nicht zu knacken.

Sie können sich die zeitliche Abfolge der getauschten Pakete ansehen und daraus Schlüsse ziehen. Wenn Ihr eigener Rechner etwa „Berlin“ heißt, sehen Sie sich jede Zeile an, in der das Wort „Berlin“ vorkommt. Dort steht auch die IP-Adresse des Verbindungspartners. Interessant sind nun alle Pakete, die vom eigenen PC ins Internet gesendet werden. Sortieren Sie die Spalte „Source“ – und schon sehen Sie alle Pakete, die Ihren eigenen Rechner verlassen haben. Über die Paketnummer finden Sie in der gespeicherten TXT-Datei leicht das gesamte Paket wieder. Die TXT-Datei können Sie mit einem Texteditor etwa nach Ihrem Hotmail-Account durchsuchen.

Details dazu hat unser Schwester-Webzine TecChannel unter dem Titel „XP-Aktivierung Bit für Bit“ veröffentlicht. Sie finden den Beitrag unter der Adresse **www.tecchannel.de/betriebssysteme/739/**. Die übertragenen Seriennummern sind inzwischen bekannt. Welche und wie viel Hardware ausgetauscht werden darf, bevor eine neue Aktivierung fällig wird, erfahren Sie mit dem Gratis-Programm XP-Info Utility (20 KB, Download unter **www.licenturion.com/fl.cgi?arg=0302**).

Bereits im August 2001 nahm Microsoft in einem White Paper (**www.microsoft.com/piracy/basics/activation/windowsproductactivationtechnicalmarketbulletin.doc**) zur Produktaktivierung Stellung. Dort heißt es: „At no time is personally identifiable information secretly gathered or submitted to Microsoft as part of activation.”, sinngemäß übersetzt: Bei der Aktivierung werden personenbezogene Daten zu keinem Zeitpunkt übertragen. Nach allem, was bis jetzt bekannt geworden ist, stimmt das wohl. Allerdings lassen sich mit den Daten Statistiken über installierte Hardware erstellen und nutzen. Wem diese Datenbestände zugänglich sind, weiß nur Microsoft. Dass diese Daten von Microsoft weitergegeben werden, ist zwar nicht leicht beweisbar, aber eher wahrscheinlich.

Die Daten, die bei der Produktaktivierung übertragen werden, sind nach einem komplizierten Verfahren verschlüsselt, so dass mit einem Sniffer-Protokoll hier nichts in Erfahrung zu bringen ist.

Ruhe bewahren: Noch kein Grund zur Panik

Die dargestellten Untersuchungen zeigen eines ganz deutlich: Die Phone-Home-Aktivitäten von Windows XP sind derzeit in fast allen Fällen harmlos. Die mit den Microsoft-Servern ausgetauschten Infos erfolgen in den allermeisten Fällen im Klartext und sind damit leicht nachvollziehbar. Die Ursache hierfür liegt darin, dass die Internet-Protokolle alle Daten im Klartext übertragen, eine Verschlüsselung findet so gut wie nie statt und ist mit nicht unerheblichem Aufwand verbunden. Auch Kompatibilitätsprobleme (der Empfänger kann die verschlüsselten Daten nicht lesen) sprechen gegen den Einsatz von Verschlüsselung.

Dass bei Kommunikationsprogrammen wie dem Messenger die meisten Daten über Microsoft-Server übertragen werden und dort theoretisch ausgewertet werden können, sollten Sie jedoch wissen. Sensible Daten sollten deshalb grundsätzlich verschlüsselt werden – mit dem für privaten Einsatz kostenlosen Programm Pretty Good Privacy für Win 95/98/ME, 2000 und XP (PGP, **www.pgpi.org**, Download 7,3 MB und ◉ auf Heft-CD) lassen sich zum Beispiel Mails einfach und effektiv verschlüsseln (mehr dazu ab ▷ Seite 124). In Chats oder auf Web-Boards sollten Sie solche Daten niemals preisgeben.

Kritisch wird es immer dann, wenn verschlüsselte Daten gesendet werden. Die sind zwar per Paketanalyse leicht sichtbar zu machen, lassen sich jedoch nicht ohne spezielle Knackprogramme lesen. Zudem kann das Dechiffrieren von Verschlüsselungen je nach Algorithmus sehr zeitaufwändig werden und viel Rechenleistung erfordern.

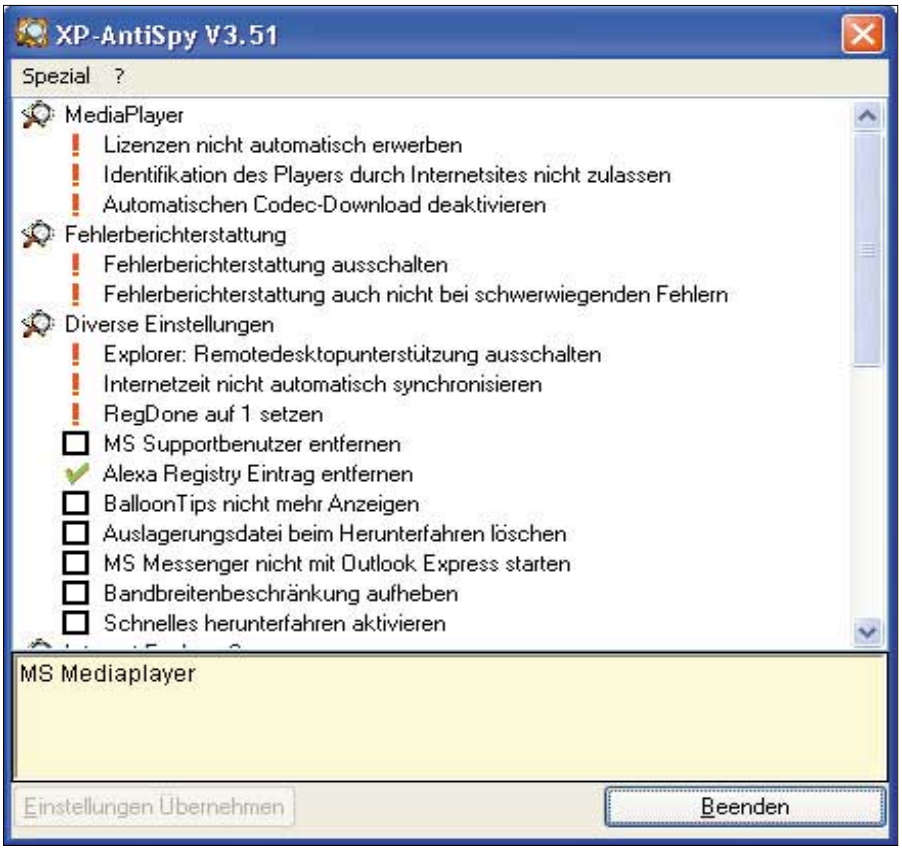
Die einzige Stelle, an der SSL-verschlüsselte Daten an diverse Microsoft-Server gesendet werden, ist die Anmeldung bei Hotmail/Passport. Das ist unumgänglich, wenn Sie den Windows-XP-Messenger einsetzen möchten, jedoch ist hier eine Verschlüsselung auch wünschenswert. Ohne diese Sicherheitsfunktion könnten Sie zum Beispiel im Firmennetzwerk ausspioniert werden, und Unbefugte würden Zugang zu Ihren Postfächern erhalten.

Die gute Nachricht ist, dass Windows XP derzeit nicht zu den Spionage-Anwendungen gehört, abgesehen von der Produktaktivierung. Klar ist jedoch auch, dass sich das jederzeit ändern kann. Durch Online-Updates kann schließlich jede beliebige Änderung am Betriebssystem durchgeführt werden.

Inzwischen fast normal, jedoch von Anwendern nicht gerne gesehen, ist das Sammeln und Weitergeben oder Verkaufen von Kontaktdaten und Mailadressen. Wer Hotmail oder Passport nutzt, muss sich darüber im Klaren sein, dass seine Mailadresse schnell weitergegeben wird – die Folge sind zumeist Werbemails.

Wer sein System sauber halten möchte, überwacht beharrlich die Internet-Verbindungen aller Programme. Personal Firewalls leisten hier gut Dienste, da sie fast jede Verbindung zum Internet bemerken. Durch eine Paketanalyse lässt sich dann feststellen, was wohin gesendet wird.

Burkhard Müller



Auf einen Blick: Mit XP-Antispy stellen Sie die meisten Phone-Home-Aktivitäten einfach per Mausklick ab. Das Programm ändert dazu lediglich einige versteckte Schlüssel in der Windows-Registry

Wie Angreifer Passwörter aushebeln

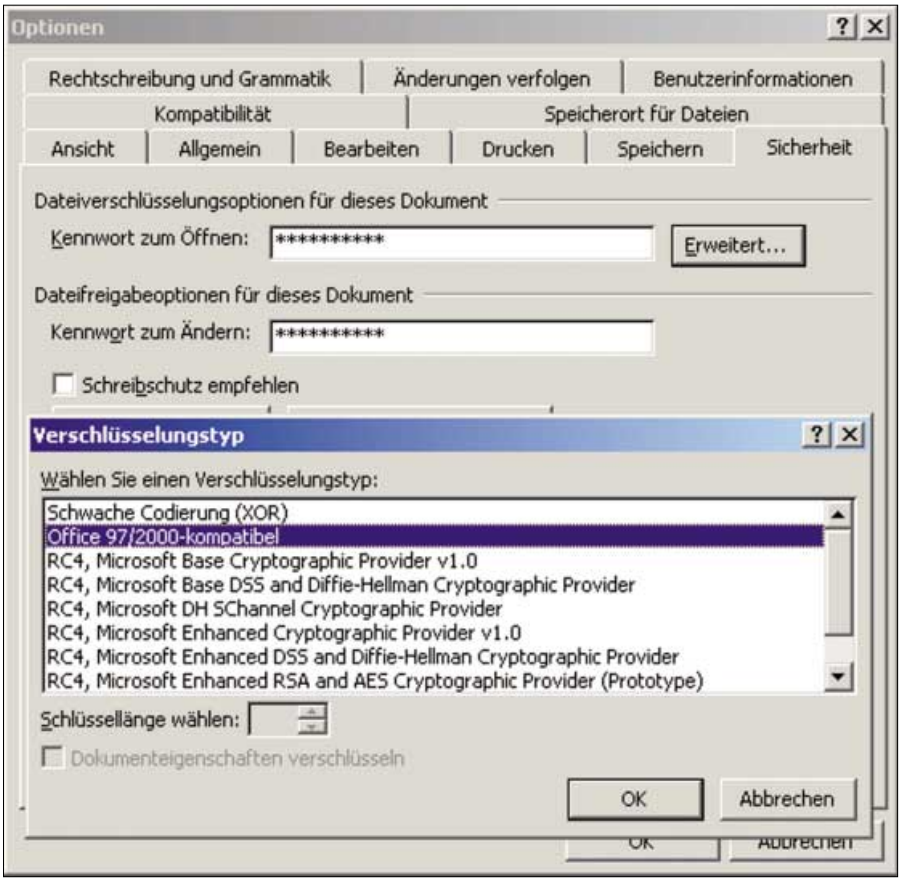
Einbruch mit Dietrich

Sie schützen vertrauliche Geschäftsunterlagen und private Office-Dokumente mit Passwörtern. Wir möchten Sie warnen: So einfach sind diese Schutzvorrichtungen zu knacken.

▸Es gibt verschiedene Motive, Dokumente mit einem Passwort zu schützen. An erster Stelle steht der naheliegendste Grund: Sie wollen nicht, dass Dritte Kenntnis vom Inhalt Ihrer Dateien bekommen und einsehen können, was Sie erstellt haben. Auch Veränderungsschutz ist ein häufiger Grund für die Verwendung eines Kennworts, etwa bei besonders wichtigen Dokumenten wie Vertragsentwürfen, Redevorlagen oder Produktinfos sowie Schriftstücken, die für einen gewissen Zeitraum einer Veröffentlichungssperre unterliegen. Nur Sie als Ersteller haben dank Passwortschutz die Möglichkeit, Teile des Dokuments oder das ganze Werk zu bearbeiten.

Passwörter-Einsatz: Im Büro und am Familien-PC

Die Verwendung von Passwörtern ist darüber hinaus beim gemeinsamen Zugriff auf Dateien und Ordner im Netzwerk mit Kollegen oder zu Hause mit anderen Familienmitgliedern ratsam. Insbesondere Kinder und Heranwachsende treibt eine natürliche Neugier häufig dazu, alle vorhandenen Laufwerke zu durchsuchen und Dateien mit interessant klingenden Namen zu öffnen. In Firmen kann zwar ein Mitarbeiter normalerweise nicht auf die Dokumente seiner Kollegen zugreifen, doch während der Besprechung oder der Mittagspause steht der PC oftmals einem direkten Fremdzugriff offen. Im Übrigen halten Sie durch ein Passwort auch neugierige Netzwerkadministratoren ab, die auf alle gespeicherten Daten Zugriff haben.



Keine sichere Dateiverschlüsselung: Die zu Office 97/2000 kompatible Verschlüsselung von Word XP ist unsicher. Sie verwenden daher besser einen der angebotenen RC4-Algorithmen

Anwendungsprogramme bieten nur unzureichenden Schutz

Anwendungsprogramme wie Word, Excel, Quickbooks oder das Wiso Sparbuch bieten beim Speichern von Dokumenten die Option, ein Kennwort zu vergeben, das beim Öffnen der Datei eingegeben werden muss – ansonsten ist kein Zugriff möglich. In puncto Passwortschutz verfolgen die Software-Hersteller zwei unterschiedliche Ansätze: Ladesperre für Dateien oder Vollverschlüsselung aller Daten. Bei der Ladesperre wird der Datei-Inhalt nicht verschlüsselt, sondern es wird der Datei lediglich ein Kennwort angehängt, das der Anwender beim Laden eingeben muss. Die Vollverschlüsselung verändert dagegen sämtliche Daten. Die Grenzen sind fließend, denn häufig wird eine Ladesperre mit einem einfachen Krypto-Algorithmus kombiniert.

Info: Codes knacken

Der in Anwendungsprogrammen integrierte Passwortschutz sorgt in den meisten Fällen für eine trügerische Sicherheit. Durch den Einsatz von Passwort-Recovery-Tools umgehen vergessliche Benutzer wie auch böswillige Computer-Hacker den Kennwortschutz.

Im einfachsten Fall reicht es bei primitiv mit einer Ladesperre geschützten Dokumenten aus, die Datei in einem beliebigen Text- oder Hexeditor zu öffnen und sich den tatsächlichen Inhalt anzuschauen. Mit Hilfsprogrammen wie dem kostenlosen Textgrabber 2.2 (◉ auf Heft-CD oder Download unter **www.textgrabber.de**, 2,52 MB) geht das sogar noch einfacher: Die Software extrahiert den gesamten unter Windows darstellbaren Textinhalt einer Datei und schreibt die Zeichen in eine Textdatei, die Sie mit Word oder jedem anderen Textprogramm bequem durchsuchen können. Verschiedene Filtereinstellungen helfen sogar beim Aussortieren unerwünschter Zeichen.

Passwort weg, was tun? Nachschlüssel gibt's zur Genüge

Um passwortgeschützte Dateien in der verknüpften Anwendung öffnen zu können, muss man entweder das Passwort kennen oder es aus der Datei entfernen. Hacker haben besonders leichtes Spiel bei unzureichenden Kennwörtern, denn hier führt schlichtes Raten immer noch am schnellsten ans Ziel. So ist der eigene Name oder der von Familienangehörigen ein beliebtes Passwort.

Das wichtigste Handwerkszeug von Hackern sind jedoch Passwort-Recovery-Tools, die als elektronischer Nachschlüssel arbeiten. Dabei versuchen die Utilities zunächst das chirurgische Entfernen des Passworts innerhalb des Binärcodes der kennwortgeschützten Datei. Das Kennwort wird dazu einfach überschrieben oder gelöscht.

Hersteller von Knackprogrammen haben bei der Analyse der Dokumentenstruktur in den allermeisten Fällen einfaches Spiel: Statt die Datei beim Speichern vollständig zu verschlüsseln, also die gesamte ursprüngliche Dateistruktur durch ein undurchsichtiges Zahlen- und Buchstabenwirrwarr zu ersetzen, lassen viele Hersteller die Datei in ihrem ursprünglichen Zustand und platzieren nur einen Code an einer vordefinierten Position, falls Sie beim Speichern des Dokuments ein Passwort angeben. Beim Öffnen der Datei schaut die jeweilige Anwendung nach, ob an der betreffenden Stelle ein Kennwort vorhanden ist, und fordert bei Bedarf zur Passworteingabe auf. Diese Schutzvariante kommt bei den meisten

Adobe-Acrobat-Dateien (Extension PDF) im Visier: Schneller als das Ausprobieren aller Passwörter über einen Brute-Force-Angriff geht das methodische Durchprobieren eines Wörterbuchs

Office-Programmen zum Einsatz. Für den Hersteller der Software hat dieses nachlässige Schutzverfahren den Vorteil, dass die Programmierer keine zeitaufwändige Vollverschlüsselungsroutine integrieren müssen.

Verschlüsselung: Sichere Algorithmen gegen das Knacken

Schwieriger zu knacken sind vollständig verschlüsselte Datenpakete. Je länger der Schlüssel ist, desto schwieriger ist es, die Daten zu knacken. Lässt sich der Dateischlüssel nicht entfernen, führt das systematische Ausprobieren aller möglichen Buchstaben- , Zahlen- und Sonderzeichenkombinationen ans Ziel. Knackprogramme attackieren die Datei bei dieser Brute-Force-Methode je nach Prozessorgeschwindigkeit mit bis zu mehreren Tausend Zeichenkombinationen pro Sekunde. Abhängig von der Komplexität des Schlüssels kann das Ausprobieren mehrere Stunden bis Tage dauern – und ein Volltreffer ist längst nicht in jedem Fall sicher. Für eine Beschleunigung beschränken Hacker die Länge des Passworts und verwenden ein Dictionary (Wörterbuch). Wörterbuchdateien mit mehreren Millionen Einträgen gibt es im Internet für alle wichtigen Landessprachen. Sie bestehen aus einer alphabetisch sortierten Liste von Namen, Bezeichnungen sowie Begriffen, die von Knackprogrammen der Reihe nach ausprobiert werden.

Gegen Knackprogramme ist kein Kraut gewachsen

Die von uns im Rahmen dieses Beitrags getesteten Passwortknackprogramme halten das, was sie versprechen. Entweder wird die mit einem Codewort geschützte Datei innerhalb weniger Augenblicke durch das gezielte Entfernen der Kennung entschützt, oder ein vorhandenes Passwort wird durch gezieltes Austesten aller Kombinationen ermittelt. Für sicherheitsbewusste Anwender bedeutet dies, dass sie sich keinesfalls ausschließlich auf die in Office-Programmen und in anderen Anwendungen eingebauten Kennwortschutzfunktionen verlassen dürfen.

Christoph Metzger ▶

OFFICE-KNACKSUITE

Advanced Office 2000 Password Recovery 1.20

System: Windows 95/98/ME, NT 4, 2000, XP
Sprache: Englisch
Preis: 60 US-Dollar (Standard Edition)
Quelle: www.elcomsoft.com (934 KB)

Das Dechiffrierpaket russischer Software-Entwickler entfernt den Passwortschutz bei fast allen Office-Dokumenten.

Das Decodierpaket beinhaltet ein gemeinsames Hauptprogramm, über das sich in der Standard-Version Passwörter in den Microsoft Office-Dokumenten von Word, Excel, Access und Microsoft Money dechiffrieren lassen. Sogar im Internet Explorer gespeicherte Zugangsdaten ließen sich mühelos auslesen. Dabei ist das Entschlüsseln sowohl für „Öffnen"-Passwörter wie auch für „Ändern"-Codes vorgesehen. In der doppelt so teuren Professional Edition bearbeitet das Utility auch die Dateitypen von Microsoft Project, Powerpoint sowie Visio und kann Windows-95/98-Backups öffnen. Nach dem Start der Software wählen Sie das gewünschte Suchverfahren – „Wörterbuch" oder „Brute-Force" – aus, grenzen auf Wunsch die Länge des Passworts ein und starten den Suchvorgang. Ein Statusbalken am unteren Fensterrand zeigt den Fortschritt der Kennwortsuche. Einmal getroffene Einstellungen speichern Sie zur späteren Verwendung in einer Projektdatei. Über die Schaltfläche „Benchmark" wird die Hackgeschwindigkeit des PCs berechnet und als Resultat in Passwörter pro Sekunde angezeigt. Je höher der Wert ist, desto kürzer ist die wahrscheinliche Knackzeit. Als besonders hartnäckig erweisen sich Office-Dokumente mit eingebetteten Visual-Basic-Projekten, die Sie über die reguläre Passwortsuche nicht herausbekommen. Für diese Fälle steht eine „VBA Backdoor" zur Verfügung.

STERNCHEN AUFDECKEN

I-Opus Passwort Decoder XP 4.02

System: Windows 95/98/ME, 2000, XP
Sprache: Deutsch
Preis: 30 Euro
Quelle: www.iopus.com (500 KB)

Dieses Tool macht Schluss mit Kennwort-Eingabefeldern, die Passwörter als Sternchen darstellen und Sicherheit vorgaukeln.

Sie haben zahlreiche Passwörter vergeben und eines davon vergessen? Mit etwas Glück verdeckt das Codewort-Eingabefenster Ihr Passwort durch Sternchen, die Sie mit I-Opus Passwort Decoder XP im Klartext anzeigen lassen können. Dazu belauscht die Software die aktuell geöffneten Anwendungsfenster und versucht, verborgene Kennwörter über den Direktzugriff auf das entsprechende Fenster auszulesen und anzuzeigen. Das Hilfsprogramm ist besonders für den Einsatz auf Web-Seiten mit Anmeldemaske geeignet, für die Sie das Passwort nicht von Hand eingeben, sondern automatisch vom Webbrowser vervollständigen lassen. Um das verdeckte Passwort anzuzeigen, starten Sie den I-Opus Passwort Decoder XP und ziehen das sichtbare Schlüsselsymbol auf das entsprechende Kennworteingabefeld Ihrer Anwendung. Anschließend ändert sich die Fensterrahmenfarbe, und kurze Zeit später zeigt I-Opus die Kennung an. Damit das Programm richtig funktioniert, müssen Sie I-Opus Passwort Decoder XP zuerst freischalten. Die Registriergebühr beträgt rund 30 Euro – das ist viel Geld für ein so einfach gestricktes Tool. Wer nicht mit Windows 2000 oder XP arbeitet, kann stattdessen zur kostenlosen Alternative Win-Dietrich 2.00 (auf Heft-CD oder Download unter **www.baxbex.de**, 143 KB) greifen. Das Tool funktioniert nach demselben Schema.

SOFTWARE FREISCHALTEN

Outlook Password 3.5

System: Windows 95/98/ME, 2000, XP
Sprache: Englisch
Preis: 35 US-Dollar
Quelle: www.soft4you.com

Das Utility deaktiviert ein einmal eingegebenes Kennwort bei geschützten Postfachdateien und Offline-Ordnern von Outlook.

In einem Informationsmanager wie Outlook sammeln sich schnell jede Menge persönlicher Daten an, die Sie besser mit einem Kennwort vor neugierigen Blicken schützen. Vergessen Sie Ihr Passwort, ist der Schaden allerdings groß, denn neben Anschriften und Telefonnummern sind auch Ihre Mails und Ihr Terminkalender weg. Mit dem Passworthilfsprogramm Outlook Password 3.5 rücken Sie kennwortgeschützten Postfachdateien (Datei-Erweiterung PST) sowie Offline-Ordnern (OST) zu Leibe und verschaffen sich wieder Zugang zu Ihren unzugänglichen Daten. Das Programm besteht im Wesentlichen aus einem Fenster, über das Sie die mit einem Passwort geschützte Outlook-Datei auswählen. Anschließend führt Outlook Password ohne weitere Benutzeraktionen eine Dechiffrierung des Passworts durch, zeigt das Ergebnis in einem weiteren Fenster an und startet auf Wunsch Outlook. Über die Tastenkombination <Strg>-<V> fügen Sie das Passwort über die Zwischenablage in das Kennworteingabefenster von Outlook ein. Auf der Internet-Seite **http://passwordnow.com** bietet der Hersteller übrigens auch ein Online-Recovery verloren gegangener Codewörter an. Dazu müssen Sie Ihre Datei auf den Server des Betreibers laden, der das Passwort rekonstruiert und Ihnen die entschützte Datei zurücksendet. Abgerechnet wird dieser Service über die Kreditkarte je nach Aufwand.

PASSWORT-KOMPLETTPAKET

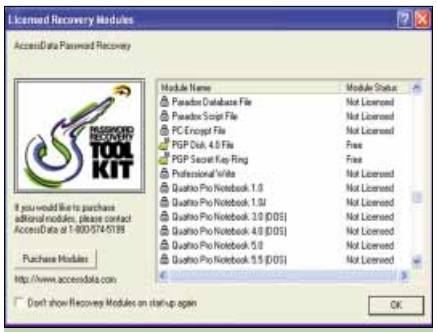
Passware Kit 5.1

System: Windows 95/98/ME, NT 4, 2000, XP
Sprache: Englisch
Preis: 395 US-Dollar
Quelle: www.lostpassword.com (7 MB)

Mehr Entschlüsselungsroutinen in einem Programmpaket bietet kein anderer Hersteller. Allerdings ist der Preis recht happig.

▸Das Passware Kit 5.1 ist eine Sammlung verschiedener Password Recovery Tools und deckt den gesamten Office-Anwendungsbereich ab, mit dem ein durchschnittlicher Anwender im gewöhnlichen Büroalltag in Berührung kommt. Das Spektrum der dechriffrierbaren Dateiformate reicht hierbei von Word, Excel, Access, Powerpoint und Outlook in den Versionen 97 bis XP bis hin zu Outlook Express, Adobe Acrobat PDF, Lotus 1-2-3, Symantec ACT, Filemaker, Lotus Organizer, Wordperfect und komprimierten ZIP. Sogar das Entschlüsseln des Betriebssystempasswords von Win NT 4, 2000 und XP ist möglich. Im Visier von Passware stehen zudem verschiedene Finanz-Software-Produkte, darunter Lexware Quicken und Quickbooks. Wenn Sie das Passwort einer Datei entfernen möchten, starten Sie das passende Knackmodul, legen den Recovery-Umfang fest und ziehen die Datei zum Start per Drag & Drop auf das Passware-Fenster. Leistung hat ihren Preis, und so schlägt das Passware Kit mit knapp 400 US-Dollar zu Buche – damit ist das Paket alles andere als ein Schnäppchen. Die Zielgruppe von Passware sind vornehmlich Unternehmenskunden. So kann eine IT-Abteilung mit Hilfe des Passware Kits denjenigen Anwendern zu Hilfe kommen, die sich nicht mehr an ein bestimmtes Kennwort erinnern, oder dort rettend eingreifen, wo ein geschasster Mitarbeiter Sabotage betrieben hat.

KENNWORT-ENTSCHLÜSSELUNG



Password Recovery Toolkit

System: Windows 95/98/ME, NT 4, 2000, XP
Sprache: Englisch
Preis: 495 US-Dollar (Standard Edition)
Quelle: www.accessdata.com

Mit dem Password Recovery Toolkit retten Sie Dokumente, bei denen Sie sich nicht mehr an das richtige Passwort erinnern können.

▸Haben Sie die Passwort-Speicherfunktion in einem Anwendungsprogramm verwendet und erinnern sich nun nicht mehr daran, mit welchem Passwort Sie Zugang bekommen? Dann können Sie die Datei schnell und einfach mit dem Password Recovery Toolkit knacken. Als Besonderheit beinhaltet Password Recovery Toolkit zwei Knack-Tools für das Verschlüsselungsprogramm Pretty Good Privacy (PGP). Sowohl „PGP Disk 4.0 Dictionary Attack“ als auch „PGP Secret Key Ring Dictionary Attack“ basieren auf der Brute-Force-Methode und probieren unentwegt alle Passwortmöglichkeiten der Reihe nach aus. Ob dieser Angriff zum Ziel führt, hängt vom Einzelfall ab – eine Garantie gibt es selbstverständlich nicht. Die Software wird in zwei unterschiedlichen Ausstattungen angeboten: Die Standard Edition des Password Recovery Toolkit kostet schon happige 495 US-Dollar und enthält alle Module außer den Knackprogrammen für Windows NT 4 und Novell Netware. Beide sind im noch teureren Password Recovery Toolkit Professional enthalten, für das Sie sage und schreibe 1200 US-Dollar investieren müssen. Das Programm selbst ist mit einer Dongle-Diskette kopiergeschützt, die beim Programmstart im Laufwerk liegen muss, anderenfalls arbeitet Password Recovery Toolkit nur im Demomodus. Preis und Module zielen eindeutig auf den Einsatz in Firmenumgebungen.

ARCHIVDATEIEN ÖFFNEN

Visual Zip Password Recovery Processor

System: Windows 95/98/ME, NT 4, 2000, XP
Sprache: Englisch
Preis: 30 US-Dollar
Quelle: www.alpinesnow.com

Bei ZIP-Dateien klappt das Entfernen eines Passworts durch Ausprobieren mit Visual Zip Password Recovery Processor nicht immer.

▸Visual Zip Password Recovery Processor versucht, mit einem Codewort geschützte ZIP-Archivdateien durch systematisches Ausprobieren aller möglichen Buchstaben- und Zahlenkombinationen (Brute Force) zu entschlüsseln. Die Software-Schmiede Alpine Snow bietet ein buntes Portfolio an Knackprogrammen an und hat die beim Überlisten von Passwortschutzverfahren gesammelten Erfahrungen in das Tool einfließen lassen. So versucht eine Heuristikfunktion, den erforderlichen Zeitaufwand für das Entschlüsseln zu reduzieren. Eine integrierte Statistik zeigt die Anzahl der bisher durchgeführten Entschlüsselungsversuche und die Geschwindigkeit, mit der das Tool arbeitet, in Kennwortkombinationen je Sekunde. Um weiter Zeit zu sparen, geben Sie eine minimale und maximale Kennwortlänge vor. Für einen Aufpreis von 20 Dollar bietet der Hersteller eine umfangreiche Wortliste mit rund 4,5 Millionen Begriffen an, die aus den Bereichen Namen, Filmtitel, Fremdwörter, Fachbegriffe, öffentliche Plätze und so weiter stammen und aus über 20 unterschiedlichen Sprachen zusammengetragen wurden. Damit ist die Wortliste die ideale Basis für Kennwortrecherchen über die Brute-Force-Attacke. Die Liste können Sie übrigens auch mit beliebigen anderen Recovery-Programmen benutzen, die mit reinen Textdateien umgehen können. ■

Vorbeugen durch Datensicherung

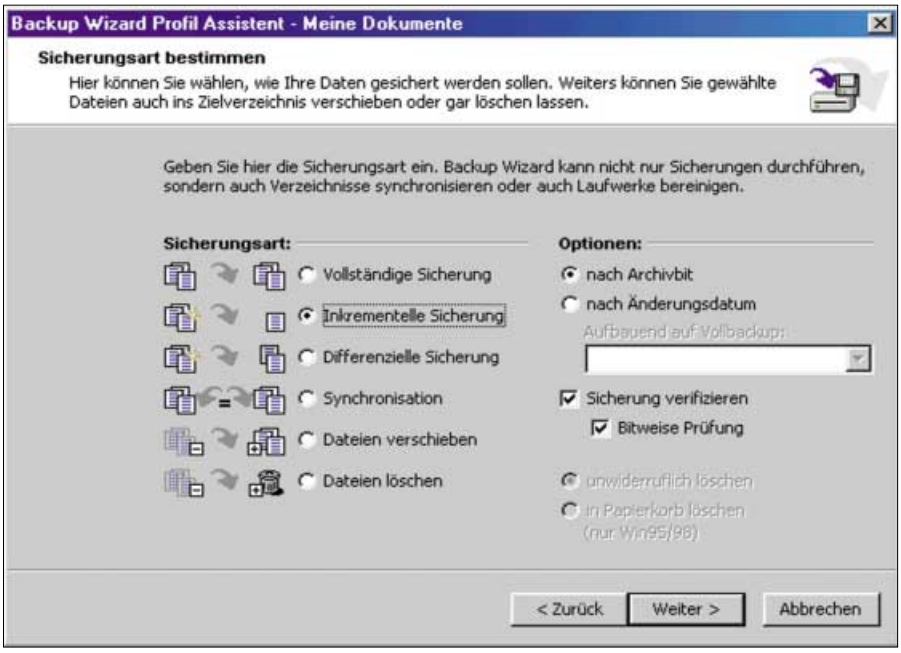
Vorsorgemaßnahmen

Wer seine Daten regelmäßig sichert, steht im Falle einer Hackerattacke oder eines Defekts auf der sicheren Seite. Einfach die Sicherungskopie einspielen und weiterarbeiten.

▸Bereits ein voreiliger Programmaufruf eines aus dem Internet geladenen, angeblich bahnbrechenden Tools kann ausreichen, um einen Trojaner zu starten und wichtige Dateien wie Steuererklärung, Dissertation oder Rechnungskopien ins Daten-Nirwana zu katapultieren. Und obwohl sich jeder PC-Besitzer über die latent im Hintergrund lauernde Gefahr bewusst ist, kommt auf kaum einem privat genutzten Rechner ein reines Backup-Programm zum Einsatz.

Denn während Festplattenkloner wie Drive Image und Norton Ghost inzwischen zur Grundausstattung aller ambitionierten und sicherheitsbewussten Anwender gehören, fristen Backup-Utilities nach wie vor ein Schattendasein. Die meisten PC-Benutzer handeln hier immer noch nach der Devise, „mir passiert so etwas bestimmt nicht“. Und das, obwohl jeder Anwender vertrauliche und wichtige Daten auf seinem PC ablegt.

Doch ist der Datenverlust erst einmal eingetreten – sei es durch einen Festplattendefekt oder einen zerstörerischen Virus – ist guter Rat im wahrsten Sinne des Wortes teuer. Schließlich lassen sich die verlorenen Daten nur noch mit speziellen Wiederherstellungs-Tools wie beispielsweise Ontrack Easy Recovery für Windows 95/98/ME, NT 4, 2000 und XP (**www.ontrack.de/easyrecovery/professionaledition.asp**, 199 Euro, Testversion ◉ auf Heft-CD) retten und restaurieren.



Qual der Wahl: Je mehr unterschiedliche Sicherungsarten ein Backup-Programm (hier: Backup Wizard 2000) anbietet, desto besser und einfacher lassen sich sensible Daten in regelmäßigen Abständen sichern

Dabei ist die Auswahl an Backup-Software in allen Preislagen sehr groß. Der Unterschied zwischen Tools aus der Free- und Shareware-Ecke und Vollpreisprodukten lässt sich an drei Kriterien festmachen. So beschränken sich die günstigen Lösungen im Allgemeinen auf die Sicherung unter den Consumer-Betriebssystemen Win 95/98/ME – respektive den Dateisystemen FAT16 und FAT32, die Auswahl der Sicherungsmedien ist eingeschränkt, und auch in Sachen Administration stehen nicht allzu viele Optionen bereit. Doch dafür sind die einfach gestrickten Lösungen weitaus intuitiver zu bedienen – ein nicht zu unterschätzender Vorteil für den Privatanwender.

Info: Daten-Backup

Obwohl die regelmäßige Datensicherung zu den wichtigsten Schutzmaßnahmen gehört, setzt kaum ein Anwender ein effizientes Backup-Tool ein. Dabei bieten nahezu alle modernen Programme eine Vielzahl benutzerfreundlicher Optionen und intelligenter Funktionen, mit denen Sicherung und Wiederherstellung sensitiver Dateien problemlos und schnell von der Hand gehen.

Diese Kriterien zeichnen das ideale Backup-Tool aus

Gerade weil sich in der Share- und Freeware-Szene so viele Backup-Programme tummeln, fällt die Auswahl nicht unbedingt leicht. Erschwerend kommt hinzu, dass sich viele Anwender nicht unbedingt darüber im Klaren sind, worauf es bei einer Datensicherungs-Software eigentlich ankommt. Um Ihnen die Auswahl zu erleichtern, sagen wir Ihnen, welche Funktionen und Features wirklich wichtig sind.

Die ideale Backup-Software verfügt über Assistenten, die Schritt für Schritt durch den Einrichtungsvorgang führen und diese einmal festgelegten Rahmenbedingungen als immer wieder zu verwendende Profile speichern. Von Vorteil ist es, wenn bereits einige solcher Profile zum Sichern von Standardverzeichnissen

(Windows, Eigene Dateien, Favoriten) und typischer Software wie Outlook Express mit dabei sind.

Wünschenswert ist es auch, dass Funktionen des Backup-Programms im Windows-Explorer über das Kontextmenü der rechten Maustaste zu erreichen sind, da dies das Sichern bestimmter Dateien um ein Vielfaches erleichtert.

Beim Durchführen des eigentlichen Backups müssen die drei Varianten vollständig, inkrementell (es werden nur diejenigen Dateien gesichert, die seit dem letzten Backup verändert wurden) und differenziell (Backup der Dateien, die seit der letzten vollständigen Sicherung geändert wurden) zur Auswahl stehen, damit jeder Anwender seine eigene Backup-Strategie realisieren kann.

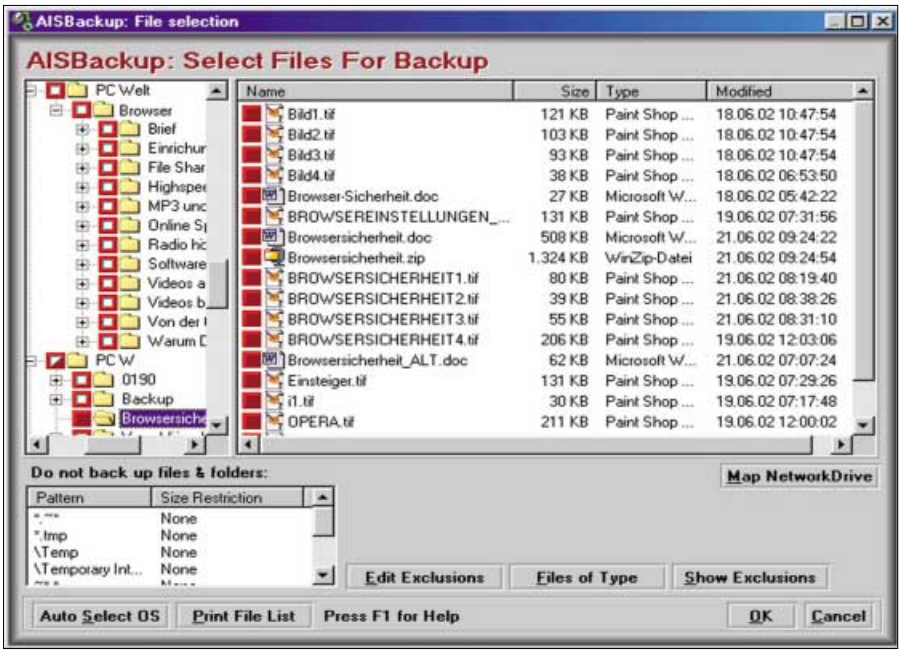
Ein Zeitplaner zur automatischen Datensicherung ist ebenso unumgänglich, wie Verifizierung, Verschlüsselung, Komprimierung und Passwortschutz des gesicherten Archivs. Ähnliches gilt auch für die Wahl des Sicherungsmediums: Je mehr Datenträger unterstützt werden desto besser. Denn selbst wenn Sie nicht über Netzlaufwerke, Zip- und Jaz-Wechselmedien oder gar einen DVD-Recorder verfügen, sind Sie mit einem Programm, das diese Medien bereits unterstützt, für die Zukunft gerüstet.

Die wichtigsten kostenlosen oder als Shareware vertriebenen Backup-Tools stellen wir Ihnen im folgenden vor; über vier leistungsfähige Profi-Lösungen informieren wir Sie im Kasten „Kommerzielle Backup-Lösungen: Darf's auch etwas mehr sein?“ auf ▷ Seite 40.

Ais Backup 1.0.5.137

Das englischsprachige Ais Backup 1.0.5.137 für Windows 95/98/ME (2,7 MB, **www.aiscl.co.uk**, Registriergebühr: 30 US-Dollar, ◉ auf Heft-CD) schreibt gesicherte Dateien auf USB- und Firewire-Festplatten, Netzlaufwerke und Wechselmedien vom Typ Zip- und Jaz-Drive sowie DVD-RAM; Bandlaufwerke werden hingegen nicht unterstützt.

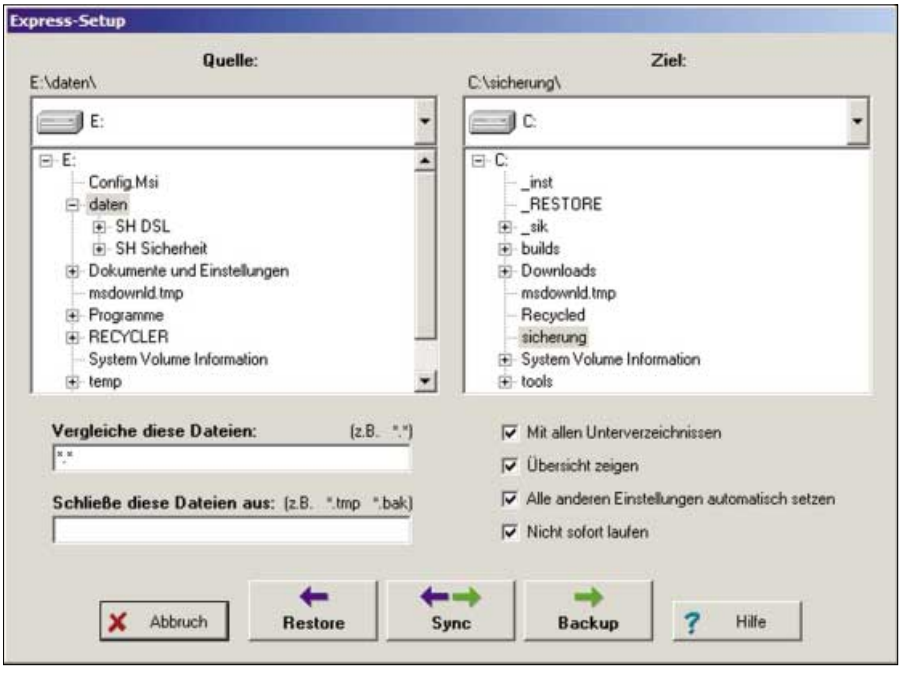
Nach dem ersten Programmstart wird der Anwender von einem Assistenten durch die grundlegenden Konfigurationsschritte wie beispielsweise Auswahl der Backup-Verzeichnisse und des CD-Brenners sowie Art des Backups (Sicherung von Daten oder Systemdateien) geführt. Sehr gut: Sie können an dieser Stelle auch festlegen, ob besonders große Dateien (zwischen 25 und 500 MB) während der Sicherung automatisch komprimiert werden sollen. Die Definition der Backup-Parameter (Ziellaufwerk, Kompressionsrate und Passwortschutz) ist überaus intuitiv, da Sie die nötigen Rahmenbedingungen mit Hilfe des integrierten Script-Managers festlegen. Optional zur Sicherung eigener Inhalte können Sie ein Backup auch um alle Windows-Dateien erweitern. Beim Anlegen einer Sicherung steht es Ihnen offen, bereits vorhandene Backups zu überschreiben oder mehrere Versionen anzulegen.



Volle Kontrolle: Ais Backup ermöglicht nicht nur die exakte Auswahl der zu sichernden Komponenten, sondern erlaubt auch den Ausschluss bestimmter Dateien und Ordner von der Sicherung

Backer 5.04

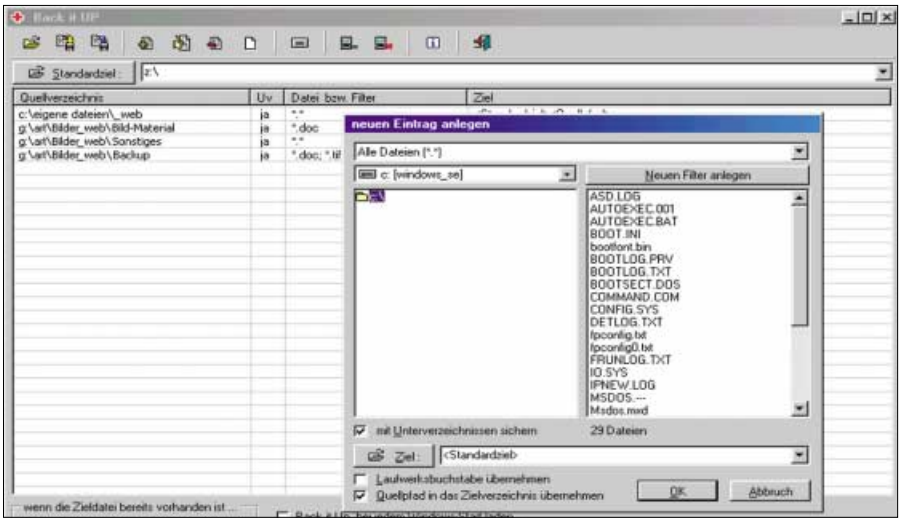
Unter der schlicht gehaltenen Benutzerführung von Backer 5.04 für Windows 98/ME, NT 4, 2000 und XP (◉ auf Heft-CD und unter **www.leanware.de**, 1,56 MB, Registriergebühr: 35 Euro) steckt eine leis-



Schnelle Sicherung: Bei der deutschsprachigen Shareware Backer können Anwender ohne lange Konfiguration Daten von einem Laufwerk auf ein anderes Medium sichern, das von Windows unterstützt wird

tungsfähige Backup-Software. Dabei unterstützt das Tool nicht nur die Sicherung von Dateien, sondern bietet auch Zusatzfunktionen wie Transfer, Archivierung und Synchronisation. Letztere erfolgt entweder mit Hilfe einer PC-Direktverbindung per Kabel, über die Irda-Schnittstelle oder eine DFÜ-Verbindung.

Bei der Datensicherung stehen Ihnen zwei Wege offen. Minimalen Arbeitsaufwand bietet das Express-Setup, bei dem vor dem Start lediglich die wichtigsten Parameter (Quell- und Ziellaufwerk, Dateimaske und Unterverzeichnisse) vorgegeben werden. Ein wenig diffiziler gestaltet sich die traditionelle Datenspiegelung. Denn hier legen Sie nicht nur die typischen Einstellungen fest, sondern können darüber hinaus auch Profi-Features wie etwa das Kürzen von Pfadbezeichnungen und den automatischen Aufruf des Programms per Zeitplaner aktivieren. Als Sicherungsmedien können alle vom Windows-System angesprochenen Laufwerke genutzt werden.



Einfache Handhabung: Back it up bietet zwar kaum weiterführende Optionen, ist dafür aber auch von Gelegenheitsanwendern binnen weniger Minuten zu bedienen

Back it up 1.23b

Die deutschsprachige Freeware Back it up 1.23b für Windows 95/98/ME, NT 4, 2000 und XP (239 KB, **www.squint.de/backitup.htm** und ◉ auf Heft-CD) ist das ideale Programm für all jene PC-Besitzer, die noch keinerlei Erfahrungen mit Datensicherung haben und deswegen auf der Suche nach einem einfach zu bedienenden Tool sind. Dementsprechend beschränken sich die Benutzereingriffe auf die

Kommerzielle Backup-Lösungen: Darf's auch etwas mehr sein?

Profi-Anwender, denen der Funktionsumfang der vorgestellten Share- und Freeware-Tools nicht ausreicht, müssen zu einer kommerziellen Software greifen. Allerdings sind Programme wie beispielsweise Retrospect Desktop Backup 5.6, Bright Stor Arc Serve 2000 Backup und Veritas Backup Exec 8.6 nicht nur äußerst komplex handzuhaben, sondern auch ungemein teuer. Somit ist der Einsatz dieser hochpreisigen Produkte eigentlich nur denjenigen Nutzern zu empfehlen, bei denen ein Datenverlust zu gravierenden finanziellen Einbußen führen würde. Zudem werden nahezu ausschließlich die Server-Betriebssysteme Windows NT 4/2000 sowie Novell Netware und Linux unterstützt.

Bright Stor Arc Serve 2000 Backup

Wie nahezu alle Profi-Lösungen wird auch dieses Backup-Werkzeug (**www.ca.com/arcserve/replace/**, rund 500 Euro) in mehreren Varianten angeboten. Ob Lotus Notes unter Windows NT, mit Raid-Unterstützung oder Open-File-Directories unter Novell Netware – mit dieser zentral zu administrierenden Datensicherung schützen besonders mittelständische Unternehmen ihre Daten.

Nova Backup Workstation 6.6

Die Workstation-Version des vor allem in den USA sehr populären Backup-Programms (**www.no-panic.com/backup/n_backup.html**, rund 55 US-Dollar) bietet ein ausgezeichnetes Preis-Leistungs-Verhältnis und ist somit auch für Heimanwender interessant. Die Spanne der unterstützten Sicherungsmedien umfasst Bandlaufwerke, CDs und DVDs und alle Arten von IDE- und SCSI-Festplatten.

Retrospect Desktop Backup 5.6

Als eines von wenigen Spezial-Tools arbeitet das Programm (**www.dantz.com**, rund 230 Euro) nicht nur unter Windows NT 4 Workstation, 2000 Professional und XP, sondern unterstützt auch Windows 95/98/ME und sogar angeschlossene Macintosh-Rechner. Als Sicherungsmedien können lokale Festplatten, Streamer, Wechselmedien wie Zip- und Jaz-Laufwerke und alle Varianten von CDs und DVDs verwendet werden.

Für Unternehmen und kleinere Büros geeignet: Veritas Backup Exec 8.6 bietet perfekte Einblicke in die interne Struktur der jeweiligen Datensicherungsaufgaben

Veritas Backup Exec 8.6

Der Klassiker unter den Profi-Backup-Programmen (**www.veritas.com/de/produkte/backup/**, rund 560 Euro) verrichtet seinen Dienst in lokalen Netzwerken und Remote-Systemen, die auf Windows NT 4 oder 2000 aufsetzen. Darüber hinaus stehen auch Speziallösungen für SQL-, Exchange- und Oracle-Server, Novell Netware und sogar SAP R/3-Umgebungen zur Verfügung.

Vorgabe von Quelldateien und Zielverzeichnis, den Umgang mit gleichnamigen Dateien sowie den automatischen Aufruf des Programms beim Windows-Start. Falls die Gesamtgröße der zu sichernden Dateien die Kapazität des Zielmediums übersteigt, kann die Sicherung auf mehrere Datenträger aufgeteilt werden.

Die Sicherungen werden entweder auf Festplatte (sowohl lokal als auch Netzlaufwerk), Zip-Laufwerk oder CD geschrieben. Bei letzterer Methode ist aber zu beachten, dass Sie eine zusätzliche Packet-Writing-Software (zum Beispiel Packet CD, Direct CD oder In CD) benötigen, damit die Rohlinge nach dem UDF-Verfahren beschrieben werden können.

Backup Wizard 2000

Backup Wizard 2000 für Windows 95/98, NT 4 und 2000 (**www.enovative.net/backup.html** und ◉ auf Heft-CD, Registriergebühr: 25 Euro) setzt bei der Datensicherung auf das Profil-Prinzip. Für den Anwender hat das den Vorteil, dass er beim Backup eine weitaus größere Kontrolle über die zu sichernden Dateien erhält. So können Sie das Programm beispielsweise mit wenigen Mausklicks dazu veranlassen, alle Word-Dateien in einem Verzeichnis und alle Excel-Tabellen in einem anderen Ordner zu speichern. Bei der Generierung dieser Profile kommt ein Assistent zum Einsatz, der Sie durch den kompletten Konfigurationsprozess begleitet.

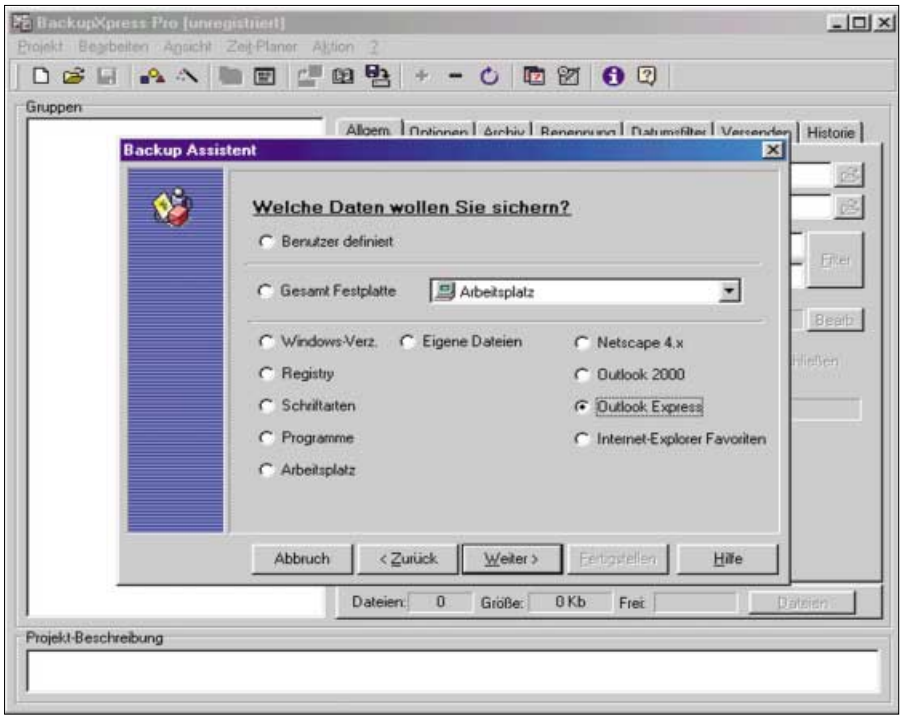
Falls Ihnen die Grundfunktionen des Programms ausreichen, genügt das Deaktivieren der Option „Fortgeschrittene Einstellungen anzeigen“, um die Profil-Einrichtung um ein Vielfaches zu vereinfachen. Im Gegenzug müssen Sie aber auf wichtige Funktionen wie zum Beispiel eine bitweise Verifizierung der Sicherungsdatei, das automatische Einloggen auf einem Netzlaufwerk oder die zusätzliche Datenverschlüsselung verzichten.

Für die Sicherung werden lokale und über das Netzwerk ansteuerbare Laufwerke, Wechselmedien (Jaz, Zip und LS120) sowie CD-R- und CD-RW-Laufwerke mit Packet-Treibern akzeptiert.

Back to Zip 4.10

Als auf die Wünsche von Einsteigern zugeschnittenes Tool beschränkt sich Back to Zip 4.10 für Win 95/98/ME, 2000 und XP (584 KB, ◉ auf Heft-CD, **www.onlinetimer.de/btz.html**, Registriergebühr: 10 Euro) auf die wichtigsten Funktionen. Dazu gehören die zeitgesteuerte Datensicherung (unter Zuhilfenahme des Windows-eigenen Taskplaners), die Dateiauswahl mittels des Archiv-Attributs oder des Änderungsdatums und die Vorgabe einer optionalen Kompressionsrate. Weiterführende Funktionen sind der Passwortschutz, das Verteilen einer Sicherung auf mehrere Volumes, die Erzeugung selbstextrahierender Datei-Archive sowie das Ausschließen bestimmter Dateitypen. Gut: Einmal getroffene Einstellungen lassen sich in einem Sicherungsprofil speichern.

Die so zusammengestellten und archivierten Daten werden dann mit nur einem Mausklick auf das ausgewählte Sicherungsmedium (alle vom Windows-Explorer angezeigten Laufwerke werden unterstützt) geschrieben, wobei als Dateiname auf Wunsch auch Datum und Uhrzeit der Sicherung verwendet werden dürfen.



Vorbildliche Benutzerführung: In Sachen Anwenderfreundlichkeit und Komfort gehört Backup Xpress Pro zu den mit Abstand besten Hilfsprogrammen der Free- und Shareware-Szene

Backup Xpress Pro 2.72

Nach dem Programmstart von Backup Xpress Pro 2.72 für Windows 95/98/ME (1,70 MB, **www.xpertdesign.de** und ◉ auf Heft-CD, Registriergebühr: 29 Euro) werden Sie von einem Assistenten empfangen, der Sie beim Anlegen eines Projekts unterstützt. Sehr hilfreich: Wie beim bereits vorgestellten Backup Wizard 2000 können Sie sich auch hier zwischen dem Einsteiger- und dem Fortgeschrittenen-Backup entscheiden. Wer sich für die einfache Variante entscheidet, muss die gewünschten Datensicherungsparameter (Quelldateien, Zielpfad, Dateifilter) durch Eingaben auf sechs Registerkarten definieren; eine Auswahl häufig durchgeführter Spezial-Backups wie beispielsweise Sicherung des Windows-Verzeichnisses, der Registry oder von Outlook Express stehen ebenfalls zur Verfügung.

Fortgeschrittenen Nutzern stehen zusätzliche Einstellungen wie die exakte Wahl der Backup-Methode (vollständig, inkrementell oder differenziell), und der Kompressionsmethode sowie die Überprüfung der Daten nach der Sicherung und eine Verschlüsselung zur Verfügung. Die so erzeugten Archive werden dann entweder auf lokalen Festplatten, Netzlaufwerken und Wechselmedien gesichert oder per Internet-Verbindung auf einen FTP-Server übertragen. Ein weiteres Plus ist die nahtlose Einbindung in das Windows-Explorer-Kontextmenü der rechten Maustaste. So reicht ein Klick im Explorer aus, um die Funktion „Quick Copy“ aufzurufen und die Daten schnell und einfach zu sichern. ▶

DS-Backup 1.7

DS-Backup 1.7 (1 MB, ◉ auf Heft-CD und unter **www.ds-software.de/backupd.htm**, Registriergebühr: 25 Euro für Privatanwender, 75 Euro für gewerbliche Kunden) unterstützt zwar nur die Betriebssysteme Windows 95/98 und NT 4, bietet im Gegenzug aber ein breit gefächertes Funktionsspektrum an, das sogar semiprofessionellen Ansprüchen genügt. Angefangen bei der Option, zeitgesteuerte Backups anzulegen, über die Datei-Auswahl mittels Wildcards bis hin zur optionalen Komprimierung der zur Sicherung ausgewählten Dateien – das kleine Backup-Tool überzeugt auf ganzer Linie.

Die Auswahl der vom Programm unterstützten Backup-Medien ist ebenfalls bemerkenswert, da neben den üblichen Medien (Diskette, Festplatte und Netzlaufwerke) auch SCSI-Bandlaufwerke, FTP-Server und Wechsellaufwerke vom Typ Zip, Jaz und sogar Syquest angesprochen werden. Und damit sowohl Konsistenz als auch Sicherheit der gespiegelten Daten jederzeit gewährleistet sind, setzt das Tool auf die Kombination aus speziellem Prüfmechanismus und Verschlüsselung mit Hilfe des bewährten Blowfish-Algorithmus.

Optionsvielfalt: Hinter der etwas verspielt wirkenden Bedienerführung von DS-Backup verbergen sich viele sinnvolle Funktionen, mit denen sich etwa eine Datensicherung komprimieren oder verschlüsseln lässt

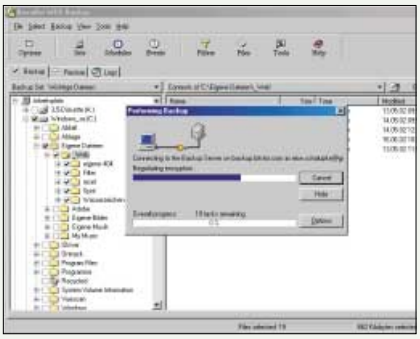
Einzige Einschränkung: Wie schon bei Back it up 1.23b müssen Sie auch bei diesem Programm zusätzlich ein spezielles Packet-Writing-Programm einsetzen, um die zu sichernden Dateien nach dem UDF-Standard auf eine CD brennen zu können.

Genie Backup Manager 1.1

Der Genie Backup Manager 1.1 für Windows 98/ME, 2000 und XP (1,81 MB, Download unter **www.genie-soft.com/default.html** und ◉ auf Heft-CD, Registriergebühr: 49,95 Dollar) setzt auf eine aufgeräumt

Online-Backup: Datensicherung im Web

Was in den USA bereits seit Jahren von diversen Unternehmen wie beispielsweise Nova Stor (**http://services.online-backup.com/overview.asp**, 17,95 US-Dollar monatlich), Virtual Backup (**www.virtualbackup.com/indexseg.html**, ab 40 US-Dollar pro Jahr) und Bitstor (**www.bitstor.com/main_bitstor.html**) angeboten und verstärkt auch von Privatpersonen genutzt wird, steckt hier zu Lande immer noch in den Kinderschuhen. Die Rede ist von Online-Backups, also der Datensicherung im Web.



Web-Server als Backup-Medien: In den USA auch für Privatanwender bereits gang und gäbe

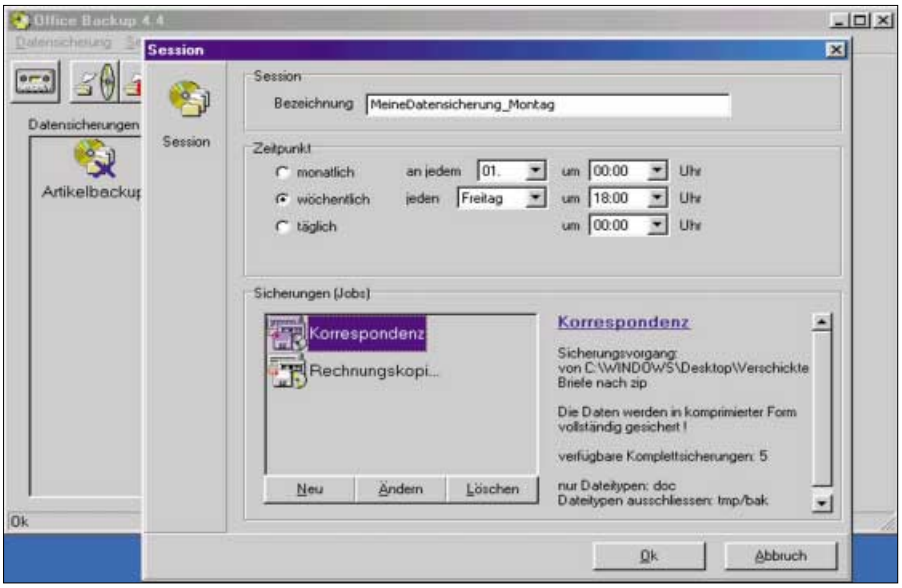
Das Funktionsprinzip ist dabei ebenso einfach wie intelligent: Anstatt die lokalen Speichermedien (Festplatte, CD oder Wechsellaufwerk) als Backup-Medium zu verwenden, werden die Daten über eine standardmäßige Online-Verbindung auf den Hochsicherheits-Server des Anbieters übertragen. Die Vorteile für den Anwender liegen auf der Hand: Es muss kein teures Spezialprogramm erworben werden, Anschaffung und Konfiguration spezieller Sicherungsmedien entfallen und da die gespiegelten Daten nicht lokal abgelegt sind, lassen sich diese selbst im Extremfall (etwa bei Diebstahl oder Wohnungsbrand) problemlos wiederherstellen.

Allerdings ist diese Methode auch mit einer unübersehbaren Schwäche behaftet. Denn während bei lokal durchgeführten Backups die Größe der Sicherungsdateien nur durch die Kapazität des Speichermediums (auf eine DVD passen immerhin 4,7 GB) begrenzt ist, stößt man bei Online-Backups schnell an die Grenze des Unzumutbaren. Selbst mit einer schnellen Internet-Anbindung, wie Sie etwa Q-DSL Home (Upstream 256 kbps, effektiv also 32 KB/s) zur Verfügung stellt, dauert der Upload von 700 MB (die Kapazität der gängigen CDs) mehr als sechs Stunden.

Somit ist diese Art der Datensicherung eigentlich nur denjenigen Anwendern zu empfehlen, die einerseits über eine schnelle Internet-Anbindung via DSL oder Standleitung verfügen und andererseits nur die allerwichtigsten Daten auf einem Remote-Server sichern wollen. Als mehr als gute Alternative empfiehlt sich hier der Kauf eines gebrauchten Rechners, der als Teil des lokalen Netzwerks ausschließlich für Backup-Zwecke verwendet wird.

wirkende Bedienerführung, die Ihnen nach dem Programmstart die drei Optionen „Backup Now“, „Restore Now“ und „Schedule Backup“ bereitstellt. Sowohl bei der Definition eines als „Backup Job“ bezeichneten Projekts als auch bei der Wiederherstellung einer Sicherung kommt ein Assistent zum Einsatz, der die wichtigsten Parameter abfragt.

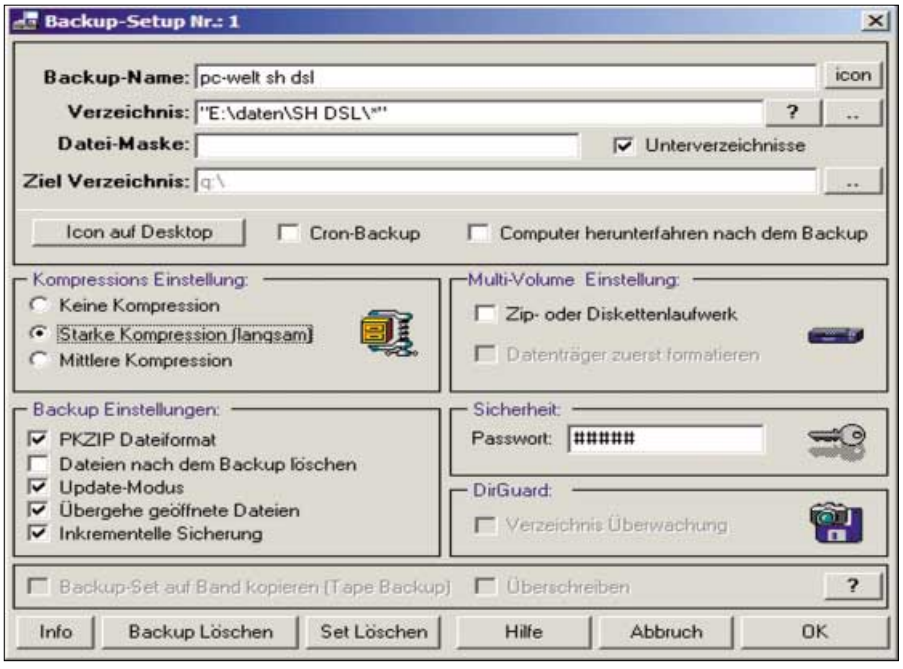
Ob Auswahl des Sicherungsmediums (Festplatten und Netzlaufwerke, Wechselmedien und CD), Art des Backups (vollständig, inkrementell und gespiegelt) oder Kompressionsstufe – die wichtigsten Funktionen sind implementiert. Darüber hinaus steht eine ganze Reihe bereits vorgefertigter Backup-Profile bereit, mit denen Sie typische Standardaufgaben wie die Sicherung von Outlook (sowohl Version 2000 als auch XP), der Favoriten und des Fontverzeichnisses bequem durchführen können.



Intelligentes Funktionsprinzip: Bei Office Backup können mehrere Sicherungsaufgaben zu einem Backup-Profil zusammengefasst und automatisch ausgeführt werden

Office Backup 4.4

Auch wenn es die Programmbezeichnung vermuten lässt, beschränkt sich der Funktionsumfang von Office Backup 4.4 für Windows 95/98/ME (3,21 MB, auf Heft-CD, **www.gwdedv.de/office_backup.html**, Registriergebühr: 25 Euro) nicht auf die Sicherung von Microsofts Büro-Komplettpaket. Vielmehr handelt es sich bei diesem Tool um ein ungemein leistungsfähiges Programm, das sich in erster Linie an den fortgeschrittenen Anwender richtet, der volle Kontrolle über die zu sichernden Dateien erhalten will und dafür auf Assistenten verzichten kann. Das zugrunde liegende Funktionsprinzip dreht sich um so genannte „Sessions“ (Backup-Profile), die jeweils mehrere „Jobs“ (Datensicherungsaufgaben) umfassen können. Somit ist es beispielsweise problemlos möglich, unterschiedliche Sicherungsaufgaben zu einem einzigen Profil zusammenzufassen. Das sorgt für Übersicht. Die Konfiguration der jeweiligen „Jobs“ ist allerdings nicht ganz einfach, da das entsprechende Dialogfeld recht schlicht gehalten ist. Dies ändert aber nichts an der Tatsache, dass alle wichtigen Optionen wie die Wahl der auszuschließenden Dateitypen, der Backup-Methode (vollständig oder inkrementell) und der Anzahl der verfügbaren Komplettsicherungen angeboten werden.



Alle Funktionen im Blick: ZD Backup lässt sich dank vorbildlicher Bedienerführung einfach handhaben und eignet sich daher vor allem für Einsteiger, zumal das Programm kostenlos ist

ZD Backup 1.13

Die Freeware für Windows 95/98, NT 4, 2000 und XP (3,41 MB, **www.point2click.de/zback.htm** und auf Heft-CD) unterstützt bis zu 20 Backup-Profile, die aus Gründen der Übersichtlichkeit mit speziellen Icons gekennzeichnet werden können. Auf Seiten der Optionen stehen Kompressionseinstellung, inkrementelle Sicherung, Passwortschutz sowie ein automatisches Löschen nach erfolgtem Backup zur Verfügung. Alle vom Programm durchgeführten Tätigkeiten werden zudem in einer speziellen Protokolldatei gespeichert.

Die so zusammengestellten Sicherungen können auf allen im Windows-Explorer aufgelisteten Laufwerken eingespielt werden. Handelt es sich dabei um Wechsellaufwerke, teilt das Tool die Backup-Datei automatisch in passende Häppchen auf. Wichtiger Hinweis: Um Daten auch auf SCSI-QIC-Streamern von Wangtek oder Tandberg zu sichern, wird das Gratis-Zusatz-Tool Z-Tape Dump 1.06 für Win 98, NT 4 und 2000 (2,6 MB, unter **www.point2click.de/ztape.htm**) benötigt.

Stefan Forster

Windows mit Bordmitteln absichern

Endlich sicher sein

Sie schützen Ihren PC mit diversen Passwörtern für Bios, Bildschirmschoner und Freigaben? Die vermeintliche Sicherheit ist in Sekunden dahin. Lesen Sie, auf was Sie achten müssen.

▸Wer nicht gerade im stillen Kämmerlein mit seinem Windows-PC arbeitet, ist allerlei Gefahren ausgesetzt: Büro-PCs können von den Kollegen ausspioniert werden, und auch die Daten auf der Festplatte sind alles andere als sicher. Da helfen auch keine Passwörter, denn diese sind im Handumdrehen geknackt. In Netzwerken ist es noch viel gefährlicher. Wer kennt denn nicht die Versuchung, mal einen Blick auf die freigegebenen Verzeichnisse des Kollegen zu werfen? Mit schnellen PCs lassen sich ganze Netzwerke in Rekordzeit scannen und die Passwörter im Schnelldurchgang entschlüsseln, sofern es sich um Windows-9x/ME-Rechner handelt. In Netzen mit geringer Sicherheit finden auch Trojaner und Viren schnell ein Zuhause. Die meisten Tricks, Hacks und Attacken auf fremde PCs funktionieren im LAN am besten, viele allerdings auch über das Internet. Sie können sich aber davor schützen. Dieser Beitrag beschreibt eine Vielzahl von Löchern in Windows-Systemen und zeigt, wie Sie diese erkennt und abdichten. Zahlreiche Tools helfen dabei, Sicherheitsprobleme aufzudecken, allerdings lässt sich damit auch Unfug treiben. Wer hat es schon gern, wenn seine Passwörter in der Firma per Schnüffel-Software ausgespäht werden? Jedoch: Das Wissen um diese Lücken sollte dazu führen, sich besser schützen zu können, um schließlich ein möglichst sicheres Windows einzurichten. So sicher, wie es nun mal geht. Dabei geht es in der Hauptsache um Windows 98, 98 SE und Windows ME, da diese Systeme derzeit noch am weitesten verbreitet sind. Zu Windows 2000 und XP finden sich aber auch einige Hinweise.

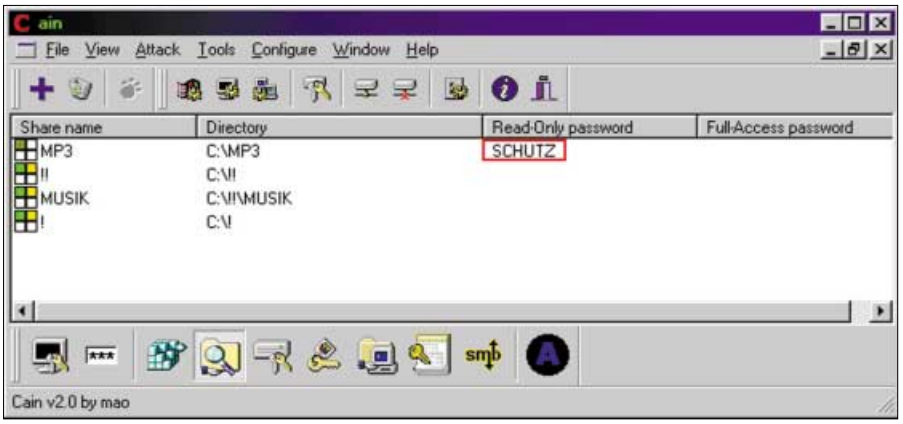
Info: Windows-Schutz

Hat ein Hacker die ersten Hürden genommen und ist in Windows eingedrungen, dann stehen ihm quasi alle Türen offen. Oftmals erleichtern unsichere Passwörter, fehlerhafte Einstellungen und Unwissenheit der Anwender die Einbrüche.

Bios-Passwörter: Listen kursieren im Internet

Eine einfache Art, seinen PC vor der Nutzung durch Unbefugte zu schützen, besteht in der Verwendung eines Bios-Passworts. Alle Bios-Hersteller bieten diese Möglichkeit. Wird nach dem Einschalten des PCs nicht das richtige Kennwort eingegeben, geht es nicht mehr weiter. Im Prinzip eine gute Methode, könnte man denken. Leider ist sie durch Tüftler in den letzten Jahren zunehmend unsicherer ge-

worden. Die Bios-Hersteller haben Standard-Passwörter eingebaut, die beispielsweise zu Wartungszwecken benötigt werden. Durch Probieren sind im Laufe der Zeit immer mehr Passwörter gefunden und im Internet veröffentlicht worden. Wer so ein Standard-Passwort kennt, kann sich damit unbemerkt Zutritt zum PC verschaffen. Im Internet finden sich zahllose Listen mit Bios-Kennwörtern. Übrigens betrifft das nicht nur Bios-Passwörter, auch Netzwerk-Switches und -Router sind betroffen.



Passwortknacker deluxe: Die Software Cain 2.0 knackt verschiedene Windows-Passwörter auf Knopfdruck – so etwa auch Kennwörter, die im Cache eines Windows-95/98-Systems abgelegt sind

Autostart: Ausführen feindlicher Programme verhindern

Eine der größten Bedrohungen geht von Backdoor-Programmen aus. Diese erlauben – einmal installiert – die Fernsteuerung eines PCs über das lokale Netz oder das Internet. Die meisten Adressabfragen, die von Intrusion-Detection-Systemen und Personal Firewalls erkannt werden, sind Trojaner-Pings – die Backdoor SubSeven ist am meisten verbreitet. Jeder Trojaner muss irgendwie aktiviert werden, um seine Arbeit zu verrichten, am besten beim Start des Betriebssystems. Die einfachste Art, ein Programm unter Windows automatisch zu starten, besteht darin, es in den Autostart-Ordner zu kopieren. Per Voreinstellung ist der Autostart-Ordner in C:\Windows\Startmenü\Programme\Autostart gespeichert. Dies lässt sich aber über einen Eingriff in die Windows-Registry ändern. Im Schlüssel „Hkey_Current_User\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders“ gibt der Wert „Startup“ den Pfad zum Autostart-Ordner an. Der Pfad lässt sich somit leicht ändern. Solche selbständig startenden Programme sind leicht erkennbar. Auch über die noch aus Windows-3.x-Tagen bekannten INI-Dateien lassen sich Programme ausführen. So können im Abschnitt „[windows]“ der WIN.INI am Anfang der Datei ebenso selbständigstartende Programme eingetragen werden:

```
[windows]
load=<Programm.exe>
run=<Programm.exe>
```

In der SYSTEM.INI sorgt die Zeile „shell=Explorer.exe c:\windows\notepad.exe c:\autoexec.bat” im Abschnitt „[boot]“ ebenfalls für das automatische Ausführen einer Software beim Windows-Start. In diesem Beispiel wird Notepad gestartet. Auch die AUTOEXEC.BAT lässt sich benutzen, allerdings wird diese Datei nur beim Öffnen einer DOS-Box abgearbeitet. Besser geeignet ist WINSTART.BAT im Windows-Ordner, eine ganz normale Batch-Datei, die vor dem Starten von Windows ausgeführt wird. Alle diese Methoden sind leicht erkennbar. Anders verhält es sich mit Autostart-Einträgen in der Registry. Schlüssel, die immer beachtet werden, sind:

- „Hkey_Local_Machine\Software\Microsoft\Windows\Current Version\Run“
- „Hkey_Current_User\Software\Microsoft\Windows\Current Version\Run“
- „Hkey_Local_Machine\Software\Microsoft\Windows\Current Version\RunOnce“
- „Hkey_Current_User\Software\Microsoft\Windows\Current Version\RunOnce“

Diese vier Schlüssel werden jedes Mal ausgeführt, wenn sich ein Anwender anmeldet. Die nächsten beiden Schlüssel sind beim Login wichtig:

- „Hkey_Local_Machine\Software\Microsoft\Windows\Current Version\RunServices“
- „Hkey_Local_Machine\Software\Microsoft\Windows\Current Version\RunServicesOnce“

Sie starten Systemdienste wie die Remote Registrierung. „Hkey_Local_Machine\Software\Microsoft\Windows\Current Version\RunOnce\Setup“ wird nach dem Setup von Windows aufgerufen oder wenn über „Systemsteuerung, Software“ Programme (de-)installiert werden.

Eine Prüfung auf installierte Autostart-Programme nehmen fast alle Trojaner-Scanner vor, etwa Anti-Trojan 5.5 (25 Euro, auf Heft-CD oder Download unter **www.anti-trojan.net**) oder ein Autostart-Konfigurator wie die Freeware Autostart Manager 1.42 (auf Heft-CD oder unter **www.wt-rate.com**). Sie bieten auch eine Säuberung an.

Lokale Passwörter: Mit Tools leicht zu knacken

Windows 9x speichert Passwörter in PWL-Dateien im Windows-Verzeichnis. Damit überhaupt bei der lokalen Anmeldung ein Passwort abgefragt wird, müssen Sie die Benutzerverwaltung unter „Systemsteuerung, Benutzer“ einschalten. Damit verfügt jeder Anwender über einen Benutzernamen. Der Name der Passwortdatei setzt sich aus diesem Namen mit maximal acht Buchstaben und der Endung PWL zusammen. Für den Anwender „Administrator“ existiert also die Passwortdatei ADMINIST.PWL. PWL-Dateien sind mit dem RC4-Algorithmus verschlüsselt, der als ziemlich sicher gilt. Das Format ist geheim, so dass nur Microsoft PWL-Dateien benutzt. Vitas Ramanchauskas hat jedoch auf seiner Homepage (**http://soft4you.com/vitas/pwl.htm**) etliche Details zu PWL-Dateien zusammengetragen. PWL-Dateien lassen sich zum Beispiel mit dem Kommando “copy c:\windows*.pwl a:” auf Diskette kopieren und später in aller Ruhe untersuchen. Dazu kursieren ver-

schiedene Programme im Internet. Cain 2.0 (▷Kasten „Diese Sicherheits-Tools sollten Sie kennen“ auf Seite 49) zum Beispiel listet alle Passwörter aus dem Cache blitzschnell auf und kann Kennwörter in PWL-Dateien durch Ausprobieren mit der so genannten Brute-Force-Attacke knacken. Wer sich jetzt mit einem Administrator-Zugang für einen Server oder sogar für einen Domänencontroller auch bei Windows 9x anmeldet, gewährt Hackern Zugriff aufs Netz.

Lückenhafter Schutz: Passwörter für Windows-Bildschirmschoner sind keineswegs sicher. Dieses kleine Hilfsprogramm knackt ein definiertes Kennwort in Bruchteilen von Sekunden

Passwörter: Einmal eingegeben sind sie im Cache gespeichert

Eine weitere typische Schwäche von Windows-Systemen ist der Passwort-Cache. Dort sind alle während einer Sitzung eingegebenen Passwörter permanent zwischengespeichert. Was als benutzerfreundliche Funktion gedacht war, kann sich aber schnell als katastrophales Sicherheitsloch erweisen wie etwa in folgendem Szenario: Ein Anwender hat PC-Probleme. Der freundliche Administrator hilft ihm, muss aber dazu administrative Rechte haben. Also meldet er sich mit seinem Admin-Account an und löst das Problem. Danach meldet er sich ab und geht wieder. Das hätte er lieber nicht machen sollen. Der Anwender fischt jetzt nämlich per Passwortknacker blitzschnell das Administrator-Passwort aus dem Cache. Vielleicht ist er jetzt sogar Domänen-Administrator, denn das funktioniert auch unter Windows 2000 und XP. Daher sollten Sie nie vergessen, den Passwort-Cache abzuschalten. Auch beim Neustart des PCs bleibt der Cache erhalten. Der Passwort-Cache lässt sich unter Windows 9x im Schlüssel „KLM \Software\Microsoft\Windows\Current Version\Policies\Network“ abschalten. Legen Sie dort den neuen DWORD-Wert „DisablePwdCaching“ an, und weisen ihm den Wert „1“ zu. Alternativ können Sie eine Richtlinie mit dem Policy-Editor anlegen. Starten Sie Windows, und überprüfen Sie die Wirkung mit Cain, indem Sie den Cache-Inhalt anzeigen lassen. Sie erhalten die Meldung „No passwords found“. Der Cache ist also erfolgreich gelöscht und bleibt es auch. In diesem Schlüssel finden Sie auch den Wert „Hide SharePwds“, der per Voreinstellung auf „1“ gesetzt ist. Er legt fest, ob die beiden Freigabe-Passwörter für Lesen und Schreiben bei Windows 9.x im Klartext angezeigt werden. Steht dieser Wert auf Null, erscheinen die Passwörter im Klartext und verlieren damit ihren Sinn.

Der Passwort-Cache des Internet Explorers lässt sich in diesem Schlüssel abschalten: „Hkey_Current_User\Software \Microsoft\Windows\CurrentVersion\Internet Settings”. Setzen Sie den Wert „DisablePasswordCaching“ auf „1“. ▶

Schotten dicht: Kleine Netzwerke sichern

Ein großes Sicherheitsproblem in Windows-95/98-Peer-Netzwerken ist der Anmeldedialog, der mit einem Klick auf die ‹Esc›-Taste oder über „Abbrechen“ in der entsprechenden Dialogbox einfach umgangen werden kann. Windows lädt dann zwar keine Netzwerktreiber, aber der lokale Zugriff auf das System ist erlaubt. Über einen kleinen Registry-Eingriff können Sie allerdings die Eingabe von Benutzername und Passwort erzwingen. Der PC lässt sich dann zwar immer noch von Diskette booten – doch dagegen hilft letztlich nur das Ausbauen des Diskettenlaufwerks.

Family-Logon: Ein Windows-98-PC kann zur Netzanmeldung gezwungen werden

Um eine Netzwerkanmeldung zu erzwingen, installieren Sie das „Microsoft Family Logon“ (ab Windows 98) und definieren es als primären Netzwerk-Client. Der primäre Netzwerk-Client ist derjenige Client, der beim Anmelden an Windows das Passwort abfragt. Dies erledigen Sie im Konfigurationsregister der Netzwerkeigenschaften. Stellen Sie im Bereich „Primäre Netzwerkanmeldung“ das „Family Logon“ ein. Sobald Sie die Eigenschaften der Netzwerkumgebung schließen, werden Sie aufgefordert, die Windows-98-CD einzulegen. Nachdem Windows 98 einige Daten auf Ihren PC kopiert hat, müssen Sie diesen neu starten, damit die Änderungen wirksam werden. Bis jetzt lässt sich das Family Logon immer noch per ‹Esc›-Taste umgehen. Dies verhindern Sie, indem Sie im Registry-Schlüssel „Hkey_Local_Machine \Network\Logon” den Wert „MustBeValidated vom Typ REG_DWORD“ erzeugen und ihm den Wert „1“ für eingeschaltet zuweisen („0“ bedeutet abgeschaltet). Damit ist die ‹Esc›-Taste beim Einloggen nicht mehr funktionsfähig.

Das Knacken von Win-2000/XP-Passwörtern ist um einiges schwieriger. Sie sind in der SAM-Datenbank oder im Active Directory gespeichert, die keinen Zugriff erlauben, solange Windows 2000/XP läuft. Hacker installieren also ein zweites Win 2000/XP auf dem Rechner und können dann mit entsprechenden Knackprogrammen aus dem Internet die Datenbank bearbeiten. Mit denselben Methoden wie Hacker könnten Sie als Administrator vorgehen, um zu prüfen, wie sicher Ihr Netzwerk ist. Das Untergrund-Tool L0pht Crack wurde früher verwendet, um online Win-NT-Passwörter zu erschnüffeln. Diese sind in der Registry gespeichert, auf die ein Administrator Remote-Zugriff hat. So war es etwa möglich, die Passwörter anderer Admin-Kollegen berechnen zu lassen. Der Nachfolger von L0pht Crack heißt LC4 (**www.securitysoftwaretech.com**). Der aggressive Brute-Force-Crack ist in der 15-Tage-Testversion jedoch nicht mehr enthalten.

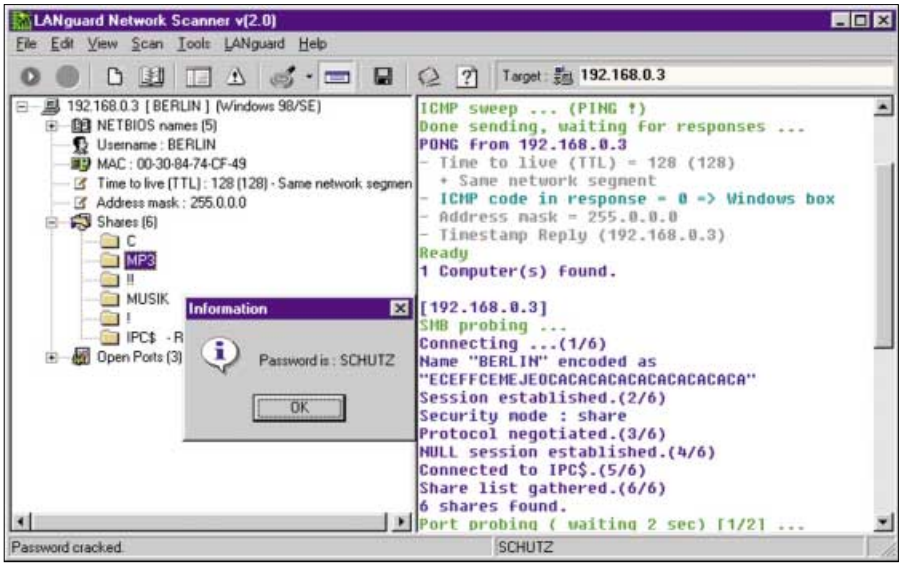
Von Last Bit Software (**www.soft4you.com**) gibt es weitere Knack-Tools, die in der Regel erst nach dem Erwerb einer Lizenz funktionieren. Erwähnt sei noch das Tool Revelation 2.0 (englischsprachige Freeware, Download unter **www.snadboy.com**), das zeigt, was sich hinter den Sternchen in Passworteingabefeldern verbirgt.

Bildschirmschoner: Passwort leicht zu umgehen

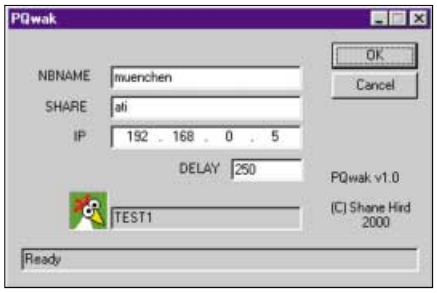
Eine weitere Schwachstelle in Windows 95/98 und ME ist der Bildschirmschoner. Man kann ihn mit einem Passwortschutz versehen. Das wird gerne in Büros gemacht, wenn man den Arbeitsplatz kurz verlassen muss, aber nicht will, dass jemand anderes Zugang zum PC hat. Die einfachste Methode besteht darin, den Rechner einfach auszuschalten. Das bemerkt der Eigentümer natürlich, und der Angreifer muss sich mit Stromausfall oder ähnlichem herausreden. Geschickter ist es, in Abwesenheit des Eigentümers ein Crack-Tool für Bildschirmschonerpasswörter wie den Windows 95/98 Srceen Saver Password Cracker 2.0 (▷Kasten auf Seite 49) laufen zu lassen. Abhilfe bringt nur der Umstieg auf Windows 2000/XP, das eine vorübergehende Abmeldung des Anwenders erlaubt. Bei Windows 95 war es noch möglich, mit <Ctrl><Alt><Entf> den Taskmanager aufzurufen, um den Bildschirmschoner einfach zu beenden. Seit Win 98 funktioniert das aber nicht mehr.

Freigaben knacken: Kein Schutz durch Passwörter möglich

Ein Sicherheitsloch stellen die so genannten Freigaben in einem Windows-Netzwerk dar. Sie sind notwendig, um Daten mit anderen PCs auszutauschen, allerdings gibt es verschiedene Möglichkeiten, Ordner für den Zugriff über das Netzwerk zu konfigurieren. In Peer-to-Peer-Netzwerken mit Windows-9x-Rechnern müssen Sie dazu auf dem Server (der PC, der die Freigabe anbietet) die Datei- und Druckerfreigabe einschalten. Über den



Sicherheits-Tool: Languard 2.0 ist ein für den privaten Einsatz kostenloser Netbios-Scanner: Er durchsucht IP-Adressbereiche nach Freigaben und ermittelt die verwendeten Passwörter



Geknackt: Die Freigabe „ati“ auf dem PC „muenchen“ ist mit dem Passwort „test1“ geschützt

Eintrag „Freigabe“ des Kontextmenüs eines Ordners stellen Sie im Register „Freigabe“ die Art des Zugriffs ein. Der Freigabename ist ein Netbios-Name, der in der Netzwerkumgebung der anderen PCs zusammen mit dem Kommentar erscheint. Ist die Freigabe passwortgeschützt, sieht man bei Freigaben unvorsichtiger Anwender gelegentlich das Passwort im Kommentarfeld. Der Zugriffstyp „schreibgeschützt“ erlaubt zwar nicht das Ändern oder Löschen von Daten, jedoch das Anzeigen. „Lese-/Schreibzugriff“ heißt Vollzugriff: Löschen erlaubt. „Zugriff abhängig vom Kennwort“ ist die einzige Möglichkeit, eine Freigabe mit einem Passwort zu versehen. Für Lesen und Schreiben können Sie jeweils ein eigenes (anderes) Passwort angeben. Netbios-Passwörter können über das Netzwerk geknackt werden. Die Tools Pqwak 1.0 und 2.0 von Shane Hird (▷Kasten auf Seite 49) verwenden eine simple Brute-Force-Attacke: Sie probieren nacheinander alle möglichen Kombinationen von Buchstaben aus und finden so fast immer das Kennwort. Einfache Passwörter knackt Pqwak in Bruchteilen von Sekunden.

Pqwak ist nicht sauber programmiert. Es fehlen einige Zeichen, die in Netbios-Passwörtern erlaubt sind, so dass es nicht alle Freigabepasswörter findet. Tools wie Pqwak benötigen den Rechner-Namen (Netbios-Name) des Ziel-PCs, seine IP-Adresse sowie den Namen der Freigabe, die geknackt werden soll. Pqwak wird von vielen Viren- und Trojaner-Scannern als Schadprogramm gemeldet.

Netbios-Scanner: Suchen nach Informationen

Angreifer, die die Freigabenamen nicht kennen, benutzen einen so genannten Netbios-Scanner wie Languard 2.0 (▷Kasten auf Seite 49) oder ältere Programme

wie Legion 2.1 sowie den Shares Finder. Diese scannen IP-Adressbereiche nach Freigaben. In einem LAN funktioniert das sehr gut, im Internet hingegen sind Freigaben eher selten anzutreffen. Das Knacken von Freigabepasswörtern können Sie verhindern, indem Sie eine Domäne mit Windows 2000/XP oder NT-Server einrichten, die alle Zugriffe auf Freigaben verifiziert. Zum Knacken muss ein Konto auf dem Server gehackt werden, was schwieriger ist.

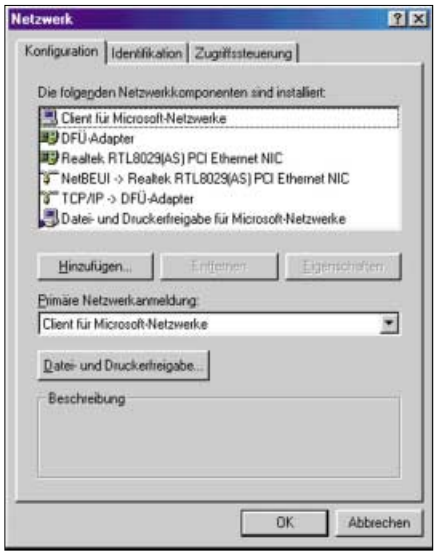
Halbwegs sicher: Windows 2000 und XP

Ist ein Windows-PC im Netzwerk, ist die Zugriffssteuerung komplizierter. Unter Windows 2000/XP werden Berechtigungen von Benutzern und Gruppen in der „Access Control List" (ACL) verwaltet. Jede Freigabe enthält so eine Liste. Greift ein PC mit Windows 95/98/ME auf einen Rechner mit Windows 2000/XP zu, muss die Freigabe auf Windows 2000/XP entweder die Gruppe „Jeder" in der ACL haben oder bei aktiviertem Gastkonto die lokale Gruppe „Gäste" oder die lokale Gruppe „Netzwerk" in die ACL aufnehmen. Das Gastkonto ist per Voreinstellung deaktiviert. Vor solchen Angriffen können Sie sich nur schützen, indem Sie die Datei- und Druckerfreigabe abschalten. Damit können Sie nicht mehr auf Netzwerkressourcen zugreifen, was in den meisten Fällen nicht akzeptabel ist. Mehr Sicherheit liefert im Netzwerk nur eine Domäne oder wenigstens ein Anmelde-Server.

Protokolltrennung: Sicher, aber meistens wenig sinnvoll

Besonders gefährlich sind Freigaben auch deshalb, weil der Zugriff auf sie auch über das Internet möglich ist. Dazu wird hauptsächlich TCP-Port 139 benutzt. Um Ports zu blockieren, setzen Sie am einfachsten eine Personal Firewall ein. Ist der Port 139 blockiert, besteht keine Gefahr, anderenfalls schon, falls Sie auch tatsächlich Freigaben definiert haben. Ein offener Port 139 bedeutet, dass das SMB-Protokoll (Server Message Block) oder eine Emulation wie Samba unter Linux auf dem Zielsystem aktiv ist. SMB wird grundsätzlich in Microsoft-Netzwerken eingesetzt – ohne einen offenen Port 139 gibt es auch keine Netzwerkfunktionen. Port 139 wird geöffnet, sobald der Client für Microsoft-Netzwerke in der Netzwerkumgebung installiert wird. Ab Windows 2000 kann auf Netbios verzichtet werden, SMB läuft dann über Port 445 – das ist der Microsoft Verzeichnisdienst.

Eine Schutzmöglichkeit ist die Trennung der im Netz verwendeten Protokolle von denen, die im Internet zum Einsatz kommen. Ein Internet-Gateway in einem Netzwerk verfügt über zwei Anschlüsse: einen über das DFÜ-Netzwerk zum Internet Provider und einen zweiten für die Netzwerkkarte ins LAN. Das DFÜ-Netzwerk funktioniert als Multi-Protokoll-Router: Über den Provider kommen Daten über TCP/IP herein und werden in das LAN geleitet, das zum Beispiel mit dem Netbeui-Protokoll arbeitet. Die Protokollumsetzung erledigt das DFÜ-Netzwerk. Ein Angreifer kommt theoretisch über TCP/IP bis zum DFÜ-Netzwerk, aber dann nicht mehr weiter, weil das passende Protokoll fehlt. Um weiterzukommen, bräuchte er Netbeui, doch das steht über das Internet nicht zur Verfügung. Er könnte allenfalls über einen offenen Port 139 auf Freigaben des Gateway-PCs zugreifen, falls dort welche definiert sind. In einem Microsoft-Netzwerk ist das aber unvermeidlich. Als Transportprotokolle dürfen Netbeui oder TCP/IP laufen. Das aus der Novell-Welt stammende IPX/SPX mit dem Client für Netware funktioniert



Windows 98 als Internet-Gateway: Ohne TCP/IP im lokalen Netz laufen viele Internet-Programme nicht

nicht. Für eine Protokolltrennung müssen Sie folgende Netzwerkkomponenten auf dem Internet-Gateway installieren:

- Client für Microsoft-Netzwerke
- DFÜ-Adapter
- Netzwerkkarte
- Netbeui (gebunden an die Netzwerkkarte)
- TCP/IP (gebunden an den DFÜ-Adapter)
- Datei- und Druckerfreigabe für Microsoft-Netzwerke

Die Netzwerkkonfiguration auf den Workstations sieht so aus:

- Client für Microsoft-Netzwerke
- Netzwerkkarte
- Netbeui (gebunden an den Client für Microsoft-Netzwerke)
- Datei- und Druckerfreigabe für Microsoft-Netzwerke

Für noch mehr Sicherheit sollte eine Personal Firewall zum Einsatz kommen.

Burkhard Müller

Diese Sicherheits-Tools sollten Sie kennen

Programm	Adresse	Lizenz	Info
Cain 2.0	http://fusionhack.iespana.es/fusionhack/ Cracking/passwordpc.htm	kostenlos	Passwort-Detektor für Windows 95 und 98
Languard 2.0	www.gfisoftware.de/de/lannetscan/index.htm	kostenlos	Netbios-Scanner mit vielen Optionen
LC4 / L0pht Crack	www.securitysoftwaretech.com/lc3	350 US-Dollar	Passwort-Detektor für Windows NT 4 und 2000
Pqwak 1.0/2.0	http://spisa.act.uji.es/spi/progs/codigo/www.hack.co.za/exploits/os/win/98/	kostenlos	Brute-Force-Attacke für Freigabepasswörter
Windows 95/98 Screen Saver Password Cracker 2.0	http://home.netpower.no/kenra/pwdcrack/	kostenlos	deckt Passwörter des Bildschirmschoners unter Windows 95/98/ME auf

Was Firewalls wirklich taugen

Windows-Mauerbau

Personal Firewalls sollen Einzelplatz-PCs oder kleine Netzwerke vor Angriffen aus dem Internet schützen. Lesen Sie, ob die Produkte ihren Marketing-Aussagen gerecht werden können.

▸Der Markt für Personal Firewalls ist heiß umkämpft: Black Ice wurde an ISS verkauft, Biodata hat Insolvenz angemeldet, und die Nachfolgegesellschaft steht in den Startlöchern, Tiny Software hat die alte Version der Personal Firewall an Kerio verkauft und kommt gleichzeitig mit einem runderneuerten Produkt auf den Markt. Sygate bietet ebenfalls ein erweitertes Produkt. McAfee strickt seine neue Personal Firewall sogar völlig um, nur die Produkte von Symantec und Zone Labs bieten ein einigermaßen konstantes Bild. Gleichzeitig setzt der Newcomer Agnitum mit dem Produkt Outpost neue Maßstäbe — diese Firewall ist zudem für den privaten Gebrauch kostenlos. Updates fast aller Produkte finden in der Regel mehrmals pro Jahr statt. Die Zielgruppen sehen die meisten Hersteller in Unternehmenskunden. Gute Zeiten für private Anwender: Etliche Produkte sind für den privaten Gebrauch kostenlos.

Dieser Test stellt eine Momentaufnahme der zur Zeit am Markt befindlichen Produkte dar. Der Trend geht immer mehr zu Rundum-Sicherheitslösungen: Virenscanner, Content-Blocker und Sandbox inklusive. Gleichzeitig werden die Produkte immer komplizierter: Ohne fundierte Netzwerk-Kenntnisse sind viele Firewalls (etwa die Testsieger) nicht sinnvoll einsetzbar.

Info: Firewalls im Test

Viele renommierte Software-Hersteller sind in den lukrativen Markt mit Sicherheitsprogrammen eingestiegen. Heimanwender greifen allerdings gerne zu den kostenlosen Alternativen. Wir haben die Produkte für Sie getestet.

Kontrolle: Anwendungsfilter sortieren Angriffe aus

Personal Firewalls bestehen aus mehreren Sicherheitskomponenten: Anwendungsfilter, Paketfilter, Sandbox-Lösungen sowie Kombinationen daraus.

Anwendungsfilter sind am einfachsten zu bedienen. Sie überprüfen den Zugriff Ihrer Programme auf das Internet und führen Positiv- und Negativ-Listen, in denen festgehalten ist, ob einer Anwendung der Zugriff auf das Internet erlaubt ist oder nicht (auch schwarze und weiße Listen genannt). Anwendungsfilter (ein Beispiel ist Zone Alarm) sind „lernfähig“: Nach der Installation sind beide Listen leer. Sobald ein Programm auf das Internet zugreift, meldet sich der Anwendungsfilter und verlangt vom Anwender die Entscheidung über den Zugriff: zulassen oder verweigern. Bei typischen be-

kannten Internet-Anwendungen wie Mailprogrammen oder Webbrowsern und FTP-Clients ist die Entscheidung einfach zu treffen: Sie benötigen immer Internet-Zugriff. Anders verhält es sich bei unbekannten Programmnamen: Ist einem unbekannten Programm der Zugriff zu gewähren oder lieber nicht? Hier muss man sich kundig machen, um was für ein Programm oder um was für einen Dienst es sich handelt. Im Zweifelsfall ist der Zugriff zu verweigern. Nachforschungen auf Hersteller-Sites, in Newsgroups oder auf Webboards können hier hilfreich sein.

Paketfilter: Komplexe Regeln sorgen für Sicherheit

Paketfilter sind etwas komplizierter: Sie betrachten IP-Adressen und Port-Nummern von Quelle und Ziel sowie das ACK-Bit von IP-Datagrammen beziehungsweise der eingebetteten TCP-Header. Anhand der Sockets (IP-Adresse plus Port-Nummer) lässt der Paketfilter Verbindungen zu oder verwirft sie. Mit Paketfiltern werden so genannte Regelwerke aufgebaut. Sie bestehen aus einer Reihe von Filtern, die nacheinander abgearbeitet werden, bis eine Regel zutrifft. Ist das nicht der Fall, können „unerkannte" Pakete erlaubt oder verboten werden. Am sichersten ist es, alles zu verbieten, was nicht erkannt wird.

Per Definition erkennen – statische – Paketfilter keinen ein- und ausgehenden UDP-Datenverkehr wie etwa DNS-Pakete, da die UDP-Header nicht über die entsprechenden Bits verfügen. Ein statischer Paketfilter kommt daher nur für verbindungsorientierte Dienste auf festen Port-Nummern zum Einsatz.

Eine Erweiterung stellen die dynamischen Paketfilter dar, die heute überwiegend im Einsatz sind. Dynamische Paketfilter berücksichtigen außer den Sockets auch den Kontext einer Verbindung. Sie „merken" sich ausgehende Verbindungen und erkennen Antworten von außen als Reaktion auf eine Anfrage von innen. Damit erkennen sie auch verbindungslose Dienste wie DNS auf beliebigen Ports. Die Kontextinformationen verfügen über ein Verfallsdatum, nach dessen Ablauf die Verbindung beendet wird. Die Technik von dynamischen Paketfiltern wird als Stateful Inspection (statusbehaftet) bezeichnet – das drückt die Berücksichtigung des Status einer Verbindung aus.

PC-WELT-Testsieger kommerzielle Produkte:

Norton Internet Security 2002 Professional 4.5

Das neue Norton-Produkt setzt eine lange Tradition fort: Hohe Sicherheit, viele Funktionen und zahllose Einstellmöglichkeiten sind seit jeher Kennzeichen dieser Firewall. Allerdings setzt auch die Norton Firewall einige Kenntnisse über Netzwerktechnik voraus, um den Sinn vieler Funktionen zu verstehen.

Sandboxes: Programme werden in Quarantäne ausgeführt

Sandbox-Lösungen schränken die „Bewegungsfreiheit" von Programmen ein. Für jedes installierte Programm muss eine Sandbox definiert werden, die zum Beispiel den Zugriff auf die Registry durch das Programm regelt. Die Konfiguration von Sandboxes ist recht aufwändig, besonders auf „fetten" Clients. Sie erlauben aber eine recht gute Abwehr vor allem

PC-WELT-Testsieger kostenlose Produkte:

Outpost Free 1.0.1617

Shootingstar Outpost macht der Konkurrenz das Leben schwer: Hohe Sicherheit, viele Funktionen, gelungene Bedienerführung, deutschsprachige Version, gute Dokumentation und ein hervorragendes Forum werden von keinem anderen kostenlosen Produkt in diesem Umfang so geboten. Outpost setzt jedoch einige Kenntnisse über Protokolle voraus und ist daher für unerfahrene Anwender weniger geeignet. Der Lerneffekt ist nicht zuletzt durch die gute Dokumentation und das spezifische Forum hoch. Beides ist jedoch englischsprachig.

von Viren. Viele Produkte kombinieren mehrere dieser Funktionen und sind bestrebt, die Konfiguration möglichst einfach zu halten. Sie sollten allerdings wissen: Viele Personal Firewalls sind bereits geknackt worden.

Burkhard Müller

Im Überblick: Personal Firewalls

Produkt	Internet-Adresse	Betriebssysteme	Preis	Seite
Esafe Desktop 3.1	www.esafedesktop.com	Win 95/98/ME, NT 4, 2000, XP	Vollversion 82 Euro, Update 59 Euro	52
McAfee Personal Firewall 3.02	www.mcafee.com	Win 95/98/ME, NT 4, 2000, XP	29,95 US-Dollar (inkl. Abonnement für 1 Jahr)	53
Norton Internet Security 2002 Profess. 4.5	www.symantec.com	Win 95/98/ME, NT 4, 2000, XP	99,95 Euro	54
Outpost Free 1.0.1617	www.agnitum.com	Win 95/98/ME, NT 4, 2000, XP	kostenlos für privaten Gebrauch	56
Sphinx 2.0	www.pcfirewall.de	Win 95/98/ME, NT 4, 2000, XP	zur Zeit nicht erhältlich	56
Steganos Online Shield 1.51	www.steganos.com	Win 95/98/ME, NT 4, 2000, XP	49,95 Euro	57
Sygate Personal Firewall 5.0	www.sygate.com	Win 95/98/ME, NT 4, 2000, XP	kostenlos für privaten Gebrauch	58
Tiny Personal Firewall 3.0	www.tinysoftware.com	Win 95/98/ME, NT 4, 2000, XP	kostenlos für privaten Gebrauch	59
Windows-XP-Firewall	www.microsoft.com	Win XP	in Windows XP enthalten	60
Zone Alarm 3.1.291	www.zonelabs.com	Win 95/98/ME, NT 4, 2000, XP	kostenlos für privaten Gebrauch	60

= auf Heft-CD

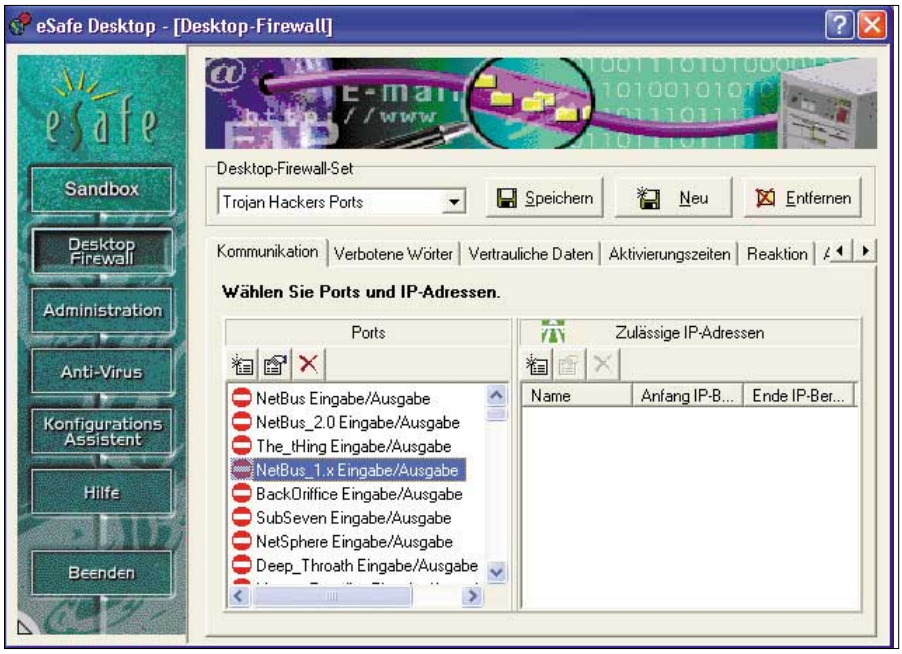
Esafe Desktop 3.1: Das Multitalent

Esafe Desktop 3.1 von Aladdin ist ein Rundum-Sicherheitsprogramm und soll Schutz vor so genanntem Malicious Code bieten, also vor allem vor Viren, Trojanern, ungebetenen Scripts und ähnlichen ausführbaren Quellcodes. Zu diesem Zweck enthält das Produkt zusätzlich zu einer Firewall einen Virenscanner, eine Sandbox sowie den Systemmonitor zur Überwachung von Änderungen an bestimmten Dateien.

Der Schutz vor bösartigen Programmen beruht auf der so genannten Sandbox-Technologie: Für jedes Programm lässt sich dabei eine eigene Sandbox definieren. Sie legt fest, was das Programm darf, zum Beispiel auf welche Ordner es wie zugreifen darf. Das Programm darf die Sandbox nicht verlassen, so dass gefährlicher Code bei richtiger Konfiguration keinen Schaden anrichten kann.

Das Modul Desktop Firewall kontrolliert die Verwendung der Ports. Dazu bietet es so genannte Desktop-Firewall-Sets. Dabei handelt es sich um vordefinierte Port-Beschränkungen. Das Set „Trojan Hackers Ports“ enthält beispielsweise eine große Anzahl der Ports, die bevorzugt von Trojanern benutzt werden. Diese Ports sind in diesem Set deaktiviert. Auch eigene Sets lassen sich hier problemlos definieren.

Die Sets enthalten Regeln. Eine solche Regel bestimmt beispielsweise, wie Ports verwendet werden dürfen. Für jeden Port lässt sich einzeln einstellen, wie Datenverkehr über ihn stattfinden darf: eingehend, ausgehend oder in beiden Richtungen. Außerdem kann dieser Port aktiviert oder deaktiviert sein. Für jede Regel gibt es auch Ausnahmen. Das sind Hosts, für die diese Regel nicht gilt. Hosts werden über ihren Namen oder über ihre spezifische IP-Adresse angegeben.



Vordefinierte Regeln: Esafe bietet Firewall-Sets, die mit verschiedenen Regeln die Verwendung der Ports kontrollieren. Hier sind standardmäßig zahlreiche Trojaner-Ports gesperrt

Schutzzone: Nicht jede Anwendung darf ins Internet

Die Application Firewall überwacht den Internet-Zugriff installierter Programme. Nur Internet-Programme, die sich in einer vordefinierten Sandbox befinden, haben Zugriff. Möchte ein anderes Programm eine Verbindung ins Internet herstellen, meldet sich die Firewall, und der Zugriff muss erst vom Anwender erlaubt werden.

Das Set-Prinzip wird auch auf einen Content-Filter angewendet. Dieser durchsucht Mailadressen und -inhalte, Internet-Adressen sowie Namen von Newsgroups und Inhalte von Dateien nach verbotenen Wörtern. Das Set besteht aus einer Liste mit verbotenen Wörtern. Vordefinierte Listen enthalten etwa Themen wie Hacker, Rassismus oder Drogen. Ein weiteres Feature ist die Verschlüsselung definierbarer Zeichenketten. Hier geben Sie beispielsweise Ihre Kreditkartennummer an. Jedes Mal, wenn diese über das Internet übertragen werden soll, kann sie verschlüsselt werden.

Die Firewall-Funktionen von Esafe sind recht knapp ausgefallen, dafür enthält das Produkt eine Sandbox, einen Virenscanner, einen Content-Filter sowie weitere Kontrollfunktionen wie den Systemmonitor, der Änderungen an bestimmten Systemdateien überwacht. Die Testscans zeigten allerdings, dass die Ports trotz definierter Regeln teilweise nicht blockiert waren.

Präventivmaßnahmen: Schutz vor unbekannten Programmen

Zu den Sicherheitsfunktionen von Esafe Desktop gehören auch die „proaktiven“ Techniken: So erkennt das Produkt zum Beispiel Mutationen bekannter Makroviren und durchsucht unbekannte Dateien nach Befehlen, die typischerweise von Viren verwendet werden. „Smartscan“ untersucht ausführbare Dateien daraufhin, ob die Datei-Endung auch tatsächlich dem Dateityp entspricht, indem interne Bitstrukturen untersucht werden – ein ziemlich komplizierter Vorgang.

Esafe kann sowohl auf Einzelplatzrechnern als auch in Firmennetzen eingesetzt werden. Für größere Installationen bietet Aladdin eine ganze Palette von Esafe-Produkten an: Esafe-Gateway, Esafe-Mail, die Econsole sowie die Desktop-Produkte bilden zusammen eine komplexe Sicherheitslösung, die alle gefährdeten Stellen eines Netzwerks überwacht.

Esafe Desktop 3.1

Info: Aladdin
www.esafedesktop.com
Preis: Vollversion 82 Euro, Update 59 Euro

⊕ **komplette Sicherheitslösung inklusive Virenscanner und Content-Blocker**
⊖ **etwas unübersichtlich, viele Fenster sind zu klein, aufwändige Konfiguration**

Funktionen	●●●●○
Sicherheit	●●●●○
Bedienung	●●●●○
Gesamt	●●●●○
Preis-Leistungs-Verhältnis	●●●●○

Testurteil: besonders zur Abwehr von Schadprogrammen geeignet. Das Programm bietet relativ wenig Firewall-Funktionen.

McAfee Personal Firewall 3.02: Nicht abzuschalten

Die Personal Firewall von McAfee ist eine Application Firewall – sie kontrolliert also den Internet-Zugriff von Anwendungen. Das optisch ansprechend gestaltete, deutschsprachige Produkt im Windows-XP-Look bietet zahlreiche Funktionen, schützt aber fast zu perfekt. Recht schlecht ist die Dokumentation.

Nach der Installation wird die Firewall mit einem Konfigurationsassistenten eingerichtet. Wichtig hierbei ist der Zugriff auf die eigenen Freigaben von Computern innerhalb eines LAN sowie der eigene Zugriff auf die Freigaben anderer Computer. Die McAfee Firewall kann damit ohne Probleme in einem Netzwerk betrieben werden. Beide Zugriffe sind in der Voreinstellung abgeschaltet. Danach folgt die Erkennung Internet-fähiger Programme. Dazu durchsucht der Assistent die Festplatten und führt die gefundenen Programme in einer Liste auf. Dort können Sie den Internet-Zugriff von Programmen erlauben. Sinnvoll ist das zum Beispiel für den Internet Explorer oder andere „vertrauenswürdige" Programme.

Das übersichtliche Hauptfenster der Firewall besteht aus mehreren Bereichen: Über Links rufen Sie die Liste der vertrauenswürdigen Anwendungen sowie das Aktivitätsprotokoll auf. Zusätzlich kann das Programm nach einem Update im Internet suchen. Der „Firewall Intrusion Monitor" enthält eine ominöse grafische Anzeige, die wohl die Anzahl der Verbindungsversuche und/oder Angriffe anzeigen soll. Daneben ist der „Notausschalter."

McAfee Personal Firewall 3.02

Info: McAfee
www.mcafee.com
Preis: 29,95 US-Dollar (inklusive Abonnement für 1 Jahr)

⊕ **hohe Schutzwirkung, zahlreiche Funktionen**
⊖ **Bedienung gewöhnungsbedürftig**

Funktionen	●●●●○
Sicherheit	●●●●●
Bedienung	●●●○○
Gesamt	●●●●○
Preis-Leistungs-Verhältnis	●●●●○

Testurteil: McAfee Firewall 3.02 gehört nicht zu den besten Produkten, erwies sich jedoch im Test als akzeptabel.

McAfee Firewall: Das Hauptfenster der Firewall im Windows-XP-Look ist übersichtlich in Informationsbereiche aufgeteilt und bietet einen schnellen Zugriff auf alle relevanten Optionen

Die Hauptfunktion der Firewall besteht in der Überwachung des Internet-Zugriffs von Anwendungen. Dazu führt das Programm eine Liste mit Internet-Anwendungen, die bei der Installation bereits gefüllt wird. Startet ein der Firewall unbekanntes Internet-Programm, erscheint eine Warnung, und Sie können den Zugriff zulassen oder nicht. Erlauben Sie etwa dem Newsreader Free Agent Internet-Zugriff und schauen sich dann die automatisch erzeugten Filterregeln an, so erkennen Sie drei erlaubte Verbindungen:

- eingehend, UDP/IP, Port 53
- ausgehend, UDP/IP, Port 53
- ausgehend, TCP/IP, Port 119

Über Port 53 laufen die DNS-Anfragen, über 119 läuft der News-Dienst. Für jede Anwendung können Sie Regeln definieren, die ein- und ausgehende Datenpakete bestimmter Protokolle unter Verwendung von Port-Bereichen filtern. Zu den Protokollen gehören:

- TCP
- UDP
- ICMP
- IPX/SPX
- IPX
- IP

IPX lässt sich blockieren, aber nicht filtern. Für das Internet sind die ersten drei sowie IP wichtig. Bereits bei der Installation lässt sich über die Eigenschaften der Netzwerkkarte der Zugriff auf die eigenen Freigaben verhindern sowie der eigene Zugriff auf die Freigaben anderer Computer abschalten. Bei eingeschalteter Reporting-Funktion erscheint im „Details"-Fenster, welcher Anwender von welchem Rechner gerade auf welche Freigabe zugreift. Diese Netbios-Sitzungen lassen sich auch unterbrechen.

Stummer PC: Keine Antwort auf Hackeranfragen

McAfee Firewall schützt vor dem so genannten Nuking beziehungsweise vor dem „Denial of Service" (DoS). Nuking-Angriffe treten in vielen Formen auf. Sie haben meistens nur ein Ziel: das Opfer vom Server oder Netzwerk zu trennen. Einige Nukes crashen auch das Betriebssystem. Für ältere Windows-Versionen gibt es zahlreiche Patches, die in Windows XP bereits enthalten sind.

Bei Netbios- und Port-Scans liefert ein mit der McAfee Firewall geschützter Rechner bei entsprechend restriktiver Konfiguration gar keine Informationen. Problem: Die Firewall lässt sich zwar abschalten, der Schutz bleibt aber aktiv. Erst nach einer kompletten De-Installation liefern die Port-Scans wieder die üblichen Informationen.

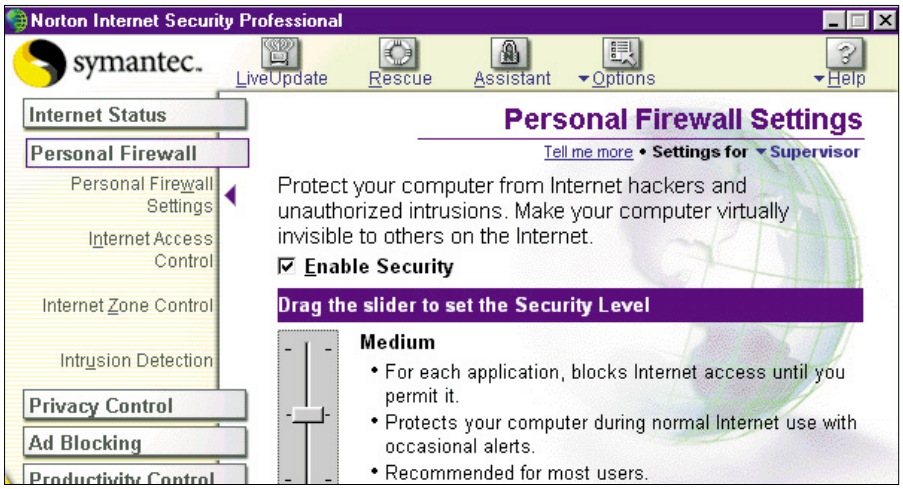
Das Aktivitätsprotokoll ist ungenügend und zeigt neben Datum und Uhrzeit nur spärliche Infos an – etwa dass eingehende TCP-Verbindungen geblockt wurden, jedoch nicht, von wem sie kamen. Immerhin erkennt die Firewall so genannte Null-Sessions im Protokoll, sofern die Überwachung der Freigaben eingestellt ist. ▶

Norton Internet Security 2002 Professional 4.5: Großkämpfer

Norton Internet Security 2002 4.5 (NIS) von Symantec enthält neben einer Firewall auch einen Content- und Werbe-Blocker, einen Schutzmechanismus für persönliche Daten, ein Kindersicherungssystem sowie einen Virenscanner. Wir betrachten ausschließlich die Eigenschaften der deutschsprachigen Firewall, die auch als eigenständiges Produkt erhältlich ist.

Nach der Installation inklusive LiveUpdate führt auf Wunsch ein Assistent durch die Konfiguration des Produkts. Unter anderem untersucht die Firewall dabei die Festplatten nach Internet-fähigen Anwendungen und stellt daraus eine Liste mit Berechtigungen für jedes gefundene Programm zusammen. Mit Hilfe dieser Liste können Sie den Zugriff aller erkannten Programme erlauben, sperren oder protokollieren. Für jede Anwendung stellen Sie eine eigene Regel auf oder modifizieren eine vorhandene.

NIS ist bereits vorkonfiguriert: Auf Port-Scans reagiert es nicht, und auch Ping-Nachrichten werden nicht beantwortet. Damit ist der PC im Internet praktisch nicht auffindbar. Die Netbios-Ports, die für die Datei- und Druckerfreigabe nötig sind, sind ebenfalls blockiert, allerdings auch für Anwender in einem LAN.



Drei Schutzstufen: Sie bieten verschieden hohe Sicherheit beim Umgang mit Anwendungen, aktiven Inhalten sowie für die Reaktion auf bekannte Hackerangriffe (Port-Scans)

Die Norton-Firewall ist eine Application Firewall. Sie steuert den Zugriff von Anwendungen auf das Internet mittels Regeln, die verglichen mit anderen Produkten wie zum Beispiel Zone Alarm recht komplex sind. Über eine Zonenkontrolle stufen Sie andere Computer als vertrauenswürdig oder nicht ein. Computer, denen man vertraut, werden in einer „Trusted"-Liste eingetragen. Dazu ist der Name oder die IP-Adresse des Computers anzugeben, ein Adress-Bereich oder ein Subnetz. Das ist auch der Schlüssel für die Zugriffserlaubnis für andere Computer in einem LAN: Das eigene Netz wird einfach in die Liste der Trusted Zones eingetragen. Jeder Computer in dieser Liste hat so Zugriff auf Ihren PC, als ob es die Firewall gar nicht gäbe. Computer in der eingeschränkten Zone werden dagegen vollständig blockiert, hier sollten sich also angreifende Systeme befinden, sofern sie zum Beispiel über die Protokolldateien identifiziert sind.

Die Intrusion Protection verhindert eine Antwort auf Port-Scans und schaltet die Funktion „Autoblock" ein.

Die Firewall können Sie in drei Schutzstufen einstellen, die den Umgang mit Anwendungen, aktiven Inhalten wie Java

Personal Firewalls: Testverfahren und Beurteilung

Alle Produkte wurden als Testversionen von den Websites der Hersteller geladen (außer Norton Internet Security und Windows XP Firewall) und auf einem frisch aufgesetzten Windows XP Professional installiert. Der Zustand der Ports wurde mit den Programmen Nmap 2.54 Beta 33 unter Suse Linux 8.0 sowie mit Languard 2.0 ermittelt. Online Port-Scans wurden bei Sygate (**http://scan.sygatetech.com**) und Gibson Research (**http://grc.com**) durchgeführt. Ein besonderes Augenmerk wurde auf die von Angriffen immer gefährdeten Netbios-Ports gelegt sowie auf das Unterdrücken von ICMP-Nachrichten.

Die Beurteilung der Produkte erfolgte in drei Kategorien mit folgender Gewichtung:

Funktionen:	30%
Sicherheit:	50%
Bedienung:	20%

Funktionen
Die Anzahl der zur Verfügung stehenden Funktionen eines Produkts lässt bereits einige Aussagen zu. Da der Trend immer mehr zu kompletten Sicherheitslösungen inklusive Content-Blocker, Sandbox und Virenscanner geht, wurden diese Funktionen mit bewertet. Die Funktionen gehen mit 30 Prozent in die Gesamtwertung ein.

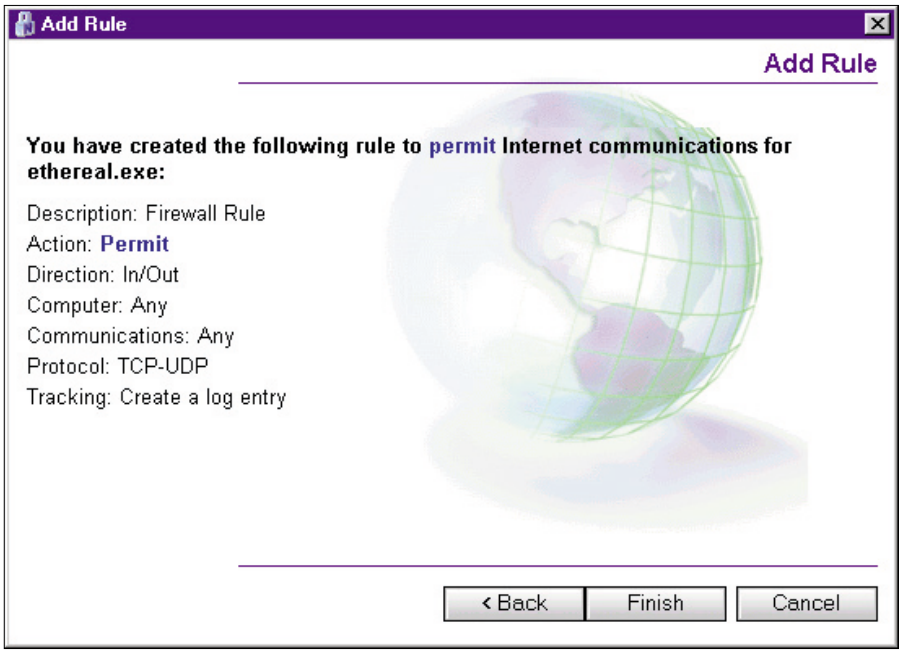
Sicherheit
Die beschriebenen Tests erfassten zumindest einen Teil der tatsächlich gebotenen Sicherheit. Punkte gab es für eine hohe Sicherheit bereits in der Voreinstellung. Dazu gehört das Blockieren aller Ports sowie von ICMP. Die Sicherheit ist das wichtigste Kriterium einer Firewall (und das wichtigste Kaufargument), deshalb war uns dieser Bereich 50 Prozent wert.

Bedienung
Eine einfache, intuitive Bedienung ist gerade für weniger versierte Anwender wichtig. Die Funktionen müssen klar erkennbar und zumindest ansatzweise im Programm erklärt sein. Wichtige Funktionen müssen im Hauptfenster integriert sein. Die Bedienung schlägt mit 20 Prozent zu Buche.

Gesamt
Die Detailergebnisse in den drei genannten Kategorien ergeben zusammen das Gesamturteil, das Rückschlüsse auf die tatsächliche Leistung zulässt.

Preis-Leistungs-Verhältnis
In diese Wertung fließt ein, dass einige Produkte kostenlos sind. Wenn Sie bereit sind, Geld auszugeben, ist diese Bewertung nicht auschlaggebend.

und Acitve X sowie die Reaktion unter anderem auf Port-Scans beeinflussen. In der Voreinstellung „Medium“ müssen Sie den Internet-Zugriff von Anwendungen erst erlauben, Active-X-Controls und Java-Applets dürfen laufen, und auf Port-Scans wird nicht reagiert. In der hohen Sicherheitsstufe gibt es zusätzliche Informationen, da bei Active-X-Controls und Java-Applets nachgefragt wird, die übrigen Einstellungen entsprechen der mittleren Einstellung. Die niedrige Sicherheitsstufe blockiert bekannte Programme mit Sicherheitslücken, sonst ist alles erlaubt. Jede dieser drei Einstellungen lässt sich verändern und auch wieder auf „Werkseinstellungen“ zurücksetzen.



Übersichtlich und praktisch: Am Ende einer Regeldefinition in Norton Internet Security 2002 erscheint eine Zusammenfassung der vom Anwender festgelegten Eigenschaften

Assistenten: Hilfe bei der Regelerstellung

Die einfachste Art, vorhandene Internet-Anwendungen in die Regelliste aufzunehmen, besteht darin, sie vom Assistenten automatisch suchen zu lassen. Die Zugriffsart steht damit für die Anwendungen auf „automatisch“, die von der Firewall erkannt und als ungefährlich eingestuft werden. Diese Internet-Zugangskontrolle ist abschaltbar, jedoch wird dann bei einem Internet-Zugriff das Erstellen einer Regel von Hand notwendig.

Die Konfiguration der Regeln von Hand ist zumindest am Anfang sinnvoll, damit der Anwender einen Überblick darüber erhält, welche Beschränkungen überhaupt zur Verfügung stehen. Greift eine Anwendung auf das Internet zu, führt ein Assistent durch die Regelerstellung. Zunächst erfolgt die Angabe, wie mit dem fernen Computer verfahren werden soll: Zugriff erlauben, blockieren oder überwachen. Bei der Überwachung erscheint immer dann ein Eintrag in der Protokolldatei, wenn diese Regel zutrifft.

Das nächste Regelkriterium legt die Richtung der Verbindung fest: zu oder von einem Computer oder in beide Richtungen. Im Normalfall geben Sie hier ausgehende Verbindungen an (kein eigener Server-Betrieb). Es folgt die Angabe, für welche Computer die Regel gilt. Zur Wahl stehen alle oder eine Liste mit Namen, IP-Adressen (auch Bereichen) oder Subnetzen. Damit können Sie diese Regel auf bestimmte PCs anwenden. Im einfachsten Fall geben Sie alle an, bei Verwendung eines Proxy-Servers die IP-Adresse des Proxys. Zudem können Sie einen Netzwerk-Adapter auswählen, für den diese Regel gelten soll. Es folgt die Angabe der erlaubten Protokolle – TCP, UDP oder beide – sowie der zugelassenen Ports. Wird die Verwendung von Ports eingeschränkt, so ist die Port-Nummer (auch mehrere oder Bereiche) zusammen mit der Eigenschaft „lokal“ oder „entfernt“ anzugeben. Bei Verwendung eines Proxy-Servers steht hier etwa „remote 8080“, da der ferne Proxy-Server in diesem Beispiel über Port 8080 angesprochen werden muss. Zuletzt legen Sie fest, ob ein Eintrag im Protokoll vorgenommen werden soll, sobald die Regel zutrifft.

Regeln: Individuelle Konfigurationen einstellen

Sie können für jede Anwendung einen ganzen Satz von Regeln definieren. Zum Beispiel kann der Internet Explorer auch FTP-Transfers durchführen und zwar ein- und ausgehend über die Datenleitung (Port 20) und ausgehend über die Befehlsleitung (Port 21). Für diese Fälle sind jeweils Regeln zu definieren. In der Liste der Regeln kommt es darauf an, ob eine Regel oben oder unten steht, denn diese Liste wird von oben nach unten abgearbeitet. Trifft eine Regel zu, wird sie ausgeführt, und eine spätere nicht mehr beachtet. Die Regelerstellung ist komplex. Wer will, kann sich damit stundenlang beschäftigen. ICMP können Sie ebenfalls genau einstellen: ICMP-Nachrichten (zum Beispiel 0 für „Echo Reply“) können Sie blocken (Voreinstellung für Typ 0, 3 und 11) oder einfach zulassen, indem Sie eingehende ICMP-Nachrichten vom Typ „Echo Request“ akzeptieren und alle Typen für ausgehenden Verkehr freigeben.

Wer eine einfach zu bedienende Personal Firewall sucht, ist mit dem Norton-Produkt schlecht bedient. Es bietet zwar eine automatische Konfiguration. Wer die Möglichkeiten voll nutzen möchte, muss sich jedoch genau mit den Regeln auseinandersetzen.

Norton Internet Security 2002 Professional 4.5

Info: Symantec **www.symantec.com**
Preis: 99,95 Euro

⊕ viele Funktionen, integriert mit anderen Symantec-Produkten
⊖ Fachwissen erforderlich

Funktionen	●●●●●
Sicherheit	●●●●●
Bedienung	●●●●○
Gesamt	●●●●●
Preis-Leistungs-Verhältnis	●●●●○

Testurteil: komplexes, gut dokumentiertes Produkt mit zahlreichen Sicherheitsfunktionen. Die nicht Windows-konforme Bedienung ist gewöhnungsbedürftig.

Outpost Free 1.0.1617: Deutschsprachige Freeware

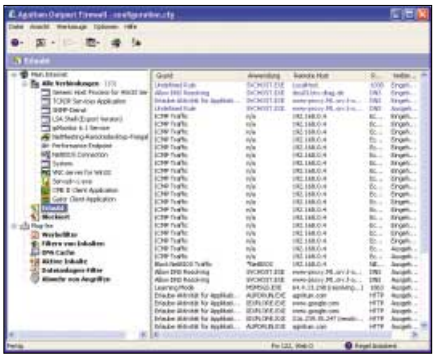
Mit Outpost Free bietet Hersteller Agnitum – unter anderem bekannt durch den sehr guten Trojaner-Scanner Tauscan – eine mehrsprachige, für den privaten Gebrauch kostenlose und dennoch leistungsstarke Personal Firewall.

Outpost ist sowohl ein dynamischer Paket- als auch ein Anwendungsfilter. Die Regeln bestehen aus Werten für IP-Adressen und Port-Nummern von Quelle und Ziel sowie für das Transportprotokoll (TCP oder UDP). Die Software enthält einen Satz vordefinierter Regeln, die so genannten Presets. Für typische Internet-Anwendungen wie Browser, ICQ, MSN Messenger und andere sind hier Regeln vordefiniert. Outpost stellt zwar dynamische Paketfilter zur Verfügung, erlaubt aber beispielsweise nicht die Kontrolle der Bits, die für den Verbindungsaufbau zuständig sind, durch den Anwender.

Netbios ist in der Voreinstellung abgeschaltet. Damit sind natürlich auch die Freigaben des Rechners, auf dem Outpost installiert ist, blockiert. Die Lösung ist einfach: Kreuzen Sie im Register „System“ in den Optionen das Kontrollkästchen „Erlaube NetBIOS Kommunikation“ an, und tragen Sie unter „Einstellungen“ die IP-Adressen oder das Subnetz ein, dem vertraut wird – das ist das eigene LAN.

Outpost erlaubt das gezielte Blocken von ICMP-Nachrichten. Jede Nachricht lässt sich für ein- und ausgehenden Verkehr sperren. Wenn Sie also ein Echo Reply auf ein Ping unterbinden möchten, aktivieren Sie „Echo Reply“ in der Spalte „Aus“. Das ist auch die Voreinstellung.

Als weitere Funktion enthält Outpost eine Warnung vor bestimmten Mailanhängen. Dazu gehören etwa ausführbare Dateien oder VB-Scripts. Auf Port-Scans und ICMP-Nachrichten reagiert das Produkt nicht, die Netbios-Ports sind blockiert. Outpost enthält noch eine Reihe weiterer Funktionen: Schutz vor aktiven Inhalten, Werbe- und Cookie-Filter seien noch erwähnt sowie eine Unterstützung von Plug-ins. Somit können Sie weitere Funktionen hinzufügen.



Übersichtlich: Die für Privatnutzer kostenlose Firewall Outpost Free zeigt alle relevanten Details

Outpost Free 1.0.1617

Info: Agnitum
www.agnitum.com
Preis: kostenlos für privaten Gebrauch

⊕ **hohe Sicherheit, übersichtlich, mit Plug-ins erweiterbar, gut dokumentiert**
⊖ **keine Auswertung von Logdateien**

Funktionen	●●●●●
Sicherheit	●●●●●
Bedienung	●●●●●
Gesamt	●●●●●
Preis-Leistungs-Verhältnis	●●●●●

Testurteil: Die zur Zeit beste Personal Firewall am Markt kann bereits in der Version 1.x überzeugen.

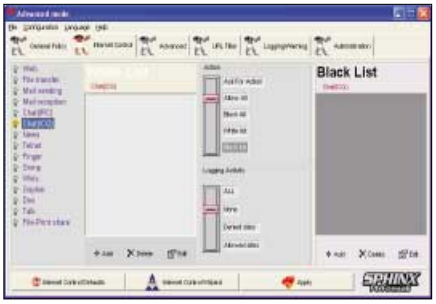
Sphinx 2.0: Made in Germany – Zukunft ungewiss

Obwohl der Hersteller Biodata Insolvenz angemeldet hat, soll die Personal Firewall Sphinx 2.0 weiterleben. Das Bedienkonzept der Sphinx Firewall unterscheidet zwischen Anfänger und Experten, wobei im Anfänger-Modus lediglich einige Register ausgeblendet sind. Wer das Produkt ernsthaft einsetzen will, sollte auf jeden Fall mehrere Tage Einarbeitungszeit mit einplanen.

Das kleine Hauptfenster wird durch den Sphinx-Knopf bestimmt: Damit können Sie „alles erlauben“ oder „alles verbieten“ – das funktionierte im Test auch richtig, wie wir mit Netbios-Scannern wie Languard 2.0 und auch Online-Scannern geprüft haben. In der Einstellung „alles verbieten“ sind alle Ports blockiert (stealth), ICMP und die Netbios-Ports für Filesharing sind abgeschaltet.

Sphinx setzt eine so genannte Statusüberwachungstechnologie ein (stateful inspection), die eingehenden Datenverkehr daraufhin prüft, ob er eine Reaktion auf eine vorher ausgehende Verbindung ist.

Den Zugriff von außen etwa durch Trojaner oder Port-Scans regeln Sie in vier Stufen: „Erlauben“ und „Blockieren“ sind selbst erklärend. Die Einstellung „Abfrage einblenden“ zeigt bei jedem Zugriff ein Alarmfenster. Alternativ lässt sich eine „Warnung speichern“, die im Warn- oder Protokoll-Monitor erscheint. Wird der Sphinx-PC gescannt, lässt ihn das völlig kalt, es erscheint überhaupt keine Meldung – einfach nichts. Lediglich Scans auf den Ports 80 und 443 sowie ICMP-Anfragen (Pings) werden im Protokoll-Monitor vermerkt. Zum Erkennen eines Port-Scans dürfte das zu wenig sein. Unter „Voreinstellungen“ richten Sie bestimmte Funktionen der Firewall für die Betriebsarten „Netzwerk“, „Modem/ISDN“ und „Individuell anpassen“ ein. Betroffen sind die Einstellungen für eingehende Netbios-Broadcasts, Identifikations-Broadcasts, Nicht-IP-Protokolle, ICMP- und Fragment-Blocking sowie IP-Spoofing. Das Register „Internet-Kontrolle“ enthält vordefinierte Dienste wie Web, FTP oder News. Die „Internet-Kontrolle“ regelt den Zugriff auf Dienste von außen.



Listen führen: Mit der weißen und schwarzen Liste lassen sich vordefinierte Dienste kontrollieren

Sphinx 2.0

Info: Biodata
www.pcfirewall.de
Preis: zur Zeit nicht erhältlich

⊕ **viele Funktionen, deutschsprachig**
⊖ **Arbeitsweise teilweise nicht transparent**

Funktionen	●●●●○
Sicherheit	●●●●○
Bedienung	●●●●○
Gesamt	●●●●○
Preis-Leistungs-Verhältnis	●●●●○

Testurteil: Sphinx 2.0 bietet eine hohe Sicherheit, wenn man sich ausreichend mit der Konfiguration des Produkts beschäftigt.

Steganos Online Shield 1.51: Einfach, aber mit Schwächen

Mit der Personal Firewall Steganos Online Shield setzt die deutsche Steganos GmbH auf einfache Bedienbarkeit. Das Programm ist optisch ansprechend gestaltet, leicht bedienbar und sollte den Anwender nicht überfordern. Die Zielgruppe dürften damit Anwender sein, die an technischen Details weniger interessiert sind, aber dennoch einen ausreichenden Schutz ohne viel Aufwand erwarten.

Das Hauptfenster besteht aus einem großen „Notausschalter", mit dem sich alle Verbindungen mit nur einem Mausklick schnell kappen lassen. Darunter befinden sich grafische Anzeigen für ein- und ausgehenden Datenverkehr. Links sind die Prozesse aufgeführt, die gerade eine Online-Verbindung unterhalten, rechts sind die Ereignisse aufgelistet – in der Regel Verbindungsversuche.

Das Produkt gehört in die Gruppe der Anwendungs-Firewalls, es blockiert also den Internet-Zugriff von Anwendungen. Startet eine dem Programm noch unbekannte Internet-Anwendung, meldet sich die Firewall, und Sie können der Anwendung den Zugriff erlauben oder nicht.

So sind Sie immer aktuell über die Internet-Aktivitäten informiert: Das übersichtliche Hauptfenster von Steganos Online Shield zeigt die wichtigsten Informationen auf einen Blick an

Betriebsarten: Jeder Anwendung wird eine Regel zuteil

Alle auf diese Art erfassten Anwendungen führt die Firewall in einer Liste, die Sie sich über das Hauptfenster unter dem Punkt „Anwendungen" anzeigen lassen. Das Produkt unterscheidet für jede Anwendung drei Betriebsarten: „Lokale Verbindung" bezieht sich auf das LAN. Solche Verbindungen können Sie in den meisten Fällen erlauben. „Internet Verbindungen" sollten Sie sorgfältig beobachten. Verdächtigen Anwendungen oder Prozessen ist der Zugriff zu verbieten. In der Betriebsart „Server" laufen nur wenige Programme, beispielsweise Filesharing-Tools und natürlich eigene Server wie FTP- oder Web-Server. Für jedes Programm können Sie in jeder Betriebsart den Zugriff auf „Immer", „Nie" oder „Fragen" einstellen.

Die Funktionsweise des Produkts wird durch die drei Sicherheitsstufen geprägt. Bei „sehr hoher Sicherheit" werden alle eingehenden Verbindung grundsätzlich abgelehnt, ausgehende Verbindungen hängen von den Einstellungen für die betreffende Anwendung ab. ICMP wird in dieser wie auch in der Stufe „hohe Sicherheit" blockiert. Netbios ist ebenfalls blockiert. In diesen beiden Sicherheitsstufen kann weder auf Freigaben im LAN oder über das Internet zugegriffen werden noch über einen Netzwerkdrucker gedruckt werden. Eine Liste mit vertrauten Hosts oder vertrauten Subnetzen hätte hier Abhilfe gebracht. Die Stufe „normale Sicherheit" erlaubt ICMP und Netbios, allerdings gibt der PC damit viele wichtige Informationen preis, die eigentlich niemanden etwas angehen. Netbios-Scans mit Languard bei „normaler Sicherheit" zeigen die typischen Informationen, wie sie ein ungeschützter PC verrät: Alle Netbios-Namen, Benutzernamen von Anwendern, Gruppen, offene Ports, laufende Dienste und so weiter. Die Scans wie auch Zugriffe auf Freigaben werden von der Firewall als eingehende Verbindungen korrekt erkannt. Bei jedem erkannten Verbindungsversuch öffnet sich ein Fenster (mit einem dramatischen Sound) mit den Daten des fernen Rechners (IP-Adresse, Portnummer und Transportprotokoll). Über die Schaltfläche „Mehr Info" fordern Sie weitere Daten über den „Angreifer" an.

Protokoll: Alle Aktivitäten werden aufgezeichnet

Sind Sie Opfer vieler Port-Scans, schalten Sie dieses Fenster besser aus – es nervt dann einfach zu sehr – und begnügen sich mit der Aufzeichnung im Protokoll. Das Protokoll enthält Datum, Uhrzeit, IP-Adresse, ferne und lokale Port-Nummer sowie das verwendete Transportprotokoll für eingehende Verbindungen.

„Angriffswarnungen" lassen sich als SMS auf ein Handy schicken. Doch was nützt diese gutgemeinte Funktion, wenn Sie nicht zu Hause sind um den „Notausschalter" zu betätigen?

Das Produkt wird aufgewertet durch den kostenlosen Anti-Dialer für registrierte Kunden. Er überwacht Dial-up-Verbindungen und fordert bei einer unbekannten DFÜ-Verbindung eine Bestätigung des Anwenders an. Damit soll er die ungewollte Einwahl eines Dialers über eine teure Telefonnummer verhindern. Bei jedem Programmstart überprüft der Anti-Dialer, ob sich im DFÜ-Netzwerk irgendwo teure Vorwahlnummern befinden, und schlägt gegebenenfalls Alarm. Die Liste der unerwünschten Vorwahlnummern ist erweiterbar.

Online Shield ist ein leicht zu bedienendes Produkt, das in der hohen Sicherheitsstufe einen guten Schutz bietet. ▶

Steganos Online Shield 1.51

Info: Steganos
www.steganos.com
Preis: 49,95 Euro

⊕ einfach zu bedienen
⊖ weniger Funktionen als die Konkurrenz

Funktionen	●●●○○
Sicherheit	●●●●○
Bedienung	●●●●●
Gesamt	●●●●○
Preis-Leistungs-Verhältnis	●●●●○

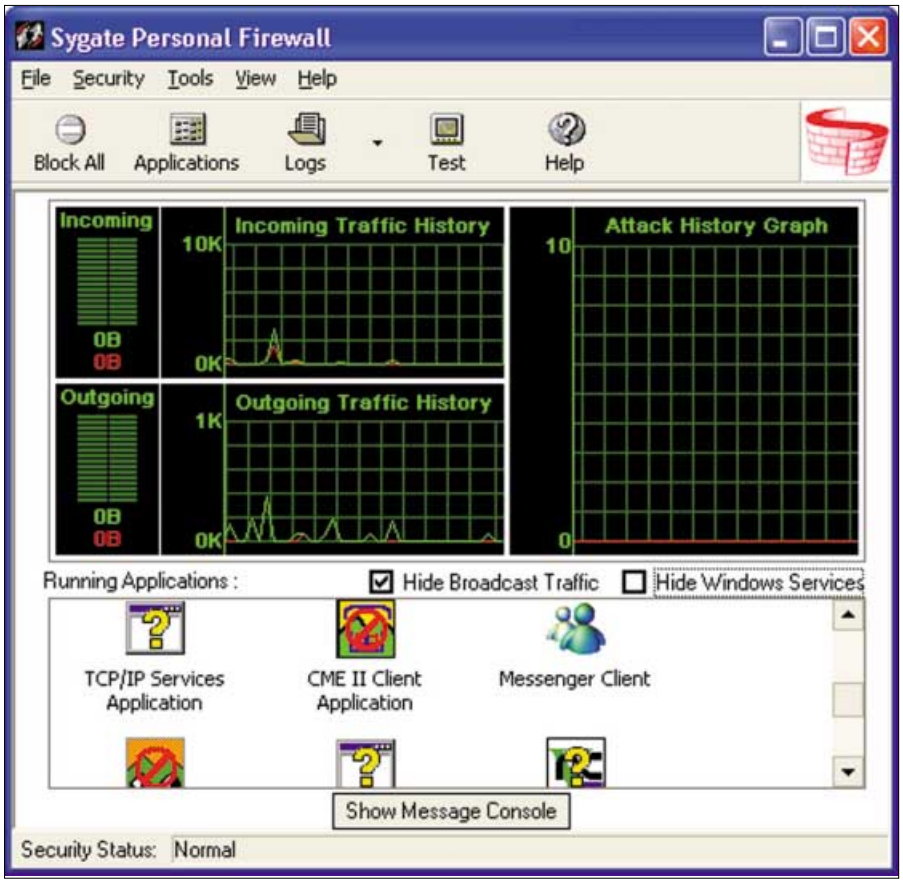
Testurteil: Steganos Online Shield ist für Einzelplatz-PCs geeignet, vor allem wenn man sich nicht mit technischen Details beschäftigen möchte. Das Produkt muss dafür aber in der hohen Sicherheitsstufe betrieben werden.

Sygate Personal Firewall 5.0: Profi-Wächter

Sygate Personal Firewall 5.0 arbeitet auf Anwendungsebene. Sie fasst Sicherheitseinstellungen in drei Stufen zusammen. Die Extremeinstellungen sind „Block all" und „Allow all", voreingestellt ist „Normal". Nach der Installation befindet sich das englischsprachige Programm im Lernmodus. Wird eine Anwendung mit Internet-Zugriff gestartet, fragt die Firewall, ob der Zugriff gestattet ist, und erstellt eine Regel.

Bei einer Regel können Sie für jede Anwendung lokale und ferne TCP- oder UDP-Ports angeben. Zudem kann jede Anwendung eine Liste mit vertrauten IP-Adressen führen, das ist in einem lokalen Netzwerk von Nutzen. Die Ausführung einer Anwendung, während der Bildschirmschoner läuft, lässt sich unterbinden. Schließlich können Sie bestimmte Zeiten angeben, während der eine Anwendung auf das Internet zugreifen darf.

Die Firewall läuft als Dienst unter allen Windows-Versionen. Sie schaltet die Netzwerkumgebung auf Wunsch aus und verhindert die Datei- und Druckerfreigabe. Bei einem Einbruchsversuch schlägt die Firewall Alarm und versendet eine Mail.



Auf einen Blick: Das Hauptfenster der Sygate Firewall zeigt alle laufenden Internet-Programme sowie den erzeugten Datenverkehr detailliert an und erlaubt dadurch viele Rückschlüsse

Logdateien: Hier wird alles mehrfach protokolliert

Die erfassten Ereignisse schreibt die Software in mehrere Protokolldateien: Security-, System- und Traffic-Log. In dieser Version neu hinzugekommen ist eine Paket-Log, die in der Art eines Sniffers Paket-Dumps speichert und anzeigt. Diese Funktion bietet sonst keine der getesteten Personal Firewalls. Allerdings ist sie noch als rudimentär zu bezeichnen, so fehlt es beispielsweise an Markierungen im Hexdump.

Sygate Personal Firewall 5.0

Info: Sygate
www.sygate.com
Preis: kostenlos für privaten Gebrauch

- ⊕ **übersichtlich und leicht zu bedienen, hohe Sicherheit bereits in der Voreinstellung**
- ⊖ **einige Funktionen sind nur in der kostenpflichtigen Pro-Version enthalten**

Funktionen	●●●●○
Sicherheit	●●●●●
Bedienung	●●●●○
Gesamt	●●●●◐
Preis-Leistungs-Verhältnis	●●●●●

Testurteil: konsequente Weiterentwicklung eines guten Produkts, die durchweg überzeugen konnte.

Wer darf, wer nicht: Die Regeln erlauben den Internet-Zugriff

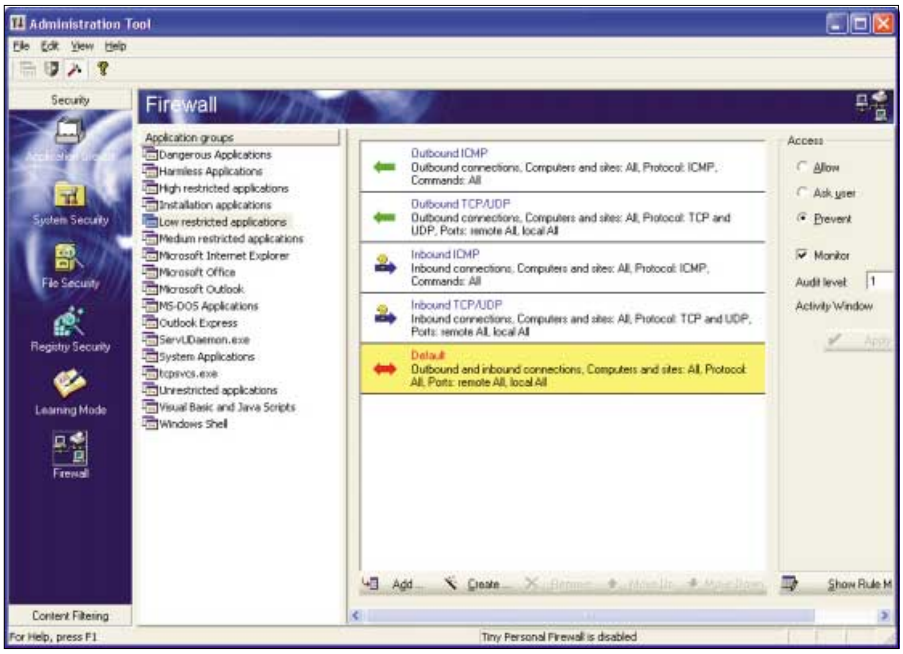
Gesendete Datenpakete erkennt die Firewall und bietet üblicherweise die Regelerstellung an. Sie können an dieser Stelle aber auch den Inhalt des gesendeten Pakets anzeigen lassen. Hieraus lassen sich interessante Informationen gewinnen, wenn Sie wissen möchten, welche Daten an wen gesendet werden. Zu den angezeigten Informationen gehören das sendende Programm zusammen mit der Prozess-ID unter Windows XP sowie IP-Adressen und Port-Nummern der Verbindung. Es folgen Informationen zu Ethernet sowie zu IP- und TCP-Protokoll. Schließlich werden die Nutzdaten hexadezimal und in Ascii angezeigt. Wie fast alle Personal Firewalls arbeitet auch Sygate auf Anwendungsebene. Sicherheit erreicht sie durch Blockieren bestimmter Anwendungen. Jedoch lassen sich für jedes Programm Regeln definieren, die nur bestimmte IP-Adressen und Ports für die Kommunikation erlauben. Nmap-Scans bleiben bereits in der Voreinstellung wirkungslos, ICMP und die Netbios-Ports sind blockiert.

Die Liste der Verbesserungen in dieser Version ist beachtlich: So überwacht die Firewall Protokolltreiber und soll damit verhindern, dass zum Beispiel Trojaner eigene Protokolle für die Kommunikation installieren. Broadcast-Verkehr wird gefiltert und damit das Logging vereinfacht. Der Schutz vor fragmentierten IP-Datagrammen wurde optimiert – das soll Systemabstürze durch diese Art von Angriffen verhindern. Weitere Neuerungen betreffen einen verbesserten Schutz vor Denial-of-Service-Angriffen sowie das Lauschen von Trojanern auf bestimmten Ports ohne Kenntnis des Anwenders. Erwähnenswert ist der Sygate Online Service (SOS), der allerdings in der Vergangenheit nicht immer korrekte Ergebnisse lieferte, sowie das gut besuchte Forum in englischer Sprache.

Tiny Personal Firewall 3.0: Mit Sandbox und Content-Filter

Die populäre Tiny Personal Firewall 3.0 (TPF) von Tiny Software ist in der Version 3.0 stark erweitert worden – die alte Version 2.1.4 wird nun von Kerio (**www.kerio.com**) vertrieben. Die Neuerungen betreffen vor allem die Sandbox, die bösartige Programme am Ressourcen-Zugriff hindern soll, und die Content-Filter, die aktive Inhalte wie Java-Applets und Active-X-Controls überwachen.

Die englischsprachige Firewall besteht aus einer Anwendung für die Administration, der Engine für die Low-Level-Treiber für Ndis und TDI sowie einem Activity-Fenster, das Infos über bestehende Internet-Verbindungen anzeigt. Engine und Activity-Fenster starten Sie über ein Symbol im Gerätefeld der Taskleiste.



Vordefiniert: Die Firewall-Regeln erleichtern den Einstieg in die komplexe und gerade für Einsteiger bisweilen undurchsichtige Konfiguration der Tiny Personal Firewall enorm und bieten schnellen Schutz

Schutzzone: Ohne Legitimation geht rein gar nichts

Die Sandbox dient dem Schutz von Ressourcen wie der Registry und dem Dateisystem, soll aber auch Zugriffe auf bestimmte Dienste verhindern und gefährliche Systemaufrufe bemerken. Das Starten von Kindprozessen durch ein bösartiges Programm wird ebenfalls verhindert. In der Vergangenheit ist mit solchen Tricks vor allem der Internet Explorer überlistet worden: Mit wenig Aufwand kann damit jede Firewall getunnelt werden. Dabei werden beliebige Daten an der Firewall vorbeigeschleust. Jede ausführbare Datei wird in Kategorien wie „eingeschränkt“ oder „nicht eingeschränkt“ eingeordnet, die bestimmten Beschränkungen unterliegen. Einige Kategorien sind bereits vordefiniert, zum Beispiel für Outlook oder den Internet Explorer. Sie können die Sandbox sehr fein justieren, was jedoch einige Einarbeitungszeit erfordert. Die Konfiguration ist insgesamt komplex.

Dazu passend verfügt die Firewall über ein Modul zur Browser-Cache-Verwaltung, einen Cookie-Manager, URL- und Mailfilterung sowie einen optionalen Virenscanner von McAfee.

Tiny Personal Firewall 3.0

Info: Tiny Software
www.tinysoftware.com
Preis: kostenlos für privaten Gebrauch

⊕ **viele Funktionen**
⊖ **komplizierte Konfiguration**

Funktionen	●●●●●
Sicherheit	●●●●●
Bedienung	●●●●○
Gesamt	●●●●●
Preis-Leistungs-Verhältnis	●●●●●

Testurteil: Die TPF fordert vom Anwender einiges: Das Produkt meldet ständig Vorfälle, die entsprechend behandelt werden müssen. Die Konfiguration ist aufwändig, das englischsprachige Handbuch mit rund 100 Seiten ist für Anwender ausreichend, sagt aber nichts über die interne Funktionsweise.

Fingerabdruck: Eindeutige Kennzeichnung der Programme

Firewall-Regeln sind ebenfalls für Kategorien sowie bekannte Anwendungen vordefiniert. Sie basieren auf der Richtung der Datenübertragung (Inbound, Outbound), dem Protokoll (TCP, UDP, ICMP), der fernen IP-Adresse sowie dem lokalen und fernen Port. Gut gelungen ist das Auditing: Alle protokollierten Ereignisse können Sie übersichtlich im Browser aufrufen und sortieren lassen.

Mit den Fingerprints verhindert die Firewall das Austauschen von harmlosen Programmen durch bösartige – ein beliebter Trick, um zum Beispiel einen Trojaner zu tarnen. Dazu ist es jedoch notwendig, dass alle ausführbaren Programme erfasst und in Kategorien eingeteilt werden. Das gilt auch für jede neu installierte Anwendung. Insgesamt ist diese Art von Sicherheitstechnik zwar gut, aber recht aufwändig zu konfigurieren.

In der Voreinstellung nach der Installation reagiert Tiny Personal Firewall auf keinerlei Verbindungsversuche aus dem Internet: Alle Nmap-Port-Scans werden geblockt (stealth), ICMP wird nicht beantwortet und die Netbios-Ports sind ebenfalls blockiert.

Gleiche Software: Mal kostenlos, mal nicht

Tiny Software platziert seine Firewall sowohl im privaten als auch im geschäftlichen Bereich. Für Privatanwender ist das Produkt kostenlos, Geschäftskunden zahlen 39 US-Dollar, Volumenlizenzen werden angeboten. Im gewerblichen Bereich spielt die Fernwartung eine große Rolle. Diese Funktion ist neu in dieser Version. Sie erlaubt die zentrale Konfiguration der Sicherheitseinstellungen aller Desktop-Firewalls durch einen Server – ein Feature, das sich bei kaum einem anderen Produkt findet.

Die TPF stellt recht hohe Anforderungen an das Wissen des Anwenders. Für die richtige Regelerstellung ist einiges Know-how erforderlich. Aufgrund der großen Verbreitung dieses Produkts finden sich aber etliche Tipps im Internet. ▶

Windows-XP-Firewall: Gratis mit an Bord

Die Firewall von Windows XP (Internet Connection Firewall, ICF) ist vom Typ Stateful Inspection (statusbehaftet), das heißt, sie berücksichtigt eingehende Datenpakete im Zusammenhang mit vorher ausgehenden. Die ICF bietet ein Port-Mapping, wie es von Routern bekannt ist, so-

Internet Connection Firewall

Info: Microsoft
www.microsoft.com
Preis: in Windows XP enthalten

⊕ **gute Sicherheit, einfach zu bedienen, Port-Mapping**
⊖ **wenig Funktionen, kaum dokumentiert**

Funktionen	●●●○○
Sicherheit	●●●●●
Bedienung	●●●●○
Gesamt	●●●●○
Preis-Leistungs-Verhältnis	●●●●●

Testurteil: Die ICF bietet eine hohe Sicherheit bei eingehenden, nicht jedoch bei ausgehenden Verbindungen.

wie eine Blockierung von ICMP. Über das Port-Mapping wird ein Zugang aus dem Internet zum Beispiel zu einem Web-Server im LAN durch die Firewall hindurch ermöglicht. Die ICF kann für jedes Verbindungsgerät wie DFÜ-Adapter oder Netzwerkkarte getrennt konfiguriert werden. Damit ist einerseits ein Schutz vor Zugriffen aus dem Internet gegeben, andererseits lässt sich damit auch ein PC in einem LAN vor Zugriffen schützen. Die ICF können Sie sowohl auf Einzelplatz-PCs mit direktem Internet-Anschluss als auch für ein kleines LAN über die Internetverbindungsfreigabe einschalten.

Beim Test der ICF in den Voreinstellungen mit Online-Scannern wie Sygate Online Service waren alle Wellknown-Ports (1-1023) sowie etliche typische Trojaner-Ports unsichtbar (stealth). Auch die Netbios-Ports UDP und TCP 135 bis 139, die für die Freigaben verantwortlich sind, sind stealth. Damit ist der Zugriff auf Ihre Freigaben über das Internet unterbunden. Allerdings bemerkt die ICF keinen ausgehenden Datenverkehr, Spyware oder Trojaner bleiben damit unbemerkt. Der Betrieb einer zusätzlichen Personal

Vordefinierte Firewall-Regeln: Sie erleichtern den Einstieg in die komplexe Konfiguration

Firewall wie Zone Alarm, Outpost oder Sygate 5.0 ist daher ratsam.

Die zweite wesentliche Schutzfunktion der ICF besteht im Blocken von ICMP-Nachrichten. Die ICF bietet zwar nur wenige Funktionen, die Schutzwirkung ist jedoch gut. Das Port-Mapping ist eine Besonderheit, die die meisten anderen Produkte nicht zu bieten haben.

Zone Alarm 3.1.291: Gratis und vielseitig

Das für den privaten Gebrauch kostenlose englischsprachige Zone Alarm funktioniert als Application Firewall und Intrusion Detection System (IDS), erkennt also sowohl eingehenden als auch ausgehenden Datenverkehr.

Über eine „Lock" genannte Schaltfläche mit dem Symbol eines Vorhänge-

Zone Alarm 3.1.291

Info: Zone Labs
www.zonelabs.com
Preis: kostenlos für privaten Gebrauch

⊕ **gute Sicherheit, einfach zu bedienen**
⊖ **keine Regelerstellung, bislang nur in englischer Sprache**

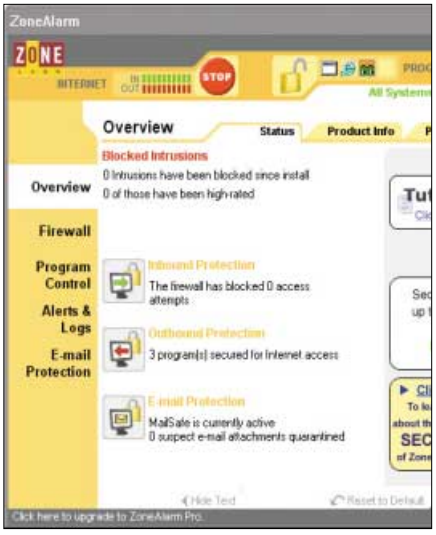
Funktionen	●●●●○
Sicherheit	●●●●●
Bedienung	●●●●●
Gesamt	●●●●◐
Preis-Leistungs-Verhältnis	●●●●●

Testurteil: gute Firewall, für Einsteiger geeignet.

schlosses sperren Sie den Internet-Zugriff aller Programme und über die Stop-Schaltfläche – eine Art Notaus- oder Panik-Schalter — unterbrechen Sie sofort sämtlichen Internet-Verkehr.

„Overview" zeigt den Status der Firewall an. Dazu gehören erkannte Einbruchsversuche, die Anzahl eigener Programme mit Internet-Zugang sowie die Anzahl suspekter Mail-Anhänge. Über „Firewall" legen Sie eine von drei Sicherheitsstufen für das LAN sowie das Internet fest. Wichtig ist hier der Stealthmode der höchsten Sicherheitsstufe. Er verhindert, dass der eigene PC nach außen sichtbar ist, und ist für das Internet die sinnvolle Voreinstellung. Im eigenen LAN sollten Sie hingegen die mittlere Stufe einstellen. In der niedrigsten Stufe ist die Firewall abgeschaltet. Unter „Program Control" stellen Sie ein, ob ein Programm fragen muss, bevor es eine Verbindung herstellt. Dort befindet sich auch eine Liste aller Programme, die Zone Alarm kennt.

Der Lernmodus erstellt automatisch Regeln. Sobald ein Programm Internet-Zugriff wünscht, öffnet sich ein Fenster mit dem Programmnamen. „Yes" erlaubt



Wichtige Funktionen: Das Hauptfenster von Zone Alarm mit den aktuellen Sicherheitseinstellungen

den Zugriff, mit „No" wird er untersagt. Da sich die Regeln nicht speichern lassen, müssen Sie das Prozedere im Falle einer Windows-Neuinstallation wiederholen.

Bei den Scans in der hohen Sicherheitsstufe zeigte der Gibson Research Scan alle Ports als „stealth" an. Zone Alarm ist einfach zu bedienen und erfordert keine tieferen Kenntnisse der Materie.

Schnelleinstieg Personal Firewalls

Die Firewall-FAQ

Wer sich für Personal Firewalls interessiert, muss ihre Arbeitsweise verstehen. Mit unserem Firewall-Ratgeber im Frage-und-Antwort-Stil eignen Sie sich das erforderliche Basiswissen an.

Suchmaschinen liefern beim Suchbegriff Firewall mehrere Hundert bis Tausend Treffer. So ist die Anzahl kommerzieller Websites und privater Homepages zum Thema PC-Absicherung kaum mehr zu überblicken. Gerade Einsteiger finden kaum Antworten auf grundlegende Fragen zu Firewalls. Wir haben die wichtigsten Einsteiger-Fragen und kompakte Antworten in dieser FAQ gebündelt.

1. Firewall – was ist darunter zu verstehen?

Firewalls trennen zwei Netzwerke voneinander, zum Beispiel ein Firmennetzwerk, ein kleines Heimnetzwerk oder einen Einzelplatz-PC (inneres Netzwerk) vom Internet (äußeres Netzwerk). Die Anwender im inneren Netzwerk können etwa im Web surfen und E-Mail nutzen, vom äußeren Netzwerk gelangt aber niemand auf die Computer des inneren Netzwerks. Es gibt Hard- und Software-Firewalls, wobei sich letztere nicht zuletzt aufgrund günstiger Preise durchsetzen.

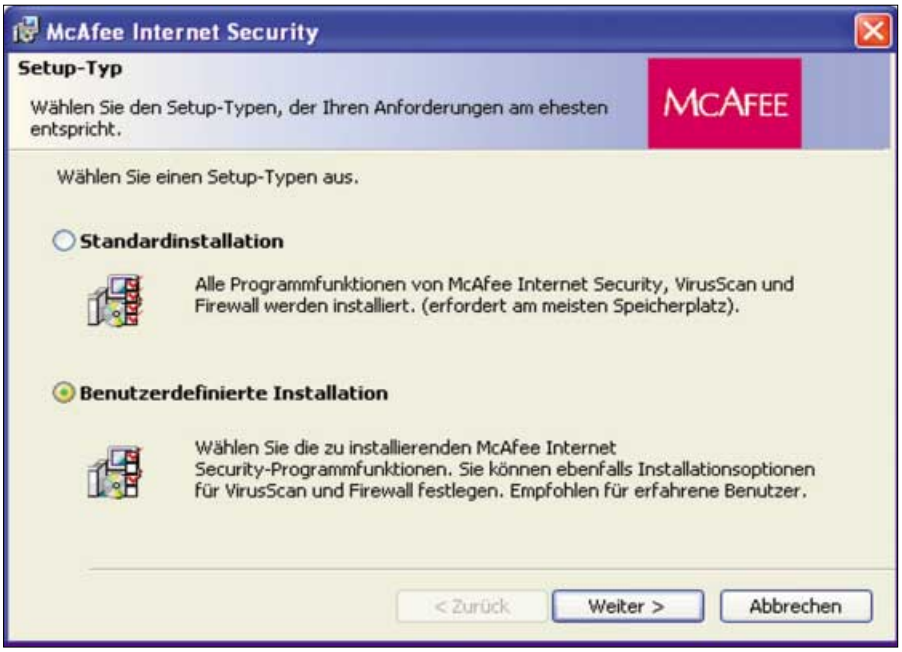
2. Warum sollte ich eine Firewall einsetzen?

Es gibt mindestens vier gute Gründe für den Betrieb einer Personal Firewall:

- Um falsch konfigurierte Rechner zu schützen
- Um installierte Trojaner und Viren zu erkennen
- Um versteckte Ad- und Spyware zu identifizieren
- Um etwas über Sicherheit in Netzwerken erfahren

Info: Personal Firewall

Die kostenlosen Schutzprogramme erfreuen sich großer Beliebtheit und rangieren in den Download-Statistiken ganz weit oben. In unserer FAQ erfahren Sie Wissenswertes über die Arbeitsweise.



Sorgfältige Planung: Bereits vor der Installation einer Personal Firewall sollten Sie eine Liste aller Anwendungen erstellen, die Verbindung zum Internet benötigen, und deren Port-Adressen herausfinden

Eine falsche Rechnerkonfiguration betrifft besonders nach außen sichtbare Netzwerkfreigaben und aus Unwissenheit des Anwenders installierte Server-Software wie etwa den Internet Information Server bei Windows 2000/XP. Eine Personal Firewall blockiert diese Dienste.

Trojaner und Viren werden teilweise erkannt, da sie eine Verbindung ins Internet aufbauen müssen oder auf eine solche warten. Heimliche Verbindungsversuche sollten von einer guten Firewall erkannt werden. Von den derzeit kursierenden Ad- und Spyware-Varianten geht zwar keine wirkliche Gefahr aus – sie versenden „nur“ unbemerkt Informationen vom Anwender-PC ins Internet. Dennoch ist es sinnvoll, die Werberoboter von der Festplatte zu verbannen.

Den Meldungen der Firewall sollte der Anwender so lange nachgehen, bis er weiß, was sie bedeuten: Handbücher lesen, Support-Seiten studieren und Diskussionsforen oder Newsgroups lesen hilft beim Verständnis.

3. Welche Firewall soll ich verwenden? Welche ist gut?

Diese Frage ist nicht leicht zu beantworten. Die meisten Produkte bieten eine gute Basis-Schutzwirkung und reichen für einen Einzelplatzrechner oder ein kleines Netzwerk aus. Es ist wichtig zu verstehen, wie das Produkt funktioniert, um sich nicht in falscher Sicherheit zu wiegen. Einfach zu bedienende Produkte

wie Zone Alarm (Workshop ab ▷ Seite 64) sind für Anwender empfehlenswert, die sich nicht zu sehr mit Netzwerksicherheit beschäftigen möchten, ihren PC aber dennoch einigermaßen schützen wollen. Komplexere Produkte wie Outpost oder Norton Internet Security (im Test ab ▷ Seite 50) bieten mehr Konfigurationsmöglichkeiten, erfordern aber auch einen höheren Wissensstand.

4. Wie kann ich prüfen, ob mein Rechner sicher ist?

Alle Firewalls blockieren Ports, über die Verbindungen in das Internet hergestellt werden und umgekehrt. Um zu prüfen, ob die Ports offen, geschlossen oder blockiert sind, verwendet man Portscanner. Wer einen Einzelplatzrechner hat, nutzt am besten Online-Portscanner, die aber meistens nur bestimmte Port-Bereiche untersuchen. Sygate bietet zum Beispiel einen Online-Portscanner unter der Adresse **http://scan.sygatetech.com** an. Der Sygate Online Service (SOS) scannt verschiedene Port-Bereiche, die von typischen Diensten wie HTTP oder FTP, aber auch von Trojanern genutzt werden, und meldet den Zustand der Ports. Ein offener Port kann für eine Verbindungsaufnahme aus dem Internet genutzt werden – er stellt eine Tür in Ihren Rechner dar. Auch geschlossene Ports melden einem potenziellen Eindringling: Hier ist etwas. Der sicherste Zustand ist der Stealth-Zustand. Ein Port im Stealth-Zustand gibt überhaupt keine Antwort, jede Anfrage wird kommentarlos verworfen. SOS wie auch die Testseite des Datenschutzexperten Steve Gibson unter der Adresse **http://grc.com** testen Ports auf den Stealth-Zustand. Bei GRC wählen Sie „Shieldsup!“ und dann „Probe my Ports!“.

Verschiedene Testseiten können jedoch verschiedene Ergebnisse liefern. Dann sollten Sie zunächst die Seriosität der Seiten abwägen. Testseiten von Firewall-Herstellern verfolgen möglicherweise bestimmte unternehmenspolitische Ziele, unabhängige Seiten eher nicht. Auch gibt es fehlerhafte Testseiten. Unstimmigkeiten müssen Sie jedenfalls klären.

In einem lokalen Netzwerk liefern Portscanner wie Superscan 3.0 (englischsprachige Version ◉ auf Heft-CD oder unter **www.foundstone.com**) und Languard (englischsprachige Version ◉ auf Heft-CD oder unter **www.gfi.com/languard/**) detaillierte Informationen nicht nur über die Ports. Solche Scanner funktionieren natürlich auch im Internet.

Auf dem Laufenden: Portale zum Thema Sicherheit – hier das deutschsprachige Blue Merlin (**www.bluemerlin-security.de**) – informieren über Personal Firewalls und Sicherheits-Scanner

5. Ich habe offene Ports. Bin ich angreifbar?

Ja. Wer Dienste wie Web- oder FTP-Server im Internet anbietet, läuft immer Gefahr, dass diese kompromittiert werden. Ständig werden Fehler in Server-Software gefunden, die verschiedenste Angriffe erlauben. Als Gegenmaßnahme bleibt nur die Installation der jeweils neuesten Sicherheits-Patches der Hersteller. Zu den gefährlichen Ports gehört Port 139, der für die Freigaben in Windows-Netzwerken (Netbios-Netzwerken) zuständig ist. Dieser Port sollte auf der Internet-Schnittstelle grundsätzlich unsichtbar sein. Zum Testen eignen sich Online-Scanner, die aber nur kleine Ausschnitte aus dem gesamten Portbereich – meistens nur einige „Wellknown Ports“ sowie einige wenige typische Trojaner-Ports – testen. Verbindungen auf Ports größer als 1023 werden häufig nicht erfasst. Dort befindet sich die Spielwiese der Backdoors und Trojaner. Ein- und ausgehende Verbindungen auf solchen Ports sollten von der Firewall erkannt werden. Verlassen kann man sich jedoch nicht darauf. Alle aktiven Sockets (IP-Adressen und Portnummern) kann man leicht mit dem Kommandozeilen-Befehl „netstat -an“ anzeigen lassen. Das Problem dabei: Verbindungen können schnell geöffnet und auch wieder geschlossen werden. Wenn man nicht innerhalb dieses Zeitfensters den Netstat-Befehl ausführt, bleibt die Verbindung unerkannt.

6. Kann ich im kleinen LAN eine Personal Firewall einsetzen?

Ja. Die meisten Produkte bieten inzwischen LAN-Unterstützung. Wichtig ist die Unterscheidung zwischen interner Netzwerkanbindung ins LAN und externer Internet-Verbindung. Im Idealfall lässt sich die Firewall für beide Schnittstellen unterschiedlich konfigurieren. Die meisten Produkte bieten diese Unterscheidung jedoch nicht, sondern erlauben stattdessen die Angabe von vertrauten IP-Adressen, -Bereichen oder Subnetzen. Das eigene Netzwerk sollte immer mit privaten IP-Adressen konfiguriert sein (zum Beispiel 192.168.x.x), die dann in der Firewall als vertrauenswürdig („trusted“) eingetragen werden. Der Zugriff auf solche Adressen über das Internet funktioniert nicht, da sie nicht geroutet werden.

Ist bereits ein LAN eingerichtet und wird später eine Firewall dazugeschaltet, müssen die im LAN benötigten Dienste in der Firewall freigeschaltet werden.

7. Warum funktioniert das LAN mit der Firewall nicht mehr?

Ruhe bewahren. Die Firewall macht das, was sie machen soll: Sie blockiert Dienste und Verbindungen und zwar alle. Ein- und ausgehende Verbindungen müssen

erst explizit erlaubt werden, damit etwas funktioniert. Meistens funktionieren nach der Installation einer Personal Firewall die Freigaben im LAN nicht mehr, dann ist so zu verfahren wie in der vorhergehenden Antwort beschrieben. Auch typische Client-Verbindungen wie ICQ oder IRC müssen erst in der Firewall freigeschaltet werden. Betroffen sind grundsätzlich alle Internet-Anwendungen, auch News- und FTP-Clients, Online-Spiele, Filesharing-Tools oder Instant Messenger-Clients, Netmeeting und so weiter. Der Betrieb solcher Produkte in einem LAN kann durchaus problematisch sein: Die Firewall muss all diese Verbindungen unterstützen. Mit einer geeigneten Produktkombination aus Proxy-Server und/oder Firewall sowie eventuell bestimmter Software auf den Clients kann jedoch jeder Dienst im LAN verfügbar gemacht werden. Ein beliebter Trick ist etwa der Einsatz von Sockscap (Download kostenlos für private Nutzung und verschiedene Betriebssysteme unter **www.socks.nec.com/reference/sockscap.html**) um Socket-Anwendungen wie Filesharing-Tools im LAN zu betreiben.

8. Was sagen Blue-Screens nach der Firewall-Installation aus?

Das Produkt ist nicht mit der vorhandenen Software-Installation kompatibel oder umgekehrt. Dieser seltene Fall ist meistens auf eine „vermurkste" Windows-Installation zurückzuführen: Software-Fehler können Windows lahm legen und eine Neuinstallation erforderlich machen. Je mehr Software installiert und unvollständig oder falsch konfiguriert wird, desto kürzer kann die Windows-Lebensdauer sein. Nach einer Windows-Neuinstallation sollte die Firewall einwandfrei laufen.

Eine weitere Möglichkeit: Die Firewall kommt nicht mit den Netzwerkkartentreibern zurecht, beispielsweise mit den verbreiteten DSL-Treibern von Robert Schlabbach. In diesem Fall ist das Produkt unbrauchbar.

9. Bringt mir eine zweite Firewall mehr Sicherheit?

Wahrscheinlich nicht. Firewalls klinken sich auf der Ebene der Netzwerkkartentreiber ein und filtern dort den Datenverkehr. Je mehr Prozesse dort eingreifen, desto höher ist die Absturzgefahr. Ein Produkt sollte ausreichen, um den gewünschten Sicherheitsgrad zu erreichen. Zwei Firewalls behindern sich.

Unvollständige Produktbeschreibungen: Die Herstellerangaben im Internet verraten nicht, wie eine Firewall im Alltag zu bedienen ist. Aufschluss bieten kostenlose Demoversionen

10. Was bedeuten die Meldungen über Angriffe?

Das sind meistens Fehlalarme. Einige Produkte wie Zone Alarm aber auch die McAfee-Firewall schlagen bei fast jedem ankommenden Datenpaket Alarm. In den meisten Fällen handelt es sich dabei um Portscans oder zufällig erfolgte Verbindungsversuche. Die Protokolle geben Auskunft darüber. Leider sind viele Logdateien sehr schlecht lesbar, manche zeigen nicht einmal die fernen IP-Adressen an, so dass eine Zurückverfolgung unmöglich ist. Einige Produkte liefern zu jedem vermeintlichen Angriff Links ins Web, wo sich Informationen über die Art des Verbindungsversuchs nachlesen lassen. Die hektische Betriebsamkeit mancher Personal Firewall soll nur einreden: Ich passe auf und war eine gute Investition.

11. Ich werde gehackt, was soll ich tun?

Ruhe bewahren! Die Entscheidung, ob Sie tatsächlich gehackt worden sind oder nicht, ist extrem schwer zu treffen. In den Logdateien werden die IP-Adressen angezeigt, die Verbindungsversuche unternommen haben. Längst nicht alle davon sind Einbruchsversuche. Ein reiner Port-Scan ist noch kein Einbruch, sondern der Normalfall. Wer „always on" und sehr aktiv im Internet ist, kann mit mehreren Scans pro Minute rechnen. Wichtig ist, welcher Port gescannt wurde. Auch das steht in den Logdateien. Scans auf „Wellknown Ports" sind immer verdächtig. Werden die Ports 21, 25, und 80 gescannt, ist ein Einbruchsversuch wahrscheinlich. Ist zum Beispiel Port 1214 gescannt worden, war das Tausch-Tool Kazaa aktiv: Ein anderer Kazaa-Nutzer hat versucht, eine Verbindung zu Ihnen herzustellen. So verhält es sich natürlich auch mit anderen Filesharing-Tools.

12. Wie kann ich einen Angreifer zurückverfolgen?

Wird ein Angreifer vermutet, können Sie seine IP-Adresse mit Tools wie dem englischsprachigen Visual Route (◉ auf Heft-CD und unter **www.visualroute.com**; Registriergebühr: 40 US-Dollar) ausfindig machen. Neben dem Standpunkt seines Einwahl-Routers ist der Besitzer der IP-Adresse leicht ausfindig zu machen. Eine Abfrage seiner IP-Adresse bei **http://www.ripe.net/perl/whois** liefert seinen Namen und den Provider. Mit diesen Informationen sendet Sie eine Mail an den Provider. Meistens wird der aber nichts unternehmen, es sei denn, ein Einbruch ist nachgewiesen. Das ist aber schwierig.

Burkhard Müller

Workshop Zone Alarm Personal Firewall

Vandalen-Killer

Im Internet lebt es sich mitunter gefährlich. Personal Firewalls wie Zone Alarm bieten Schutz vor ungebetenen Gästen. Aber nur dann, wenn sie richtig konfiguriert sind.

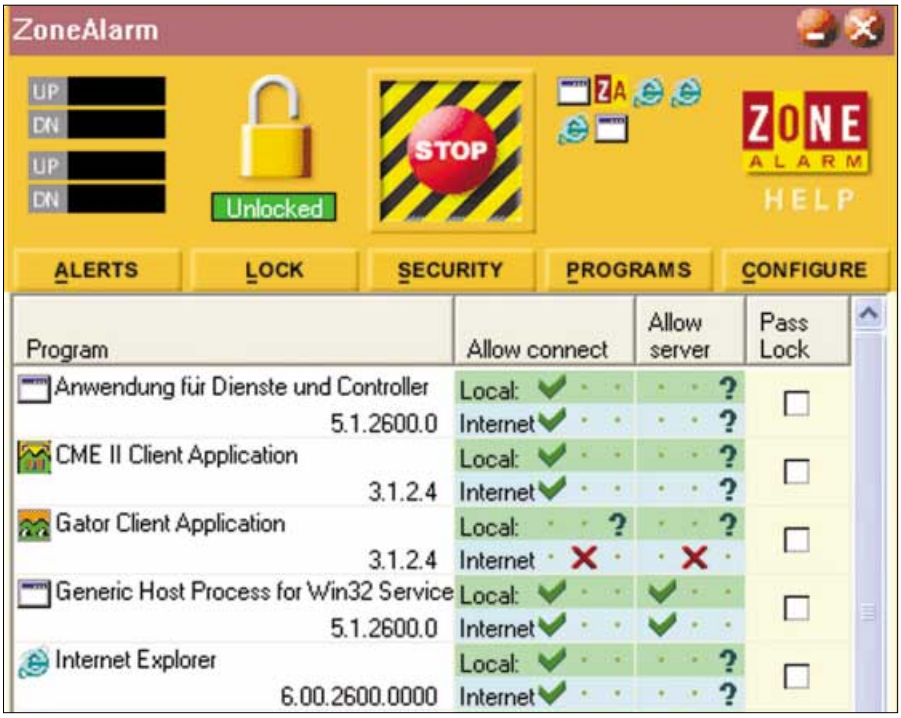
▸Personal Firewalls sollen einen PC oder ein kleines Netzwerk vor Eindringlingen aus dem Internet schützen und Verbindungen vom eigenen PC in das Internet bemerken, wie sie zum Beispiel von tückischen Trojanern oder Spy- und Adware hergestellt werden.

Eine der beliebtesten und bekanntesten Personal Firewalls ist Zone Alarm von Zone Labs. Das Programm ist für den privaten Gebrauch kostenlos. Die aktuelle Freeware-Version 2.6 für Windows 95/98/ME sowie NT 4, 2000 und XP finden Sie auf Heft-CD. Die neue Version 3.0 mit einigen erweiterten Funktionen und neuer, überarbeiteter Oberfläche ist hingegen kostenpflichtig und wird nur als Testversion für 30 Tage zum Download angeboten (**www.zonelabs.com**, englischsprachige Version für Windows 95/98/ME sowie NT 4, 2000 und XP, 4 MB). Bei einer Online-Registrierung werden 50 Dollar fällig.

Zone Alarm ist im Gegensatz zu komplexen Unternehmens-Firewalls einfach zu verstehen, aber – inklusive Dokumentation – nur in englischer Sprache verfügbar. Die folgenden Seiten geben eine Einführung in den Umgang mit Zone Alarm, sie können damit als deutschsprachiges Handbuch verstanden werden. Informationen über weitere Firewall-Techniken sowie über eine Rückverfolgung von Angreifern finden sich in den Kästen.

Info: Zone Alarm 2.6

Seit knapp vier Jahren auf dem Markt, hat sich Zone Alarm als beliebteste Firewall etabliert. Mit wenigen Handgriffen ist Zone Alarm eingerichtet und schützt Ihren PC vor Angriffen aus dem Internet. Wir zeigen Ihnen, worauf Sie achten müssen.



Listenverfahren: In der Programmliste von Zone Alarm legen Sie die Zugriffsart auf das lokale Netzwerk und das Internet fest. Jede Server-Tätigkeit muss vom Anwender erlaubt werden

Anwendungsfilter: Wer darf ins Internet und wer nicht?

Zone Alarm arbeitet als so genannter Anwendungsfilter. Diese Filter überprüfen den Zugriff von Programmen auf das Internet. Sie führen Positiv- und Negativ-Listen, in denen festgehalten ist, ob einer Anwendung der Zugriff auf das Internet erlaubt ist oder nicht (auch schwarze und weiße Listen genannt). Anwendungsfilter sind „lernfähig“: Nach der Installation sind beide Listen leer. Sobald ein Programm auf das Internet zugreift, meldet sich der Anwendungsfilter und verlangt vom Anwender die Entscheidung über den Zugriff: zulassen oder verweigern. Bei typischen bekannten Internet-Anwendungen wie Mailprogrammen, Webbrowsern und FTP-Clients ist die Entscheidung einfach zu treffen: Sie benötigen immer einen Internet-Zugriff. Anders verhält es sich bei unbekannten Anwendungen: Soll der Zugriff gewährt werden oder lieber nicht? Hier müssen Sie sich kundig machen, um was für ein Programm oder um was für einen Dienst es sich handelt. Im Zweifelsfall verweigern Sie den Zugriff. Nachforschungen auf Hersteller-Websites und in Newsgroups können hier hilfreich sein.

Konfiguration: Einfach mit Hilfe des Tutorials

Nach der Installation von Zone Alarm – ein PC-Neustart ist nicht nötig – erfolgt eine kleine Führung durch die Funktionen der Firewall. Nachfolgend die einzelnen Schritte des Tutorials:

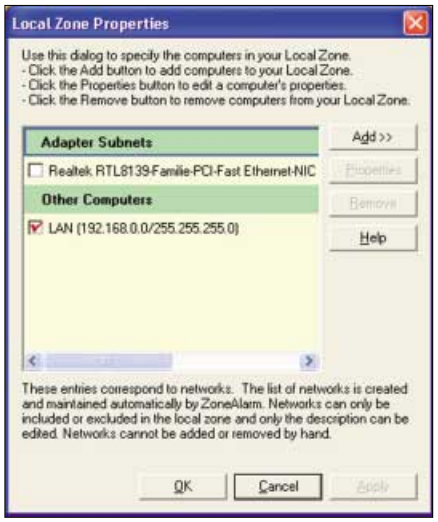
Schritt 1: Begrüßungsmeldung.
Schritt 2: Vorstellung des „Program Alerts"– das Alert-Fenster erscheint immer dann, wenn Zone Alarm eine ausgehende Verbindung entdeckt hat, wenn also ein Programm versucht, eine Internet-Verbindung herzustellen.
Schritt 3: Das „Program Panel"– hier werden die Antworten (siehe Schritt 2) gespeichert. Sie lassen sich jederzeit ändern und anpassen.
Schritt 4: Erklärung des Funktionsprinzips – die Kommunikation mit dem Internet erfolgt über Ports, die mit den Türen eines Gebäudes vergleichbar sind. Zone Alarm blockt den gesamten ein- und ausgehenden Datenverkehr bis auf die Verbindungen, die der Anwender ausdrücklich erlaubt. Durch den „Stealth Mode" (unsichtbar) kann der PC nicht vom Internet aus erkannt werden.
Schritt 5: Das Fenster „Firewall Alert" hat eine ähnliche Bedeutung wie die Meldung „Program Alert", erkennt aber eingehende Verbindungen. Der PC, der versucht, eine Verbindung herzustellen, wird anhand seiner IP-Adresse erkannt.
Schritt 6: Erklärung des Zonenkonzepts – „Local Zone" und „Internet Zone".
Schritt 7: Abschluss des Tutorials.

Während dieser sieben Schritte wird nichts konfiguriert oder eingestellt, sie dienen lediglich dazu, dem Anwender einen kurzen Funktionsüberblick zu geben.

Das Hauptfenster in Zone Alarm verstehen

Das übersichtliche Hauptfenster ist grafisch ansprechend gestaltet. Am linken Rand befinden sich vier Balken für die Upload- und Download-Anzeigen. Die beiden oberen Balken zeigen die aktuelle Internet-Aktivität. Der grüne Balken zeigt den Download, der rote den Upload an. Das Programm, das gerade im Internet aktiv ist, wird auf der rechten Seite als blinkendes Icon dargestellt. Darf das Programm auch als Server agieren, wird dies durch eine kleine Hand unter dem Programmsymbol angezeigt. Die beiden unteren Balken stellen Up- und Download über einen längeren Zeitraum dar.

Über eine „Lock" genannte Schaltfläche mit dem Symbol eines Vorhängeschlosses sperren Sie den Internet-Zugriff aller Programme und über die Stopp-Schaltfläche – eine Art Not-Aus- oder Panik-Schalter – stoppen Sie sofort sämtlichen Internet-Verkehr und kappen die Leitung. Hinter dem Zone-Alarm-Logo befindet sich eine informative, allerdings englischsprachige Online-Hilfe.



Eigenes Netzwerk: In der lokalen Zone lassen sich vertraute Hosts oder Subnetze definieren

Up- und Download-Aktivitäten stellt Zone Alarm in einem kleinen Icon im Gerätefeld der Taskleiste dar. Das Programm lässt sich aber auch vollständig in die Taskleiste integrieren: In den Eigenschaften der Taskleiste erscheint unter dem Menüpunkt „Symbolleisten" der Eintrag „Zone Alarm Desktop Band". Ist er mit einem Haken markiert, erscheint Zone Alarm als eigene Symbolleiste in der Taskleiste. Von dort können Sie sie mit der Maus auch als eigenständiges kleines Fenster auf den Desktop ziehen.

Tech-Info: So funktionieren Personal Firewalls

Jede Firewall ist mehr ein Konzept als ein Produkt: Sie kann im einfachsten Fall auf einem einzigen PC installiert sein, auf dem auch weitere Dienste und Anwendungen laufen können. In größeren Netzwerken kommen meistens mehrere Rechner zum Einsatz, auf denen jeweils eine Sicherheitskomponente installiert ist. Zu diesen Komponenten gehören:

- Statische Paketfilter
- Dynamische Paketfilter (Proxy-Server)

Statische Paketfilter sind einfache Programme, sie bieten nur einen rudimentären Schutz und sind nicht erweiterbar. Proxy-Server bieten eine größere Flexibilität hinsichtlich der Dienste, die im internen Netz genutzt werden können. Eine Kombination von beiden führt zu einem Zwischennetz – der so genannten demilitarisierten Zone (DMZ). Das ist die derzeit sicherste Lösung, die einen höchstmöglichen Schutz vor Attacken aus dem Internet bietet.

Dynamische Paketfilter berücksichtigen den so genannten Kontext einer Verbindung: Die Firewall merkt sich jede ausgehende Verbindung in einer Liste. Kommt eine Antwort aus dem Internet, kann die Firewall anhand dieser Liste entscheiden, welcher Client ursprünglich die Verbindung aufgebaut hat und erlaubt die Kommunikation. Kann kein Client ermittelt werden, wird die Verbindung blockiert. Statische Paketfilter werden zunehmend durch dynamische ersetzt. Diese Art von Filter wird häufig auch in DSL-Routern eingesetzt.

Neben diesen beiden Filtern gibt es weitere Sicherheitskomponenten, die sich auch in Personal Firewalls finden. Diese bestehen aus einer oder mehreren der folgenden Sicherheitskomponenten:

- Anwendungsfilter
- Paketfilter (statisch oder dynamisch)
- Sandbox-Lösungen

Anwendungsfilter überprüfen den Zugriff von Programmen auf das Internet über Positiv- und Negativlisten. Darin enthalten sind die Namen der Anwendungen, die auf das Internet zugreifen dürfen, beziehungsweise die Namen derer, die blockiert werden. Beim erstmaligen Start einer neu installierten Anwendung wird der Filter durch automatisches Lernen aktiviert.

Sandboxes verhindern den Zugriff einer Anwendung auf bestimmte System-Ressourcen wie die Windows-Registrierdatenbank oder das Dateisystem. Die Konfiguration ist meistens komplex, Sandboxes stellen aber einen guten Schutz vor Viren und anderen Schädlingen dar und verhindern deren Verbreitung.

Das Hauptfenster enthält fünf Schaltflächen, über die Sie die Firewall konfigurieren: „Alerts“ zeigt Verbindungsversuche an, mit „Lock“ sperren Sie den Internet-Zugriff zu bestimmten Zeiten, über „Security“ legen Sie eine von drei Sicherheitsstufen für das interne Netzwerk sowie das Internet fest. „Programs“ zeigt eine Liste aller Programme an, die Zone Alarm bekannt sind, und mit „Configure“ nehmen Sie einige allgemeine Einstellungen vor, zum Beispiel, ob Zone Alarm beim Windows-Start automatisch geladen werden soll.

Alerts: Nervig, aber manchmal durchaus nützlich

Das Alert-Fenster zeigt die Verbindungsversuche aus dem Internet an, die Zone Alarm registriert hat. Jeder Versuch ist mit der IP-Adresse der Gegenseite – sofern verfügbar – sowie der Port-Nummer angegeben, über die die Verbindungsaufnahme versucht wurde. Werden Sie Opfer eines Port-Scans, sammeln sich hier schnell einige Hundert Meldungen.

Die Warnungen lassen sich auch in eine Logdatei schreiben, die sich per Voreinstellung im Verzeichnis „%systemroot%\Internet Logs\Zalog.txt“ befindet.

Ist „Show the alert popup windows“ angekreuzt, geht bei jedem Verbindungsversuch ein Fenster mit den Daten der Gegenseite auf: IP-Adresse und Port oder Protokoll, das für den Versuch verwendet wurde. Das ist jedoch nervig und wenig praktikabel. Sie müssen dann nämlich jedes dieser Fenster wegklicken und werden in der eigentlichen Arbeit behindert.

Lock: Alle Internet-Zugriffe temporär abschalten

Mit Lock ist eine Sperre des Internet-Zugriffs gemeint. Sie lässt sich über die gleichnamige Schaltfläche konfigurieren. Per Voreinstellung ist die Sperre abgeschaltet. Schalten Sie die Sperre ein, geben Sie unter „Engage lock“ eine Zeitspanne in Minuten an, nach der der Zugriff gesperrt wird.

Über die Option „Engage Internet lock when screen saver activates“ wird die Sperre automatisch eingeschaltet, sobald der Windows-Bildschirmschoner aktiv wird. Das Umgehen dieser Sperre, die sich in der Programmliste für jedes Programm einschalten lässt, können Sie hier für alle Programme erlauben oder verbieten.

Zugriff erlaubt oder nicht: Jede Anwendung, die ins Internet will, muss erst an Zone Alarm vorbei

Security: Zonenkonzept für mehr Sicherheit

Zone Alarm verwaltet zwei Zonen: die lokale und die Internet-Zone. Die lokale Zone enthält alle Computer, denen uneingeschränkt vertraut wird. Dazu gehört das eigene Netzwerk (LAN), aber auch Computer aus dem Internet. Über die Schaltfläche „Advanced“ nehmen Sie Host, IP-Adressbereiche oder Subnetze in die lokale Zone auf. Zu Beginn ist sie leer.

Der Generic Host Process for Win32-Services

Windows-XP-Anwender werden sehr schnell mit dem ominösen „Generic Host Process for Win32-Services“ Bekanntschaft machen, der gleichermaßen als Client und Server fungieren möchte. Die Internet-Aktivität wird von Zone Alarm erkannt und gemeldet.

Anhand dieses Prozesses lässt sich sehr einfach aufzeigen, was alles hinter so einer Meldung stecken kann und was Sie alles daraus lernen können. Dieser Prozess (SVCHOST.EXE, im Taskmanager unter „Prozesse“ zu sehen) erscheint gleich viermal in der Prozessliste: Zweimal unter dem „System“-Konto sowie je einmal unter den Konten „Netzwerkdienst“ und „Lokaler Dienst“. Er fasst mehrere Prozesse, unter anderem aus Sicherheitsgründen, zu den vier besagten Instanzen zusammen. Läuft Svchost beispielsweise unter dem Konto „Lokaler Dienst“, vereint der Prozess die folgenden Windows-Funktionen:

- TCP/IP Netbios Hilfsprogramm
- Remote Registry
- Simple Service Discovery Protocol (SSDP-Suchdienst)
- Web Client Services

Das TCP/IP Netbios Hilfsprogramm ermöglicht das Ausführen von „NetBIOS over TCP/IP“ (NBT) und der Netbios-Namensauflösung. Der SSDP-Suchdienst ist neu in Windows XP und erlaubt das Finden von UPnP-Geräten (Universal Plug & Play).

Svchost benötigt weder Benutzernamen noch Passwort im Netz: Verbindungen zu diesem Prozess erfolgen statt dessen über eine so genannte Null-Session, das sind Verbindungen zu IPC$. IPC$ wird für die so genannten Remote Procedure Calls verwendet, mit deren Hilfe ein Computer Funktionen auf einem anderen Computer über das Netzwerk aufrufen kann. Weitere Informationen über diese Prozesse finden sich unter „Dienste“ in der Computerverwaltung. In den Eigenschaften des Dienstes „Netzwerkverbindungen“ heißt es zum Beispiel: „Verwaltet Objekte im Ordner ‚Netzwerk- und DFÜ-Verbindungen‘, in dem sowohl LAN-, als auch WAN-Verbindungen angezeigt werden“. Läuft Svchost unter dem Konto „Netzwerkdienst“ stellt er die DNS-Client-Funktion zur Verfügung, unter dem „System“-Konto laufen sogar 29 verschiedene Prozesse.

Daraus muss man schließen: Der Svchost sollte nicht blockiert werden, da sonst wichtige Windows-Funktionen ebenfalls blockiert werden. Windows-eigene Prozesse, die von sich aus auf das Internet zugreifen, muss man wohl oder übel zulassen oder durch Ausprobieren feststellen, was nach dem Blocken nicht mehr funktioniert. Weitere Informationen zu diesem rege diskutierten Thema finden sich unter: **www.bugnet.com/analysis/0201/sfxpfbi2.html**.

Alle Computer, die nicht Mitglied der lokalen Zone sind, gehören automatisch zur Internet-Zone. Für jede Zone stellen Sie eine von drei Sicherheitsstufen ein: „Low“, „Medium“ oder „High“. Die Voreinstellung für die lokale Zone ist „Medium“. In dieser Sicherheitsstufe werden alle Einstellungen der Programmliste beachtet, und die Internet-Sperre bleibt funktionsfähig. Insbesondere wird lokaler Zugriff auf Freigaben erlaubt, eine Einstellung, die in der hohen Sicherheitsstufe natürlich fehlt. Alle Zugriffe aus dem LAN sind erlaubt. In der hohen Sicherheitsstufe werden alle Ports blockiert, die nicht ausdrücklich zugelassen werden. Zone Alarm verwendet dabei den Stealth Mode, der einen Port nicht nur blockiert, sondern von außen unsichtbar macht. Damit sieht es so aus, als sei der Computer nicht vorhanden. In der niedrigen Sicherheitsstufe bleiben die Netbios-Dienste (Datei- und Drucker-Sharing) aktiviert, so dass sich zum Beispiel jemand zu Ihrem PC hin verbinden und sogar auf Ihrem Drucker etwas ausdrucken kann – und das nicht nur im LAN, sondern bei geeigneter Konfiguration auch über das Internet.

In der Internet-Zone haben die Sicherheitsstufen eine etwas andere Bedeutung. Bei „Medium“ werden etwa die Netbios-Dienste geblockt, im Gegensatz zur lokalen Zone. Die hohe Sicherheitsstufe ist die Voreinstellung für die Internet-Zone. Auch bei Zone Labs hat man auf Würmer

Spannend wie ein Krimi: Rückverfolgen von Angreifern

Versucht ein Programm oder ein Prozess, eine Verbindung in das Internet herzustellen, meldet Zone Alarm den betreffenden Prozess und zeigt die IP-Adresse des Zielrechners im „Programm Alert“ an. Mit dieser IP-Adresse lassen sich Informationen gewinnen, die häufig auf eine Person oder Firma schließen lassen. Mit etwas Glück bringt man sogar die Telefonnummer des Verantwortlichen in Erfahrung und kann sich gegebenenfalls dort beschweren, ohne den eigenen Schreibtisch verlassen zu müssen.

Als Beispiel für eine Rückverfolgung verwenden wir die Meldung „CMESys.exe möchte eine Verbindung zu 64.94.89.146 herstellen“.

1. Zunächst ist die IP-Adresse anzupingen (ping 64.94.89.146): In diesem Fall kommt keine Antwort zurück, die Adresse ist also nicht vorhanden, oder ICMP (Ping) wird von einer Firewall blockiert. Wir vermuten Letzteres.

Mysteriöser Internet-Zugriff: Was hinter dieser Meldung steckt, muss man selbst herausfinden

2. Ein Tracert (Befehl „tracert 64.94.89.146“) geht über Washington nach San Jose und verliert sich dort. Die Spur führt also an die Westküste und sagt uns: Die IP-Adresse ist vorhanden.

3. Wir geben die IP-Adresse im Browser ein, vielleicht läuft ja dort ein Webserver. Das Ergebnis ist positiv: Es erscheint zwar keine Seite, dafür aber der Hinweis, dass der Zugriff auf diese Seite gesperrt ist. Irgendetwas muss da also sein.

4. Jetzt wird es spannend: Über **www.ripe.net** führen wir eine Whois-Suche durch, erhalten aber nur die Antwort, dass diese Adresse woanders in der Welt registriert ist. Ripe ist für die Vergabe von IP-Adressen in Europa zuständig (in Deutschland ist es die Denic). Da wir bereits wissen, dass wir an der Westküste suchen müssen, werfen wir die Suchmaschine Google an und suchen nach „whois usa“. Der erste Treffer führt uns zu **http://ws.arin.net/cgi-bin/whois.pl**, der amerikanischen Registrierungsstelle für IP-Adressen. Dort geben wir die IP-Adresse ein und erhalten die Antwort: Diese Adresse gehört zu Gator.com. Mit dieser Information sehen wir uns **www.gator.com** an. Die Arin-Datenbank zeigt im Gegensatz zur Denic aus Sicherheitsgründen keine Telefonnummern an, telefonisch beschweren können wir uns daher noch nicht.

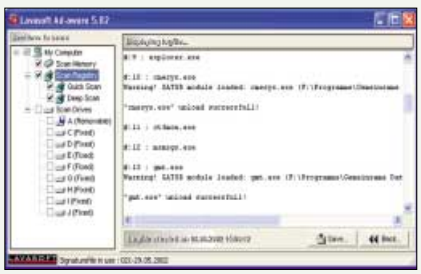
5. Wer Gator noch nicht kennt, sucht in Google. Das Ergebnis: Gator ist eine Firma mit Sitz in Kalifornien, die auf Online-Werbung spezialisiert ist.

6. Die verdächtige Anwendung wird also wahrscheinlich ein Werbe-Trojaner sein: Mit dem kostenlosen Werbekiller Ad-Aware (Lavasoft, **www.lavasoftusa.com**, 3 MB, ◉ auf Heft-CD) für Windows 95/98/ME sowie NT 4, 2000 und XP verschaffen wir uns Gewissheit. CME II wird als Werbe-Trojaner identifiziert und kann von Ad-Aware eliminiert werden.

Das war ein einfaches Beispiel, weil Gator als Hersteller von Werbeprogrammen zur Genüge im Internet bekannt ist. Der Weg der Informationsbeschaffung ist aber immer der gleiche. Da Arin die Adresse mitgeteilt hat, können wir nun weiter recherchieren und die Telefonnummer herausbekommen.

Natürlich beschwert sich niemand telefonisch bei Gator, in anderen Fällen kann das aber wichtig sein: Bei der Denic kann man die Telefonnummer des „admin-c“ in Erfahrung bringen, das ist der technisch Verantwortliche für die IP-Adresse(n). Im Falle eines echten Angriffs von dieser IP-Adresse sollte der admin-c sehr an dieser Information interessiert sein.

Schwierig wird es bei dynamisch zugewiesenen IP-Adressen wie zum Beispiel bei T-Online oder AOL. Hier verliert sich die Spur im Rechenzentrum der Online-Dienste, und man kann nur noch eine Beschwerde an die Abuse-Adresse des Providers senden (**abuse@‹provider›.de**). Bei den Providern darf man sich allerdings kaum Hoffnung machen, dass sie auf solche Beschwerden reagieren.



Riskante Software: Ad-Aware hat Parasiten aufgespürt und kann die Werbekomponenten entfernen

wie Iloveyou reagiert und eine „MailSafe e-mail protection“ genannte Funktion eingebaut, die VB-Script-Dateien in Mailanhängen aufspürt. Dabei wird lediglich die Endung .VBS erkannt. Die Pro-Version von Zone Alarm kann hingegen 46 Dateitypen erkennen. Erhalten Sie einen solchen Anhang, ändert Zone Alarm die Datei-Endung, so dass das Script nicht mehr ohne weiteres ausgeführt werden kann, und zeigt das Symbol etwa in Outlook mit einem großen roten Kreuz an. Eine deutliche Warnung. Öffnen Sie dennoch den Anhang, erhalten Sie eine Fehlermeldung von Zone Alarm.

Programs: Weiße und schwarze Listen zur Identifizierung

Der Lernmodus von Zone Alarm erstellt automatisch einfache Regeln. Sobald ein Programm Internet-Zugriff wünscht, öffnet sich ein Fenster mit dem Programmnamen. Mit „Yes“ wird der Zugriff erlaubt, mit „No“ untersagt.

Kreuzen Sie das Kontrollkästchen „Remember the answer each time I use this program“ an, trägt Zone Alarm dieses Programm in eine Liste ein. Beim nächsten Start dieses Programms verwendet Zone Alarm die Einstellungen in dieser Liste und fragt nicht mehr nach. Je mehr Programme auf das Internet zugreifen, desto länger wird diese Liste.

Die Programmliste zeigt außer dem Produktnamen und dem Speicherort auch Versionsnummer, Erzeugungsdatum und Dateigröße an. Über die Spalte „Allow connect“ stellen Sie den Zugriff auf das lokale Netzwerk und auf das Internet in drei Stufen ein: Erlauben, verbieten oder nachfragen. In der Spalte „Allow Server“ sollten Sie ein Kreuzchen machen, falls Sie selber irgendeine Art von Server betreiben. Das betreffende Programmsymbol erscheint dann im Hauptfenster mit einer kleinen Hand, um die Server-Tätigkeit anzuzeigen.

Mit „Pass Lock“ wird die temporäre Internet-Sperre für dieses Programm aufgehoben. Während des Locks hat dieses Programm dann weiter Internet-Zugriff.

Die einmal erstellten Zugriffsbedingungen für die Programme lassen sich allerdings nicht speichern und müssen von Ihnen somit auf einem neu installierten System noch einmal festgelegt werden. Bei einem Upgrade von einer früheren

Verbindung abgelehnt: Zone Alarm bemerkt die Online-Aktivität einer unbekannten Anwendung

Version werden diese Einstellungen jedoch übernommen, selbst nach einer erneuten Installation findet Zone Alarm die Einstellungen wieder. Führen Sie einen Online-Sicherheitsscan Ihres Systems in der hohen Sicherheitsstufe (empfohlene Einstellung für das Internet) durch, so zeigt Gibson Research (**http://grc.com**) alle Ports als „stealth“ an, Sygate Online-Service (**scan.sygatetech.com**) als „blocked“.

Was Zone Alarm nicht leisten kann

Wie bei allen Personal Firewalls sollten Sie sich auch bei Zone Alarm nicht allzu sehr in Sicherheit wiegen. Das Blockieren von Anwendungen ist zwar in vielen Fällen aufschluss- und lehrreich, vor allem wenn es um das Erkennen von Trojanern und Spyware geht, die heutigen Angriffstechniken sind jedoch subtiler. Schon im letzten Jahr sind etwa die Leak-Tests, etwa von Steve Gibson, (**http://grc.com**), bekannt geworden, die Daten durch die Firewall hindurch an einen Server im Internet senden („tunneln“) und auch Daten von diesem empfangen können. Solche Vorfälle lösen regelmäßig Updates der Firewall-Produkte aus. Jedoch muss auch das Leak-Test-Programm genau wie ein Trojaner zuerst installiert und dann gestartet werden.

Der Ersatz von systemnahen Programmen wie dem Internet Explorer, die von Haus aus erlaubten Internet-Zugriff haben, durch einen Trojaner ist ebenfalls ein beliebter Trick, um Daten an der Firewall vorbei zu schmuggeln. Abhilfe schaffen hier Prüfsummen für jedes Programm mit Internet-Zugriff, die von der Firewall erstellt und überwacht werden. Solche Manipulationen entdeckt Zone Alarm nicht. Auch hier muss erst wieder ein fremdes Programm installiert werden.

Guter Schutz bei wenig Funktionen

Zone Alarm ist einfach zu bedienen und erfordert keine tieferen Kenntnisse der Materie. Es ist deshalb gut für Einsteiger geeignet. Das Programm sowie die offizielle Dokumentation sind derzeit nur in englischer Sprache vorhanden. Für den Schutz eines Einzelplatz-Internet-Rechners und für die Anbindung eines kleines Netzes an das Internet ist Zone Alarm gut geeignet. Paket- und Protokollfilter sowie komplexe Regeln fehlen allerdings.

Was bringt der Einsatz der kostenpflichtigen 3er-Version?

Zu den erweiterten Funktionen von Zone Alarm Pro 3.0 gehören neue Datenschutzfunktionen wie etwa ein Werbeblocker und eine Cookie-Kontrolle, die eine ungewollte Übertragung persönlicher Daten verhindern soll. Zudem sollen Sie auch vor so genannten Web-Bugs geschützt werden. Diese sammeln persönliche Daten, wenn sie in einer HTML-formatierten Mail oder auf einer Website hinterlegt sind. Die Sicherheitsfunktionen für lokale Netze, einschließlich drahtloser Netzwerke, wurden weiter verbessert: Eine Statusanzeige gibt an, welche Netzwerke aktiv sind und ob sie vertrauenswürdig („trusted“) sind oder nicht („untrusted“). Über „Program Control“ können Sie nicht nur wie bisher festlegen, welche Programme eine Verbindung mit dem Internet aufbauen dürfen, sondern auch einzelne Komponenten dieser Programme erfassen. Somit können keine zuvor als vertrauenswürdig eingestuften Programme von Trojanern modifiziert und missbraucht werden. Der Alert Advisor bietet nun eine kontextabhängige Hilfe zu bestimmten Sicherheitsthemen an und kann die Adresse jedes Angreifers abbilden. Außerdem kann Zone Alarm Pro 3.0 nun auch verhindern, dass aktive Inhalte, einschließlich Javascript und Active-X-Controls, ausgeführt werden. Die Version 3.1 steht in den Startlöchern und wird beim Erscheinen dieser Ausgabe bereits verfügbar sein.

Burkhard Müller

Webbrowser optimal einrichten

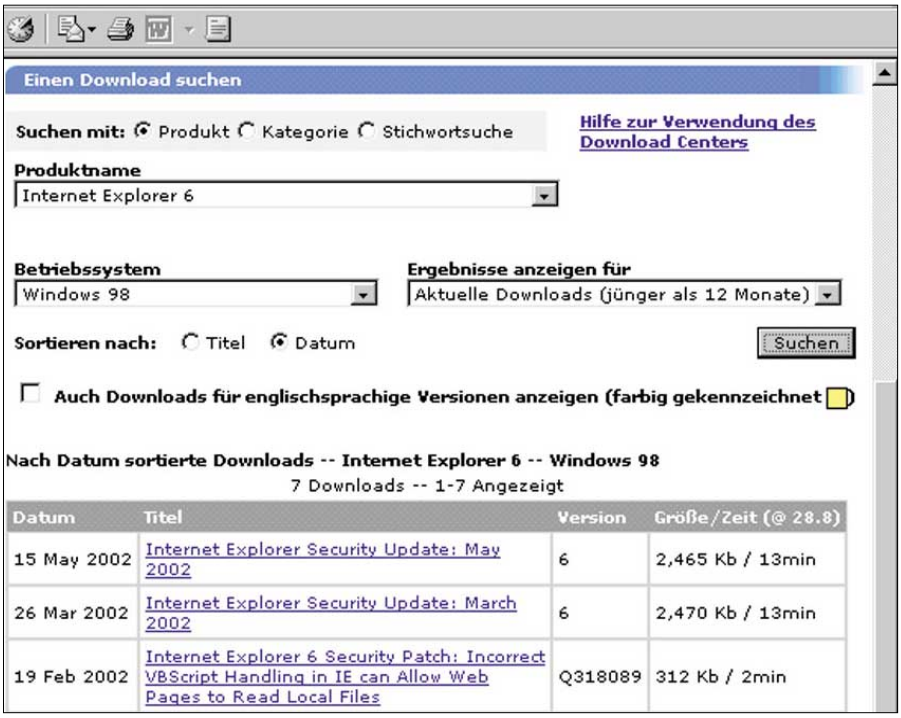
Sicher durchs WWW

Vielsurfer sind ständig Gefahren ausgesetzt. Mit den richtigen Browser-Einstellungen schützen Sie sich vor Spionage-Cookies, gefährlichen Scripts und zerstörerischen Active-X-Controls.

▸Es ist ein offenes Geheimnis, dass nahezu jeder sicherheitsbewusste PC-Anwender spezielle Security-Tools wie beispielsweise Virenscanner, Desktop-Firewall und Anti-Dialer-Programm einsetzt, um sich vor gefährlichen Angriffen aus dem Internet zu schützen. Doch was ist mit all den zerstörerischen Active-X-Komponenten, gefährlichen Javascripts und neugierigen Cookies? Sollen auch diese Löcher gestopft werden, müssen Sie sich mit den diversen Sicherheitseinstellungen der Internet-Browser auseinandersetzen. Denn ganz gleich, ob Sie den Microsoft Internet Explorer, Netscape oder Opera einsetzen – die nach der Installation verwendeten Grundeinstellungen sind nicht mehr als ein unglücklicher Kompromiss zwischen Sicherheit auf der einen und Benutzerfreundlichkeit auf der anderen Seite.

Ein wichtiger Hinweis vorweg: Anders als Netscape und Opera, die stets komplett überarbeitete Versionen zum Download anbieten, betreibt Microsoft Flickschusterei und stellt in unregelmäßigen Abständen neue Patches, Updates und Service Packs für seine Browser bereit. Mit diesen – teilweise mehrere Megabyte großen – Dateien werden aber nicht nur Sicherheitslöcher gestopft, sondern auch bekannte Programmfehler behoben, oder es wird der Funktionsumfang von Browser und kombiniertem News- und Mail-Client Outlook Express erweitert.

Bevor Sie sich jedoch an das Einspielen von Updates machen, müssen Sie die exakte Versionsnummer des verwendeten Browsers in Erfahrung bringen. Bei den Microsoft-Produkten klicken Sie dazu im Menü „?“ auf den Befehl „Info“, Netscape-Anwender wählen „Hilfe, Info über Netscape 6“, und beim Opera-Browser erreichen Sie diesen Dialog über „Hilfe, Über Opera“.



Gesucht und gefunden: Wer dem Active Setup von Microsoft nicht über den Weg traut, findet alternativ alle Updates auch mit Hilfe der Download-Suche zum manuellen Einspielen

Info: Surf-Sicherheit

Wer die Standard-Sicherheitseinstellungen des Browsers verwendet, ist Angriffen aus dem Internet nahezu schutzlos ausgeliefert. Denn erst mit den richtigen Einstellungen werden Internet Explorer, Netscape und Opera resistent gegen aktive Inhalte, spionierende Cookies und gefährliche Websites.

Wo finde ich aktuelle Microsoft-Updates?

Möchten Sie sich in Eigenregie auf die Suche nach aktuellen Updates für den Internet Explorer machen, stehen Ihnen gleich zwei Möglichkeiten offen. Der schnellste Weg führt über das fest im Betriebssystem integrierte „Windows Update“, das Sie über das Start-Menü aufrufen oder im Internet Explorer (Menü „Extras“) anwählen. Nach einer kurzen Überprüfung der installierten Komponenten genügt ein Klick auf den Link „Produktupdates“, um alle passenden Aktualisierungen aufzulisten. Es wird hierbei zwischen „Wichtigen Aktualisierungen und Service Packs“ sowie „Empfohlenen Updates“ unterschieden, was die Übersicht erhöht und nicht ganz so erfahrenen

Windows-Anwendern die Auswahl erleichtert. Wer diese Seite beispielsweise mit der Urversion von Windows 98 (Microsoft-intern als 4.10.1998 bezeichnet) und dem Internet Explorer 5.5 (mit eingespieltem Service Pack 1) ansteuert, findet zwei als unumgänglich gekennzeichnete Aktualisierungen – Service Pack 2 für den Internet Explorer sowie ein Paket wichtiger Updates. In letzterem befinden sich 13 Sicherheits-Updates – die Installation ist also sehr zu empfehlen.

Dazu markieren Sie das gewünschte Update und klicken auf den am oberen Seitenrand zu findenden Button „Download". Auf der folgenden Seite werden Ihnen noch einmal alle ausgewählten Aktualisierungen angezeigt; mit „Download starten" leiten Sie anschließend die Übertragung ein.

Für Profis: Manuelles Update über das Download-Center

Erfahrene Anwender können auf das automatische Windows-Update verzichten und sich für die traditionelle Methode entscheiden. Auf der Microsoft-Website (**www.microsoft.de**) klicken Sie auf den Link „Download Center", um in die entsprechende Rubrik zu gelangen. Im Bereich „Einen Download suchen", wählen Sie das zu aktualisierende Produkt aus der Liste aus, stellen das verwendete Betriebssystem ein und starten die Recherche mit „Suchen". Ein Klick auf den entsprechenden Link führt Sie dann direkt zur Update-Seite. Die eigentliche Installation erfolgt entweder wie gewohnt durch das Herunterladen und Ausführen der Datei oder per Active Setup direkt aus dem Web heraus.

Clever: Microsofts Active Setup ausgetrickst

Mit dem Service Pack 2 für den Internet Explorer 5.01 hat Microsoft die herkömmliche Download-Routine abgeschafft und sich voll und ganz dem Active Setup verschrieben. Bei dieser Variante laden Sie sich zunächst eine kleine Datei (bei den Service Packs knapp 500 KB) auf den Rechner und starten diese dann lokal, um eine Online-Verbindung zum Update-Server herzustellen. Nach einem kurzen Datenaustausch, bei dem überprüft wird, ob überhaupt ein Update erforderlich ist und falls ja, welche Komponenten benötigt werden, werden die entsprechenden Dateien direkt vom Microsoft-Server installiert.

Der große Nachteil dieser Methode: Falls Sie Ihr Betriebssystem neu einspielen müssen, sind alle auf diese Weise installierten Browser-Updates verloren. Doch hier hilft Ihnen ein kleiner Kniff weiter.

Um die Active-Setup-Routine auszutricksen, wählen Sie nach der Bestätigung der Lizenzvereinbarung „Minimal installieren oder Browser anpassen" und klicken auf „Weiter". Im folgenden Dialog entscheiden Sie sich für die gewünschte Installationsmethode und klicken auf die Schaltfläche „Erweitert", um ein zusätzliches Optionsmenü zu aktivieren. In diesem markieren Sie „Nur Download" und bestätigen die Auswahl mit „OK" sowie „Weiter".

Zum Abschluss legen Sie noch den Speicherort für die zu ladenden Dateien fest und geben an, für welche Windows-Betriebssystemversionen das Service Pack benötigt wird. Ein Klick auf „Weiter" führt Sie zur ServerAuswahlseite, auf der Sie den Download starten. Nach erfolgreicher Datenübertragung wechseln Sie in den zuvor ausgewählten Ordner und starten die Installation durch einen Doppelklick auf die entsprechende EXE-Datei.

Sicherer surfen: Ein guter Kompromiss zwischen Sicherheit und Benutzerkomfort ist wichtig

Internet Explorer: Wichtige Sicherheits-Updates

Damit Sie sich nicht durch die teilweise sehr unübersichtliche Microsoft-Website klicken müssen, listen wir in der folgenden Tabelle die wichtigsten Updates, Patches und Service Packs zum Thema Sicherheit auf.

Browser-Version	Update	Dateigröße	Verbesserung	Betriebssystem
IE 5.01	Service Pack 1	8,2 MB	unter anderem 128-Bit-Verschlüsselung	Windows 95/98, NT 4 und 2000
IE 5.01	Service Pack 2	zwischen 6 und 17 MB	zahlreiche Bug- und Sicherheitsfixes	Windows 95/98, NT 4 und 2000
IE 5.01 SP2	Security Update Mai 2002	1,89 MB	stopft sechs neue Sicherheitslöcher	Windows NT 4 und 2000
IE 5.5	Service Pack 1	zwischen 100 KB und 30 MB	zahlreiche Sicherheitsfixes und Aktualisierungen	Windows 95/98/ME, NT 4 und 2000
IE 5.5	Service Pack 2	zwischen 8,42 und 28 MB	zahlreiche Sicherheitsfixes und Aktualisierungen	Windows 95/98/ME, NT 4 und 2000
IE 5.5 SP1	Security Update Mai 2002	2,47 MB	stopft sechs neue Sicherheitslöcher	Windows 95/98/ME, NT 4 und 2000
IE 5.5 SP2	Security Update Mai 2002	2,12 MB	stopft sechs neue Sicherheitslöcher	Windows 95/98/ME, NT 4 und 2000
IE 6.0	Security Update Mai 2002	2,41 MB	stopft sechs neue Sicherheitslöcher	Windows 95/98/ME, NT 4, 2000 und XP

Sicherheit für Einsteiger im Internet Explorer 5/5.5

Sind alle wichtigen Updates eingespielt, geht es an das Fein-Tuning der jeweiligen Sicherheitseinstellungen. Die dafür zuständige Registerkarte „Sicherheit“ erreichen Sie im Internet Explorer über „Extras, Internetoptionen“.

Der Microsoft-Browser teilt alle Inhalte in die beiden Zonen „Internet“ und „Lokales Intranet“ ein und bietet zudem die Möglichkeit, Web-Seiten als vertrauenswürdig oder eingeschränkt zu kennzeichnen. Der Unterschied zwischen den beiden letztgenannten besteht darin, dass als standardmäßig eingestellte Sicherheitsstufen „sehr niedrig“ beziehungsweise „hoch“ gewählt wurde.

Weniger versierte Anwender, die sich nicht im Detail mit den Sicherheitseinstellungen auseinandersetzen möchten, können jeder Zone eine von vier vordefinierten Sicherheitsstufen zuweisen. Dazu markieren Sie die gewünschte „Zone“ und klicken auf den Button „Standardstufe“. Ziehen Sie anschließend den vertikalen Schieberegler auf die gewünschte Sicherheitsstufe, und bestätigen Sie die Änderung durch Klicks auf „Übernehmen“ und „OK“.

Achtung: Falls Sie sich hier für die Sicherheitsstufe „hoch“ entscheiden (und das ist auch zu empfehlen), müssen Sie eine wichtige Änderung manuell durchführen. Dies ist deswegen nötig, da in der höchsten Sicherheitseinstellung nicht nur Active-X-Komponenten, Cookies und Scripts ignoriert werden, sondern auch der Datei-Download deaktiviert ist. Um dieses Manko zu beheben, klicken Sie im Register „Sicherheit“ auf „Stufe anpassen“ und aktivieren im Bereich „Download, Dateidownload“ das Optionsfeld „Aktivieren“. Nach Klicks auf „OK“, „Übernehmen“ und „OK“ ist das Herunterladen wieder möglich.

Bei den im Register „Erweitert“ untergebrachten Optionen sind drei Einstellungen vorzunehmen. Unter „Browsing“ sollten Sie unbedingt die „Automatische Überprüfung auf Aktualisierungen von Internet Explorer“ deaktivieren, um das ungewollte Einspielen eines Updates zu unterbinden. Bei Bedarf, also dann, wenn Sie den Browser tatsächlich nach neuen Dateien suchen lassen wollen, schalten Sie diese Option einfach wieder an. Nicht

Nicht vergessen: Auch die auf der Registerkarte „Erweitert“ versteckten Einstellungen im Internet Explorer sind von größter Wichtigkeit in Sachen Sicherheit im Internet

minder wichtig ist auch der Umgang mit Zertifikaten, die im Zusammenhang mit sicheren Web-Seiten von Banken, Kreditkartenunternehmen und Online-Shops (erkennbar am verwendeten Protokoll Https – Hypertext Transfer Protocol Secure) zum Einsatz kommen. Denn da hier sensitive Inhalte wie zum Beispiel Persönliche Identifikationsnummer (PIN), Transaktionsnummern (TAN) und Kreditkartendaten übertragen werden, ist höchste Vorsicht geboten. Aus diesem Grund sollten die beiden Optionen „Auf zurückgezogene Serverzertifikate überprüfen“ und „Auf zurückgezogene Zertifikate von Herausgebern überprüfen“ aktiviert werden. Diese Einstellungen gelten übrigens auch für Profis.

Sicherheit für Profis im Internet Explorer 5/5.5

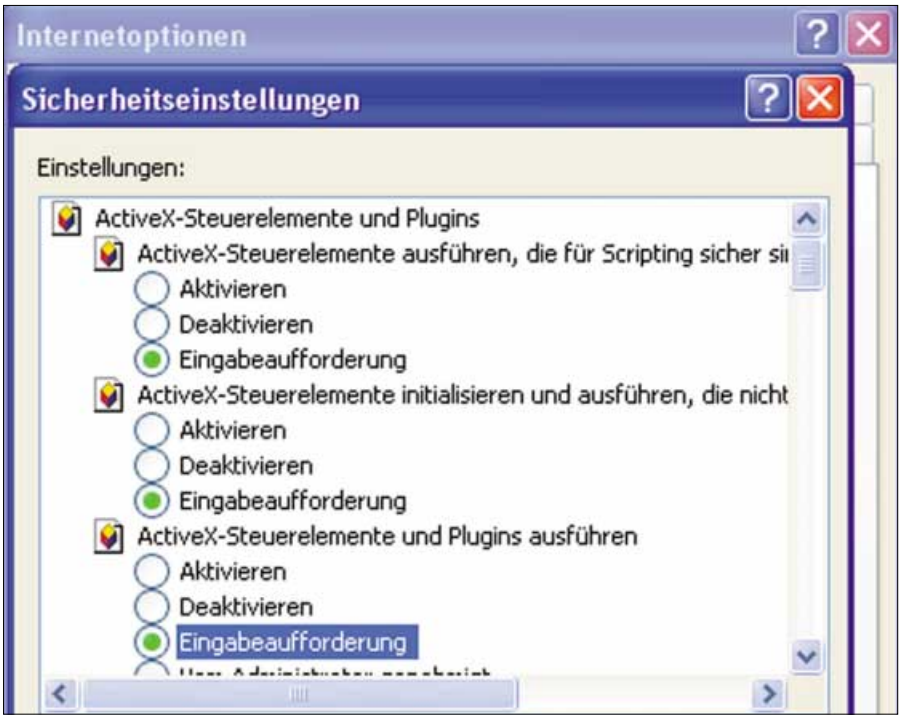
Möchten Sie als Profi alle Einstellungen selbst festlegen, sollten Sie dabei stets an die Faustregel denken, nach der Sicherheit in jedem Fall vor Bedienkomfort geht. Im Klartext bedeutet diese ungeschriebene Regel, dass Sie lieber einen Klick mehr hinnehmen sollten als dem Browser freie Hand beim Umgang mit Active-X-Controls, Cookies und Scripts zu lassen.

Somit ist es ratsam, alle Active-X-Optionen bis auf „Download von signierten ActiveX-Steuerelementen“ kurzerhand zu deaktivieren. Ebenso rigoros sollten Sie auch mit Cookies umgehen, da sich mit Hilfe der auf Ihrem Rechner abgelegten Textdateien nahezu Ihr komplettes Surfverhalten nachvollziehen lässt. Der große Nachteil dieser stringenten Sicherheitseinstellung: Werden keine Cookies mehr akzeptiert, müssen Sie beim Zugriff auf passwortgeschützte Seiten wie zum Beispiel Diskussionsforen stets Benutzername und Kennwort eintippen. Und zwar nicht nur beim erstmaligen Aufruf der Startseite, sondern bei jedem einzelnen Zugriff auf Nachrichten und Foren.

Noch tiefer wirkt sich die empfohlene „Java-Einstellung“ aus. Denn sobald Sie „Java deaktivieren“ auswählen, kann der Browser einen Großteil der Web-Seiten nicht mehr korrekt darstellen, da nahezu alle wichtigen Webangebote auf diese objektorientierte Programmiersprache setzen. Um dieses Problem zu umgehen und trotzdem keine Abstriche bei der Sicherheit zu machen, sollten Sie in regelmäßi-

gen Abständen nach neuen Patches suchen und diese umgehend einspielen. Im Gegenzug können Sie sich dann für die Einstellung „Hohe Sicherheit“ entscheiden. Ähnliches gilt auch für die im Bereich „Scripting“ zusammengefassten Optionen. Einerseits gehören auf Javascript oder Visual Basic basierende Scripts inzwischen zur Grundausstattung von Websites, andererseits sind es gerade diese Inhalte, die für große Gefahr sorgen können. Und genau dieser negative Aspekt veranlasst immer mehr Profis dazu, bei allen drei Einstellungen auf „Deaktivieren“ zu klicken.

In der Rubrik „Verschiedenes“ sind vor allem die beiden Einstellungen „Programme und Dateien in einem IFRAME starten“ sowie „Subframes zwischen verschiedenen Domänen bewegen“ umgehend zu deaktivieren, da diese Funktionen trotz mehrfacher Aktualisierung von Seiten Microsofts nach wie vor dazu genutzt werden können, gefährliche Websites zu tarnen – ein sehr großes Sicherheitsleck. Falls Sie die „Installation von Desktopobjekten“, das „Ziehen und Ablegen oder Kopieren und Einfügen von Dateien“ oder die „Zugriffsrechte für Softwarechannel“ regeln möchten, sind die Einstellungen „Deaktivieren“, „Eingabeaufforderung“ und „Hohe Sicherheit“ angebracht. Nicht ganz so einfach gestaltet sich die Einstellung „Unverschlüsselte



Nur wenig Unterschied: Die von Microsoft angebotenen Sicherheitseinstellungen des Internet Explorers in der 6er-Version unterscheiden sich kaum von denen der Vorgängerversionen

Formulardaten übertragen“. Zwar stellen Übertragungen von nicht verschlüsselten Text-Strings ein potenzielles Sicherheitsrisiko dar, doch wird durch die Deaktivierung selbst die Nutzung so unverfänglicher Angebote wie Suchmaschinen nahezu unmöglich. Die Option „Eingabeaufforderung“ stellt hier einen guten Kompromiss dar.

Sicherheit für alle im Internet Explorer 6

Der zur Grundausstattung von Windows XP gehörende Browser verfügt zwar über einige neue Features und erfreut so manchen Anwender durch seine bunte Bedienerführung, doch unter der Haube stehen Ihnen – abgesehen von der intelli-

Keine Überraschung: Auch AOL und T-Online nutzen den Internet Explorer

Da weder AOL noch T-Online über einen eigenen Browser verfügen, sondern auf den Internet Explorer setzen, gelten die in den entsprechenden Abschnitten dieses Artikels aufgeführten Hinweise auch für Mitglieder der beiden großen Online-Dienste. Dies entbindet Sie jedoch nicht von der Aufgabe, die innerhalb der Client-Software angebotenen Sicherheitsparameter anzupassen.

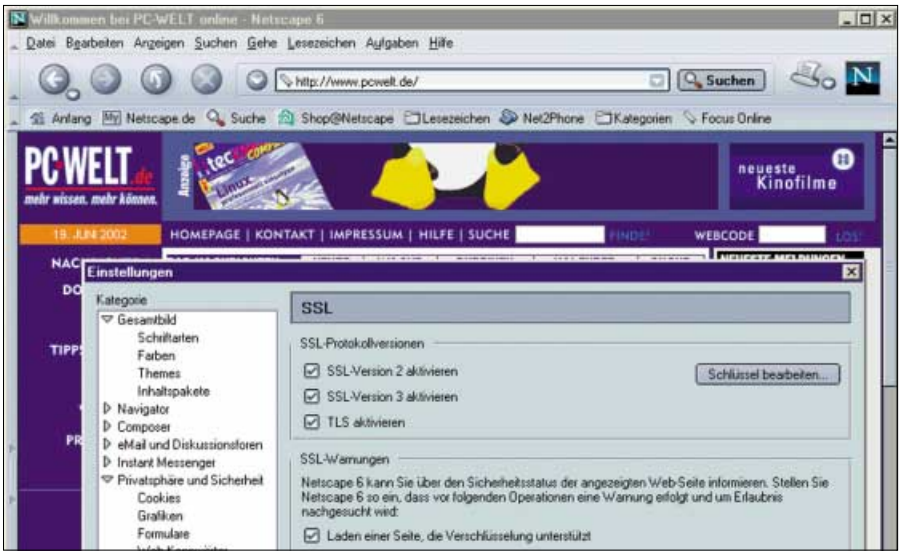
Bei AOL 7.0 erreichen Sie dieses Menü über „Organisieren, Einstellungen, Präferenzen“. Ein Klick auf den Hyperlink „Internet-WWW“ öffnet den – ein wenig reduzierten – Sicherheits-Dialog des Internet Explorers, in dem Sie die entsprechenden Einstellungen gemäß unseren Vorgaben festlegen können. Bei den „Download-Präferenzen“ sollten Sie unbedingt die beiden Optionen „Hinweis vor dem Download anzeigen“ und „Automatisches Dekomprimieren / keine Dekomprimierung“ aktivieren, um eine größere Kontrolle über heruntergeladene Dateien zu erhalten.

Nutzer von T-Online, die bereits den brandneuen, auf dem Internet Explorer 5.x basierenden T-Online-Browser 4.505 für Windows 98/ME sowie Windows 2000 Professional und XP (5 MB, **http://service.t-online.de/t-on/down/brow/ar/CP/ar-download-t-online-browser.html**) einsetzen, rufen die Sicherheitseinstellungen über „Optionen, Einstellungen“ auf. Mit der in der Rubrik „Erweitert“ untergebrachten Schaltfläche „Optionen“ gelangen Sie direkt zu den Einstellungen des Internet Explorers, die Sie nach dem Muster der zuvor aufgezeigten Hinweise anpassen. Empfehlenswert ist außerdem, die Checkbox „Pop-Up Fenster immer im Vordergrund“ zu deaktivieren, damit die störenden Werbeeinblendungen dauerhaft in den Hintergrund verbannt werden.

Alter Bekannter: Der T-Online-Browser basiert auf dem Microsoft Internet Explorer 5.x

genten Cookie-Verwaltung sowie einigen neuen Einstellungen unter „Sicherheitseinstellungen, Verschiedenes“ – nahezu die gleichen Sicherheitsoptionen wie beim Internet Explorer 5.5 zur Auswahl. Somit gelten die bereits aufgezeigten Grundeinstellungen für Einsteiger und Profis auch in der 6er-Version.

Den speziellen Cookie-Dialog rufen Sie im Dialog „Internetoptionen“ über das Register „Datenschutz“ auf. Ein Klick auf den Button „Erweitert“ öffnet ein weiteres Fenster, in dem Sie die Option „Automatische Cookiebehandlung aufheben“ aktivieren und sich sowohl bei „Cookies von Erstanbietern“ als auch bei „Cookies von Drittanbietern“ für den Befehl „Sperren“ entscheiden. Damit Sie bei Ihren Besuchen auf häufig angesteuerten, per Passwort geschützten Seiten nicht immer Benutzername und Kennwort eingeben müssen, schließen Sie den Dialog mit „OK“ und klicken im Register „Datenschutz“ unter „Websites“ auf „Bearbeiten“. Hier können Sie dann all diejenigen



Vorbildliche Sicherheits-Features: Auch wenn Netscape 6 von Haus aus gegen Active-X-Controls immun ist, müssen einige Einstellungen für mehr Sicherheit beim Surfen angepasst werden

Webseites eingeben, bei denen die zuvor definierte Cookie-Behandlung ignoriert werden soll. Und falls Sie während des Surfens bemerken, dass eine von Ihnen besuchte Seite vergessen wurde, doppelklicken Sie einfach auf das in der unteren Statusleiste des Browsers angezeigte Icon „Datenschutzbericht“, markieren die entsprechende URL und wählen „Zusammenfassung“. Im folgenden Dialog le-

Sicherheit auf Norwegisch: Opera 6 richtig konfigurieren

Der smarte, handliche Browser aus dem hohen Norden begeistert Internet-Nutzer seit jeher durch seine ressourcenfreundliche Programmierung, die vielfältigen Zusatzfunktionen und den hohen Sicherheitsstandard. So bietet nur Opera (**www.opera.com**) ein spezielles Sicherheitsmenü, über das Sie mit genau zwei Mausklicks (Menü „Datei“, Befehl „Schnelleinstellungen“) oder einem Tastendruck (‹F12›) die wichtigen Vorgaben einsehen und verändern können. Dafür nimmt man auch gerne in Kauf, dass die Kompatibilität zu einigen Web-Seiten nach wie vor zu wünschen übrig lässt und ein Teil des Browser-Fensters der unregistrierten Version zudem von einem Werbebanner in Beschlag genommen wird.

Den eigentlichen Security-Dialog erreichen Sie über „Datei, Einstellungen“. Eine der wichtigsten Optionen, „Java Script“, ist unverständlicherweise in der Rubrik „Schriften und Farben, Multimedia“ versteckt. Wie bei den anderen beiden gängigen Browsern sollten Sie sich auch bei Opera für eine Deaktivierung entscheiden.

Ein weiteres, oftmals vergessenes Sicherheitsrisiko stellen Office-Dokumente dar. Hierzu stellt Opera eine ausgeklügelte Routine zur Verfügung, mit der Sie die „Behandlung der Dateitypen“ exakt definieren können. Den gleichnamigen Dialog erreichen Sie über die Rubrik „Programme und Pfade, Dateitypen“. Hier sollten Sie darauf achten, dass die standardmäßige Einstellung „Bestimme Vorgangsweise bei unzuverlässigem MIME-Typ durch Dateinamenserweiterung“ auch wirklich aktiv ist. Ist dem so, markieren Sie der Reihe nach die für Makroviren anfälligen MIME-Typen „application/msword“ und „application/vnd- msexcel“, klicken auf „Bearbeiten“ und beantworten die Frage „Was soll Opera bei diesem Dateityp machen“ mit „Downloaddialog zeigen“. Alternativ dazu können Sie bei Word-Dokumenten auch einen anderen Dateibetrachter („Mit anderem Programm öffnen:“) wie Wordpad oder Star Office festlegen.

Der dritte Benutzereingriff betrifft die Cookies. Wechseln Sie hierzu in die Rubrik „Netzwerk, Privatsphäre“, und schalten Sie die voreingestellte Option „Cookies aktivieren“ ab. Alternativ dazu können Sie sich auch für die Kombination aus „Cookies nur von ausgewählten Servern annehmen“ und

Ausgezeichnetes Opera-Feature: Die integrierte Cookie-Verwaltung gehört zu den Highlights

„Nur Cookies für jeweiligen Server annehmen“ entscheiden. Welche Server und Domains dabei akzeptiert werden sollen, legen Sie nach einem Klick auf „Bearbeiten der Serverfilter“ selbst fest. Abschließend aktivieren Sie noch „Beim Beenden von Opera alle Cookies löschen“, „Warnung bei nicht erlaubten Domänen“ sowie „Warnung bei nicht erlaubten Pfaden“ und verlassen den Einstellungsdialog mit „Übernehmen“ und „OK“. Die Änderungen werden übrigens beim Update auf eine neue Version übernommen.

gen Sie dann die neuen, nur für diese Seite gültigen Cookie-Regeln fest.

Im Dialog „Sicherheitseinstellungen" legen auf Sicherheit bedachte Anwender zusätzlich zu den bereits beim Internet Explorer 5 beschriebenen Einstellungen Folgendes fest: Die Optionen „gemischte Inhalte zeigen" und „Meta Refresh zulassen" werden „Deaktiviert".

Sicherheit für Nutzer von Netscape 6.2.x

Im Vergleich zum Internet Explorer (sowohl 5/5.5 als auch 6) geht die manuelle Konfiguration der Sicherheitseinstellungen beim einstigen Marktführer Netscape 6.2.x weitgehend problemlos und ungleich schneller vonstatten. Dies liegt nicht zuletzt daran, dass Netscape keinerlei Active-X-Controls unterstützt und hier von Haus aus mehr Sicherheit bietet.

Das für die Sicherheitsaspekte zuständige Menü öffnen Sie über „Bearbeiten, Einstellungen". In der linken Auswahlspalte klicken Sie im Abschnitt „Privatsphäre und Cookies" auf „Cookies", um festzulegen, wie Netscape mit den kleinen, spionagefreudigen Textdateien umgehen soll. Empfehlenswert sind hier die Einstellungen „Nur an die ursprüngliche Seite gesendete Cookies akzeptieren" und „Warnmeldung vor dem Akzeptieren von Cookies", da dies den goldenen Mittelweg zwischen Benutzerkomfort (Bestätigen von Warnmeldungen) und Sicherheit darstellt. Darüber hinaus können Sie über „Aufgaben, Privatsphäre und Sicherheit" jederzeit den integrierten „Cookie-Manager" aufrufen, der Ihnen beim Umgang mit diesen Dateien helfend zur Seite steht und weitere Optionen bietet.

Eine weitere in dieser Rubrik unbedingt notwendige Einstellung betrifft die Behandlung von gesendeten Formulardaten. Um zu verhindern, dass beispielsweise vertrauliche Passwörter und andere Benutzerkennungen in falsche Hände geraten, ist es unumgänglich, dass die im Bereich „SSL" untergebrachte Option „Senden von Formulardaten von einer unverschlüsselten Seite zur anderen" aktiviert ist. Dies ist zwar nach der Installation standardmäßig so eingestellt, eine regelmäßige Überprüfung der Einstellungen kann aber nicht schaden.

Über „Erweitert" gelangen Sie zu einem wichtigen Dialog, in dem die Behandlung von Java-Applets und Javascript-Komponenten geregelt wird. Während Sie die Java-Einstellungen getrost im aktiven Zustand belassen können, plädieren Profis in Sachen Javascript für eine etwas strengere Konfiguration und hebeln die Einstellung „JavaScript für eMail & Diskussionsforen aktivieren" aus, da gerade in Mails versteckte aktive Inhalte über ein enormes Gefährdungspotenzial verfügen. Wer sein System sogar komplett abschotten möchte und dafür selbst eine fehlerhafte Darstellung von Web-Seiten in Kauf nimmt, entfernt auch das Häkchen bei „JavaScript für Navigator aktivieren".

Stefan Forster

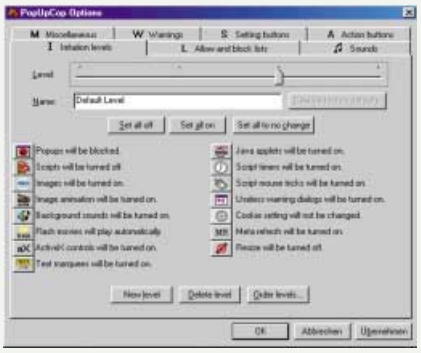
Add-ons: Noch mehr Browser-Sicherheit durch Zusatz-Tools

Auch wenn sich die Sicherheit der drei wichtigsten Browser durch gezielte Benutzereingriffe signifikant erhöhen lässt, greifen ambitionierte Surfer oftmals zu zusätzlichen Mitteln, um maximalen Schutz zu gewährleisten. Angefangen bei einer umfassenden Cookie-Verwaltung über Werbeblocker bis hin zum Verwischen verräterischer Surfspuren – der Share- und Freeware-Markt liefert für nahezu alle Einsatzgebiete das passende Security-Tool.

Anwender, die noch nicht mit dem Internet Explorer 6 im Netz unterwegs sind, aber trotzdem eine intelligente Cookie-Verwaltung einsetzen möchten, sollten ihr Software-Arsenal um das englischsprachige Tool Cookie Crusher 3.0.4.35 für Windows 98/ME, NT 4, 2000 und XP (325 KB, **www.thelimitsoft.com/cookie/** und ◉ auf Heft-CD, Registriergebühr: 15 US-Dollar) erweitern. Der besondere Clou: Das Programm meldet nicht nur alle empfangenen Cookies, sondern informiert Sie auch gleich über deren Sinn und Zweck (zum Beispiel Werbung oder Nachverfolgung des Surfverhaltens), so dass Sie jederzeit zwischen akzeptablen und unerwünschten Cookies unterscheiden können.

AOL-Mitgliedern steht mit dem englischsprachigen Cache and Cookie Washer 4 for AOL für Windows 95/98/ME, NT 4, 2000 und XP (812 KB, **www.webroot.com/washaol.htm** und ◉ auf Heft-CD, Registriergebühr: 15 US-Dollar) ein sehr intelligentes Tool zur Verfügung. Das Funktionsspektrum deckt das Löschen des Cache-Verzeichnisses und die Behandlung eintreffender oder bereits auf der Festplatte abgelegter Cookies ab. Das Tool gibt es in einer speziellen Version übrigens auch für den Internet Explorer und Netscape.

Nicht minder empfehlenswert ist das bewährte Programm Webwasher 3.0 für Windows 95/98/ME, NT 4 und 2000 (1021 KB, ◉ auf Heft-CD oder Download unter **www.webwasher.de/de/products/wwash/download_win.htm**). Der ausschließlich für Privatanwender kostenlose Werbeblocker kann Banner, Animationen, Scripts und Pop-up-Fenster gnadenlos unterdrücken. Und da die beiden letztgenannten Komponenten verstärkt als Transportmittel für die Installation unerwünschter 0190-Dialer missbraucht werden, sollte Webwasher zur Grundausstattung aller sicherheitsbewussten Surfer gehören.



Keine Chance für Pop-ups und Scripts: Mit Popup Cop surfen Sie ungestört und werbefrei

In eine ähnliche Richtung geht auch die englischsprachige Shareware Pop-up Cop 1.2 für Windows 95/98/ME, NT 4, 2000 und XP (415 KB, **www.popupcop.com**, auch ◉ auf Heft-CD, Registriergebühr: 20 US-Dollar). Ob Active-X-Controls, Javascript oder Pop-up-Fenster – nahezu jeder von Webdesignern genutzte Trick lässt sich per Mausklick aushebeln. Einzige Einschränkung: Der Pop-up-Polizist arbeitet nur mit dem Internet Explorer (ab Version 5) zusammen. Für schnellen Zugriff lässt er sich in der Menüleiste des Microsoft-Browsers verankern.

So gelangen Viren und Trojaner auf Ihren Rechner

Alarmstufe Rot

Zur Verbreitung gefährlicher Software haben Programmierer eine Reihe ausgebuffter Möglichkeiten ersonnen, hinterhältige Programme auf Ihren PC zu schmuggeln.

In den vergangenen Monaten hat die Anzahl von Viren, Würmern und anderer so genannter „Malware" stark zugenommen. Malware sind kleine Programme, von deren Existenz auf Ihrem PC Sie nichts wissen, die aber einen immensen Schaden anrichten können. Um die Platzierung dieser Software zu verschleiern, bedienen sich deren Programmierer immer ausgeklügelterer Tarnungen und Techniken.

Info: Virenbefall

Windows-PCs sind durch Virenbefall besonders verwundbar – aus diesem Grund sollten Sie Viren von Anfang an fern halten. Dazu müssen Sie die potenziellen Einfallstore der Schadprogramme auf Ihrem PC kennen. Wir liefern die nötigen Infos.

Dabei kommen fast alle Schädlinge, die derzeit im Umlauf sind und sich verbreiten, per E-Mail ins Haus. Dies betrifft im Prinzip sowohl Makroviren als auch ganz normale Bootsektor- oder Dateiviren. Die meisten Schädlinge gelangen als Dateianhänge (Attachments) zu Ihnen.

Sicherheitslücke: E-Mail als zentraler Angriffspunkt

Sie bekommen zum Beispiel ein beliebiges Programm oder ein Dokument von einem Freund oder Kollegen per Mail zugeschickt, das mit einem Virus verseucht ist, der vom Absender nicht erkannt wurde. Zusammen mit der harmlosen Software-Empfehlung oder Textdatei kopieren Sie zugleich den Virus auf Ihre Festplatte, der beim ersten Start der Software oder beim Öffnen des empfangenen Dokuments aktiv wird.

Besonders hinterhältig sind elektronische Nachrichten mit verseuchten Datei-Anhängen, die von einem Ihnen bekannten Absender stammen, aber ohne dessen Wissen versendet wurden. Im Vertrauen darauf, dass der Bekannte, der als Absender der Nachricht angezeigt wird, schon ein gutes Programm weiterempfehlen wird, starten Sie die Software und aktivieren damit sowohl die enthaltene Schadroutine als auch die Virenreplikation, über die sich der Schädling fortpflanzt. Viren und Trojaner dieser Gattung versenden sich heimlich an alle Empfänger, die im Adressbuch des Mailprogramms eingetragen sind, oder verfügen über spezielle Routinen, um Mailadressen und Textfragmente aus bereits empfangenen Mails für den Nachrichtentext zusammenzutragen. Häufig werden dazu Dateien aus dem Cache des Webbrowsers systematisch ausgelesen und die in den

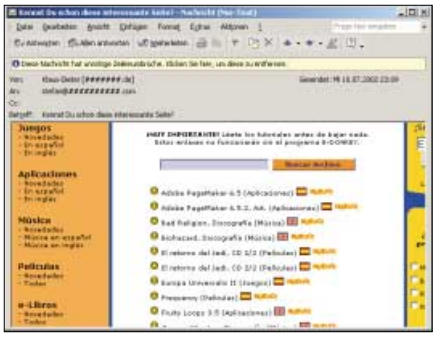
HTML-Dokumenten enthaltenen Adressen zum Mailversand extrahiert. Damit der Anwender des zum Versand verwendeten PCs nichts vom brisanten Massenmailing mitbekommt, beseitigt der Virus nach getaner Arbeit alle Spuren im Mailprogramm.

Vorgaukeln angeblicher Sicherheitslöcher

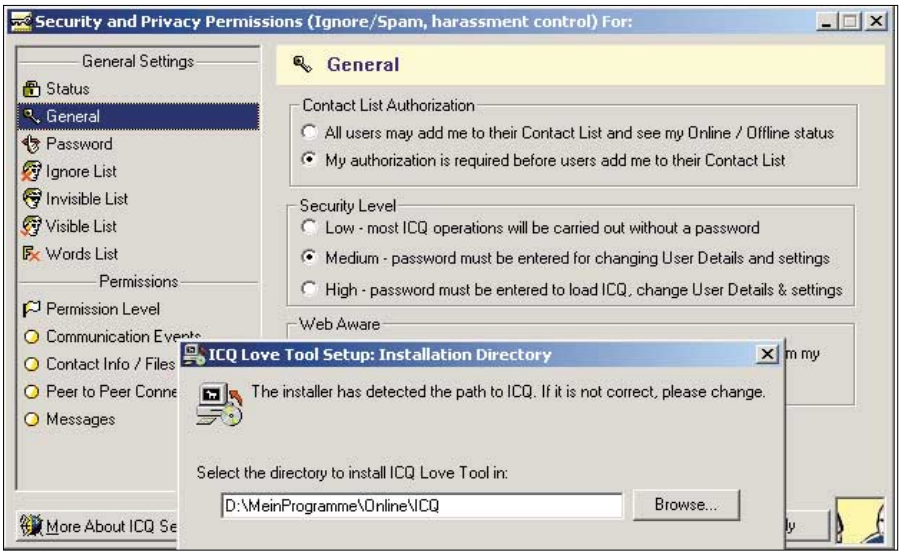
Eine beliebte Masche, Schädlinge an den Mann zu bringen, besteht in der unaufgeforderten Zusendung angeblicher Tuning-Tools, Computerspiele, Bilder oder Videoanimationen. Besonders Erfolg versprechend für Angreifer ist das Vortäuschen angeblicher Sicherheitslöcher, die in Wirklichkeit überhaupt nicht vorhanden sind. Der Virus besorgt sich auf den PCs seiner Opfer mit den bereits beschriebenen Tricks Mailadressen und versendet anschließend Standardmails mit Inhalten wie „Hallo. Sie haben mir eine virenverseuchte E-Mail geschrieben – wahrscheinlich ist Ihr PC verseucht. Anbei ein Tool, mit dem Sie den Virus ganz einfach auf Knopfdruck beseitigen können. Viele Grüße“.

Anwender im deutschsprachigen Raum, werden insofern gewarnt, als die meisten Mailwürmer Englisch „sprechen“, selbst wenn der Absender aus Deutschland stammt. Da der Nachrichtentext vom Virenprogrammierer zumeist in Englisch gehalten ist, ist er leichter als Fälschung erkennbar.

Ahnungslose Anwender lassen sich auch leicht durch angeblich neue Versionen bekannter Freeware oder Betriebssystemaktualisierungen täuschen. So wurde in der Vergangenheit eine breit angelegte Attacke mit einer vorgeblich neuen Version eines Trojanerscanners durchgeführt. Offenbar animiert durch das angeblich



Was steckt dahinter? Spam-Mails sind durch Links und eingebettete Informationen gefährlich



Messenger im Visier: Ohne Kenntnis des Anwenders unterwandern Hackprogramme die in Instant Messengern, wie ICQ eingebauten Sicherheitsfunktionen zum Schutz der Privatsphäre

nutzbringende Tool und in Panik haben viele Anwender den Datei-Anhang übereilt ausgeführt, ohne die Authentizität des Absenders zu überprüfen.

Infekte sind auch ohne Interaktivität möglich

Dass Infektionen überhaupt stattfinden können, liegt nicht immer an der Gleichgültigkeit oder Unkenntnis von Computernutzern. Einige Viren nutzen Sicherheitslücken in den Active-Scripting-Komponenten des Internet Explorers aus, über die Schädlinge auf den Rechner gelangen können. Mailprogramme wie Outlook, Outlook Express oder Eudora, die den Internet Explorer zur Anzeige HTML-formatierter Nachrichten verwenden, können in den Nachrichtentext eingebettete Kommandos direkt ausführen. Damit Outlook die eingebetteten Kommandos auch ausführt, muss im Mailprogramm lediglich die Sicherheitszone „Internetzone“ anstelle der besser geschützten „Zone für eingeschränkte Sites“ ausgewählt sein.

Gefahr eines Angriffs auch beim Chatten

Eine weitere Strategie zur Verbreitung von Malware ist der Kontakt über Instant Messenger oder IRC-Chat-Software. Für den Angreifer von Vorteil ist die direkte Verbindungsaufnahme zu potenziellen Opfern, wie sie bei Chats prinzipiell gegeben und auch gewollt ist. Der Täter nutzt die Anonymität des Internet-Kontakts gezielt aus, um seinen fernen Gesprächspartnern während eines unverbindlichen Plauschs eine Datei unterzujubeln.

Um den Zielrechner zu infizieren, ist es in vielen Fällen nicht einmal erforderlich, dem Chatpartner eine Wirtsdatei aufzuschwatzen. Unzulänglichkeiten in Chatprogrammen wie ICQ, dem Microsoft Messenger oder verbreiteten IRC-Clients wie Mirc unterlaufen die eingebauten Schutzfunktionen. Im Internet finden sich verschiedene Hacker-Tools, mit deren Hilfe sich Gesprächspartner trotz anders lautender Programmoptionen ohne deren ausdrückliche Erlaubnis zur Liste der Kontakte zufügen lassen. Damit nehmen zweifelhafte Zeitgenossen Verbindung auf und fügen Sie in ihre Kontaktliste ein, auch wenn Sie dies nicht wollen. Eine Autorisierung vor dem Chat ist dann nicht mehr erforderlich. Ähnliche Tools gibt es auch zum Überlisten der Bestätigung zum Empfang von Dateien. Danach braucht der Angreifer nur abzuwarten, bis der arglose Anwender die heimlich übertragene Datei auf seinem PC findet und startet.

Gerne spielen Gauner im Chat auch eine andere Identität vor, um Ihr Vertrauen zu erschleichen. Wer von einem scheinbar hilfebedürftigen PC-Nutzer ohne Vorwarnung angechattet wird mit der Bitte, doch bei einem PC-Problem etwa mit Word zu helfen, bekommt kurze Zeit später möglicherweise eine virenversetzte Datei zugeschickt.

Christoph Metzger

Abwehrstrategien für mehr Datensicherheit im Netz

Attacken abwehren

Computerviren in Verbindung mit dem Internet stellen eine erhebliche Bedrohung für Ihren PC dar. Wir zeigen, wie Schutz aussehen muss, und liefern Ihnen das nötige Grundlagenwissen.

Viren, Trojaner und Würmer sind Sabotageprogramme, die sich an Dateien oder E-Mails auf dem Zielrechner hängen. In Bezug auf das Internet stellt diese Sabotage-Software ein ganz besonderes Sicherheitsrisiko dar, denn die vernetzten Umgebungen sorgen für eine rasche Ausbreitung der Plagegeister.

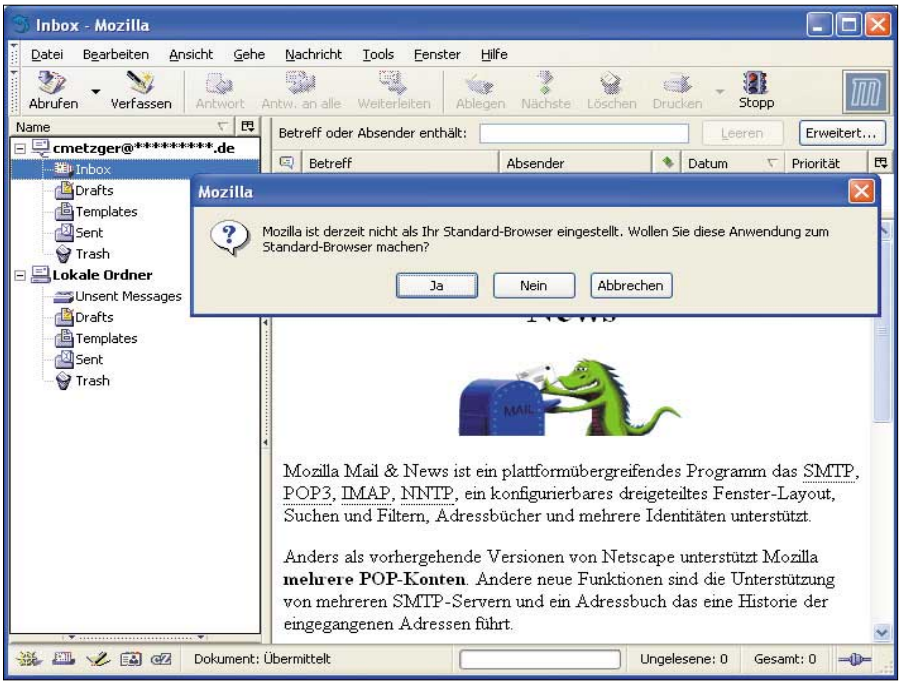
Die Trennung zwischen Viren und Würmern ist schwierig – die meisten Angriffe über E-Mail sind sowohl das eine als auch das andere. Während der Infizierung verwandelt sich eine normale Datei oder eine gewöhnliche Mail in einen Virusträger. Von diesem Zeitpunkt an kann die infizierte Mail oder Datei selbst Daten infizieren.

Warum Viren und Trojaner funktionieren

Würmer wie Sircam, Klez oder Melissa sind nur deshalb so wirkungsvoll, weil die Mails mit dem verhängnisvollen Datei-Anhang scheinbar von Bekannten kommen. Stammt eine Mail von jemandem, mit dem sie in Kontakt stehen, neigen viele Menschen dazu, Warnhinweise und Sicherheitsmeldungen zu ignorieren und die lästigen Schaltflächen einfach wegzuklicken. In vielen Unternehmen treten die Angestellten mit dem Lesen von virulenten Mails eine Lawine los, der die Techniker kaum gewachsen sind.

Info: Abwehr

Die Autoren von Viren, Würmern und Trojanern setzen ihre destruktiven Programme auf Einfallstore an, die fast alle Windows-PCs besitzen. Wenn Sie diese Schotten dicht machen, reduzieren Sie die möglichen Angriffsflächen.



Es muss nicht immer Outlook sein: Der Einsatz einer alternativen Mail-Software anstelle von Outlook oder Outlook Express reduziert die Gefahr, Opfer eines typischen Outlook-Wurms zu werden

Der wichtigste Grund, weshalb sich Würmer so schnell verbreiten, ist aber die Tatsache, dass ein Großteil der Windows-Nutzer seine Nachrichten mit Outlook oder Outlook Express liest. Weil Outlook Express auf nahezu jedem Windows-Rechner installiert ist und der große Bruder Outlook zusammen mit Microsoft Office auf den PC kommt, sehen es sehr viele PC-Nutzer als selbstverständlich an, eines der beiden Programme für ihre Mailkommunikation einzusetzen.

Bekannte Schwächen: So sicher sind Microsoft-Programme

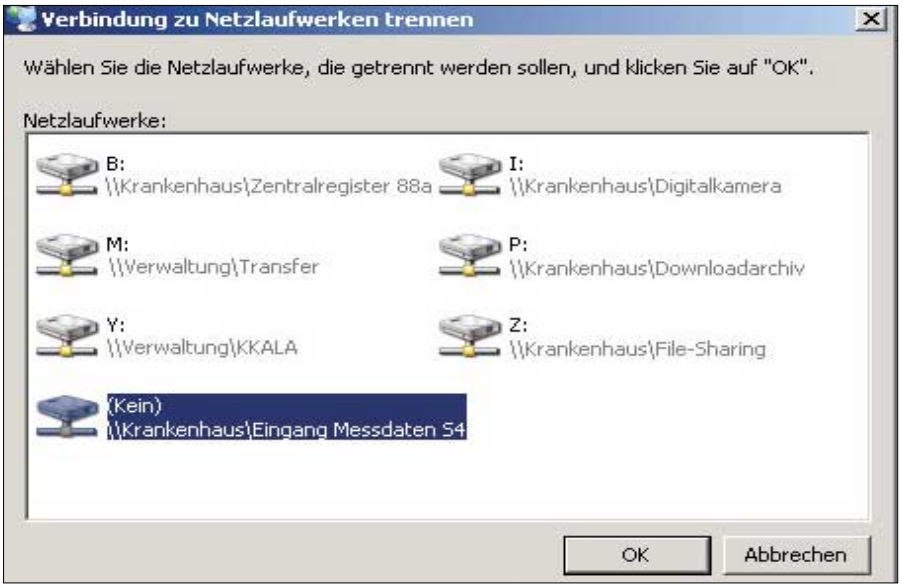
Trotz aller Sicherheits-Upgrades und Programmaktualisierungen hat es Microsoft versäumt, Outlook und Outlook Express wirklich sicher zu machen. Outlook Express läuft standardmäßig mit der Sicherheitszone „Internet“, die zwar mehr Funktionen bei der Anzeige von Nachrichten bietet, jedoch deutlich unsicherer ist als die „Zone für eingeschränkte Sites“. Bei der Office-Komponente Outlook XP und Outlook 2000 mit Service Pack 2 hat Microsoft radikale Maßnahmen ergriffen und global zahlreiche Datei-Anhänge blockiert, die Anwender im normalen Kommunikationsalltag für gewöhnlich verwenden. Access Datenbanken (Datei-Endung MDB), Microsoft Installationspakete (MSI) oder Photo-CD-Bilder (PCD) lassen sich zwar verschicken, doch sobald Sie selbst eine Nachricht mit Dateien erhalten, deren Typ gesperrt ist, deaktiviert Outlook den Anhang automatisch. Anwender, die sich über die restriktiven Datei-Anhang-Sicherheitseinstellungen von Outlook ärgern, schalten die Sicherheitsvorkehrungen über ein spezielles Plug-in

oder ein paar Registry-Einträge einfach ab und unterlaufen dadurch sämtliche Präventivmaßnahmen.

Ausgetrickst: Client-Vielfalt erschwert Angriffe per Mail

Die Software-Monokultur macht es für Virenschreiber einfach, vorhandene Sicherheitslücken auszunutzen und sich bestimmte Eigenheiten dieser Programme zunutze zu machen. Daraus ergibt sich eine einfache, aber sehr wirkungsvolle Vorbeugemaßnahme – der Einsatz eines alternativen Mailprogramms, das als Angriffsziel weniger lohnenswert ist. Anwender, die einen anderen Mail-Client verwenden oder mit anderen Betriebssystemen arbeiten, sind in vielen Fällen immun gegen Angriffe solcher Würmer. Empfehlenswerte Gratis-Mailer sind beispielsweise in den Browsern Netscape 6.2.3 (25 MB, **www.netscape. com** und auf Heft-CD) oder Mozilla 1.0 (10 MB, **www.mozilla.org** und auf Heft-CD) enthalten. Ebenfalls kostenlos einsetzen dürfen Sie das seit kurzem in deutscher Sprache erhältliche Pegasus Mail 4.01 (3,7 MB, **www.pmail.com** und auf Heft-CD) sowie das englischsprachige Eudora 5.1.1 (6,4 MB, **www.eudora.com** und auf Heft-CD, werbefreie Version: 30 US-Dollar).

Wer ein Mailprogramm mit umfangreichen Makrofunktionen, Vorlagen und PGP-Einbindung bevorzugt, greift zur Shareware The Bat 1.61 (5,7 MB, Programm und deutsche Sprachdatei unter **www.ritlabs.com** und auf Heft-CD, Registriergebühr: 39 Euro), von dem es mit Secure Bat sogar eine Variante mit speziellen Verschlüsselungsfunktionen gibt.



Ohne Netzverbindung: Nicht benötigte Laufwerksverknüpfungen im Netz können Sie bis zur nächsten Benutzung trennen, damit Viren keine Chance haben, sich unbemerkt auszubreiten

Sicherheitsmaßnahme: Unbenutzte Laufwerke abmelden

Die Fortpflanzungsroutinen vieler Würmer und Trojaner richten ihre Angriffe gegen alle bereitgestellten Laufwerke und mit dem Anwender-PC vernetzten Rechner. In Netzwerken mit globalen Freigaben wie zum Beispiel „C:\“oder „D:\Daten“ haben Viren leichtes Spiel und können alle Daten des freigegebenen Laufwerks befallen, was zur Verseuchung des gesamten Datenbestands führen kann. Diese Art der Laufwerksfreigabe ist besonders in privaten Netzwerken und kleineren Büros verbreitet.

Es ist sicherer, vorübergehend nicht benötigte Netzlaufwerke abzumelden und erst bei Bedarf wieder zu verbinden. Anwendungsspezifische und mit einem Passwort geschützte Freigaben – etwa für Office-Programme, Netzwerkspiele oder zum Bildertausch – sind eine gute Sicherungsmaßnahme. Das ist mit einem gewissen Verlust an Komfort verbunden, den Sie aber zugunsten der höheren Sicherheit in Kauf nehmen sollten.

Web-Bugs: Kein Virus, aber trotzdem ärgerlich

Haben Sie eine Desktop Firewall auf Ihrem Computer installiert? Dann kennen Sie dieses Szenario: Sie haben auf einer Website einen Newsletter abonniert, der Ihnen als Mail zugestellt wird. Nachdem die erste Ausgabe des Rundbriefs in Ihrem Postfach liegt, öffnen Sie die Nachricht in Ihrem Mailprogramm. Augenblicklich schlägt die Firewall Alarm, weil das Mailprogramm online gehen und Zugriff auf das Internet haben möchte, obwohl alle im Newsletter verwendeten Bilder bereits mit der Nachricht selbst übertragen wurden.

Die Ursache für dieses merkwürdige Verhalten ist kein eingebetteter Wurm oder Virus, sondern sind die so genannten Web-Bugs. Dabei handelt es sich um Hyperlinks auf kleine, zumeist nur 1 mal 1 Pixel große transparente Grafiken, die für den Empfänger einer Nachricht unsichtbar versteckt sind. Weil die Grafiken absichtlich nicht mit verschickt wurden, versucht Ihre Mailprogramm, diese Mini-Bilder direkt vom Server des Newsletter-Versenders oder einer Marketingfirma zu laden.

Web-Bugs haben nur eine Aufgabe: Sie sollen das Leseverhalten des Empfängers ausspionieren. Wird die Grafik vom Server geladen, so wird dieser Vorgang dort mit Datum, Uhrzeit und IP-Adresse mitprotokolliert. So kann der Betreiber des Newsletters sehen, wann und wie viele Leser die Newsletter-Meldung tatsächlich geöffnet haben, und detaillierte Statistiken anlegen. Zusammen mit weiteren Angaben, die Sie beispielsweise beim Bestellen des Newsletters gemacht haben, lassen sich Nutzerprofile erzeugen.

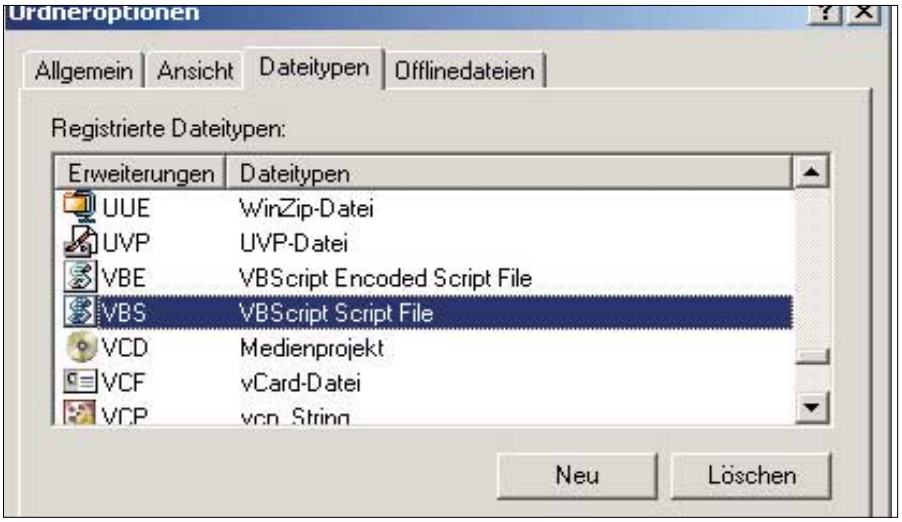
Dieses harmlose Verhalten können Sie durch eine entsprechende Regel in Ihrer Firewall dauerhaft unterbinden. Eine Gefahr für Ihren PC geht von Web-Bugs im Unterschied zu echten Viren allerdings nicht aus. Auf Web-Bugs stößt man auch beim Surfen im Internet. Auch hier startet der als Grafik in HTML-Syntax einer Seite eingebettete Web-Bug die heimliche Protokollierung aller Nutzeraktivitäten.

VBS abschalten: So werden Scriptviren matt gesetzt

Visual Basic Script (VBS) und Windows Scripting Host (WSH) sind zwei miteinander verwandte und bei Wurm- und Virenprogrammierern sehr beliebte Scriptprogrammiersprachen für Windows. Das mag sicherlich an der Tatsache liegen, dass die stark an Basic angelehnten Scriptsprachen im Gegensatz zu einer komplexen Hochsprache wie C++ vergleichsweise einfach gehalten sind. Zum anderen bieten sie einen reichhaltigen Funktionsumfang im Umgang mit Dateien, der für Viren allemal ausreicht.

Die meisten Anwender können auf Visual Basic Script und Windows Scripting Host verzichten. Wer Windows nicht über entsprechende Scripts automatisiert oder um eigene Erweiterungen ergänzt, kann auch ohne die direkte Ausführung von VBS und WSH aus dem Windows-Explorer leben. Dadurch entziehen Sie solchen Viren den Nährboden, die Ihnen beim Surfen im Netz untergeschoben oder per Mail zugeschickt werden und Ihnen bei ausgeschalteten Datei-Erweiterungen eine harmlose Datei vorgaukeln. Es gibt einige Programme, die VBS und WSH benötigen und die möglicherweise nicht mehr funktionieren, wenn Sie die Dateiverknüpfungen löschen. In diesem Fall müssen Sie abwägen, ob Ihnen die Funktionalität oder mehr Sicherheit wichtiger ist.

Durch das Löschen der Dateinamensverknüpfungen für „.VBS“ und „.WSH“ lassen sich VB- und WSH-Scripts nicht mehr starten. Unter Windows XP etwa ru-



Häufig sinnvoll: Wenn Sie keine Scriptprogramme mit den Dateinamenserweiterungen VBS und WSH verwenden, können Sie die Verknüpfungen im Windows Explorer entfernen

Schadensfällen vorbeugen – PC sicher einrichten

Die Einnistung von Trojanern, Würmern und Viren können Sie mit einer geeigneten Abwehrstrategie von Anfang an verhindern. Ziel ist es dabei, einige relevante Standardvoreinstellungen so zu verändern, dass Schädlingsprogramme, die auf ein standardisiertes Betriebssystem vertrauen, keine Angriffsfläche mehr finden.

Standardpfade verändern

Installieren Sie das Betriebssystem und sämtliche Anwendungen nicht in den standardmäßig vorgegebenen Systempfaden, sondern geben Sie benutzerdefinierte Speicherorte an. Dazu müssen Sie normalerweise im Installationsprogramm anstelle des Express-Setups den erweiterten Installationsmodus auswählen. Geben Sie für Windows beispielsweise den Setup-Ordner „\Meinwindows“ an, und installieren Sie Ihre Anwendungen im Ordner „\Meinesoftware“ „anstelle von \Programme. Schadprogramme, die nicht auf Systemvariablen zurückgreifen, sondern mit den bekannten vorgegebenen Pfaden arbeiten, verpassen dann ihr Angriffsziel und laufen wirkungslos ins Leere.

Mehrere Konten verwenden

Starten Sie die Benutzerverwaltung, die Sie bei Win XP in der Computerverwaltung finden („Start, Programme, Verwaltung, Computerverwaltung, Lokale Benutzer und Gruppen“). Überprüfen Sie, ob das Gastkonto deaktiviert ist. Richten Sie über „Aktion, Neuer Benutzer“ ein zusätzliches Benutzerkonto mit eingeschränkten Rechten ein, und vergeben Sie ein Kennwort. Arbeiten Sie im Alltag mit diesem Konto, das keinen Zugriff auf systemrelevante Einstellungen hat. Analog gehen Sie unter Win 2000 vor.

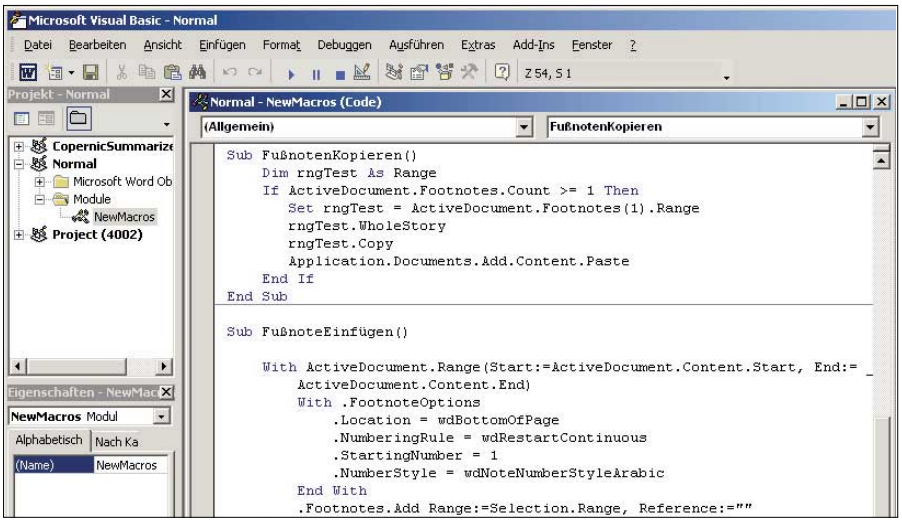
Hardware-Profile einsetzen

Ein Hardware-Profil umfasst einen Satz von Anweisungen, die festlegen, welche Geräte beim Windows-Start aktiviert werden und welche Einstellungen für die Geräte gelten. Beim Installieren von Win XP wird das Hardware-Profil „Profil 1“ angelegt. Standardmäßig sind alle Geräte im „Profil 1“ aktiviert. Über Profile können Sie im PC eingebaute Hardware temporär abschalten, so dass keine Software Zugriff hat. Das ist etwa zum Schutz vor 0190-Trojanern nützlich, wenn Sie DSL nutzen, aber noch Modem oder ISDN-Karte im PC haben. Zur Profilverwaltung gelangen Sie über „Systemsteuerung, System, Register Hardware, Hardwareprofile“. Klicken Sie unter „Verfügbare Hardwareprofile“ auf „Profil 1 (Aktuell)“ und dann auf „Kopieren“. Geben Sie einen Namen für das neue Profil ein, und klicken Sie auf „OK“. Im Geräte-Manager können Sie einzelne Geräte für das neue Profil aktivieren und deaktivieren (analoges Vorgehen unter Win 2000).

Mächtiges Werkzeug: Über ein zweites Hardware-Profil schützen Sie sich vor 0190-Dialern

fen Sie zur Deaktivierung im Windows-Explorer das Menü „Extras, Ordneroptionen“ auf und klicken auf die Registerkarte „Dateitypen“. Markieren Sie den registrierten Dateityp „VBS“, und klicken Sie auf „Löschen“, um die Verknüpfung zu entfernen. Wollen Sie VBS-Dateien nicht gleich löschen, sondern lieber mit einem harmlosen Programm öffnen, klicken Sie auf die Schaltfläche „Ändern“ und wählen den „Editor“ aus der Liste der verfügbaren Programme aus. Damit verknüpfen Sie die Scriptdateien mit dem harmlosen Texteditor, der sich öffnet, sobald Sie doppelt auf eine VBS- oder WSH-Datei klicken. Unter älteren Windows-Versionen gehen Sie analog vor. Sollten Sie keine passenden Dateitypen finden, sind VBS und WSH nicht installiert. Die Anzeige aller Datei-Erweiterungen aktivieren Sie im Reiter „Ansicht“ durch das Abschalten von „Erweiterung bei bekannten Dateitypen ausblenden“.

Bei einer Neuinstallation von Software können die Dateitypen durchaus wieder aktiviert werden. Deshalb sollten Sie eine Kontrolle der Dateiverknüpfungen im Windows-Explorer vornehmen.



Hintertür Makrosprache: Programmierern von Viren bietet die verhältnismäßig einfach zu erlernende Makrosprache Visual Basic for Applications weit reichende Möglichkeiten zur Systembeherrschung

Makrovirenschleuder VBA lässt sich nicht abschalten

Ebenfalls bei Virenautoren populär ist Visual Basic for Applications (VBA), die Makrosprache von Microsoft Office und anderen Anwendungen. Sie wird häufig von Makroviren genutzt, die hauptsächlich Word- und Excel-Dokumente befallen. VBA können Sie jedoch nicht einfach durch das Löschen von Dateiverknüpfungen entschärfen, denn die Programme werden nur innerhalb der Office-Anwendungen aktiviert. Für Sicherheit sorgt ein Virenscanner mit gutem Makro-Schutzmodul. Mehr Informationen dazu lesen Sie ab ▷ Seite 84.

Christoph Metzger

Virus an Bord: So gehen Sie mit einer Infektion um

Ist der Ernstfall eingetreten und Sie haben sich ein Schadprogramm eingefangen, heißt es: Ruhe bewahren. Oberste Priorität haben der Schutz Ihrer Daten und die sichere Beseitigung der Infektion sowie aller Ansteckungsherde.

Es gibt zwei Möglichkeiten, einen Virus von Ihrem Computer zu entfernen: Sie löschen alle infizierten Dateien, oder Sie setzten den Reparaturassistenten der von Ihnen verwendeten Antiviren-Software zur Isolation und Entfernung des Eindringlings ein. Meldet Ihr Antiviren-Programm den Fund eines Schädlings, lassen Sie Ihren Virenscanner zunächst einmal nichts machen, sondern notieren sich den Namen des Virus. Unterbrechen Sie anschließend die Verbindung zum Internet oder Netzwerk, notfalls durch das Abziehen des entsprechenden Kabels.

Sichern Sie als nächstes die befallenen Daten – bei Mailviren die Postfachdatei – auf ein externes Medium wie CD-R oder ein Zip-Laufwerk. Erst jetzt lassen Sie den Virus durch die Reparaturroutine der Antiviren-Software entfernen. Es besteht immer ein gewisses Restrisiko, dass die Beseitigung fehlschlägt und die vom Virus befallenen Daten ruiniert sind. In diesem Fall können Sie über das Wechselmedium einen weiteren Reparaturversuch mit einem anderen Scanner unternehmen.

Informieren Sie sich in der Virenbibliothek Ihrer Antiviren-Software oder auf der Website eines anderen Antiviren-Programmhersteller über den Virus sowie die Infektionswege, und lesen Sie nach, welchen Schaden der Plagegeist anrichten kann. Bei Mailviren ist es besonders wichtig festzustellen, ob bereits verseuchte Nachrichten über Ihr Adressbuch von Ihrem PC aus versendet wurden. Wenn ja, sollten Sie den Adressaten eine Warnmeldung zukommen lassen. Können Sie feststellen, vom wem Sie den Virus erhalten haben, informieren Sie den Verursacher. Möglicherweise hat er bislang noch nichts vom Virus bemerkt.

Nachdem Sie die Infektion auf dem PC beseitigt haben, sollten Sie sicherheitshalber alle Festplatten, Wechselmedien, Netzwerklaufwerke, zuletzt benutzte Disketten und Backups auf Viren untersuchen lassen. Achten Sie dabei darauf, sämtliche Dateien in den Prüfvorgang einzubeziehen und nicht nur Teile der Dateien zu scannen. Auf Nummer sicher gehen Sie, wenn Sie jetzt noch eine Datensicherung aller wichtigen Daten durchführen.

Informationen: Im Lexikon Ihres Virenscanners finden Sie Beschreibungen bestimmter Viren

Tipps zur Viren- und Trojanervorbeugung

Safe Computing

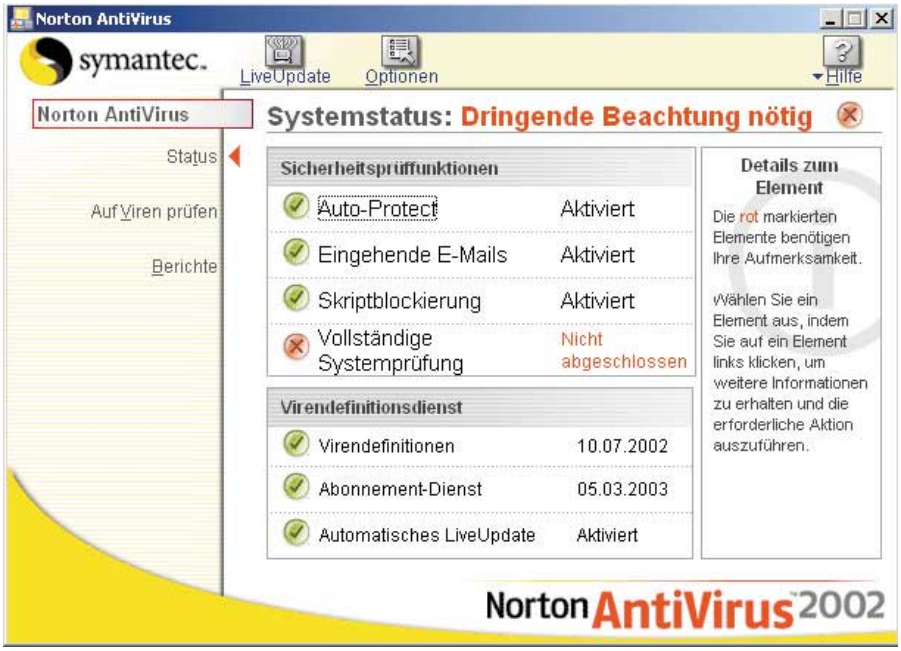
Unachtsame Anwender geraten schnell in die Fänge von Datenspionen und geben ihre Privatsphäre preis. Doch schon mit ein paar Verhaltensregeln minimieren Sie die Gefahr.

▸Mit einem aktuellen Antiviren-Programm und den richtigen Einstellungen sind Sie vor unliebsamen Überraschungen sicher. Ohne eine Antiviren-Software mit regelmäßigem Update sollten Sie keinen PC betreiben, schon gar nicht, wenn Sie oft im Internet surfen. Umfassenden Schutz vor Viren bieten Programme, die Ihre Daten mit einem Scanner und einem Wächtermodul observieren.

Der Virenscanner durchsucht den Arbeitsspeicher, Systembereiche der Festplatte und alle Dateien nach Schädlingen. Dabei legen Sie fest, ob auf lokalen Laufwerken, Disketten, anderen Wechsellaufwerken oder verbundenen Netzwerkverzeichnissen gesucht werden soll.

Der Virenwächter wird beim Start von Windows in den Arbeitsspeicher geladen und sorgt im Hintergrund für konstanten Schutz während Ihrer Arbeit. Er führt eine Virenprüfung durch, wenn Sie ein Programm verwenden, auf wechselbare Medien zugreifen oder Dokumentdateien öffnen. Bessere Programme bieten einen Browser- und E-Mail-Schutz und kontrollieren die ein- und ausgehenden Nachrichten einschließlich Datei-Anhänge und Dateien bei der Übertragung.

Wächter und Scanner zusammen sorgen dafür, dass Sie einen Virus entdecken, bevor er aktiv wird und Dateien infizieren kann. Zusätzlich bieten praktisch alle Programme eine Zeitsteuerung an. Damit regeln Sie, dass der Virenscanner in einstellbaren Abständen die ganze Festplatte durchsucht. Auch ein bequemes Online-Update für die Virendatenbank gehört heute zum Standard.



Benutzereingriff erforderlich: Ist Norton Antivirus 2002 nicht aktualisiert oder benötigt der Virenscanner aus anderen Gründen Ihre Aufmerksamkeit, erhalten Sie eine entsprechende Meldung

Für optimalen Schutz aktivieren Sie die Prüfung für alle Dateien

Moderne Antiviren-Programme verfügen über Einstellungsdialoge, über die Sie das Suchverhalten bei der Fahndung nach Viren und Trojanern steuern können. Einige Hersteller haben die Werkseinstellungen ihrer Software nicht an die neueren Entwicklungen bei der Virenverbreitung angepasst. Dadurch arbeitet mancher Scanner nicht optimal. Um hier gegebenenfalls nachbessern zu können, ist Kenntnis über die vom Scanner verwendeten Dateitypen erforderlich.

In der Vergangenheit war es üblich, sich beim Scannen von Dateien auf wenige Dateitypen zu beschränken, von denen besondere Gefahren ausgingen. Dazu gehörten insbesondere Programmdateien und Microsoft Office-Dokumente, die über Datei-Erweiterungen wie EXE, COM, SYS, DOC, DOT, XLS identifiziert wurden.

Windows verfügt jedoch über ein ganzes Arsenal an weiteren Datei-Extensionen, die sich entweder direkt aus dem Windows Explorer heraus oder über ein zusätzliches Programm ausführen lassen. Zu dieser Gruppe gehören zum Beispiel Scriptdateien. Dabei handelt es sich um reine Textdateien mit anderen Erweiterungen. Beim Aufruf eines solchen Scripts interpretiert Windows die gespeicherten Kommandos und führt die Befehle aus. Weil aktives Scripting ein wesentlicher Bestandteil aller aktuellen Windows-Versionen ist, haben Scriptda-

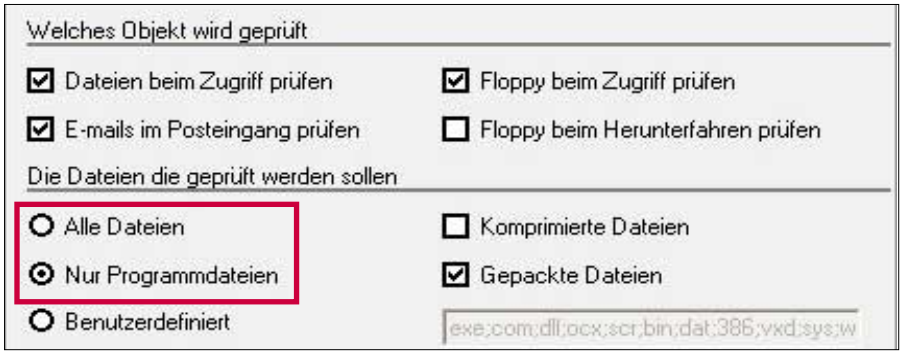
Info: Safe Computing

In Sachen Schutz vor Viren sollten Sie immer auf dem neuesten Stand bleiben. Und erst die passenden Einstellungen der Antiviren-Software sorgen dafür, dass dem Viren-Spürhund tatsächlich kein Schädling entgeht. Wir sagen Ihnen, worauf Sie achten müssen.

teien weitreichende Berechtigungen auf dem System. Dadurch können Viren Schaden auf dem PC verursachen.

Es ist nicht abzusehen, welche Anwendungs- oder Systemdateitypen findige Programmierer künftig noch als Transportmittel für ihre Angriffsprogramme verwenden werden. Trotz dieser Gefahr schließen viele Scanner manche Dateitypen beim Prüfen aus und riskieren, dass verseuchte Dateien unangetastet bleiben.

Der Grund dafür ist einfach: Der Scanvorgang ist viel schneller, wenn nicht alle Dateien geprüft werden. Angesichts der Leistung aktueller PCs können Sie minimale Einbußen zugunsten Ihrer Sicherheit verschmerzen. Schalten Sie daher die Option zum Durchsuchen aller Dateien im Virenscannermodul an.



Durchs Raster gefallen: Antiviren-Programme, die mit den Hersteller-seitigen Voreinstellungen nur bestimmte Datei-Erweiterungen prüfen, haben bei vielen neueren Viren das Nachsehen

Permanenter Hintergrundschutz durch Wächtermodul

Etwas anders sieht die Sache beim Virenwächter aus. Der arbeitet ständig im Hintergrund. Abhängig vom CPU-Tempo und der Speicherausstattung des PCs kann es sinnvoll sein, die Liste mit Datei-Erweiterungen einzuschränken. Viele Wächter bieten exakte Optionen an, bei welcher Art Datei-Operation sie die betroffene Datei prüfen: öffnen, kopieren, neu anlegen und so weiter. Sie sollten möglichst alle Optionen einschalten, damit der Wächter scharf kontrolliert.

Manche Virenwächter bieten die Option, Archivdateien zu durchsuchen. Wenn Sie viel mit Archivdateien hantieren und Ihr PC Leistungsprobleme hat, sollten Sie darauf verzichten. Das Durchsuchen dauert erheblich länger als bei normalen Dateien. Der Wächter schlägt spätestens dann Alarm, wenn Sie Dateien auspacken und auf die Platte schreiben wollen.

Unbekannte Schädlingstypen unbedingt einbeziehen

Scanner bieten als Ergänzung für die Suche mit Virensignaturen eine Option zur heuristischen Suche an. Dabei untersucht der Scanner eine Datei auf typische Merkmale für eine Infektion. Ab einer bestimmten Schwelle stuft er die Datei als infiziert ein. Je niedriger die Grenze liegt, desto höher ist die Gefahr eines Fehlalarms. Je höher die Grenze, desto eher rutscht ein echter Virus durch. Sie sollten die Heuristik in jedem Fall aktivieren.

Christoph Metzger

Prävention: 10 goldene Regeln

Mit der Beherzigung einiger weniger Regeln lässt sich die Gefahr einer Cyber-Attacke deutlich reduzieren.

1. Aktueller Virenscanner
Benutzen Sie ein aktuelles Antiviren-Programm, und halten Sie es auf dem neuesten Stand. Moderne Antiviren-Tools aktualisieren sich per Internet automatisch.

2. Virenscanner einschalten
Lassen Sie das Antiviren-Programm stets aktiv im Hintergrund laufen, auch wenn Sie sich sicher fühlen. Sobald Sie den Scanner deaktivieren, kann er verdächtige Dateien nicht erkennen.

3. Vorsicht bei Datei-Anhängen
Öffnen Sie keine Dateien, die Sie von Unbekannten unaufgefordert zugeschickt bekommen haben. Selbst wenn der lustige Bildschirmschoner von einem Freund kommt, sollten Sie sich vergewissern, aus welcher Quelle er ursprünglich stammt.

4. Schlechte Scherze
Fallen Sie nicht auf Virus-Hoaxes herein. Wenn Sie eine E-Mail-Warnung vor einem neuen Virus erhalten, gegen den es angeblich kein Gegenmittel gibt, leiten Sie die Mail nicht wie aufgefordert weiter. Informieren Sie sich etwa auf der PC-WELT-Website (**www.pcwelt.de**), ob dieser Virus tatsächlich existiert.

5. Software aktuell halten
Halten Sie Ihre Software – nicht nur Ihren Virenscanner – auf dem neuesten Stand. Sowohl für Betriebssystem, Internet-Software wie Mailprogramme und Webbrowser als auch für andere Programme gibt es immer wieder Aktualisierungen, die bekannte Sicherheitslücken schließen und Angreifern die Grundlage rauben.

6. Keine Software aus Newsgroups
Vermeiden Sie den Download von Software aus Newsgroups, denn hier kursieren besonders häufig verseuchte Dateien.

7. Informationen sammeln
Bleiben Sie auf dem Laufenden, was neue Sicherheitsbedrohungen angeht. Dann können Sie schneller reagieren, wenn Sie mit einem Virus, einem Wurm oder einer Sicherheitslücke konfrontiert sind.

8. Keine unnötigen Internet-Programme
Entfernen Sie nicht benötigte Software mit Internet-Anbindung von Ihrem Computer. Die Reduzierung der Dienste auf ein Minimum verringert die Systemanfälligkeit.

9. Kennwort-Disziplin
Setzen Sie starke Kennwörter ein, die ausreichend lang sind. Dadurch sind Ihre Passwörter nicht so leicht zu erraten oder zu knacken.

10. Privatsphäre schützen
Gehen Sie mit persönlichen Angaben wie Name, Adresse, Telefonnummer und Bankverbindung sorgsam um. Vermeiden Sie die Eingabe dieser Daten in Online-Formulare.

Virenscanner im Test

Wachhunde für Windows

Im Internet-Zeitalter verbreiten sich Viren in Sekundenschnelle. Daher sollte ein Virenscanner zur PC-Grundausstattung gehören. Unser Test zeigt auf, welche Tools etwas taugen und welche nicht.

Viren sind nicht nur ärgerlich, sie kosten private Anwender und Firmen auch richtig Geld. Allein „Code Red“ hat einen volkswirtschaftlichen Schaden von knapp zwei Milliarden Euro verursacht. Wurden Viren früher hauptsächlich über infizierte Datenträger verbreitet, so ist heute die E-Mail Transportmittel Nummer eins. Ist das System erst einmal von einem Virus befallen, übernimmt das Mailprogramm unbemerkt die weitere Verteilung des Schädlings. In Hochzeiten sind fünf bis zehn Virenmails pro Tag fast an der Tagesordnung.

Und eines haben alle Viren gemeinsam: Sie können auf der Festplatte viel Unheil anrichten. Besonders bösartige Varianten löschen Dokumente sowie Bilder und bringen Windows im schlimmsten Fall zum Absturz oder zerstören es derart, dass nur eine Neuinstallation hilft. Das ist Grund genug, einen Virenscanner zu installieren, der einen besonderen Schwerpunkt auf die Überwachung ein- und ausgehender Mails und der Online-Aktivitäten legt.

Info: Virenscanner

Wer ohne Virenscanner surft und Daten aus dem Internet lädt, spielt mit dem Feuer. Doch längst nicht alle Produkte können in der Praxis halten, was sie versprechen, so dass sich Anwender in trügerischer Sicherheit wiegen. Wir haben 15 Virenscanner für Sie getestet.

Virenprogrammierung: Mit den passenden Tools kann das jeder

Speziell die VB-Script-Viren stellen eine große Gefahr dar. Vor allem viele Würmer, die sich per Mail verbreiten, sind mit der Scriptsprache VB-Script programmiert. Besonders tückisch ist, dass einige „Construction Kits“ im Internet kursieren, mit deren Hilfe wirklich jeder PC-Benutzer in der Lage ist, einen neuen VBS-Virus zu erzeugen. Deshalb haben wir für unseren Test mit zwei verschiedenen Construction Kits je vier VBS-Würmer erzeugt. Alle Würmer wurden noch jeweils im Texteditor modifiziert, beispielsweise durch Einfügen einer Kommentarzeile oder durch einen neuen Zeilenumbruch. Auch das kann nahezu jeder Anwender machen.

Die allermeisten Virenscanner hatten damit kein Problem, denn sie verfügen über eine heuristische VBS-Suche. Das bedeutet, dass der Scanner nicht nach einer bestimmten Codezeile sucht, sondern den Code auf virentypische Merkmale analysiert. Einzelne Programme stolperten aber über ihre mangelhafte Heuristik, die entweder versagte oder zu unverständlichen Fehlalarmen führte.

Eine Besonderheit ist auch der JS/Kak@m-Virus, der in Javascript programmiert ist und sich über Mails im HTML-Format verbreitet. Hier verbirgt er sich nicht in einem Attachment, sondern sitzt wie bei einer normalen Website direkt als Script in den HTML-Daten der Mail. Durch ein älteres Sicherheitsloch des Internet Explorers (das übrigens bereits seit geraumer Zeit durch Patches geschlossen ist) wird JS/Kak@m ausgeführt, sobald der Internet Explorer die Web-Seite anzeigt. Der arglose Empfänger muss also nicht einmal erst mit einem Doppelklick ein Attachment starten.

Gefahrenquelle Outlook: Viren haben oftmals leichtes Spiel

Während viele Mailprogramme aufgrund ihrer Struktur und Arbeitsweise relativ sicher sind, ist Microsoft Outlook immer wieder – negativ – in den Schlagzeilen. Da zur Anzeige von Mails einzelne Module des Internet Explorers benutzt werden, können sich gefährliche Scriptviren in HTML-formatierten Mails ausbreiten. Viele dieser Viren arbeiten dann unbemerkt im Hintergrund und verschicken sich selbst an alle Einträge im Outlook-Adressbuch – entsprechend schnell verbreiten sie sich. Für solche Fälle ist eine Mailüberwachung Gold wert, da sie den Schädling herausfiltert, bevor er überhaupt zum Mailprogramm gelangt. Bei unserem Test haben wir uns eine entsprechend präparierte Mail selbst zugesandt.

Stolperstein: Online-Update klappt nicht immer

Ein Virenscanner schützt Sie immer nur dann wirkungsvoll gegen neueste Viren, wenn er aktuell ist. Fast täglich gibt es neue Viren, die von den Herstellern von Antiviren-Software in ihre Datenbanken aufgenommen werden müssen. Ist der Virenscanner nicht auf dem aktuellen Stand, können sich Viren auf dem lokalen System unerkannt ausbreiten und für enormen Schaden sorgen.

Um Anwendern die Aktualisierung so einfach wie möglich zu machen, setzen die Hersteller auf Online-Updates. Hierbei überprüfen die Virenscanner via Internet, ob es neue Virensignaturen und Programm-Updates gibt, laden diese und installieren sie. Einige Programme übernehmen diese Aufgabe sogar automatisch, erkennen eine Internet-Verbindung und aktualisieren sich stillschweigend.

In der Praxis ergeben sich aber überraschende Stolpersteine. Auf dem Testrechner war das Tool Smartsurfer von Web.de installiert, um die Downloads praxisnah über eine normale ISDN-Leitung abzuwickeln. Dabei benutzten wir zunächst einige besonders preiswerte Provider. Diese verwenden zur Senkung der Kosten für alle Verbindungen einen Proxy-Server. Dieser Proxy verhinderte bei F-Secure Anti-Virus und McAfee Virusscan das Online-Update beziehungsweise die Registrierung. Eine Verbindung über einen teureren Provider wie MSN löste in beiden Fällen das Problem.

Trügerische Sicherheit: Auch der Anwender muss mitspielen

Ein Virenscanner kann Ihren Windows-PC zwar grundsätzlich gegen Virusinfektionen schützen, darauf verlassen sollten Sie sich jedoch nicht. Erst im Zusammenspiel mit dem Anwender selbst wird ein wirksamer Schutz möglich. Oft sind es ein paar unbedachte Klicks auf eine geladene Datei, zu wenig Aufmerksamkeit beim Empfang von Mails unbekannter Absender oder das blinde Vertrauen beim Einlegen von Datenträgern, etwa von Disketten oder CDs, die man von jemand anderem erhalten hat.

PC-WELT-Testsieger

Den Spitzenplatz in unserem Vergleichstest teilen sich zwei Programme: **Antiviren-Kit Professional 11** (AVK) und **Norton Antivirus 2002** liegen mit der optimalen Online- und Mailüberwachung sowie einem herausragenden Virenwächter an der Spitze. AVK erzielte mit der doppelten Virensuchmaschine die besseren Suchleistungen, patzte aber bei der Unterstützung für Archive, indem es einzelne Dateien übersah. Außerdem war es nicht besonders gut beim Entfernen von Makroviren aus Dokumenten. Norton Antivirus 2002 bot das ausgewogenste Bild, überraschte aber mit einem Ausrutscher beim Internet-Download eines Word-Dokuments. **Kaspersky Antivirus Personal** konnte bei den Scanleistungen mithalten, enttäuschte aber mit einer langsamen Arbeitsweise und einem sehr hohen Ressourcenverbrauch, der nicht akzeptabel ist.

Auch wenn es Zeit kostet: Lassen Sie alle Dateien, die Sie aus dem Internet geladen haben, von einem Virenscanner überprüfen. Einige Download-Manager wie Get Right bieten sogar eine Schnittstelle zu Antiviren-Programmen, so dass Downloads automatisch vor dem Speichern auf der Platte auf mögliche Infektionen untersucht werden.

Wolfgang Nefzger

Im Überblick: Virenscanner

Produkt	Betriebssysteme	Internet-Adresse	Preis	Seite
Antivir Personal Edition 6.13	Win 95/98/ME, NT 4, 2000, XP	www.freeav.de	gratis*	86
Antiviren-Kit Professional 11	DOS, Win 95/98/ME, NT 4, 2000, XP	www.gdata.de	59,95 Euro	87
Bit Defender Home Edition 6.4.1	Win 95/98/ME, NT 4, 2000, XP	www.bitdefender.de	29,95 Dollar	88
Data Becker Antivirus 7.0	Win 95/98/ME, NT 4, 2000, XP	www.databecker.de	15,95 Euro	88
FP-Win Anti-Virus 3.0	DOS, Win 95/98/ME, NT 4, 2000, XP	www.dtp-ag.com	29,95 Euro	89
FP-Win Professional 5.12	DOS, Win95/98/ME, NT 4, 2000, XP	www.percomp.de	88 Euro	89
F-Secure Anti-Virus 5.30/5.31	DOS, Win95/98/ME, NT 4, 2000, XP	www.percomp.de	92,80 Euro	91
Kaspersky Anti-Virus Personal 4.0	DOS, Win 95/98/ME, NT 4, 2000, XP	www.kaspersky.com/de	45 Euro	91
McAfee Virusscan 6.02	DOS, Win 95/98/ME, NT 4, 2000, XP	www.mcafee.de	35 Euro	92
Norman Virus Control 5.3.2	Win 95/98/ME, NT 4, 2000, XP	www.norman.de	25,55 Euro	92
Norton Antivirus 2002	Win 98/ME, NT 4, 2000, XP	www.symantec.de	49,95 Euro	93
Ontrack Fix-it Utilities 4.0	Win 95B/98/ME, NT 4, 2000, XP	www.ontrack.de	49 Euro	93
Panda Antivirus Titanium 2.03	Win 95B/98/ME, NT 4, 2000, XP	www.panda-software.de	29,90 Euro	94
PC-Cillin 2002	Win 95B/98/ME, NT 4, 2000, XP	www.trendmicro.de	ab 49 Euro	94
Sophos Anti-Virus 3.57	DOS, Win 95/98/ME, NT 4, 2000, XP	www.sophos.de	114,84 Euro (ab 5er-Lizenz)	95

* für private Nutzung

Antivir Personal Edition 6.13

Funktionen: Das für den privaten Gebrauch kostenlose deutschsprachige Programm bietet Virenscanner, Virenwächter und Online-Update. Online ist ein 160 Seiten starkes Handbuch im PDF-Format zum Download verfügbar, das die Einarbeitung erleichtert. Das Online-Update funktionierte gut, da hierbei aber Programmänderungen übermittelt werden, ist von Zeit zu Zeit ein Download der kompletten Installationsdatei von rund 4 MB erforderlich.

Standardmäßig durchsucht der Scanner nur bestimmte, für Vireninfektionen besonders anfällige Dateitypen. Für den Test haben wir auf „Alle Dateien" umgeschaltet. Für den Scanvorgang gibt es keine weiteren Optionen, die Behandlung von infizierten Dateien lässt sich aber für Makro- und sonstige Viren getrennt einstellen. Insgesamt 18 Archivtypen kann Antivir behandeln. Bis auf einen nicht beanstandeten Melissa-Virus in einem gepackten Word-Dokument konnte Antivir überzeugen und entdeckte sogar bei CAB- und TAR-GZIP-Archiven alle infizierten Dateien.

Der Virenwächter reagierte sehr empfindlich, bereits das Überfahren einer infizierten Datei im Explorer genügte meistens für eine Warnmeldung. Das Entpacken eines ZIP-Archivs verhinderte der Wächter bei sämtlichen Dateien. Archive überwacht er nicht.

Das Entfernen von Makroviren klappte in den meisten Fällen gut, eine passwortgeschützte Word-Datei erkannte Antivir jedoch als zerstört und bot an, sie zu löschen. Auch die in Powerpoint eingebettete infizierte Excel-Tabelle konnte das Tool nicht entfernen. Die harmlosen Makros verschwanden ebenfalls regelmäßig, meistens ließ sich der Makro-Editor gar nicht mehr öffnen.

Den Download von Viren mit dem Internet-Browser verhinderte das Tool sicher und zuverlässig. Auch das Speichern und Ausführen der infizierten Mail-Attachments verhinderte Antivir sicher und ohne Grund zur Beanstandung. Der Empfang selbst blieb aber wegen der fehlenden Mailüberwachung in unseren Mail-Clients unberührt.

Fazit: Das Bild des Virenscanners ist zwiespältig. Ausgezeichneten Leistungen bei Boot-, Makro- und VB-Script-Viren standen mittelmäßige bei Trojanern gegenüber. Auffällig ist der Aussetzer bei den eigens mit Construction Kits hergestellten VBS-Viren – hier erwies sich die Heuristik als Schwachstelle des Programms.

Antivir Personal Edition 6.13

Info: H+B EDV
www.freeav.de
Preis: kostenlos (private Anwender)
299 Mark (kommerzielle Anwender)

⊕ **kostenlos, guter Update-Service**
⊖ **Schwächen bei VB-Script-Viren**

Funktionen	●●●○○
Virenscanner	●●●●○
Viren entfernen	●●●◐○
Archivbehandlung	●●●●○
Virenwächter	●●●●●
Online-Abwehr	●●●○○
Bedienung	●●●◐○
Gesamt:	●●●●○

Testurteil: Antivir 6.13 konnte durchaus überzeugen. Schwach war nur die Abwehrleistung gegen unbekannte VB-Script-Viren.

Bootviren ohne Chance: Der Wächter von Antivir hat einen Virus entdeckt und schlägt Alarm

Virenscanner: Wie wir testen (I)

Bei den Tests hat die PC-WELT neben der reinen Virenerkennung vor allem Wert auf die Überwachung von Datei- und Internet-Aktivitäten gelegt: Lässt sich eine virenverseuchte Datei mit dem Browser oder einem Download-Manager auf die Festplatte speichern? Was ist mit Viren und Würmern, die als Datei-Anhang einer Mail eintreffen? Um die Tests so transparent wie möglich zu machen, wurden die Programme – sofern möglich – auf die gleichen Optionen und Parameter eingestellt, so dass alle Dateien untersucht wurden. Im Einzelnen ging es um folgende Tests, die in der Summe die Gesamtbeurteilung ausmachen:

Funktionen
(10 Prozent der Gesamtnote)
– Online-Update
– Voreinstellungen
– Module

Virenscanner
(35 Prozent der Gesamtnote)
– 10 weit verbreitete Viren finden (teilweise in mehreren Varianten, 25 Dateien)
– 4 virenverseuchte Dateien finden, die mit dem EXE-Packer PE-Compact behandelt wurden
– 19 polymorphe Word-Makroviren finden
– Je 1000 polymorphe Dateiviren der Typen Smeg, Tpe und Mte finden
– 64 Trojanische Pferde finden
– 116 Bootviren finden
– 52 Makroviren finden
– Excel-Makrovirus als eingebettetes Objekt in einem Word-Dokument finden
– Excel-Makrovirus als eingebettetes Objekt in Powerpoint-Dokument finden
– Makrovirus in passwortgeschütztem Word-Dokument finden
– Makrovirus in passwortgeschütztem Excel-Dokument finden
– 54 VB-Script-Viren finden
– 4 HTML/Javascript-Viren finden

Viren entfernen
(10 Prozent der Gesamtnote)
– Makrovirus aus Word-Dokument (Office 2000) entfernen
– Harmloses Makro bleibt beim Entfernen eines Word-Makrovirus erhalten
– Makrovirus aus Excel-Dokument (Office 2000) entfernen
– Harmloses Makro bleibt beim Entfernen eines Excel-Makrovirus erhalten
– Makrovirus aus Excel-Embed in Powerpoint-Datei entfernen
– Öffnen der Powerpoint-Präsentation und der eingebetteten Excel-Tabelle
– Wurm Happy 99 aus dem infizierten Windows-System entfernen
– VB-Script-Viren aus befallenen HTML-Dateien entfernen

Antiviren-Kit Professional 11

Funktionen: Das von G-Data stammende Programm wurde gegenüber der letzten Version komplett erneuert und verwendet jetzt die bewährte Virensuchmaschine von Kaspersky Lab und das Modul RAV der rumänischen Firma Gecad. Es überwacht nunmehr E-Mails bereits beim Abholen. Bei der Installation übernahm das Setup die Mailkonten von Outlook Express sowie Pegasus Mail und Eudora automatisch, bei den beiden letztgenannten Programmen aber nur den Standard-Account. Hier muss der Anwender weitere Konten von Hand einrichten, wozu lediglich ein Proxy eingetragen werden muss. Das Online-Update erzwingt eine Online-Registrierung beim Hersteller. Ohne Benutzernamen und Passwort geht nichts. Die Grundeinstellungen des Antiviren-Kits (AVK) sind gut: Standardmäßig werden Archive durchsucht, die Heuristik ist eingeschaltet. Zusätzlich wurde für den Test lediglich die Option „Alle Dateien" aktiviert.

Die Archivunterstützung war überzeugend, lieferte aber wie Antivir einen Aussetzer: In den meisten Archiven übersah AVK die Datei MELISSA2.DOC. Die Ausnahme waren nur LHA- und GZIP-Archive sowie selbstentpackende RAR- und ZIP-Archive (EXE-Dateien). In Einzelfällen könnte das dazu führen, dass in einem Archiv eine infizierte Datei übersehen wird. Dafür waren passwortgeschützte Archive unübersehbar markiert und auch verschachtelte Archive kein Problem.

Der Virenwächter und die Online-Überwachung erledigten ihre Aufgaben dagegen zu 100 Prozent – besser geht es nicht. Die Mailüberwachung arbeitet sowohl mit Mapi-Programmen (Exchange-Clients) als auch mit POP3-Programmen (Pegasus Mail, T-Online Mail). Die Betreffzeile einer infizierten Mail wird um den Hinweis „Virus" ergänzt, das betroffene Attachment wird mit der Erweiterung VIR versehen und lässt sich dadurch nicht mehr ausführen. Die volle Punktzahl erreichte der Scanner zwar in keiner Kategorie, aber es fehlten auch immer nur ein oder zwei Viren.

Fazit: Der Virenscanner gibt im Grunde keinen Anlass zur Kritik, das Entfernen von Makroviren war allerdings nicht die Stärke von AVK 11. Bei Word und Excel klappte das Entfernen, allerdings verschwanden auch konsequent die harmlosen Makros. Eingebettete Dokumente mit Makroviren erkannte das Tool zwar, scheiterte aber beim Bereinigen.

Antiviren-Kit Professional 11

Info: G-Data
www.gdata.de
Preis: 59,95 Euro

⊕ zwei Virenscanner
⊖ Probleme bei Makroviren

Funktionen	●●●●◐
Virenscanner	●●●●●
Viren entfernen	●●◐○○
Archivbehandlung	●●●●○
Virenwächter	●●●●●
Online-Abwehr	●●●●●
Bedienung	●●●●◐
Gesamt:	●●●●◐

Testurteil: Das Programm glänzte vor allem durch herausragende Suchleistungen. Eine Schwäche hatte es nur beim Entfernen von Makroviren.

Einfache Bedienung: Das Programm bietet alle relevanten Optionen im schnellen Zugriff

Virenscanner: Wie wir testen (II)

Archivbehandlung
(5 Prozent der Gesamtnote)
– Topviren in Archiven vom Typ ACE, ARJ, CAB, JAR, LZH, PAK, RAR, RAR-SFX, TGZ (TAR plus GZIP), ZIP, ZIP-SFX finden
– Topviren in einem passwortgeschützten ZIP-Archiv finden
– Topviren in zwei verschachtelten Archiven (ARJ und ZIP) finden

Virenwächter
(15 Prozent der Gesamtnote)
– Infizierte Diskette mit Parity-Boot einlegen und im Explorer anzeigen
– Virus im Explorer über Kontextmenü kopieren
– Virus im Explorer über Kontextmenü ausschneiden
– Virus im Explorer per Drag & Drop verschieben
– Topviren mit dem Explorer kopieren
– Word-Dokument mit Makrovirus öffnen
– Excel-Dokument mit Makrovirus öffnen
– Word-Dokument mit eingebettetem Excel-Makrovirus öffnen
– Powerpoint-Dokument mit eingebettetem Excel-Makrovirus öffnen
– ZIP-Archiv mit virenverseuchten Dateien kopieren
– ZIP-Archiv mit virenverseuchten Dateien auspacken

Online-Abwehr
(15 Prozent der Gesamtnote)
– Wurm W32.QAZ und Makrovirus PSD 2000 (Word-Dokument) von einer Web-Seite im Internet downloaden (Internet Explorer 6.0, Netscape Navigator 6.2.2)
– Mail mit W32.QAZ als Datei-Anhang empfangen (mit Outlook Express 6, Pegasus Mail 4.0, Eudora 5.02)
– Mail mit Happy 99 im ZIP-Archiv als Datei-Anhang empfangen (mit Outlook Express 6, Pegasus Mail 4.0, Eudora 5.02)
– Maildatei-Anhang W32.QAZ speichern (mit Outlook Express 6, Pegasus Mail 4.0, Eudora 5.02)
– Maildatei-Anhang W32.QAZ direkt starten (mit Outlook Express 6, Pegasus Mail 4.0, Eudora 5.02)
– Web-Seite mit VB-Script-Virus HTML.Reality aufrufen

Bedienung
(10 Prozent der Gesamtnote)
– Installation
– De-Installation
– Desktop-Integration
– Bedienerführung
– Handbuch
– Einarbeitungszeit

Bit Defender Home Edition 6.4.1

Funktionen: Neben Scanner, Wächter, Online-Update und Zeitplaner wartet Bit Defender mit etlichen Zusatzleistungen auf. Es überwacht nämlich auch den Datenverkehr von Instant-Messaging-Programmen. Zudem werden Zugriffe auf sensible Bereiche der Registry überprüft.

Bit Defender Home Edition 6.4.1

Info: Softwin
www.bitdefender.de
Preis: 29,95 Dollar

⊕ guter Update-Service
⊖ Schwächen bei Scriptviren

Funktionen	●●●◐○
Virenscanner	●●●●○
Viren entfernen	●●●◐○
Archivbehandlung	●●●○○
Virenwächter	●●●●◐
Online-Abwehr	●●●●◐
Bedienung	●●●●○
Gesamt:	●●●●○

Testurteil: Die Virensuchleistung überzeugte, die Topviren waren kein Problem. Mangelhaft war die Erkennung unbekannter VB-Script-Viren und eingebetteter Objekte.

Die Virensuchleistung konnte in den Kernbereichen überzeugen. Die Topviren waren genauso wenig ein Problem wie Trojaner, Makroviren und bekannte VB-Script-Viren. Überall reichten die Suchergebnisse zur Spitzengruppe. Die heuristische Suche nach neuen VB-Script-Viren konnte nicht mithalten, sie fand ganze 3 von 16 VBS-Testwürmern. Auch die infizierte Excel-Tabelle innerhalb einer Powerpoint-Datei ignorierte der Scanner.

Der Virenwächter leistete insgesamt gute Arbeit, versagte aber bei der Powerpoint-Datei. Trotz Makrovirus im eingebetteten Excel-Objekt war das Öffnen erlaubt. Die Unterstützung für Archive lässt sich getrennt einschalten, funktioniert aber nur dann, wenn zusätzlich die Option „Alle Dateien“ aktiviert ist. Das Entfernen von Makroviren war für Bit Defender kein Problem, allerdings wurden dabei grundsätzlich alle Makros gelöscht.

Bei der Mailüberwachung weist eine Dialogbox auf die Erkennung eines infizierten Attachments hin. In der Mail fehlt

Virenalarm: Wird Bit Defender fündig, bietet es je nach Virentyp verschiedene Optionen an

allerdings das Attachment ohne Hinweis. Auch Scripts in einer HTML-Mail werden kommentarlos entfernt. Einen Aussetzer gab es bei Eudora: Happy 99 als Attachment konnten wir nach Bestätigung einiger Dialoge starten. Immerhin bemerkte und blockierte Bit Defender den Versuch des Wurms, sich in der Registry als Autostart-Programm einzutragen.

Fazit: Bit Defender bietet viele nützliche Features. Die Virensuchleistungen waren ausgezeichnet, die Schwächen bei der Erkennung unbekannter VB-Script-Viren und eingebetteter Powerpoint-Objekte führten zu einer Abwertung.

Data Becker Antivirus 7.0

Funktionen: Bis auf kosmetische Änderungen entspricht das Data-Becker-Programm der Standard Edition des Lizenzgebers AVG. Die Voreinstellungen des Programms sind praxisgerecht und leicht zu verstehen. Der Zeitplaner kann die Online-Updates ausführen und ansonsten nur einen Test sämtlicher Festplatten auslösen. Scan-Aufgaben mit Suchziel und Optionen lassen sich nicht anlegen.

Data Becker Antivirus 7.0

Info: Data Becker
www.databecker.de
Preis: 15,95 Euro

⊕ günstiger Preis
⊖ schlechte Archivunterstützung

Funktionen	●●●◐○
Virenscanner	●●●●◐
Viren entfernen	●●●◐○
Archivbehandlung	●●◐○○
Virenwächter	●●●●◐
Online-Abwehr	●◐○○○
Bedienung	●●●○○
Gesamt:	●●●◐○

Testurteil: Die Suchleistung war durchwachsen: Data Becker Antivirus fand alle Top-Viren, bei allen anderen Kategorien fehlten aber immer etliche Viren zur vollen Punktzahl.

Die Archivunterstützung ist mit ZIP, ARJ, RAR (auch selbstentpackend) und verschachtelten Archiven in Ordnung. Bei ZIP-Archiven fand das Tool 19 von 20 infizierten Dateien. Der Virenwächter bemerkte zwar die infizierte Diskette im Laufwerk, verhinderte aber nicht das Auspacken von infizierten Dateien aus einem ZIP-Archiv. Dafür meldete das Tool bereits beim Anklicken einer Datei im Explorer einen Virus. Auch das Öffnen von infizierten Office-Dokumenten verhinderte der Wächter sicher.

Beim Entfernen von Viren löschte das Programm in Word- und Excel-Dokumenten prinzipiell alle Makros. Dafür konnte es auch im Powerpoint-Dokument die eingebettete infizierte Excel-Tabelle reinigen – allerdings ließ sich nachher zwar die Präsentation öffnen, nicht aber die Excel-Tabelle. Dasselbe passierte bei der Word-Datei mit eingebetteter Excel-Tabelle.

Virus per Mail: Bei infizierten Mail-Attachments wird die Nachricht um einen Hinweis ergänzt

Die Online-Überwachung war beim Internet Explorer lückenlos, bei Netscape 6 konnten wir aber eine infizierte Datei auf der Festplatte speichern. Die Überwachung der E-Mail funktionierte im Test nur bei Eudora korrekt. Auch im gepackten Attachment entdeckte das Tool den Wurm. Die Mail wurde um einen entsprechenden Hinweis ergänzt.

Fazit: Data Becker Antivirus bot lediglich eine durchschnittliche Leistung bei der Virenerkennung, der Virenwächter hatte deutliche Schwächen. Die Mailüberwachung funktionierte nur bei Eudora ohne Probleme.

FP-Win Anti-Virus 3.0

Funktionen: Die Optionen von FP-Win sind sehr zurückhaltend eingestellt und müssen auf Archive oder komprimierte Dateien sowie alle Dateien erweitert werden. Das Online-Update funktionierte problemlos. Allerdings überträgt es nur neue Virensignaturen – Programm-Updates bekommt man als registrierter Kunde alle drei Monate per CD.

Bei der Archivunterstützung ist bis auf ACE, PAK und selbstextrahierende RAR-Archive alles dabei, auch verschachtelte Archive. Das passwortgeschützte ZIP-Archiv erschien allerdings nur im ausführlichen Bericht.

Der Virenwächter reagierte sehr empfindlich. Es genügte, eine Datei im Explorer mit der Maus zu überfahren, anzuklicken oder das Kontextmenü aufzurufen. Allerdings ließen sich infizierte Dateien per Kontextmenü oder Drag & Drop doch kopieren, wenn man die Warnmeldung wegklickte. Das Öffnen von infizierten Excel- und Word-Dokumenten verhinderte der Wächter dagegen sicher.

Die Online-Überwachung war weitgehend lückenlos, nur den Download des Mail-Attachments ließ FP-Win bei Outlook Express und Pegasus unbeachtet. Beim Speichern zeigte der Wächter zwar eine Warnung, die Datei befand sich aber danach doch auf der Platte. Bei Eudora wurden die infizierten Attachments nach dem Download bemerkt.

Beim Entfernen von Makroviren ist einstellbar, ob nur die Virenmakros oder alle Makros gelöscht werden sollen. Für den Fall, dass ein Virus nicht eindeutig identifiziert wird, besteht die Option, zur Sicherheit alle Makros zu entfernen.

Fazit: ein gutes Antiviren-Programm mit im Grunde überzeugenden Suchleistungen und einem ordentlichen Virenwächter. Die fehlende Mailprüfung trennt es von den Spitzenprodukten. Bei den VB-Script-Viren in HTML-Dateien machte die Software keine so gute Figur: Mehr als Löschen beherrscht sie nicht.

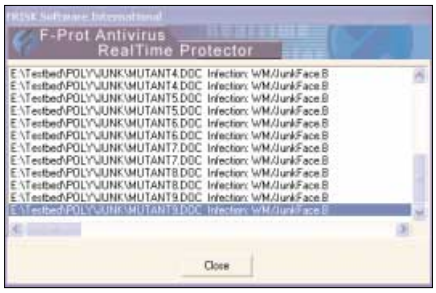
FP-Win Anti-Virus 3.0

Info: DTP AG
www.dtp-ag.com
Preis: 29,95 Euro

⊕ zuverlässiger Virenwächter
⊖ Programm-Updates nur auf CD

Funktionen	●●●◐○
Virenscanner	●●●●◐
Viren entfernen	●●●●○
Archivbehandlung	●●●◐○
Virenwächter	●●●●●
Online-Abwehr	●●●○○
Bedienung	●●●○○
Gesamt:	●●●●○

Testurteil: Der Virenscanner gab sich bei den Standardviren, Makroviren und Trojanern keine Blöße. Bei VB-Script- sowie Bootviren besteht allerdings noch Verbesserungsbedarf.



Sichere Erkennung: Makroviren in Word-Dokumenten waren für FP-Win Anti-Virus kein Problem

FP-Win Professional 5.12

Funktionen: FP-Win Professional ist mit Zeitplaner und Online-Update für Virensignaturen sowie Virenwächter komplett ausgestattet. Beim Online-Update werden nur neue Virensignaturen übertragen, Programm-Updates erhalten registrierte Kunden alle drei Monate auf CD.

Die VBS-Testviren stellten FP-Win vor Probleme, von 16 Exemplaren fand das Tool 13. Bis auf ACE, PAK und selbstextrahierende RAR-Archive unterstützt FP-Win alle Typen. Der Virenwächter ist unter Windows XP nicht zu konfigurieren und lässt sich nur aus- oder einschalten. Der Wächter reagierte sehr empfindlich und schlug schon beim Überfahren, Anklicken oder beim Aufruf des Kontextmenüs Alarm. Das Öffnen von infizierten Excel- und Word-Dokumenten verhinderte der Wächter.

Bei der Online-Überwachung konnten wir ein infiziertes Mail-Attachment bei Outlook Express speichern, das Ausführen wurde verhindert. Bei Eudora bemerkte der Wächter die Attachments sofort nach dem Download. Nach Empfang der HTML-Mail mit eingebettetem JS/Kak sperrte der Virenwächter die komplette Inbox von Eudora, so dass der Wächter vorübergehend abzuschalten und die verseuchte Mail von Hand zu löschen war. Das Entfernen von Makroviren unterstützt FP-Win mit etlichen Optionen. Für den Fall, dass ein Virus nicht eindeutig identifiziert wird, besteht die Möglichkeit alle Makros komplett aus dem Dokument zu entfernen. Eingebettete Objekte in Powerpoint konnte FP-Win nicht säubern, wohl aber in Word-Dokumenten.

Fazit: ein gutes Antiviren-Programm mit weitgehend überzeugenden Suchleistungen und einem ordentlichen Virenwächter. Die fehlende Mailprüfung trennt es von den Spitzenprodukten. Unverständlich ist, warum beim Start des Scanners über das Kontextmenü im Windows-Explorer keine Archive durchsucht werden können.

FP-Win Professional 5.12

Info: Percomp-Verlag
www.percomp.de
Preis: 88 Euro

⊕ sehr gute Online-Abwehr
⊖ fehlende Mailprüfung

Funktionen	●●○○○
Virenscanner	●●●●◐
Viren entfernen	●●●●○
Archivbehandlung	●●●◐○
Virenwächter	●●●●●
Online-Abwehr	●●●○○
Bedienung	●●●●○
Gesamt:	●●●●○

Testurteil: Der Virenscanner gab sich bei den Standardviren keine Blöße. Bei den übrigen Schädlingen fehlten jeweils nur ein paar Treffer zur vollen Punktzahl.

Variabel: Die Optionen des Virenscanners sind vielfältig einstellbar und lassen sich sichern

F-Secure Anti-Virus 5.31

Funktionen: In F-Secure sind zwei Virensuchmaschinen integriert. Die eine stammt von Frisk Software, die andere kommt von Kaspersky Lab. Zum Test verwendeten wir die Version 5.31, die es nur für Windows XP gibt. Für alle anderen Windows-Versionen ist 5.30 aktuell. Die Bedienung ist etwas unübersichtlich, die Konfiguration ist nur über die Taskleiste erreichbar. Ein Hauptprogramm im eigentlichen Sinn gibt es nicht. Interessant ist die Option des Virenwächters, bestimmte Dateien und Verzeichnisse auszuschließen. Ansonsten durchsucht der Wächter auf Wunsch auch Archive. Die Unterstützung dafür ist ausgereift, alle einschlägigen Archivtypen werden durchsucht. Leider meldet der Scanner keine passwortgeschützten Archive, die so unbemerkt durchschlüpfen können.

Der Virenwächter reagierte sehr empfindlich. Er verhinderte bei fast allen Gelegenheiten den Zugriff auf infizierte Dateien und Dokumente. Beim Auspacken eines ZIP-Archivs aber meldete er nur den ersten Virus und erlaubte dem Packer, alle nachfolgenden Viren, auf die Platte schreiben. Das Entfernen von Makroviren klappte nicht auf Anhieb. F-Secure kann nicht mit schreibgeschützten Dateien umgehen. Beim Säubern eines Word-Dokuments von einem Makrovirus war dieses anschließend defekt, so dass sich zwar der Text, nicht aber die Makros öffnen ließen. Die eingebetteten Objekte säuberte F-Secure zwar bei Word, nicht aber bei Powerpoint. Beim Online-Schutz ging dem Wächter der Download der Mail mit Viren-Attachment durch die Lappen, alle anderen Aktionen waren blockiert. Bei Eudora bemerkte F-Secure die infizierten Anhänge unmittelbar nach dem Laden.

Fazit: F-Secure ist ein wenig umständlich in der Bedienung, bot aber eine herausragende Suchleistung. Die Virensuchleistung war exzellent bis auf ein oder zwei Exemplare pro Kategorie. Der schwächste Programmteil war die Online-Abwehr.

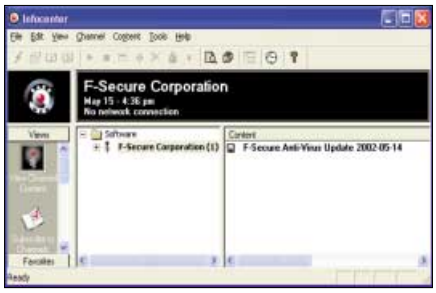
F-Secure Anti-Virus 5.31

Info: Percomp-Verlag
www.percomp.de
Preis: 92,80 Euro

⊕ **sehr gute Suchleistung**
⊖ **umständliche Bedienung**

Funktionen	●●○○○
Virenscanner	●●●●●
Viren entfernen	●●●◐○
Archivbehandlung	●●●◐○
Virenwächter	●●●●●
Online-Abwehr	●●●○○
Bedienung	●●●○○
Gesamt:	●●●●○

Testurteil: Hinter der antiquierten und bisweilen umständlichen Bedienung steckt ein Scanner mit einer sehr guten Suchleistung. Die Online-Abwehr war hingegen unbrauchbar.



Umständlich: Die Optionen in F-Secure Anti-Virus sind über das Infocenter schwer zugänglich

Kaspersky Anti-Virus 4.05

Funktionen: Die Bedienung von Kaspersky Anti-Virus Personal 4.05 (KAV) ist es etwas komplexer als bei der Konkurrenz. Die Zentrale ist das Control-Center, das die Steuerung sämtlicher Module wie Virenwächter, Zeitplaner und Online-Updates übernimmt. Die Standardeinstellungen des Scanners sind zurückhaltend: Es werden nur festgelegte Dateitypen untersucht, darunter aber Archive und komprimierte Programmdateien. Das Online-Update klappte auf Anhieb, es lädt die benötigten Dateien automatisch.

Der Virenscanner von KAV überzeugte und fand bis auf das passwortgeschützte ZIP-Archiv sowie ACE und PAK alle Viren. Den Hinweis auf die Verschlüsselung versteckt KAV im Report. Dafür sind verschachtelte Archive kein Thema.

Die Bilanz des Virenwächters ist getrübt. Beim Kopieren im Explorer übersah er den Makrovirus in einer Powerpoint-Datei. Auch beim Öffnen dieser Präsentation schlüpfte der Makrovirus in der eingebetteten Excel-Datei durch. Mit der Einstellung „Alle Dateien" erkannte KAV den Virus jedoch problemlos. Die Online-Überwachung arbeitete gut, funktionierte aber nur bei Outlook in Verbindung mit einem Exchange-Server (Mapi). Für alle privaten Anwender ist das irrelevant. Beim Entfernen von Makroviren wurden die Programmzeilen der Schadmakros bei Excel mit einer Zeichenkette überschrieben. Auf diese Weise blieben die Namen der Virenmakros erhalten – das verwirrt möglicherweise. Harmlose Makros blieben erhalten. KAV konnte eingebettete Objekte in Word-Dokumenten bereinigen. Bei der Powerpoint-Datei klappte die Reinigung eingebetteter Objekte nicht.

Fazit: Kaspersky Anti-Virus ist ein herausragendes Antiviren-Programm, das aber bei der Online-Überwachung von Mails Schwächen zeigte. Störend ist zudem die langsame Arbeitsweise. Positiv hervorzuheben sind die täglich aktualisierten Updates für die Virendatenbank. ▶

Kaspersky Anti-Virus 4.05

Info: Kaspersky Lab
www.kaspersky.com/de
Preis: 45 Euro

⊕ **hervorragende Virenerkennung**
⊖ **langsam, hoher Ressourcenverbrauch**

Funktionen	●●●●○
Virenscanner	●●●●●
Viren entfernen	●●●●◐
Archivbehandlung	●●●●○
Virenwächter	●●●●◐
Online-Abwehr	●●●◐○
Bedienung	●●●○○
Gesamt:	●●●●◐

Testurteil: KAV zeigte herausragende Leistungen und eine gute Archivunterstützung: Nur das passwortgeschützte ZIP-Archiv sowie ACE und PAK blieben verschlossen.

Scanner-Optionen: Kaspersky Anti-Virus erlaubt vielfältige Einstellungen und Anpassungen

McAfee Virusscan 6.02

Funktionen: Virusscan wurde komplett umgekrempelt und zeigt jetzt im Startbildschirm den aktuellen Status: letzter Scanvorgang, Einstellungen des Virenwächters, Alter der Virensignaturen und so weiter. Das Online-Update übernimmt ein eigenes Modul. Mangelhaft ist die Archivunterstützung: Zwar wird eine Reihe von Archiven erkannt, doch meldete der Scanner immer nur eine befallene Datei pro Archiv. Auch ein Passwortschutz im Archiv wurde nirgends erwähnt. Dafür waren verschachtelte Archive kein Problem.

Der Virenwächter war auf der Höhe der Zeit und erledigte die Aufgaben fast vollständig. Nur das Kopieren eines ZIP-Archivs mit infiziertem Inhalt blieb unbemerkt. Die Überwachung der Mailaktivitäten war je nach Programm unterschiedlich. Laut Handbuch soll die Funktion sowohl Mapi-kompatible Programme als auch POP3-Zugriffe überwachen: Outlook Express empfing ebenso wie Pegasus Mail ungerührt verseuchte Mailanhänge. Das Speichern oder Starten der infizierten Datei verhinderte der Wächter aber zuverlässig. Bei Outlook warnte Virusscan vor der Anzeige der HTML-Mail mit dem KAK-Wurm – und zeigte die Mail trotzdem an. Bei Eudora wurden alle infizierten Objekte noch während des Downloads entdeckt und deren Speicherung auf die Platte untersagt. Praxistauglich arbeitete Virusscan beim Entfernen von Viren. In Office-Dokumenten löschte es nur die Virenmakros, harmlose Makros blieben erhalten. Selbst Makroviren in eingebetteten Dokumenten innerhalb von Word und Powerpoint entfernte es. Die Dokumente konnten danach bearbeitet werden.

Fazit: McAfee Virusscan überzeugte mit ausgezeichneter Suchleistung und einem aufmerksamen Virenwächter. Es fehlen nur noch eine vollständige Archivunterstützung und die zwingende Überwachung von POP3-Mail-Accounts.

McAfee Virusscan 6.02

Info: McAfee
www.mcafee-at.home.de
Preis: 35 Euro

⊕ aufmerksamer Virenwächter
⊖ keine POP3-Mailüberwachung

Funktionen	●●●◐○
Virenscanner	●●●●●
Viren entfernen	●●●●●
Archivbehandlung	●○○○○
Virenwächter	●●●●●
Online-Abwehr	●●●◐○
Bedienung	●●●○○
Gesamt:	●●●●○

Testurteil: Die Suchleistung des Programms war herausragend. Die Leistung war dabei bei allen Modulen gleich gut. Unverständlich gelöst ist allerdings die Virenentfernung.

Gute Bedienung: McAfee Virusscan erlaubt schnellen Zugriff auf die Optionen

Norman Virus Control 5.3.2

Funktionen: Norman Virus Control 5.3.2 (NVC) ist komplett neu entwickelt und wirkt jetzt wie aus einem Guss. Die einzelnen Programmmodule Scanner, Zeitplaner, Konfigurator und Internet-Update sind eigenständig. Der Zeitplaner kann nicht nur die Festplatte durchsuchen, sondern auch neue Updates holen.

Der Virenscanner fand sämtliche Makroviren, nahezu alle Trojaner (55 von 57) und bis auf 3 alle VB-Script-Viren. Bei Bootviren (99 von 116) konnte er den Anschluss zur Spitzengruppe nicht halten. Die extra erzeugten VBS-Würmer wurden nicht erkannt. Die Archivunterstützung fällt mit ZIP, JAR und ARJ sowie verschachtelten Archiven mager aus. Beim Entfernen löschte Virus Control alle Makros im Office-Dokument. Auch das eingebettete Excel-Arbeitsblatt in der Powerpoint-Präsentation bearbeitete NVC, allerdings ließ sich die eingebettete Tabelle anschließend nicht mehr öffnen.

Der Virenwächter übersah beim Kopieren und Verschieben alle infizierten Office-Dokumente. Alle anderen infizierten (Programm-)Dateien wurden erkannt und geblockt. Das Entpacken eines ZIP-Archivs gelang zwar, aber anschließend meldete der Wächter alle 20 entpackten Virendateien. Das Öffnen von infizierten Office-Dokumenten verhinderte der Wächter. Der Download infizierter Dateien mit dem Explorer wurde sicher verhindert. Bei Pegasus und Eudora bemerkte NVC die infizierte HTML-Mail unmittelbar nach dem Empfang. Bei Eudora verhinderte der Wächter auch das Ablegen des infizierten Attachments auf der Festplatte.

Fazit: Der Virenscanner bot eine überzeugende Leistung und zeigte gute, teilweise herausragende Ergebnisse. Fehlende Mailunterstützung und die Aussetzer des Wächters bei Office-Dokumenten trüben das Bild. Die Archivunterstützung kennt nur ZIP, JAR und ARJ sowie verschachtelte Archive.

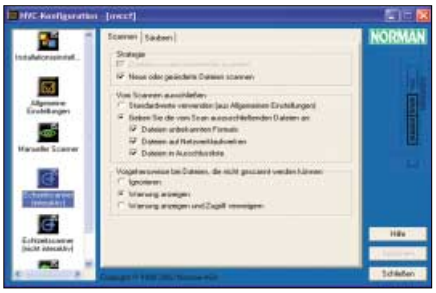
Norman Virus Control 5.3.2

Info: Norman Data Defense
www.norman.de
Preis: 25,55 Euro

⊕ ressourcenschonend
⊖ Gefahr durch Bootviren

Funktionen	●●●○○
Virenscanner	●●●●◐
Viren entfernen	●●●●◐
Archivbehandlung	●●◐○○
Virenwächter	●●●●◐
Online-Abwehr	●●●◐○
Bedienung	●●●○○
Gesamt:	●●●●○

Testurteil: NVC fand sämtliche Makroviren, nahezu alle Trojaner und bis auf 3 alle VB-Script-Viren. Bei Bootviren konnte NVC den Anschluss zur Spitzengruppe nicht halten.



Reichlich Optionen: Die Konfiguration von Norman Virus Control 5.3.2 ist übersichtlich gestaltet

Panda Antivirus Titanium 2.03

Funktionen: Unter der runderneuerten Bedienerführung stecken wenige Optionen, die auch Einsteiger beherrschen. Das Online-Update wartet beispielsweise darauf, dass eine Internet-Verbindung besteht und sucht dann automatisch nach Updates. Bei der Virensuche lässt sich die heuristische Suche lediglich ein- oder ausschalten. Kompromisslos durchsucht der Scanner immer alle Dateien, der Virenwächter bestimmte Dateitypen. Auf Wunsch prüft der Wächter auch Archive, der Scanner macht dies immer. Eine Integration im Windows-Explorer fehlt.

Polymorphe DOS- und Bootviren erkannte das Programm nur ungenügend. Dafür erkannte die Heuristik alle VBS-Testwürmer. Die Archivunterstützung erfasst alle wichtigen Archivtypen und verschachtelte Archive. Der Virenwächter verhinderte nicht nur das Kopieren von infizierten Dateien, sondern auch von Archiven mit infiziertem Inhalt. Auch das Öffnen von infizierten Dokumenten in Word und Excel verhinderte das Programm – mit Ausnahme der in Powerpoint eingebetteten Excel-Tabelle. Das Entfernen von Makroviren in den Testdokumenten gelang, die harmlosen Makros blieben erhalten.

Versuche, infizierte Dateien im Browser herunterzuladen, blockte Panda wirkungsvoll. Lediglich Scripts innerhalb von Web-Seiten entgingen dem Wächter. Die Mailüberwachung funktionierte ohne weitere Konfiguration mit allen geprüften Mail-Clients. Lediglich infizierte Objekte, die desinfiziert werden können, ließ Panda nach einer Warnmeldung passieren. Eine Sicherheitslücke ist das bei Scripts, die in HTML-Mails versteckt sind.
Fazit: Panda Antivirus Titanium hat das Zeug, in der Spitzengruppe mitzuspielen. Der Virenscanner lieferte gute Leistungen. Die Probleme mit polymorphen DOS- und Bootviren sowie die Aussetzer bei der Mailüberwachung ließen das Programm aber zurückfallen.

Panda Antivirus Titanium 2.03

Info: Panda Software
www.panda-software.de
Preis: 29,90 Euro

⊕ funktionaler Internet-Schutz
⊖ Mailintegration verbesserungswürdig

Funktionen	●●●◐○
Virenscanner	●●●●◐
Viren entfernen	●●●●●
Archivbehandlung	●●●○○
Virenwächter	●●●●◐
Online-Abwehr	●●●●○
Bedienung	●●●●○
Gesamt:	●●●●○

Testurteil: Ein guter Virenscanner mit Problemen bei polymorphen DOS- und Bootviren sowie leichten Schwächen bei der Mailüberwachung. Die Windows-Integration ist verbesserungswürdig.

Statusanzeige: Panda Antivirus Titanium weist direkt beim Start auf seine Aktualität hin

PC-Cillin 2002

Funktionen: Unter der einheitlichen bunten Benutzerführung sind alle Programmfunktionen und -einstellungen versammelt. Neben den obligatorischen Modulen Scanner, Virenwächter, Zeitplaner und Online-Update gibt es eine Personal Firewall und Unterstützung für PDAs. Auch eine Mailüberwachung für POP3-Accounts ist mit dabei. Zudem lassen sich Java-Applets und Active-X-Controls sowie einzelne URLs im Browser blocken. Die Voreinstellungen sind praxisgerecht, der Scanner durchsucht alle Dateien und Archive. Bei der Virensuche bot das Programm herausragende Leistungen bei bekannten Viren, fand aber nur 5 unserer 16 VBS-Testwürmer. Die Archivunterstützung deckt die gebräuchlichen Formate ab, ignoriert aber selbstentpackende Archive (etwa ZIP-SFX).

Der Virenwächter arbeitete zuverlässig und leistete sich im Test nur einen Aussetzer bei einer mit einem Bootvirus infizierte Diskette. Ansonsten brachten weder Archive noch infizierte Office-Dokumente den PC in Gefahr. Das Entfernen von Makroviren klappte gut, auch bei den eingebetteten Excel-Tabellen. Die harmlosen Makros blieben erhalten.

Die Online-Abwehr lässt kaum etwas zu wünschen übrig. Das Herunterladen von infizierten Dateien überwachte PC-Cillin sauber, die Mailüberwachung klappte exzellent. Während eines Downloads überprüfte der Wächter die Mails und meldete den Virenbefall. Merkwürdig das Verhalten bei einem gepackten Attachment: Obwohl anders eingestellt, ließ der Wächter die Mail nach einer Warnmeldung unverändert passieren.
Fazit: PC-Cillin hat das Zeug zum Spitzenprogramm, gerade für Anwender, die häufig online gehen. Die ansonsten herausragende Virensuchleistung trübte allerdings die Schwäche bei den VBS-Testwürmern. Bei der VB-Script-Heuristik gibt es für die Programmierer noch etwas zu tun.

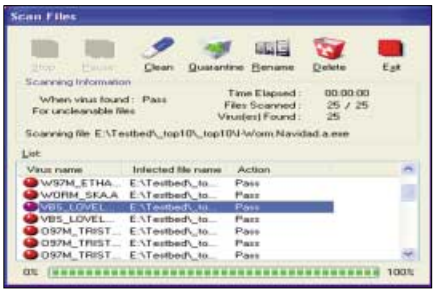
PC-Cillin 2002

Info: Trend Micro
www.trendmicro.de
Preis: ab 49 Euro

⊕ herausragender Virenwächter
⊖ Schwächen bei Scriptviren

Funktionen	●●●●○
Virenscanner	●●●●○
Viren entfernen	●●●●●
Archivbehandlung	●●●○○
Virenwächter	●●●●◐
Online-Abwehr	●●●●●
Bedienung	●●●●○
Gesamt:	●●●●○

Testurteil: Das Programm bot herausragende Suchleistungen bei bekannten Viren. Allerdings fand der Scanner lediglich 5 von 16 VBS-Testwürmern.



Gute Trefferquote: Bei der Erkennung der Topviren gab sich PC-Cillin 2002 keine Blöße

Sophos Anti-Virus 3.57

Funktionen: Das Programm ist ohne Schnörkel, bietet aber die wichtigsten Einstellungen. Standardmäßig werden Archive nicht durchsucht, die Auswahl der zu prüfenden Dateien erfolgt mit der Datei-Erweiterung. Jeden Monat erhält der registrierte Kunde eine neue Programm-CD, dazwischen gibt es teilweise mehrfach täglich Updates, die von Hand heruntergeladen und installiert werden müssen. Im Netzwerk gibt es einen automatischen Verteilungsmechanismus über ein zentrales Update-Verzeichnis. Die Archivunterstützung umfasst alle populären Dateitypen und auch selbstentpackende und verschachtelte Archive.

Der Virenscanner lieferte keine Spitzenergebnisse, zeigte sich aber solide. Einen Aussetzer leistete sich Sophos bei den Standardviren: Ausgerechnet VBS/Kournikova ging dem Scanner durch die Lappen. Ansonsten fehlten immer nur ein paar Viren. Bei den Trojanern wurden 56 von 64 Dateien erkannt.

Der Virenwächter Intercheck konnte in der Praxis nicht voll überzeugen. Das Kopieren im Explorer verhinderte der Wächter, nicht aber das Verschieben per Kontextmenü oder Drag & Drop. Dafür verhinderte der Wächter das Öffnen von infizierten Office-Dokumenten auch bei eingebetteten Objekten sicher. Die Online-Überwachung erlaubte die Übertragung und das Speichern infizierter Mail-Attachments. Das Entfernen von Makroviren beherrschte Sophos gut, harmlose Makros überlebten diese Aktion bei Excel und Word. Eingebettete Office-Objekte behandelte Sophos nur bei Excel und Word, in Powerpoint nicht.

Fazit: Sophos Anti-Virus ist ein solides Programm, das sich mit seiner Leistung im oberen Mittelfeld vor allem für Firmen empfiehlt. Der Virenwächter und damit auch die Online-Überwachung leisteten sich allerdings unentschuldbare Aussetzer. Das Online-Update verlangt zu viel Handarbeit.

Sophos Anti-Virus 3.57

Info: Sophos
www.sophos.de
Preis: 114,84 Euro (ab 5er-Lizenz)

⊕ **gute Online-Abwehr**
⊖ **nur für Firmenkunden geeignet**

Funktionen	●●○○○
Virenscanner	●●●●◐
Viren entfernen	●●●●◐
Archivbehandlung	●●●◐○
Virenwächter	●●●●◐
Online-Abwehr	●◐○○○
Bedienung	●●●○○
Gesamt:	●●●◐○

Testurteil: Der Virenscanner lieferte keine Topergebnisse, zeigt sich aber solide. Die Online-Überwachung war der schwächste Teil des Programms und führte zu einer erheblichen Abwertung.

Schlicht und effektiv: Die Bedienerführung von Sophos Anti-Virus ist leicht verständlich

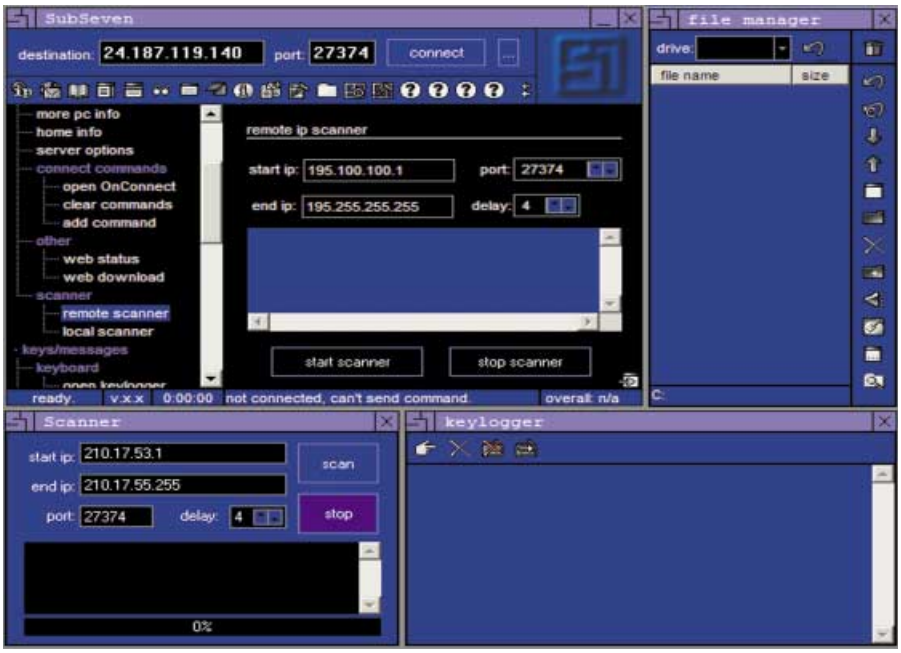
Abwehr-Tools gegen Trojanische Pferde

Trojaner ausgesperrt

Zu den gefährlichsten Schädlingen zählen Trojaner, die sich unbemerkt im System einnisten und Angreifern Tür und Tor öffnen. Dagegen helfen nur die richtigen Abwehr-Tools.

▸Immer dann, wenn Windows verdächtige oder abnormale Reaktionen zeigt, liegt der Verdacht nahe, dass ein Trojaner aktiv ist und ein Angreifer die Kontrolle über das Betriebssystem übernommen hat. Wird Windows etwa einfach heruntergefahren oder finden während einer Online-Sitzung unmotivierte Übertragungen statt, dann besteht der dringende Verdacht einer Infektion. Trojaner werden nämlich auch als eine Art Fernsteuerungs-Software bezeichnet, was ihre Arbeitsweise besser veranschaulicht. Mehr dazu lesen Sie ab ▷ Seite 76.

Experimentierfreudige Anwender, die viele Dateien unbekannter Herkunft laden, etwa Video- und MP3-Tools, sollten auf den Einsatz spezieller Anti-Trojaner-Programme nicht verzichten. Denn oft werden die Schädlinge geschickt und unbemerkt in populäre Dateien verpackt und werden bei der Installation der heruntergeladenen Dateien aktiv.



So arbeiten Hacker: Mit einem Trojaner-Client können Angreifer mühelos die Kontrolle über einen fremden PC übernehmen. Voraussetzung ist allerdings, dass dort ein Trojaner installiert ist und antwortet

Trojaner-Suche: Hier werden die Spezialisten fündig

In der Praxis müssen die Trojaner gestartet werden, damit die Gegenstelle mit ihnen Kontakt aufnehmen kann. Das kann entweder automatisch über Befehlszeilen in der WIN.INI oder SYSTEM.INI oder über folgende Schlüssel in der Windows-Registry initiiert werden:

- ▷„Hkey_Local_Machine\Software\Microsoft\Windows\CurrentVersion\Run“
- ▷„Hkey_Local_Machine\Software\Microsoft\Windows\CurrentVersion\RunOnce“
- ▷„Hkey_Local_Machine\Software\Microsoft\Windows\CurrentVersion\RunServices“
- ▷„Hkey_Local_Machine\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce“
- ▷„Hkey_Classes_Root\exefile\shell\open\command“

Erfahrene Anwender können hier theoretisch selbst nach verdächtigen Dateien suchen. Ein fälschlicherweise gelöschter Schlüssel kann jedoch dazu führen, dass Windows nicht mehr hochfährt.

Info: Anti-Trojaner

Im Prinzip sind Trojaner Schläfer, die sich monatelang ohne Aktivität im System einnisten und erst auf Zuruf aktiv werden. Bekommt ein Angreifer eine Antwort vom Trojaner, kann er die komplette Kontrolle über Ihr System übernehmen. Die speziellen Abwehr-Tools sind daher wichtiger denn je. Ab ▷ Seite 97 stellen wir Ihnen 9 Trojaner-Scanner vor.

Aktualität: Der Kampf wird oft in wenigen Stunden entschieden

Wie Virenscanner lassen sich auch Anti-Trojaner über das Internet auf den neuesten Stand bringen. Eine seit Wochen nicht mehr aktualisierte Datenbank kann gerade erst im Umlauf gebrachte Trojaner nicht erkennen und macht das Abwehrprogramm dadurch wirkungslos.

Zusammenspiel: Virenscanner, Firewall und Anti-Trojaner

Viele aktuelle Virenscanner beherrschen auch das Erkennen und Eliminieren von Trojanischen Pferden, zumal die Grenzen zwischen Virus und Trojaner immer mehr verwischen. Einen ausführlichen Test von 15 aktuellen Antiviren-Programmen finden Sie ab ▷ Seite 84.

Peter-Jürgen Rofer

TROJANER- UND PORTSCAN

Anti-Trojan 5.5

System: Windows 95/98/ME, NT 4, 2000 und XP
Sprache: Deutsch
Preis: 25 Euro
Quelle: **www.anti-trojan.net** (5,3 MB)

Scannen Sie Ihr System auf offene Ports, versteckte und aktive Trojaner, und behalten Sie die Windows-Registry und Autostart-Ordner im Blick.

▸Das deutschsprachige Programm Anti-Trojan 5 verwendet drei verschiedene Suchvarianten, um Trojaner zu erkennen. Der Portscan untersucht alle Rechner-Ports (Schnittstellen zum Internet) auf dem lokalen Rechner auf mögliche Angriffspunkte. Im Gegensatz zu einem Online-Check, wie ihn etwa Symantec anbietet, werden nicht nur die bekannten Trojaner-Ports, sondern auf Wunsch alle 65535 Ports gescannt. Das nimmt allerdings einige Minuten in Anspruch. Kommt eine Firewall zum Einsatz, bleiben die Port-Anfragen ohne Ergebnis – der PC ist sicher. Beim Registry-Scan wird das System einem Schnelltest unterzogen. Dabei wird die Windows-Registrierdatenbank untersucht und nach bekannten Speicherplätzen von Trojaner-Dateien auf der Festplatte Ausschau gehalten. Wird Anti-Trojan fündig, wird die Möglichkeit des Löschens angeboten. Das wichtigste und effektivste Suchverfahren ist der Disk-Scan. Bei dieser Option werden ganze Laufwerke oder auf Wunsch auch nur einzelne Verzeichnisse nach Trojanern abgesucht. Anti-Trojan erkennt aktuell mehr als 7500 Trojaner-Signaturen und kann optional auch gepackte Archive in den Formaten ACE, ARJ, CAB, LHA, LZH, RAR, ZIP und viele weitere mehr in die Prüfung einbeziehen. Das Online-Update hält das Programm immer auf dem neuesten Stand.

UNIVERSALLÖSUNG

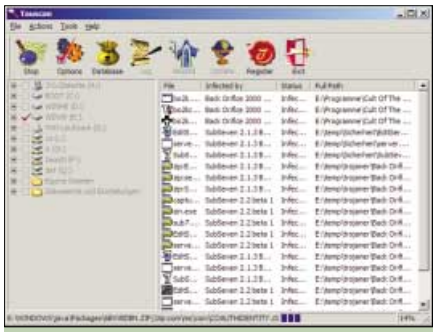
Ants 3.0

System: Windows 95/98/ME, NT 4, 2000 und XP
Sprache: Deutsch
Preis: kostenlos beziehungsweise ab 24,99 Euro
Quelle: **www.ants-online.de** (1,1 MB)

Das Tool findet bekannte Viren, Trojaner und Dialer, kann laufende Prozesse anzeigen, bietet eine Echtzeitüberprüfung und ein einzigartiges Selbstschutzsystem.

▸Hinter Ants verbirgt sich die Bezeichnung "A New Trojan Scanner", was Zweck und Einsatzgebiet besser veranschaulicht. Das Tool ist eines der Leistungsstärksten überhaupt und vereint Trojaner-, Viren- und Dialer-Erkennung (über 30.000 Varianten), Firewall, Sandbox und Echtzeitüberwachung für Systemveränderungen, wobei eine Heuristik sogar bisher unbekannte Schädlinge aufspüren kann. Ein umfangreiches Regelwerk kann Trojaner aufspüren, indem typische Aktivitäten erkannt werden. Der Autostart-Viewer listet alle Programme auf, die über die Windows-Registry oder über den Autostart-Ordner geladen werden. Außerdem zeigt Ants alle Verbindungen an, die zu Ihrem PC aufgebaut sind beziehungsweise die Ihr PC aufgebaut hat. So sehen Sie, welche Ports offen sind und Angreifern ein Angriffsziel bieten. Ein Highlight ist der Process Viewer, der alle aktuell laufenden Prozesse mit einer Vielzahl von Details auflistet. Von Ants sind zwei Versionen verfügbar: Die um einige Funktionen reduzierte Lite-Variante ist kostenlos und wird nur wöchentlich aktualisiert. Die ab 24,99 Euro teure Privat-Version bietet eine erweiterte Sandbox, Archivunterstützung sowie einen Selbstschutz und wird täglich auf den neuesten Stand gebracht. Mit dem Crypt-Modul lassen sich Dateien verschlüsseln und mit Wipe sicher löschen.

BEWÄHRTER SCANNER



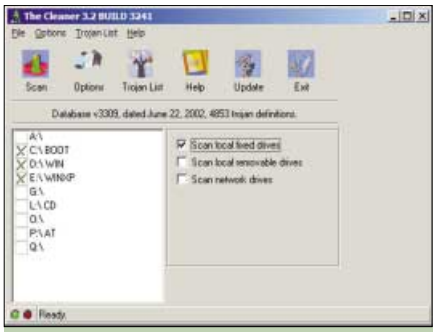
Tauscan 1.6

System: Windows 95/98/ME, NT 4, 2000 und XP
Sprache: Englisch
Preis: 29,95 Dollar
Quelle: **www.agnitum.com** (1,7 MB)

Seit Jahren eines der bekanntesten und besten Programme gegen Trojaner, schützt Sie Tauscan vor weit über 3000 Schädlingen und deren Ablegern.

▸Agnitum, der russische Hersteller von Tauscan, hat einen sehr guten Ruf und entwickelt auch die Firewall Outpost sowie das Port-Überwachungs-Tool Jammer. Der Trojaner-Scanner Tauscan kann den Arbeitsspeicher, Dateien und Archive untersuchen und stützt sich dabei auf eine Datenbank mit weit über 3000 bekannten Trojanischen Pferden. Tauscan beinhaltet eine Heuristik namens Advanced Trojan Analyser, die nach Trojaner-ähnlichem Code in Dateien sucht. Allerdings nimmt das Scannen wesentlich mehr Zeit in Anspruch, und mitunter werden auch harmlose Dateien als Schädling ausgemacht. Beim Löschen solcher Dateien sollten Sie besondere Vorsicht walten lassen. Das Programm kann so eingestellt werden, dass es nach jedem Start nach Updates sucht und diese gegebenenfalls ins System einspielt. Bei den Datei-Optionen lassen sich entweder alle Dateien, ausführbare Dateien, nur solche mit bestimmten Datei-Erweiterungen oder zuvor Gefilterte für das Scannen auswählen. Wird Tauscan dabei fündig, lassen sich die Dateien entweder automatisch oder nach Bestätigung durch den Anwender löschen. Interessant ist die von Virenscannern bekannte Quarantäne-Funktion, bei der infizierte Dateien in einen bestimmten Ordner verschoben werden. Die Reports können Sie im TXT- oder HTML-Format sichern. ▸

TROJANER-SPEZIALIST



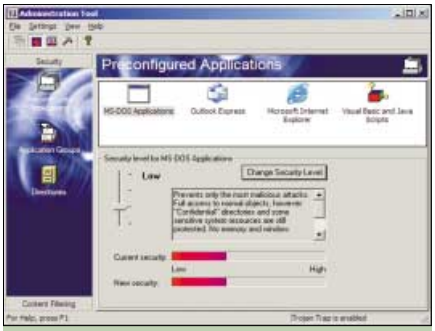
The Cleaner 3.5

System: Windows 95/98/ME, NT 4, 2000 und XP
Sprache: Englisch
Preis: 29,95 Euro
Quelle: **www.moosoft.com** (2,3 MB)

Gleich mit drei unabhängigen Programmen verspricht das Tool höchstmöglichen Schutz gegen Trojaner. Der Update-Intervall ist sehr kurz, die Erkennungsrate sehr gut.

▸Das englischsprachige Programm besteht aus drei eigenständigen Modulen: Der Scanner sucht, findet und eliminiert Trojaner. TC Active schlägt Alarm, sobald eine Trojaner-ähnliche Aktivität stattfindet. Soll beispielsweise ein neues Programm in die Windows-Registry oder den Autostart-Ordner hinzugefügt werden, erscheint eine Warnmeldung, die der Anwender bestätigen muss. TC Monitor überwacht im Hintergrund die aktuell laufenden Prozesse und zeigt diese in einer Übersicht an. Damit können Sie auf einen Blick alle Programme einsehen und Trojaner entlarven. Die beiden letztgenannten Module können übrigens dauerhaft bei jedem Windows-Start geladen werden. Dem Programm liegt eine umfangreiche Datenbank zu Grunde, die alle bekannten Trojaner mit ihren Angriffszielen und -methoden enthält. Per Online-Update bleibt The Cleaner immer auf dem neuesten Stand. Fast täglich steht eine aktualisierte Datenbank zum Download bereit. Da sich der Hersteller voll und ganz der Bekämpfung der Trojaner verschrieben hat, geht die Treffsicherheit beim Auffinden über die Quote der Virenscanner hinaus. Zu den Stärken des Programms zählt das sichere Erkennen der gefährlichsten Trojaner Back Orifice, Sub Seven, Net Bus und vieler anderer. Insgesamt kennt The Cleaner weit über 4800 Trojaner.

BESONDERE TECHNIK



Tiny Trojan Trap 3.0

System: Windows 95/98/ME, NT 4, 2000 und XP
Sprache: Englisch
Preis: 29,95 Dollar
Quelle: **www.tinysoftware.com** (6,6 MB)

Nicht als reiner Trojaner-Scanner, sondern als spezielle Sicherheitsumgebung verhindert Trojan Trap Systemveränderungen und das unbemerkte Ausführen von Programmen.

▸Das englischsprachige Programm schützt mit einer besonderen Technik vor Trojanischen Pferden. So werden jedem Programm, das der Anwender startet, bestimmte Rechte zugeordnet, die seine Aktivitäten einschränken. So lässt sich genau festlegen, ob die Anwendung in einer geschützten Umgebung (Sandbox) laufen soll oder ob sie freien Zugriff auf das System und das Internet erhält. Das gilt übrigens für jede Art von ausführbarem Code, also auch für Active-X-Controls, Java- und VB-Scripts sowie Java-Applets von Websites. Unbekannte Programme können zunächst in einer vom übrigen Rechner abgekapselten Sandbox gestartet und getestet werden. Die Windows-Registry und das Dateisystem sind dabei abgeschirmt und werden permanent auf Änderungen überwacht, so dass eine böswillige Veränderung durch Trojaner abgeblockt wird. Schon bei der Installation indiziert Trojan Trap alle gefundenen Programme und ordnet sie in bestimmte vorkonfigurierte Bereiche ein. Der Sicherheitsmechanismus von Trojan Trap schützt somit nicht nur vor feindlichen Attacken, sondern auch vor Software-Fehlern, die das System modifizieren. Soll beispielsweise eine Systemdatei bei der Installation einer neuen Anwendung ohne Rückfrage überschrieben werden, schlägt Trojan Trap Alarm und warnt vor den Veränderungen.

HOHE TREFFERQUOTE

Trojan Check 5

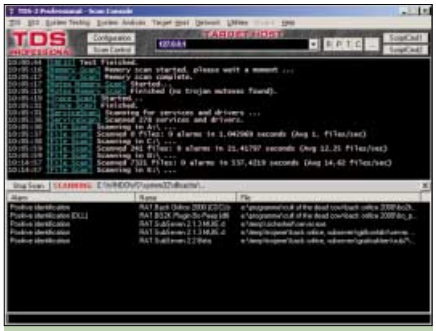
System: Windows 95/98/ME, NT 4, 2000 und XP
Sprache: Deutsch
Preis: kostenlos für privaten Gebrauch
Quelle: **www.trojancheck.de** (1,7 MB)

In diesem Tool arbeitet die gleiche Trojaner-Erkennung wie in Ants, allerdings sind einige erweiterte Funktionen dabei, die Angreifer auf verschiedene Arten aufspüren.

▸Trojan Check bietet verschiedene Ansätze, um Trojaner zu erkennen, wobei der Schwerpunkt im Überwachen der Angriffsziele des lokalen Systems liegt. Dazu überwacht das Programm alle Ports, die Windows-Registry sowie den Windows-Autostart-Ordner, zeigt Veränderungen unverzüglich an und kann sie auf Wunsch auch wieder zurücknehmen. Mit Hilfe des Prozess-Viewers erhalten Sie zahlreiche Informationen zu den laufenden Prozessen und können eine erweiterte Analyse der geladenen Module durchführen. Der integrierte Trojaner-Scanner findet Schädlinge, die auf der Festplatte gespeichert, aber noch nicht aktiviert wurden. In die Erkennung können auch so genannte Spionage-Tools einbezogen werden, die zur Überwachung von PCs verwendet werden und in ihrem Verhalten Trojanern sehr ähnlich sind. Da Hacker immer raffinierter vorgehen, wurde Trojan Check dahingehend erweitert, dass mit mehreren Datei-Endungen getarnte Dateien (etwa NAME.JPG.VBS) erkannt werden. Offene Verbindungen stellt das Tool mit dem Windows-eigenen Befehl „Netstat“ in einer eigenen Anzeige dar. Damit können Sie alle aktiven Internet-Verbindungen einsehen und verdächtige Aktionen eines Trojaners aufspüren. Über das Online-Update halten Sie Trojan Check stets auf dem aktuellen Stand.

Auf Heft-CD

PROFI-WERKZEUG



Trojan Defense Suite (TDS) 3.2.1

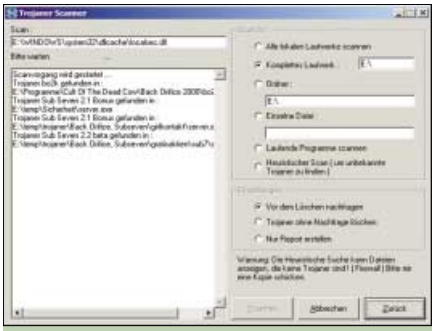
System: Windows 95/98/ME, NT 4, 2000 und XP
Sprache: Englisch
Preis: 49,95 Dollar
Quelle: www.diamondcs.com.au (7,1 MB)

Das sehr professionelle Programm arbeitet äußerst gewissenhaft und setzt in Bezug auf Funktionsumfang und Erkennungsquote Maßstäbe bei den Anti-Trojanern.

▸Das Programm besitzt einen weit größeren Funktionsumfang als alle anderen Anti-Trojaner und richtet sich auch aufgrund des hohen Preises an System- und Netzwerk-Administratoren. So stehen unter anderem ein leistungsstarkes Erkennungssystem für Trojaner, Prozess- und Speicher-Viewer, Portscanner sowie Whois- und Traceroute-Abfragen zur Verfügung. Täglich werden Updates zum Download angeboten, die automatisch geladen und eingespielt werden können. Der Prozess-Viewer ragt aus allen anderen Modulen heraus und kann neben Windows-Tasks auch 16-Bit-DOS-Anwendungen samt aller Programmbibliotheken und Laufzeitmodule überwachen. Zudem erkennt TDS Dienste und Treiber, die Windows über die Registry-Dateien lädt. Über den Autostart-Explorer lassen sich alle Anwendungen auflisten, die beim Windows-Start geladen werden. Auf Windows-NT4/2000/XP-Systemen mit NTFS-Dateisystemen entdeckt TDS sogar versteckte NTFS-Data-Streams, über die Angreifer Scripts ausführen können. Beim Scannen nach Trojanern erkennt das Programm nicht nur die Originaldateien, sondern auch modifizierte Varianten und Würmer. TDS lässt sich so einrichten, dass alle Anwendungen vor dem Starten einem ausführlichen Test unterzogen und erst danach zur Ausführung freigegeben werden.

Auf Heft-CD

KOSTENLOSE ALTERNATIVE



Trojan First Aid Kit 5.01

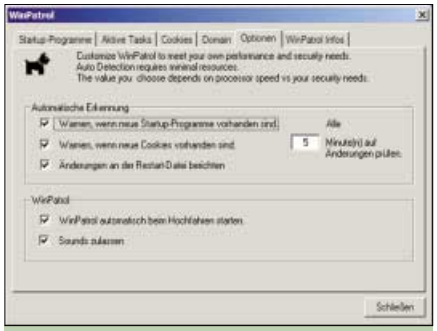
System: Windows 95/98/ME, NT 4, 2000 und XP
Sprache: Deutsch
Preis: kostenlos
Quelle: www.kryptocrew.de/snakebyte/tfak.html (200 KB)

Die Scanengine von Tfak ist nicht ganz aktuell, dafür ist ein Portscanner dabei, der gezielt entfernte Systeme auf das Vorhandensein von Trojanern untersucht.

▸Auch wenn Trojan First Aid Kit (Tfak) aus einer etwas suspekt anmutenden Quelle stammt, das kostenlose Tool dient tatsächlich der Trojaner-Abwehr. Zwar kennt Tfak mit 736 Schädlingen nicht so viele wie etwa The Cleaner oder Tauscan, aber immerhin sind die wichtigsten und am weitesten verbreiteten Varianten dabei. Zum besseren Vergleich muss aber erwähnt werden, dass Tfak nur die wirklichen Trojaner und nicht die Clienten identifiziert, wie es viele andere Programme machen. Interessant ist das Modul "Control Trojan", mit dem Sie entfernte Systeme übers Internet auf das Vorhandensein von aktiven Trojanern prüfen können. Dabei wird allerdings keine Verbindung hergestellt, die Zugriff auf den untersuchten PC erlaubt, sondern nur auf Antworten gewartet. Nach dem gleichen Schema arbeitet der Domainscanner, der komplette IP-Bereiche auf aktive Trojaner scannt. Mit Hilfe eines Heuristikverfahrens können sogar noch unbekannte oder modifizierte Trojaner aufgespürt werden – mit den von den anderen Tools bereits bekannten Problemen. Der Prozess-Viewer listet alle aktiven Programme und deren Bestandteile auf. Zudem zeigt Tfak alle Programme, die beim Windows-Start geladen werden. Der Portscanner scannt den PC nach offenen Schnittstellen ins Internet und kann so gefährliche Angriffspunkte aufzeigen.

Auf Heft-CD

ANDERER ANSATZ



Win Patrol 3.2

System: Windows 95/98/ME, NT 4, 2000 und XP
Sprache: Deutsch
Preis: kostenlos
Quelle: www.winpatrol.com (760 KB)

Im Prinzip ist Win Patrol kein Anti-Trojaner im herkömmlichen Sinn, aber trotz fehlenden Scanners gut geeignet, um Veränderungen am System festzustellen.

▸Das kostenlose Sicherheits-Utility listet alle laufenden Prozesse, Anwendungen und Cookies auf. Zu beachten ist, dass Win Patrol für Windows 98/ME entwickelt wurde und daher unter NT4-, 2000- und XP-Systemen nicht alle Funktionen bereitstehen. Für Windows 95 sind einige geringfügige Modifikationen notwendig, die auf der Website des Herstellers genauer beschrieben sind. Hinter der mitunter kindlich verspielten Bedienerführung verstecken sich einige nützliche Optionen. So werden beispielsweise alle bereits vorhandenen und neu hinzugekommenen Cookies und Programme erkannt und angezeigt. Sollen bestimmte Cookies generell gelöscht werden, muss unter „Nuts“ der Name oder eine Zeichenfolge des Cookies eingetragen werden. Bereits erhaltene Cookies löscht das Programm auch nachträglich. Unter der Registerkarte „Domain“ verbirgt sich eine Whois-Abfrage, mit der sich Inhaber einer Domain herausfinden lassen. Unerwünschte oder unbekannte Anwendungen, die beim Windows-Start automatisch geladen werden, identifiziert das Programm und kann sie dauerhaft aus der Autostart-Gruppe oder Windows-Registry löschen. Wird Win Patrol bei jedem Systemstart geladen, bleibt das Programm im Hintergrund aktiv. Win Patrol ist deutschsprachig, allerdings sind nicht alle Dialoge vollständig übersetzt. ■

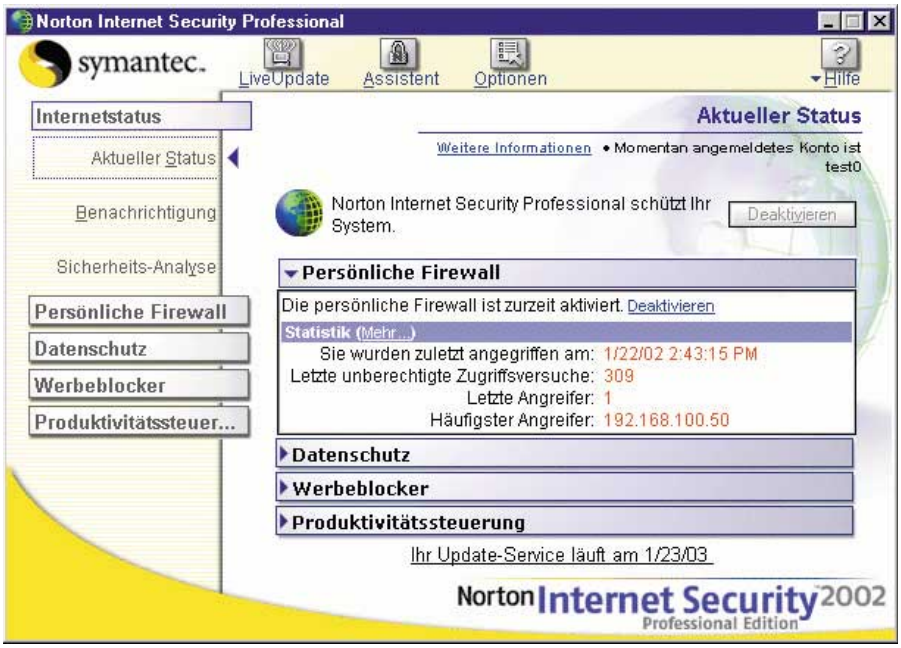
Sicherheitsgefahren bei Instant Messengern

Riskante Nachrichten

Kaum jemand weiß, dass Instant Messaging die gleichen Sicherheitsrisiken birgt wie das Versenden von Mails. Es gibt aber auch vergleichbare Schutzmechanismen.

Die Möglichkeiten der Kommunikation im Internet sind vielfältig. So hat sich in letzter Zeit eine Art Zwischenlösung aus Chat und Mail verstärkt etabliert: Instant Messaging (IM). Während der extrem schnelle Chat ein Simultangespräch, aber nur kurze Nachrichten ermöglicht, kann E-Mail recht lange Mitteilungen und sogar mehrere große Dateien enthalten. Dafür dauert die Übertragung schon mal einen Tag, wenn der Mailserver gerade mal wieder Probleme hat.

Instant Messaging ermöglicht einerseits ein beinahe simultanes Gespräch, da der Nutzer immer weiß, welcher seiner Partner online ist. Andererseits lassen sich damit gleichzeitig Dateien verschicken. Somit birgt der Dienst ähnliche Gefahren wie der Mail-Service.



Schutz durch Firewalls: Eine Desktop Firewall ist zwar kein Allheilmittel, doch kann sie die unbemerkte Kommunikation durch Instant Messenger überwachen und Attacken abblocken

Die Gefahr bilden die Datei-Anhänge

Wie bei den Mails ist auch beim Instant Messaging die Textnachricht selbst ungefährlich. Das Ascii-Format kann nämlich keine Viren oder gar Trojaner enthalten. Nur die formatierte HTML-Version bei Mails schleppt möglicherweise HTML-Viren mit, die jedoch in der Regel keine größeren Schäden anrichten. In beiden Diensten geht die große Gefahr von den Datei-Anhängen aus. Diese können – vom Absender beabsichtigt oder nicht – Viren und Trojaner enthalten oder sogar über maskierte Namensgebung reine Malware sein. Beim Instant Messaging kommen noch die Risiken durch unbewachte Eins-zu-Eins-Verbindungen zwischen den PCs beider Gesprächspartner hinzu. Über diesen Weg lassen sich sogar völlig unbemerkt Dateien auf den anderen PC übertragen. Diese direkten Verbindungen sollte man daher nur ausnahmsweise zulassen.

Stammt eine Nachricht, egal ob bei Mail oder Messaging, von einem unbekannten Absender, sollte man sie ungelesen sofort löschen. Allein das Öffnen des Datei-Anhangs kann nämlich ausreichen, damit sich das Programm auf die Festplatte speichert und dort Schaden anrichtet. Ein Herunterladen der Datei sollte erst gar nicht in Erwägung gezogen werden. Wer nun einwendet, es befinde sich ja ein Antiviren-Programm auf dem Rechner, wiegt sich in trügerischer Sicherheit. Denn schließlich kursieren immer wieder neuartige Viren oder Trojaner im Internet, für die es noch keine aktualisierten Antiviren-Updates gibt. Meist reagieren die Hersteller zwar sehr schnell und stellen binnen weniger Tage nach dem ersten Auftreten der neuen Malware eine aktualisierte Datei zur Verfügung, doch wie viele Anwender halten ihre Antiviren-Programme tatsächlich immer auf dem neuesten Stand?

Info: Viren für ICQ & Co.

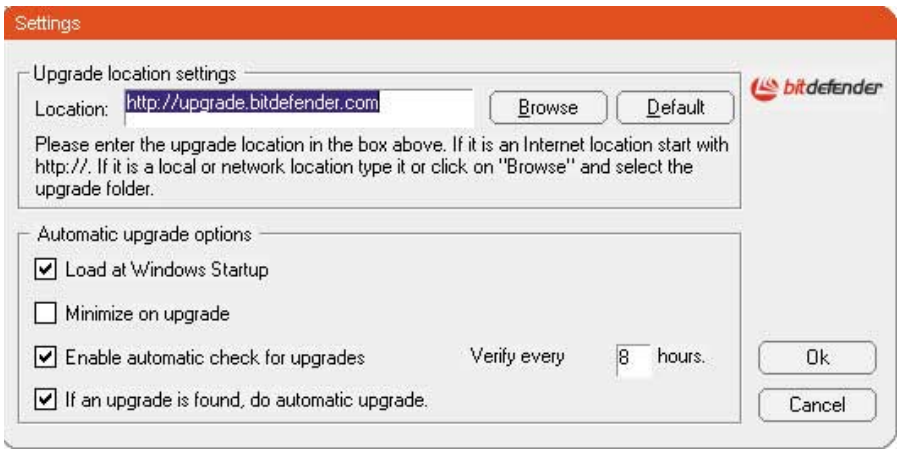
Die Programmierer von Viren, Trojanern und Script-Würmern haben es zunehmend auf Instant-Messaging-Programme abgesehen. Da bislang nur wenige Virenscanner Unterstützung für diese Tools bieten, muss der Anwender besondere Vorsicht walten lassen. Wir sagen Ihnen, welche Regeln zu beachten sind und wie Sie den Rechner mit einer Firewall zusätzlich gegen Angriffe absichern.

Messaging-Automatismen: Bedenkliche Einstellungen

Viele Instant Messenger ermöglichen außerdem Einstellungen, die das Risiko

stark erhöhen. So bieten einige den automatischen Datei-Empfang. Das heißt, jeder Datei-Anhang wird automatisch vom Rechner akzeptiert und auf die Festplatte übertragen. Selbst wenn die Datei nie per Hand geöffnet wird, kann sie dort in Ausnahmefällen Schaden anrichten. Denn Malware schreibt sich oft in die Registry-Dateien von Windows oder des Internet Explorers ein, so dass sie automatisch mit diesen geöffnet und aktiviert wird. Ein automatischer Datei-Empfang ist daher glatter Windows-Mord.

Ein weiteres Muss stellt die Kontrolle darüber dar, wer Sie auf die Kontaktliste setzen kann. Bei allen IM-Systemen muss nämlich jeder Nutzer erst den anderen Teilnehmer fragen, ob er ihn in seine Liste aufnehmen darf. Wenn Sie diese Anfragen automatisch vom Messenger akzeptieren lassen, wissen Sie natürlich nie, wer Ihnen in Zukunft auf die Nerven gehen oder Sie mit unerwünschten Dateien zuballern darf. Unaufgefordert erhaltene Spam-Mail ist schon schlimm genug, bei Messengern sollten Sie sich dadurch schützen, dass Sie die Anfragen zur Kontaktaufnahme einschalten und dann einzeln genehmigen – oder eben ablehnen.



Wenig zu tun: Die Konfiguration von Bit Defender beschränkt sich auf die Einstellungen zum automatischen Upgrade. Alle weiteren Optionen sind vorgegeben und lassen sich nicht ändern

Sind Sie trotzdem einmal auf die Liste eines Unbekannten gelangt, können sie ihn nachträglich zur „unerwünschten Person“ erklären. Dann wird die Kontaktaufnahme zwischen diesem Teilnehmer und Ihnen dauerhaft blockiert.

Außerdem können Sie bei den meisten Messengern auch einstellen, dass Sie nur Nachrichten von Personen erhalten, die in Ihrer Kontaktliste stehen. So vermeiden Sie „unverbindliche Anfragen“ von Unbekannten.

Unbedingt berücksichtigen: Tarnkappe und Passwort

Als zusätzlichen Schutz können Sie sich eine Tarnkappe überstülpen. Einige Messenger erlauben nämlich einen „Unsichtbarkeitsmodus“. Dann bleiben Sie in der Kontaktliste Ihrer Gesprächspartner immer im Offline-Status und gehen ungestört online. Der Nachrichtenempfang bleibt aber trotzdem möglich. Gute Freunde können Sie davon ausnehmen,

Mehr Sicherheit: Tipps für Ihren Instant Messenger

Mit ein paar einfachen Grundregeln schaffen Sie mehr Sicherheit für eine sorgenfreie Verwendung von Instant Messengern.

Registrierung

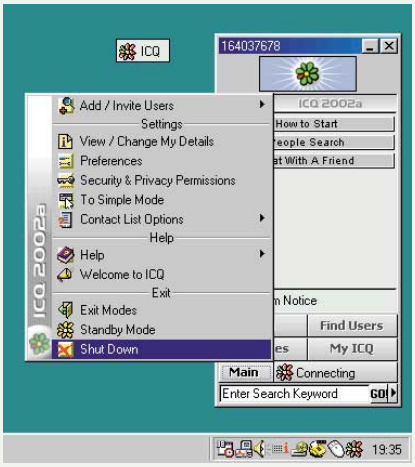
Falls möglich sollten Sie schon bei der Registrierung des Dienstes nicht alle Eingaben wahrheitsgemäß vornehmen. In der Regel überprüfen die Anbieter nur die Mailadresse. Ihr richtiger Name und Ihre Postadresse sollten niemanden etwas angehen. Nicht möglich ist dieser Trick allerdings bei Messengern, die mit anderen Diensten gekoppelt sind, zum Beispiel für AOL-Mitglieder beim AIM, bei der Passport-Anmeldung beim MSN Messenger oder beim T-Online-Messenger. In jedem Fall sollten Sie aber einen Fantasienamen für die Benutzung des Messengers angeben.

Passwort-Regeln

Verwenden Sie zur Sicherung Ihrer Messenger-Konfiguration wann immer möglich ein Passwort. Dafür gelten dann die ganz normalen Regeln: Geben Sie eine Kombination von Ziffern, Buchstaben und Symbolen ein, zum Beispiel „grUe79#d“, die mindestens acht Zeichen lang ist. Teilen Sie Ihr Kennwort niemandem mit. Reagieren Sie nie auf Anforderungen, Ihr Kennwort preiszugeben. Melden Sie sich mit diesem Passwort bei keinem anderen Dienst an. Und ändern Sie Ihr Passwort in regelmäßigen Abständen, etwa alle vier Wochen.

Programm schließen

Wann immer möglich sollten Sie den Instant-Messenger abschalten. Vor allem, wenn Sie längere Zeit nicht zu sprechen sind, also Pause machen, sich vom PC entfernen, sich intensiv mit einer bestimmten Arbeit beschäftigen oder nachts nicht mehr arbeiten, sollten Sie das Programm schließen. Verwenden Sie ICQ, dann beachten Sie dabei, dass ein einfacher Klick auf das Entfernen-Symbol in der rechten oberen Ecke nicht ausreicht. Als Zeichen, dass das Programm immer noch aktiv ist, bleiben dann noch ein Tooltip auf dem Bildschirm zu sehen sowie das ICQ-Symbol in der Statuszeile. Darauf klicken Sie mit der rechten Maustaste und dann mit der linken auf „Shut Down“. Sie können diesen Befehl auch über das „Main“-Menü erreichen. Nun ist das Programm endgültig geschlossen.



Aus die Maus: Endgültig schließen Sie ICQ über den Befehl „Shut Down“ im Main-Menü

indem Sie diese in die „Sichtbar-Liste“ eintragen. Dann erfahren sie trotz „Unsichtbarkeitsmodus“, wann Sie online sind. Umgekehrt können Sie auch bestimmte Personen in die „Unsichtbar-Liste“ aufnehmen. Sie bleiben dann zwar in deren Kontaktliste sichtbar, aber immer im Offline-Status. So erfahren diese Teilnehmer nicht, dass Sie gerade online sind.

Besonderes Augenmerk sollten Sie auf das Passwort richten, das Sie sich bei der Anmeldung zu einem Messaging-Dienst zulegen. Da dieses Passwort auf einem Server gespeichert ist, auf den unter Umständen ein Hacker zugreifen kann, sollten Sie es möglichst schnell ändern. Auch danach sollten Sie sich in regelmäßigen Abständen immer wieder ein neues Passwort aussuchen.

Einer für alle: Das durch Werbung finanzierte Programm V-Catch erkennt Viren aus Instant-Messaging-Nachrichten, Mails und Downloads – Warnung an Freunde inklusive

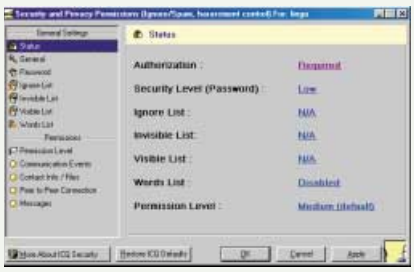
Schutz: Firewalls und Antiviren-Programme

Trotz aller Vorsichtsmaßnahmen können schädliche Programme Eingang in Ihren Rechner finden, zum Beispiel wenn ein bekannter Gesprächspartner unabsichtlich einen mit Viren oder Trojanern verseuchten Datei-Anhang schickt. Dann helfen nur Virenscanner oder Firewalls. Der Einsatz einer Firewall ist aber nicht unproblematisch: So erlaubt sie in der Regel nicht den Datei-Austausch und teilweise nicht einmal den Zugriff auf die für das Instant Messaging nötigen Ports. Die meisten Messaging-Programme streiken erst einmal komplett, wenn eine Firewall eingesetzt wird. ICQ lässt sich zwar mit einer Firewall betreiben, doch sind die dafür nötigen Einstellungen oft sehr kompliziert einzurichten.

Geschützt kommunizieren: Workshop Sicherheit in ICQ (I)

Bei der Registrierung für den ICQ-Dienst sollten Sie angeben, dass Ihre Autorisierung nötig ist, damit Nutzer Sie in ihre Kontaktliste eintragen können. Den Status sehen Sie im ICQ-Fenster unter „Main, Security & Privacy Permissions“ ein.

Der Punkt „General“ enthält unter „Contact List Authorization“ die Möglichkeit, die Autorisierungspolitik zu ändern. Allerdings sollten Sie, wie bereits erwähnt, immer eine persönliche Autorisierung wählen, also den zweiten Punkt. Sonst öffnen Sie jedermann Tür und Tor.



Kontrolle ist besser: In den Sicherheitseinstellungen können Sie den aktuellen Stand einsehen

Im Bereich „Security Level“ können Sie eine Passwort-Eingabe vor die Änderung Ihrer Angaben setzen. Sie sollten hier die mittlere Stufe anklicken, da sonst jedermann Zugriff auf Ihr ICQ erhält. Falls auch andere Personen Zugang zu Ihrem PC haben, sollten Sie die höchste Stufe einstellen. Unter „WebAware“ erlauben Sie, dass jeder Gesprächspartner Ihren Online-Status auf Ihrer Homepage sieht.

Passwort ändern

Im Sicherheits-Bereich können Sie unter „Password“ Ihr Passwort jederzeit ändern. Dazu müssen Sie nur zweimal ein neues Passwort und anschließend zur Sicherheit Ihr altes eingeben. Sie sollten das Passwort in regelmäßigen Abständen ändern, etwa alle vier Wochen, damit die Zugangsmöglichkeit anderer Personen auf Ihren Account eingeschränkt wird. Dabei sollten Sie das Häkchen vor „Save Password“ entfernen, da sonst das Passwort auf der Festplatte Ihres PCs gespeichert wird.

Gesprächspartner abblocken

Partner, die Sie in die „Ignore List“ aufnehmen, können nicht mit Ihnen in Kontakt treten. Vor allem, wenn Sie bereits schlechte Erfahrungen mit bestimmten Gesprächspartnern gemacht haben oder diese Ihnen unaufgefordert Dateien zugeschickt haben, sollten Sie diese in diese Liste aufnehmen. Ziehen Sie dazu den unerwünschten Gesprächspartner von der „Contact List“ mit der Maus in die „Ignore List“.

Sichtbar/unsichtbar

In die „Invisible List“ sollten Sie alle Teilnehmer setzen, die nicht wissen sollen, wann Sie online sind. Für diese befinden Sie sich dann immer im Offline-Status. Für alle anderen Teilnehmer ist es ganz normal in ICQ ersichtlich, wann Sie online sind. Die Personen aus der „Invisible List“ können Ihnen aber trotzdem Nachrichten schicken, die Sie auch empfangen. Wenn Sie wollen, dass Sie keine Messages mehr von einer solchen Person bekommen, verschieben

Antiviren-Programme harmonieren dagegen mit Instant Messengern meist recht gut. Das heißt aber nur, dass sie die Funktionsfähigkeit des Messengers nicht stören und ausschließlich die heruntergeladenen Dateien auf der Platte überprüfen. Damit nutzen sie ähnliche Funktionen wie bei der Kontrolle von Mailanhängen. Eigenständige Funktionen für Messenger besitzen nur wenige Programme, so etwa V-Catch. Sogar speziell für Messenger programmiert wurde Bit Defender der Firma Softwin. Diese Software überprüft die übertragenen Dateien auch bei direktem Kontakt sofort und nicht erst nach dem Download.

Bit Defender Instant Messenger 2.3

Das kostenlose englischsprachige Antiviren-Programm für Messenger, Bit Defender für Windows 95/98/ME, NT 4, 2000 und XP (**www.bitdefender.com**, auf Heft-CD), steht in fünf Varianten zur Verfügung: für ICQ (2,66 MB), Mirc (2,53 MB), MSN Messenger (2,65 MB), Yahoo Messenger (2,70 MB) und Netmeeting (2,77 MB). Die Software hält sich weitgehend im Hintergrund, so dass Sie nicht kontrollieren können, was sie so alles tut. Auch eine Protokollfunktion fehlt. Bit Defender zeigt nur an, welchen Virus es gefunden hat.

Nach der Installation empfiehlt sich ein sofortiges Upgrade. Unter „Settings“ können Sie dann die automatischen Update-Funktionen einstellen. Sie sollten hier die Voreinstellungen beibehalten, also die Überprüfung auf neue Updates alle acht Stunden bei sofortiger Aktualisierung. Da diese Software speziell für Messenger entwickelt wurde, empfiehlt sich ihr Einsatz trotz der geringen Einfluss- und Kontrollmöglichkeiten. Schließlich überprüft sie die Dateien sofort und nicht erst nach dem Herunterladen auf die Festplatte.

V-Catch 5.0

Das kostenlose, englischsprachige V-Catch für Windows 95/98/ME, NT 4, 2000 und XP (1,10 MB, **www.vcatch.com**) löst schnell Virenprobleme in Mails, Instant-Messaging-Nachrichten oder Download-Dateien. Dabei bevorzugt dieses Programm das sofortige Löschen der Malware. Es arbeitet problemlos mit bekannten Antiviren-Programmen, ICQ, Mailprogrammen, Download-Managern sowie Napster und Gnutella zusammen. Dafür müssen Sie sich jedoch bei V-Catch anmelden und einige Informationen über sich preisgeben. Da dieses Programm Adware ist, folgen entsprechende Werbemails.

V-Catch ist sehr bedienerfreundlich, die Konfiguration beschränkt sich auf die Angabe der Mailadresse oder der verwendeten Mail- und Messaging-Software. Die vorhandenen Messaging-Programme findet V-Catch anschließend weitgehend automatisch. Bei entsprechender Einstellung lädt sich das Programm die neuesten Virendefinitionen bei jeder neuen Online-Verbindung vom Server.

Sie wählen aus, ob befallene Messenger-Nachrichten, Mails oder Downloads sofort gelöscht oder im Papierkorb abgelegt werden sollen. Bei wichtigen Dateien bleibt Ihnen dann die Möglichkeit, mit Hilfe eines Virenscanners Rettungsmaßnahmen einzuleiten. Außerdem können Sie V-Catch so einstellen, dass es automatisch Ihre Bekannten per Mail über neu gefundene Viren informiert.

Günther Unterholzner

Geschützt kommunizieren: Workshop Sicherheit in ICQ (II)

Sie sie in die „Ignore List“. Die „Visible List“ ist das Pendant zur „Invisible List“. Wenn Sie für alle Welt unsichtbar surfen, sehen die Personen in dieser Liste trotzdem, ob Sie gerade online oder offline sind.

Nachrichtenempfang regulieren

Unter „Communication Events“ können Sie einstellen, welche Art von Nachrichten Sie von welcher Gruppe empfangen wollen. Dazu zählen Benachrichtigungen, Telefonanrufe, Grußkarten, ICQ-Mail, E-Mail und SMS. Aus Sicherheitsgründen empfiehlt es sich in allen Fällen, nur Personen Ihrer Kontaktliste auszuwählen. Die Auswahl „No one“ (Von keinem) kommt aber zum Beispiel für den Empfang von Telefonanrufen in Frage, wenn Sie dafür nicht ausgerüstet sind. Wenn Sie alles („Everyone“) akzeptieren, sind Sie nicht vor Belästigungen sicher. Besonders gefährlich ist überdies die Auswahl von „Auto Accept“. Dann akzeptiert der Rechner alle Nachrichten und lädt auch Datei-Anhänge ungefragt. Da diese Anhänge Viren und Trojaner enthalten können, sollten Sie in dieser Spalte keinen Punkt ankreuzen.

Kontakt-Info

Im Punkt „Contact Info“ entscheiden Sie, welche Personen auf von Ihnen zur Verfügung gestellte Informationen zugreifen können. Dazu zählen Ihre Telefonnummern, Ihr Bild und für das ICQ-Dateitauschsystem zur Verfügung gestellte Dateien. Auch hier sollten Sie höchstens den Personen in Ihrer Kontaktliste Zugriff gestatten. Vor allem bei den „Shared Files“ erhält der Partner Zugriff auf die Festplatte Ihres Rechners und kann eventuell Trojaner übertragen. Hier herrschen dann die gleichen Risiken wie in den Dateitauschsystemen Gnutella, Napster und Kazaa.

Direkte Verbindung

Die „Direct Connection“ bezeichnet die neue Version 2002 als „Peer to Peer Connection“. Der ICQ-Client stellt für einige Funktionen wie Datei-Übertragung oder Chat eine direkte Verbindung zwischen beiden Teilnehmern ohne das ICQ-Netzwerk her. Solche Verbindungen bergen große Sicherheitsrisiken, da Viren oder Spionage-Programme übertragen werden können. Daher lässt sich hier festlegen, mit wem Sie solche Verbindungen eingehen möchten: mit allen Usern („any user“), nur mit Teilnehmern, die in Ihrer Kontaktliste sind, oder nachdem Sie explizit eine solche Verbindung autorisiert haben. Empfehlenswert ist hier die letzte Einstellung.

Nachrichtenempfang: Sie entscheiden, von wem Sie welche Art von Nachrichten akzeptieren

So schützen Sie sich vor Spyware und Adware

Gegen Spionage

Inzwischen gibt es einige Tausend Programme kostenlos im Internet. Doch viele davon enthalten verdeckte Spionage-Funktionen. Wir zeigen, wie Sie Ihre persönlichen Daten schützen.

Paradiesisch: Viele Internet-Seiten quellen geradezu vor Gratis-Programmen über. Es genügen wenige Mausklicks, und schon befindet sich die gewünschte Freeware funktionsfähig auf der Festplatte. Doch Vorsicht: Viele dieser Programme enthalten versteckte Spionage-Funktionen. Sie ermitteln heimlich Informationen für die Auswahl der eingeblendeten Werbebanner. Diese zumeist von externen Herstellern programmierten Bestandteile werden je nach Sichtweise Spyware (Spionage-Software) oder Adware (Werbe-Software) genannt. Datenschützer bevorzugen den ersten Begriff, während die Software-Vertreiber das harmloser klingende Wort verwenden.

Wortstreit: Es geht um mehr als nur Buchstaben

Hinter dem Namensstreit steckt aber mehr als nur eine akademische Diskussion. Denn Adware besitzt sehr ähnliche Funktionen wie gefährliche Trojaner. Beide landen meist heimlich versteckt in Gratisprogrammen auf dem PC, speichern sich unbemerkt auf der Festplatte ab und ermitteln verborgen Informationen vom Rechner. Während Trojaner jedoch nach persönlichen Daten fahnden, sucht Adware nur nach statistisch auswertbaren Angaben wie Browser-Version oder installierte Plug-ins. Doch auch Alter, Geschlecht, Postleitzahl und Land gehören durchaus dazu.

Gerade an diesem Unterschied zwischen persönlichen und statistischen Daten erhitzen sich die Gemüter. Denn bislang verweigern die Vertreiber von Programmen mit integrierter Adware jede Kontrollmöglichkeit, welche Daten tatsächlich übertragen werden.

Das heißt, dass zur Zeit niemand weiß, welche Daten der Hersteller der so finanzierten Freeware oder Adware erhält. Und so lange nicht erwiesen ist, dass keine persönlichen Angaben wie Name, Adresse, Geburtsdatum oder Arbeitgeber herausgefiltert werden, könnte die Adware genauso wie Trojaner als Spionage-Software, Spyware, genutzt werden.

Allgemein gehalten: Die Microsoft-Website enthält nur recht unspezifische Angaben über den Datenschutz und den Umgang mit persönlichen Anwenderdaten unter Windows XP

So geht's: Arbeitsweise und Zweck von Adware

Adware landet in der Regel mit heruntergeladener Freeware auf dem Rechner und wird mit dem Programm installiert. Dabei schreibt sich die Adware unter anderem in die Registry, um automatisch bei jedem Start geöffnet zu werden. Anschließend durchsucht sie die Festplatte nach Infos. Dabei stehen die Browser-Angaben im Mittelpunkt. Die gängigen Browser stellen bereits freiwillig viele interessante Informationen zur Verfügung. Der Browser von Netscape und Microsofts Internet Explorer enthalten Angaben zum verwendeten Betriebssystem, zur Browser-Version, zu der verwendeten Bildschirmauflösung, der Spra-

Info: Spione enttarnen

Immer mehr Programme stehen im Verdacht, ahnungslose Anwender auszuspionieren und Infos über installierte Hard- und Software via Internet zu versenden. Mit den passenden Tools kommen Sie den Spionen auf die Schliche und entfernen diese vom System.

che, zu systemspezifischen Inhalten und beim Internet-Surfen auch zur IP-Adresse. Diese Daten werden anschließend bei jeder Verbindung mit dem Internet an den Server des Programmherstellers im Hintergrund übertragen.

Spyware kann durch Berücksichtigung von Cache, History und Cookies auch das Surfverhalten und über die Registrierungsangaben von Betriebssystem oder Programmen auch den Namen des Besitzers, Geburtsdatum, Adresse sowie seinen Arbeitgeber herausfinden.

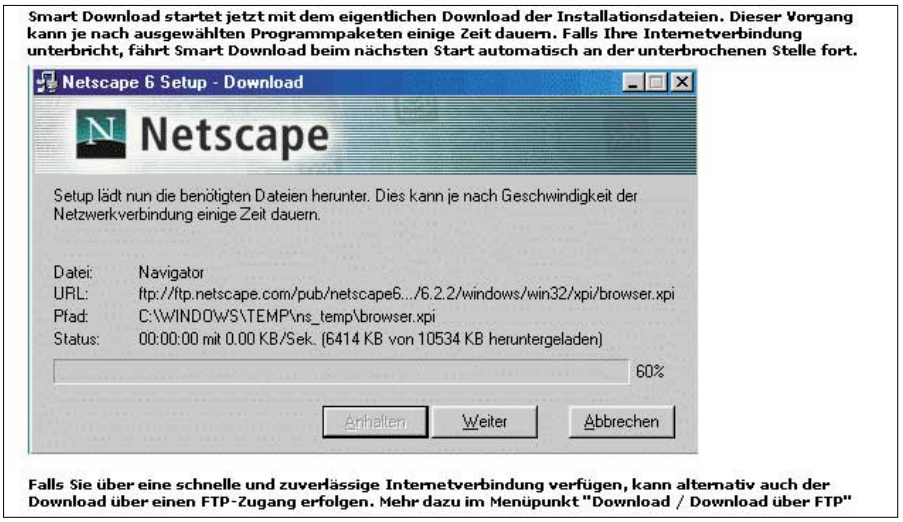
Die von Adware gesammelten statistischen Informationen werden zu verschiedenen Zwecken verwendet. So nutzen viele Anbieter von Freeware-Programmen die Angaben, um speziell auf den Anwender zugeschnittene Werbebanner in die Software einzublenden. Auch Mails, die persönliche Interessen berücksichtigen, lassen sich so verschicken. Außerdem können Programme, die auf Web-Seiten zugreifen, Musik oder Filme abspielen, automatisch die Version aufrufen, die für das verwendete Betriebssystem oder das Programm geeignet ist. Nicht zuletzt lassen sich auch personalisierte Channels einblenden oder automatisch Hinweise auf Updates des Programms setzen.

Weg mit Adware: Suche und Entfernen ist oft nicht einfach

Solange sich nicht nachprüfen lässt, welche Angaben transferiert werden, hilft Ihnen nur Vertrauen in die Hersteller. Dieses können Sie haben, müssen Sie aber nicht. Bislang wurde zwar kein Verstoß gegen Datenschutzrichtlinien oder die Übertragung persönlicher Angaben nachgewiesen, doch dieser Beweis ist aufgrund der fehlenden Kontrollmöglichkeiten auch recht schwierig.

Aber nicht nur die Unsicherheit, welche Daten übertragen werden, weckt in vielen Nutzern den Wunsch, die Adware wieder zu entfernen. Ärgerlich ist nämlich auch, dass manche Antiviren-Programme wie Antivir Personal Edition (deutschsprachiges Gratisprogramm für Windows 95/98/ME, NT 4, 2000 und XP, 3,3 MB, **www.free-av.de** und ◉ auf Heft-CD) auf diese Adware mit falschen Virenmeldungen reagieren und Anwender so verunsichern. Extern mit einem Programm gelieferte Adware lässt sich meist relativ einfach entfernen, da es sich hier um eigenständige Programme oder Plug-ins handelt. In diesen Fällen hilft meist ein Blick in den Windows Explorer und das Entfernen der Datei über das Kontextmenü. Teilweise besitzen sogar die Programme selbst eine Option, die Adware wieder zu löschen.

Falls das Programm aber die Adware-Funktionen integriert hat, gibt es kaum eine Chance. Dann lässt sich die Adware zumeist nur mit dem gesamten Programm löschen. Einige Hersteller bieten eine Adware-freie Version des Programms an – dann jedoch gegen Gebühr.



Verschwiegen: Beim Download des Netscape-Browsers wird zwar die Prozedur erklärt, aber nicht darüber informiert, dass der Smart Download Daten über den Anwender sammelt und an Netscape sendet

Berühmte Spione: Microsoft, Netscape, Real

Wer denkt, dass nur exotische Programme halbseidener Hersteller Werbe-Spione enthalten, liegt falsch. Selbst das berühmteste aller Programme besitzt Adware: Windows. So enthält der im Betriebssystem verankerte Browser Internet Explorer ab der Version 5.5 die Adware von Alexa (**www.alexa.com**). Zudem ist der Browser auch bekannt dafür, dass er immer wieder die angegebene Startseite ignoriert, um auf die MSN-Start- oder eine Update-Seite bei Microsoft zu gehen. Zu den übertragungsfreudigen Komponenten von Windows gehört beispielsweise auch der Media Player. Auch der Real Player (Version 8 Basic, deutschsprachig, für Win 95/98/ME, NT 4, 2000 und XP, 5,15 MB, **http://germany.real.com**, kostenlos) versucht ständig, Kontakt mit dem heimatlichen Server aufzunehmen. Neue Programm-Updates und personifizierte Channels werden automatisch geladen.

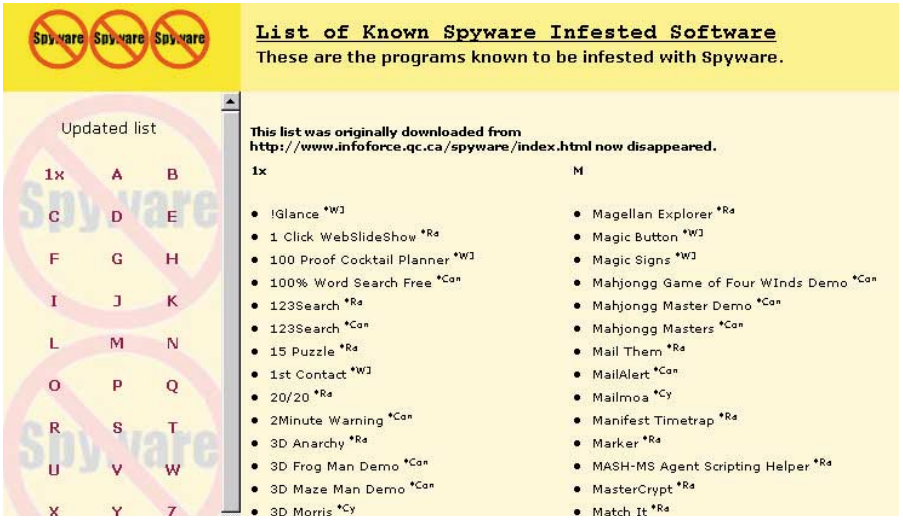
Über eine solche Phone-Home-Funktion (Phone-Home, auf Deutsch: Nach Hause telefonieren) verfügt auch der deutschsprachige Netscape-Browser 6.23 (für Windows 95/98/ME, NT 4, 2000 und XP, 10,5 MB, **www.netscape.de** oder ◉ auf Heft-CD, kostenlos) in seinem Zusatzprogramm „Smart Download“. Dieses muss vor dem eigentlichen Browser-Download heruntergeladen werden. Es überträgt aber ganz nebenbei Kundennummer, Namen und Mailadresse an Netscape sowie die Namen und URLs der damit heruntergeladenen Dateien. Sie vermeiden den Einsatz des Hilfsprogramms, indem Sie eine Vollversion des Netscape-Browsers von unserer Heft-CD installieren. Der Netscape-Browser funktioniert auch ohne Smart Download, wenn auch ohne die entsprechenden Zusatzfunktionen.

Dies alles wäre halb so wild, wenn die Hersteller auf ihre Websites deutliche Hinweise auf die Adware stellen würden. Doch nur Microsoft bietet entsprechende Erklärungen in deutscher Sprache an – und die gut versteckt. Netscape und Real

Offenherzig: Registrierungsangaben von Programmen wie Word lassen sich von Adware auslesen

verweisen sogar nur auf die englischsprachigen Seiten. In allen Fällen bleiben die Aussagen sehr allgemein.

Neben Browsern, Betriebssystemen und Playern enthalten auch die meisten Download-Manager Adware. So hat Gozilla 4.11 Free (englischsprachig, deutschsprachige Benutzerführung von Lingoware, **www.lingoware.com**, für Windows 95/98/ME, NT 4, 2000 und XP, 2,8 MB, auf Heft-CD und unter **www.gozilla.com**, kostenlos) Berühmtheit erlangt, weil er von einem der Adware-Hersteller angeboten wird: Radiate. Zumindest weisen neuere Versionen des Tools auf die enthaltene Adware hin. Als Alternative wird die werbefreie, kostenpflichtige Version erwähnt.



Überraschung: Die „List of known Spyware Infected Software“ enthält einige interessante Details, zum Beispiel, dass zahlreiche Versionen des beliebten Spiels Mah-Jongg Adware enthalten

Gegenspieler: Adware und Anti-Adware

Neben Radiate (ehemals Aureate) gibt es weitere Hersteller von Adware-Modulen. Die bekanntesten stammen von Webhancer (**www.webhancer.com**), Netsonic (Web 3000, **www.netsonic.com**), Comet Cursor (**www.cometcursor.com**), Gator (**www.gator.com**), Double Click (**www.doubleclick.com**), Conducent (Timesink, **www.safersite.com**), Cydoor (**www.cydoor.com**), Broderbund (DSS-Agent, **www.broderbund.com**) und Gratisware (**www.gratisware.com**). Eine Liste mit Spyware-Programmen bieten Safersite (**www.safersite.com/PestInfo/category_index.asp#spyware**) und Cexx.org (**www.cexx.org/adware.htm**).

Zur Entfernung von Adware gibt es Programme wie Ad-Aware 5.83 für Windows 98/ME, NT 4, 2000 und XP (871 KB, kostenlos, Download unter **www.lavasoftusa.com** oder auf Heft-CD) oder Spyblocker 5.3 (für Windows 95/98/ME, NT 4, 2000 und XP, 2,10 MB, Download unter **www.spyblocker-software.com/spyblocker**, Registriergebühr: 20 US-Dollar). Deren Nutzung führt natürlich dazu, dass die Adware-Funktionen wie die Ermittlung der Browser-Version nicht mehr funktionieren. Dann werden die entsprechenden Internet-Sei-

Endlich werbefrei: So beseitigen Sie Spyware mit Ad-Aware 5.83 (I)

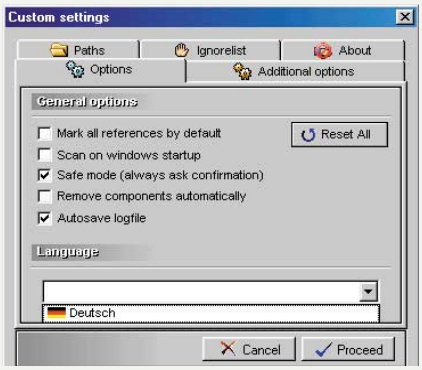
Nach dem Herunterladen der Setup-Datei von Ad-Aware (auch auf Heft-CD enthalten) und deren Installation durch Doppelklick auf AAW.EXE sowie mehrmaligem Bestätigen über „Next“ und „Finish“ befindet sich die englischsprachige Datei auf dem Desktop. Anschließend extrahieren Sie die Dateien aus dem Archiv Awadeutsch.EXE. Kopieren Sie die entpackten Dateien in den Unterordner „Lang“ des Ordners „Lavasoft Ad-Aware“. Dieser befindet sich in der Grundeinstellung unterhalb des Ordners „Programme“ auf der Festplatte C:.

Starten Sie nun das Programm Ad-Aware per Doppelklick auf das entsprechende Icon auf Ihrem Desktop. Klicken Sie auf den Button „Configuration“. Im nun erscheinenden Dialog „Custom settings“ klicken Sie auf das Textfeld unter „Language“. Wählen Sie die nun erscheinende Auswahl „Deutsch“, und klicken Sie auf „Proceed“. Eine deutschsprachige Hilfedatei steht übrigens nur für Version 4.x auf der Download-Website zur Verfügung.

Spyware suchen

Wenn Sie das Programm das erste Mal starten, sind bei den Laufwerken und Sektionen, die Ad-Aware durchsuchen soll, nur der Arbeitsspeicher und die Registry angegeben. Sie sollten daher weitere gewünschte Laufwerke im linken Fenster auswählen. Nach einem Klick auf „Start“ beginnt Ad-Aware mit der Suche nach Spyware. Diesen Vorgang können Sie jederzeit über den „Stop“-Button abbrechen. Nach dem erfolgten Scan zeigt Ad-Aware die erkannten Spyware-Dateien nach einem Klick auf „Report“ in einem Logfile an.

Nach der Auflistung aktiver Prozesse im Arbeitsspeicher stehen die gefundenen Registry-Schlüssel mit enthaltener Spyware. In unserem Test fand Ad-Aware nur die bekannte Alexa-Adware des Internet Explorers. Anschließend zeigt das Tool unter „Scanne Dateien“ die gefundenen verdächtigen Dateien auf. Mit dem Button „Speichern“ können Sie diesen Report im TXT-Format sichern. Gehen Sie nun auf „Zurück“ und dann auf „Weiter“. Danach sehen Sie eine Liste der gefundenen Dateien mit vorangestellten Kästchen. Neben dem „Typ“ (F = File für Datei, K = Key für Registry-Schlüssel) finden Sie unter „System“ die zugeordnete Adware sowie unter „Details“ den Fundort. Sie können die Dateien und Keys im Kästchen markieren und anschließend über den Button „Ausnehmen“ in die Ausnahmeliste hinzufügen – dann werden sie

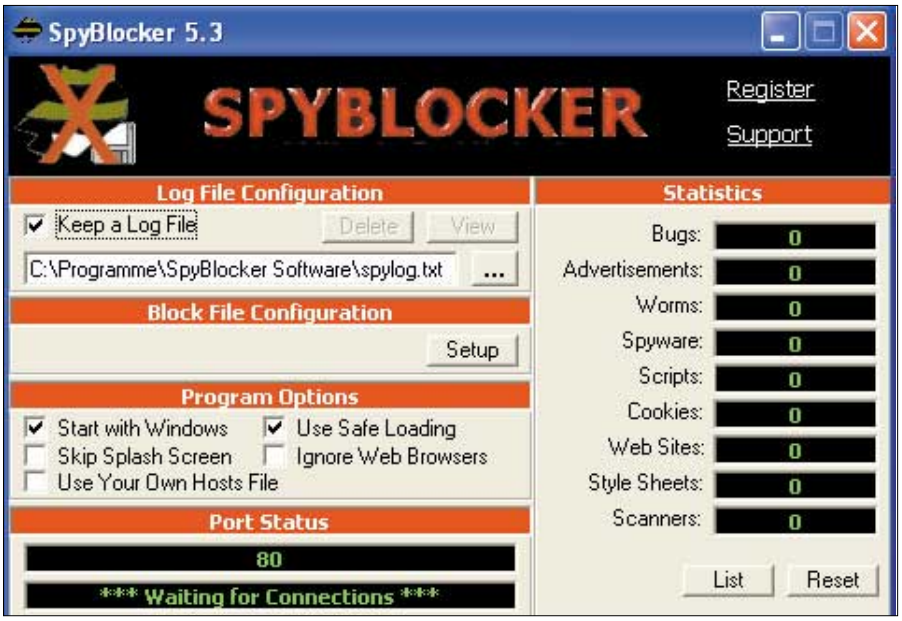


Aus Englisch wird Deutsch: Ad-Aware bietet Ihnen mehrere Sprachen zur Auswahl an

ten nicht mehr korrekt oder überhaupt nicht mehr angezeigt. Bei Programmen, die Adware enthalten, kann dies zu häufigen Abstürzen führen oder zur völligen Funktionsunfähigkeit. Bevor Sie sich somit unbrauchbare Programme einhandeln, sollten Sie sich zuverlässige Listen der Programme ansehen, die Adware enthalten. Die wohl umfangreichste finden Sie im Internet unter **http://virgolamobile.50megs.com/spyware/spyware.htm**.

Gründlich: Ad-Aware 5.83 findet fast alle Werbekomponenten

Das Programm kennt die Dateien und Registry-Einträge von Radiate, Web 3000, DSS-Agent, Alexa, Comet Cursor, Webhancer, Gratisware und Gator. Ad-Aware durchsucht intensiv die Systemverzeichnisse sowie die Registry und listet „verseuchte" Programme, DLL-Dateien oder Einträge auf. Bei ungewöhnlich installierten Spionage-Programmen gibt Ad-Aware Hinweise zur Problembehandlung. Ad-Ware ist ein gutes Tool gegen Spionage-Progamme und das ungewollte Verbreiten persönlicher Daten im Internet. Wer eine erweiterte Version inklusive eines im Hintergrund laufenden Monitorprogramms erwerben möchte, kann die Plus-Version für 12 US-Dollar bestellen. Wie Sie mit Ad-Aware arbeiten und welche Einstellungen wichtig sind, lesen Sie im Kasten „Endlich werbefrei: So beseitigen Sie Spyware mit Ad-Aware".



Spartanische Ausstattung und Oberfläche: Genauso karg wie das Layout der Hersteller-Website sind auch die Angaben zu Einrichtung und Konfiguration des Spyblockers

Arbeitet online: Spyblocker 5.3 blockt Serveranfragen

Ad-, Banner- oder Spyware wehrt der Spyblocker 5.3 ab. Im Gegensatz zu Ad-Aware handelt es sich um ein Online-Programm. Spyblocker kann daher keine

Endlich werbefrei: So beseitigen Sie Spyware mit Ad-Aware 5.83 (II)

zukünftig nicht mehr angezeigt – oder über „Speichern" in einer Backup-Datei sichern. Nach einem Klick auf „Weiter" werden die angeklickten Komponenten aus dem System entfernt.

Gelöschtes wiederherstellen

Seit der Version 5 können Sie in Ad-Aware auch gelöschte Spyware-Komponenten wiederherstellen. Dazu klicken Sie im Eingangsmenü auf den Button „Backups". Im Backup-Manager sehen Sie anschließend die erzeugten Sicherheitskopien, die Sie über „Installieren" wiederherstellen und über „Entfernen" endgültig löschen können. Der „OK"-Button führt nur wieder zurück und ändert nichts.

Ad-Aware-Voreinstellungen anpassen

Über den Button „Einstellungen" ändern Sie die Voreinstellungen des Utilitys. Unter „Pfade" stellen Sie den Speicherort für die erzeugten und verwendeten Dateien von Ad-Aware ein. Unter „Ausnahmen" können Sie bei Bedarf die Ausnahmeliste editieren.

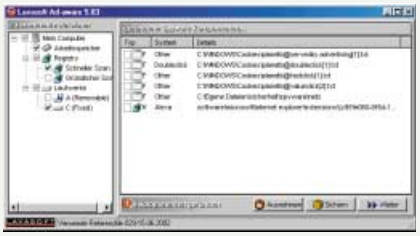
Die „Allgemeinen Einstellungen" verwalten vor allem die Automatismen des Programms, zum Beispiel den Scan bei jedem Start von Windows, das automatische Löschen gefundener Komponenten und das Speichern der Logfiles.

Das automatische Löschen von Komponenten ist nicht zu empfehlen, da die Entfernung der Spyware-Bestandteile meist auch die Funktionsunfähigkeit des entsprechenden Programms nach sich zieht. Da Ad-Aware zum Beispiel wie erwähnt die Alexa-Adware des Internet Explorers erkennt, könnte ein automatisches Löschen also dazu führen, dass der Internet Explorer – und damit ein wesentlicher Teil des Windows-Betriebssystems – nicht mehr richtig funktioniert: ein Ritt auf der Rasierklinge. Solche Fälle sollten Sie daher von vornherein „Ausnehmen".

Auch der Scan bei jedem Windows-Start kann nicht vorbehaltlos empfohlen werden, da er selbst im Schnellverfahren auf der Festplatte durchaus einige Minuten dauern kann und eventuell das parallele Arbeiten mit dem PC verlangsamt. Der automatische Scan des Arbeitsspeichers ist aber durchaus sinnvoll.

Der „Reset All"-Button bringt das Programm auf die Grundeinstellung. Dann müssen Sie aber die deutsche Sprachdatei erneut auswählen.

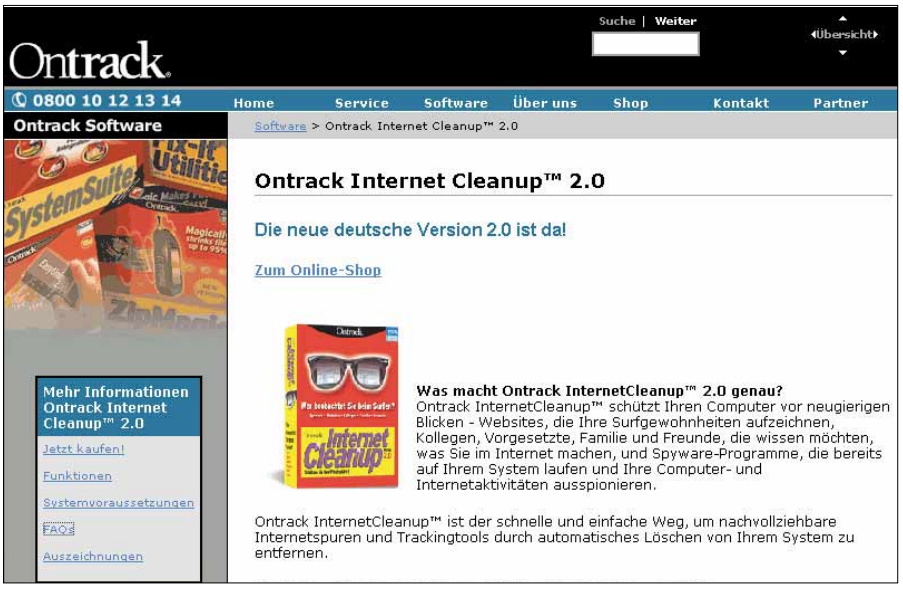
Unter „Weitere Optionen" findet sich neben den deaktivierten Funktionen der kostenpflichtigen Plus-Version die Möglichkeit, die Angaben der Logfiles um wei-



Spyware-Komponenten löschen oder nicht: Hier entscheiden Sie darüber

Software auf der Festplatte de-installieren. Es prüft stattdessen Server-Abfragen, die Informationen vom PC anfordern.

Die ungewöhnliche Bedienung erfordert etwas Zeit für die Einrichtung des Programms, zumal eine vernünftige Anweisung über dessen Einsatzmöglichkeiten fehlt. Jedoch zeigte es im Test bei einer Internet-Verbindung recht zuverlässig versuchte Serverzugriffe an. Es handelt sich hier um die Übertragung von Nutzer-Infos oder das Einschleusen von Tracking- und Advertising-Modulen, die sich als heimliche Spione in Banner-Grafiken oder Plug-in-Dateien verstecken. Spyblocker schickt dann anstelle der Daten nur transparente GIF-Grafiken, die keine Rückschlüsse zulassen. Die abgeblockten Serverdaten protokolliert es.



Peppige Oberfläche und einfache Bedienung: Modern und übersichtlich gibt sich das deutschsprachige Internet Cleanup von Ontrack – ein vielseitiges Tool für alle Fälle

Viele Funktionen: Ontrack Internet Cleanup 2.0

Nicht nur mit Werbe-Spionen, auch mit Cache-Inhalt, Active-X-Komponenten, Cookies und unerwünschten Plug-ins räumt das deutschsprachige Programm Internet Cleanup 2.0 für Win 95/98/ME, NT 4 und 2000 (20 MB, Testversion unter **www.ontrack.de** oder ◉ auf Heft-CD, Preis: 22 Euro) von Ontrack auf. Und es stellt dem Anwender dafür viele Eingriffs- und Beobachtungsmöglichkeiten zur Verfügung. Internet Cleanup sucht unter anderem Banner- oder Programmdateien mit versteckten Funktionen zum Auslesen von Cookies, Cache oder Registry. Das Entfernen dieser Adware, die als ausführbare Programme oder Bibliotheksdateien in Windows integriert ist, schaffte es sehr gut. Die Software findet Dateien der Hersteller Radiate, Netsonic, Conducent, Double Click, Webhancer, Comet Cursor, Gator, Cydoor und Flyswat.

Günter Unterholzner

Endlich werbefrei: So beseitigen Sie Spyware mit Ad-Aware 5.83 (III)

tere Details zu ergänzen. Dazu gehören deren Größe sowie der Zeitpunkt der Erzeugung und des letzten Zugriffs. Die übernommenen Einstellungen werden übrigens ebenso bei jedem Programmstart verwendet wie die zum Scan angegebenen Laufwerke und Sektionen.

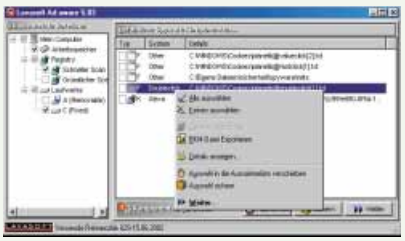
Gefundene Komponenten bearbeiten

Die Liste der gefundenen Komponenten können Sie mit weiteren Funktionen bearbeiten. Halten Sie die Maus etwa eine Sekunde lang über einen Eintrag, erscheinen ein paar weitere Informationen über die angezeigte Komponente wie die Position in der Liste und der Rootkey. Wenn Sie auf einen Spaltenkopf klicken, werden die Einträge entsprechend der Kategorie sortiert.

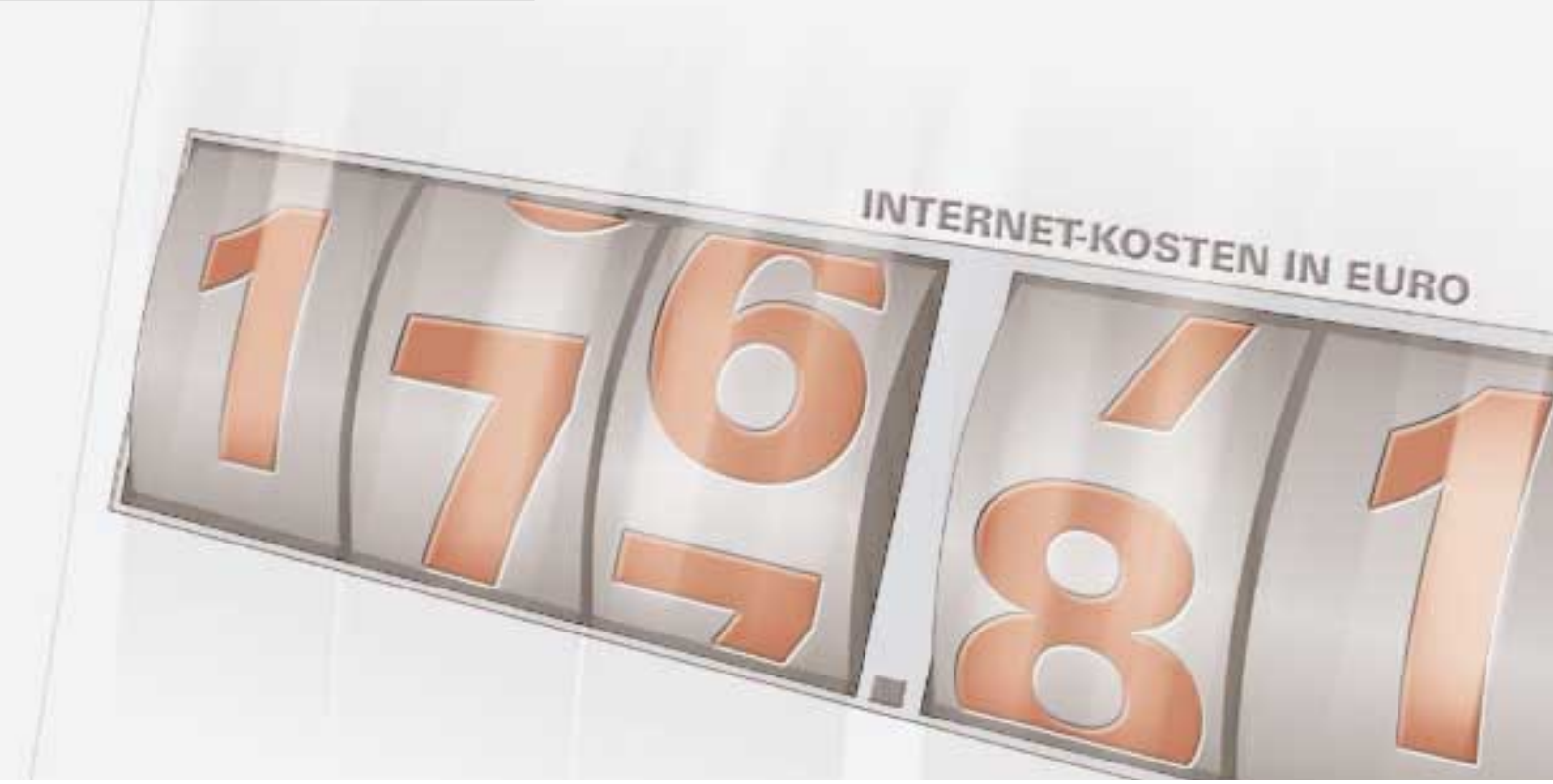
Klicken Sie mit der rechten Maustaste auf einen Eintrag, dann erscheint ein Kontextmenü mit verschiedenen Befehlen. Neben „Alle auswählen“ und „Keines auswählen“ für die Markierung aller oder keiner Komponente finden Sie den Punkt „Gehe zu Registry Key“. (Dieser Befehl ist nur bei markierten Registry-Schlüsseln aktiv, nicht dagegen bei Dateien.) Neben dem Exportieren der BKM-Datei lassen sich bei angezeigten Dateien auch die „Details anzeigen“. Dabei handelt es sich um die Datei-Eigenschaften, die auch der Windows-Explorer auflistet.

Online-Update der Spyware-Suche

Ähnlich wie Antiviren-Programme muss auch Ad-Aware mit immer neuen Spyware-Programmen und -Komponenten zurechtkommen. Die Informationen über die bekannte Spyware enthält die kleine Referenzdatei REFFILE.AWR im Ad-Aware-Ordner. Den Speicherort finden Sie auch unter „Einstellungen, Pfade, Ref.file“. Um diese Datei regelmäßig zu aktualisieren, laden Sie das kostenlose Add-on RefUpdate (**www.lavasoftusa.com/downloads**) herunter und installieren es über einen Doppelklick im Windows-Explorer. Unter „Programme, Lavasoft Refupdate“ starten Sie das Programm und wählen im Auswahlmenü unter „Select Server“ einen der angebotenen Server aus. Anschließend drücken Sie auf den Button „Connect“. Das Programm sucht nun nach einem Update des Reference-Files auf dem entsprechenden Internet-Server und lädt es herunter. Bei Bedarf können Sie unter „Options, Preferences“ den Speicherort dieser Datei ändern. Allerdings muss er immer identisch mit dem Speicherort der REFFILE.AWR in Ad-Aware sein. ■



Mehr Möglichkeiten: Im Kontextmenü gibt es weitere interessante Befehle und Optionen



Kostenfalle Internet-Dialer

Bei Anruf bankrott

Kaum ein Tag vergeht, an dem nicht neue Abzockereien mittels 0190-Dialer ans Tageslicht kommen. Dabei gibt es an der Grundidee eigentlich nichts auszusetzen.

Spezielle vom Internet Provider bereitgestellte Dialer-Programme galten vor wenigen Monaten noch als Zeichen für ein Höchstmaß an Kundenfreundlichkeit. Denn anstatt ihren Mitgliedern in spe komplizierte Anleitungen zur Einrichtung des DFÜ-Netzwerks in Textform zukommen zu lassen, verschickten die Provider lieber ein kleines Hilfsprogramm. Ein Doppelklick auf die entsprechende EXE-Datei, schon war die fertig konfigurierte DFÜ-Netzwerkverbindung eingerichtet und der Ausflug ins Internet konnte beginnen. Inzwischen ist diese Methode in Verruf geraten. Gewiefte Geschäftemacher halten an diesem Grundprinzip fest und versuchen, arglosen Anwendern auf immer raffiniertere Art und Weise heimtückische Dialer unterzuschieben und dank immens hoher Verbindungsgebühren Kasse zu machen.

Wer Premiumangebote will, muss dafür auch zahlen

Trotz aller Schreckensmeldungen, Abmahnungen und Rechtsstreitigkeiten – die oftmals gescholtenen 0190-Dialer sind nicht zwangsläufig schlecht. Schließlich gilt in der freien Marktwirtschaft nach wie vor das Gesetz von Angebot und Nachfrage. Und solange Surfer Erotik-Angebote nutzen möchten, sich über die anfallenden Kosten bewusst sind und nicht mit unlauteren Methoden zur Nutzung eines Dialers gezwungen werden, gibt es an dieser Form des Bezahlens grundsätzlich nichts auszusetzen. Ganz im Gegenteil: Durch die relative Datensicherheit – es werden schließlich weder Kontonummer noch Kreditkartendaten über die unsicheren Kanäle des Internets übertragen – kommt dieser Abrechnungsmodus vielen vorsichtigen Surfern sogar entgegen.

Ähnliches gilt aber auch für die Anbieter von Dialer-Software. Denn während sich die Dialer-Produkte der meisten deutschen Unternehmen wie beispielsweise Aconti (**www.aconti.net**), Fairdialer (**www.fairdialer.de**) und Mainpean (**www.mainpean.de**) strikt an das Grundprinzip der Offenheit halten und den Nutzer mehrmals auf alle für die Verbindung anfallenden Kosten aufmerksam machen, tricksen ausländische Unternehmen oft, was das Zeug hält.

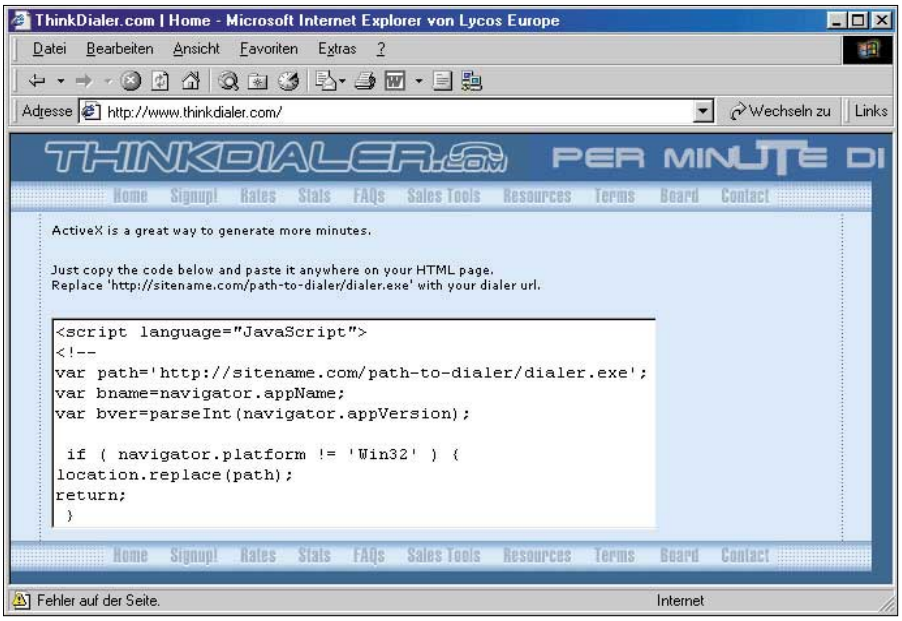
Info: 0190-Dialer

Einst als Alternative zur Zahlung per Kreditkarte gepriesen, haben sich 0190-Dialer zum Schreckgespenst aller Modem- und ISDN-Surfer entwickelt. Doch es gibt hier große Unterschiede.

Aussichten: Es zeichnet sich ein positiver Trend ab

Um sich von den vielen unseriösen Anbietern abzuheben, haben sich einige Netzbetreiber und Anbieter von Telefonmehrwertdiensten zur Freiwilligen Selbstkontrolle Telefonmehrwertdienste (FST; **www.fst-ev.org**) zusammengeschlossen. Nach eigenen Angaben verpflichtet sich der eingetragene Verein dazu, „ausgewogene Rahmenbedingungen für den Markt zu schaffen, die einerseits den Verbraucher- und Jugendschutz in den Vordergrund stellen, andererseits aber auch den Interessen und Anforderungen des Marktes gerecht werden. Ziel der FST ist es, Diensteanbieter und Netzbetreiber mit ihrem Beitritt zur Beachtung des Verhaltenskodex zu veranlassen und mittels ihrer Beschwerdestelle festgestellte Missachtungen des Kodex zu ahnden."

Zu den wichtigsten Inhalten dieses Verhaltenskodex zählen unter anderem der Verzicht auf die heimliche Einrichtung als Standardverbindung und das Verhindern einer automatischen Einwahl. Wie bereits erwähnt, halten sich die deutschen Anbieter schon jetzt weitestgehend an diese Vorgaben. Es bleibt allerdings sehr fraglich, ob sich ausländische Anbieter derart reglementieren lassen. Allerdings weist die FST aber auch ausdrücklich darauf hin, dass ein Verstoß gegen diese Regeln nicht „automatisch dazu führt, dass der Verbraucher seine Telefonrechnung nicht bezahlen muss".



Schamlos: Während sich deutsche Anbieter hinsichtlich ihrer Produkte zumeist bedeckt halten, preist diese Seite Active X als probates Mittel an, um noch mehr Geld abzuzocken („generate more minutes")

Seltsame Moral: Dialer und Abwehr-Tool aus einer Hand

Völlig groteske Situation: Eops, der deutsche Anbieter des hartnäckigen Dialers X-Diver (**www.eops.de**) bietet auf der Website Dialer-Control (**www.dialer-control.de**) ein kostenloses Anti-Dialer-Programm an. Das lediglich 503 KB große Tool Dialer Control 1.0.4.59 für Windows 98/ME, NT 4, 2000 und XP überwacht das DFÜ-Netzwerk, Tapi- und Capi-Schnittstellen sowie die COM-Ports und meldet alle versuchten Kontaktaufnahmen einschließlich angewählter Telefonnummer sowie der dazugehörigen Gebühren. In so einem Fall stehen Ihnen die Optionen offen, den Zugriff dauerhaft zu unterbinden und das Dialer-Programm automatisch zu schließen oder die Einwahl explizit zu erlauben. Doch trotz des unbestreitbar großen Funktionsumfangs bleibt ein schaler Nachgeschmack, dass ausgerechnet ein Dialer-Hersteller ein Anti-Dialer-Tool auf den Markt bringt.

Mit allen erlaubten und verbotenen Mitteln

Der schlechte Ruf der 0190-Dialer rührt vor allem daher, dass eine Vielzahl schwarzer Schafe den Anwender mit mehr oder minder üblen Tricks übers Ohr hauen möchte. Diese Betrügereien beginnen in der Regel schon damit, dass dem Surfer die Installation des Einwählprogramms verheimlicht wird. Dazu setzen die unseriösen Betreiber auf spezielle Active-X-Komponenten, die im Internet Explorer ausgeführt werden. Diese versprechen dem Anwender wahre Wunderdinge wie einen schnelleren Internet-Zugang, kostenlose Erotik oder Software gegen Hacker. Im Gegenzug schweigen sie

Gebührenübersicht: Was kosten die 0190-Nummern?

Auch wenn es klar auf der Hand liegt, wird der Aspekt oft übersehen, dass auch die Deutsche Telekom bei der Vergabe von 0190-Nummern kräftig abkassiert. Beispielsweise verdient der einstige Staatsmonopolist an jeder Minute einer 0190-8-Verbindung immerhin 0,38 Euro, bei 0190-0-Anrufen werden in der höchsten Tarifklasse sogar 0,42 Euro einbehalten. Die folgende Tabelle listet alle Kosten auf, die bei den diversen 0190-Nummern anfallen. Die Deutsche Telekom AG informiert übrigens unter **www.t-versand.de/isroot/tversand/static/preis_0190_0190_0.html** über Anrufertarife und Anbietervergütungen.

Service-Nummer	Kosten pro Minute
0190-0 Tarif 1 (auch 010xx0190-0 bei Call by Call)	0,15 Euro
0190-0 Tarif 2 (auch 010xx0190-0 bei Call by Call)	0,25 Euro
0190-0 Tarif 3 (auch 010xx0190-0 bei Call by Call)	0,12 Euro plus 0,51 Euro pro Verbindung
0190-0 Tarif 4 (auch 010xx0190-0 bei Call by Call)	0,12 Euro plus 0,77 Euro pro Verbindung
0190-0 Tarif 5 (auch 010xx0190-0 bei Call by Call)	0,12 Euro plus 1,28 Euro pro Verbindung
0190-0 Tarif 6 (auch 010xx0190-0 bei Call by Call)	0,12 Euro plus 2,05 Euro pro Verbindung
0190-5 (auch 010xx0190-5 bei Call by Call)	0,62 Euro
0190-6 (auch 010xx0190-6 bei Call by Call)	0,41 Euro
0190-7 (auch 010xx0190-7 bei Call by Call)	1,24 Euro
0190-8 (auch 010xx0190-8 bei Call by Call)	1,86 Euro

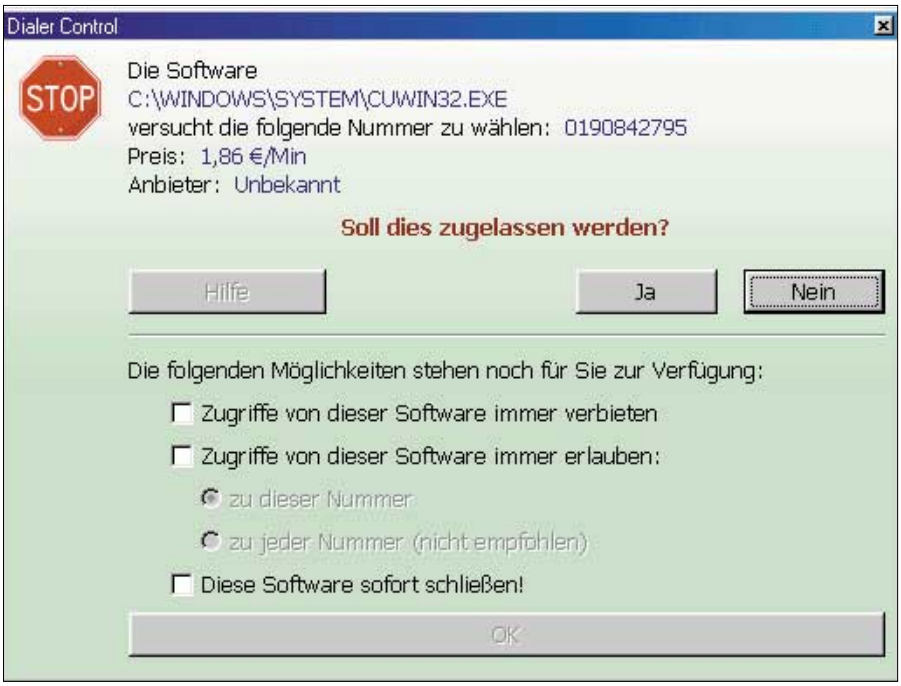
Es sind auch Spezialtarife möglich.

sich aber über die Einwahlnummer und vor allem über die anfallenden Kosten aus, so dass ahnungslose Surfer schnell in die Kostenfalle tappen.

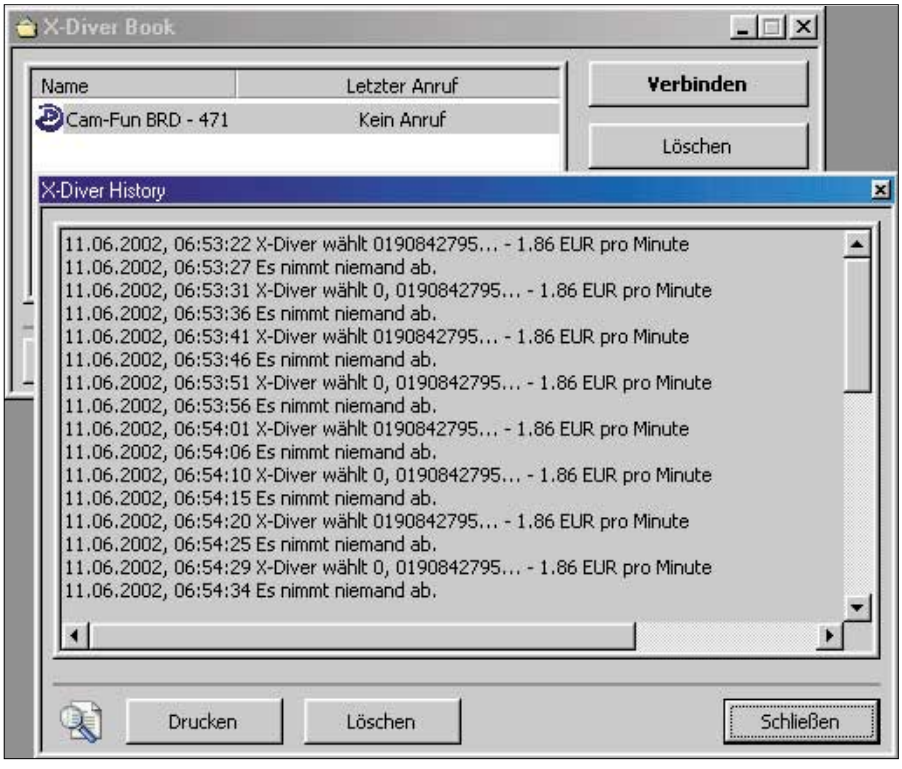
Die zweite negative Eigenschaft offenbart sich, sobald ein Programm auf dem Rechner eines Anwenders installiert wurde. Denn während von diesem selbst angelegte Netzwerkverbindungen auf die bevorstehende Kontaktaufnahme zum Internet – und auf die anfallenden Kosten – aufmerksam machen, richten die böswilligen Vertreter sich nicht selten ungefragt als Standardverbindung ein. Startet der Anwender dann seinen Browser, wird im Hintergrund automatisch eine Verbindung zu einer 0190-Nummer aufgebaut.

Noch gefährlicher: Ganz hartnäckige Programme halten die Verbindung selbst dann noch aufrecht, wenn der Benutzer glaubt, diese bereits getrennt zu haben. Im Klartext bedeutet dies, dass die Einwahl oftmals automatisch und ohne Vorwarnung erfolgt und der Anwender nicht einmal durch das typische Taskleisten-Symbol auf eine bestehende Verbindung aufmerksam gemacht wird. Im Extremfall ist ein PC-Besitzer also mehrere Stunden über eine 0190-Nummer im Internet, ohne überhaupt davon zu wissen. Und selbst wenn ein Anwender merkt, dass er in die Dialer-Falle getappt ist, und den Schädling von seinem Rechner entfernen möchte, hält der Ärger an, da sich die Programme unseriöser Anbieter nicht so einfach de-installieren lassen.

Wie Sie sich mit Windows-Bordmitteln und Zusatz-Tools am besten vor solch ungebetenen Besuchern schützen, erfahren Sie ab ▷ Seite 114.



Vom Bock zum Gärtner mutiert? Der beanstandete 0190-Dialer und die entsprechende Schutz-Software gegen eben diesen Dialer stammen von ein und demselben Hersteller



Interessante Einblicke: Bei weitem nicht alle Internet-Dialer geben sich so auskunftsfreudig wie X-Diver, der Anwender detailliert über alle seine Anwahlversuche und Verbindungen informiert

Auf der sicheren Seite: Wohl dem, der bereits mit DSL surft

Aufgrund der technischen Besonderheiten von Internet-Verbindungen per DSL (Stichwort: Dauerverbindung) müssen sich Besitzer von Breitbandanschlüssen keine Sorgen machen. Denn wo keine Telefonnummer angewählt werden kann, sind Anrufe bei 0190-Nummern unmöglich. Einzige Ausnahme: Steckt im Rechner neben der Netzwerk- auch eine ISDN-Karte oder ist ein Modem angeschlossen, um beispielsweise Faxe zu senden und zu empfangen, besteht die Gefahr des Missbrauchs. Denn da die beiden Internet-Verbindungen unterschiedliche Frequenzbänder nutzen, ist eine gleichzeitige Einwahl ins Web durchaus möglich. Weitaus häufiger kommt es aber vor, dass die DSL-Verbindung unbemerkt gekappt wird, bevor dann eine teure 0190-Verbindung aufgebaut wird. Nicht zuletzt deswegen empfehlen wir hier den Einsatz einer Firewall. Mehr zu diesem Thema lesen Sie ab ▷ Seite 50.

Wer seine ISDN-Hardware an einer Telefonanlage angeschlossen hat, findet in der dazugehörigen Bedien- und System-Software meistens eine Option, mit der sich alle 0190er-Nummern generell sperren lassen. Einzelne Rufnummern lassen sich auch wieder explizit freischalten.

Stefan Forster

Impressum

PC WELT

Redaktion PC-WELT,
Leopoldstraße 252b,
80807 München
E-Mail:
redaktion@pcwelt.de
Homepage: **www.pcwelt.de**

Tel. 089/3 60 86-222
Fax 089/3 60 86-459

Chefredakteur: Jürgen Bruckmeier (jb) (verantwortlich, Anschrift der Redaktion)
Stellvertretender Chefredakteur: Roland Bischoff (bif)
Chef vom Dienst: Andrea Kirchmeier (ak)
Redaktion Spezial 2/2002: Andrea Kirchmeier (ak)
Freie Mitarbeiter: Stefan Forster, Christoph Metzger, Burkhard Müller, Wolfgang Nefzger, Peter-Jürgen Rofer, Günther Unterholzner
Redaktionsassistenz: Ursula Istavrinos (Leitung), Christa Vetter
www.pcwelt.de: Stefan Willeke (Ressortleiter/sw), Eric Bonner (eb), Hans-Christian Dirscherl (hc), Liane M. Dubowy (lmd), Panagiotis Kolokythas (pk), Markus Pilzweger (mp)
DTP-Produktion/Disposition: Alex Dankesreiter (Leitung), Andreas Förth (leitend)
DTP-Layout: Hans Weber, Anton Paunert, Snežana Dejanović
Design: h2Design.de

Tel. 089/3 60 86-210
Fax 089/3 60 86-263
E-Mail: media@pcwelt.de

Ihr Kontakt zur Anzeigenabteilung:
Anzeigenleitung (Associate Publisher): Christoph Burkhart (-294) (verantwortlich für Anzeigen, Anschrift des Verlags)
Stellvertretende Anzeigenleitung: Reinhard Baum (-516) (verantwortlich für die Vorstellung der New-Media-Inhalte im „Promotion"-Teil der PC-WELT und auf CD-ROM; Anschrift des Verlags)
Anzeigenverkaufsleitung Markenartikel: Marcus Schardt (-219)
Mediaberatung Print, CD-ROM, Online:
PLZ 0, 3, 6, 7, 9: Petra Gryga (-188)
PLZ 1, 8: Stefan Bader (-129)
PLZ 2: Iris Haug (-854)
PLZ 4, 5: Petra Rammelsberger (-355)
Computer Direct: Helga de Gregori (-132)
Business Development: Panagiota Herbrand (-181)
Anzeigenverkauf Ausland: Daniela Radzio, Leitung, Europa, (-293), Iris Haug, Asien / USA, (-854)
Marketingleitung: Katja Martin (-320),
Leitung Marktforschung: Frank Heublein (-785)
New Media: Andreas Koschinsky (-644), Leitung Sonderprojekte: Joachim Herbert (-121, freier MA)
Leitung Anzeigendisposition: Rudolf Schuster (-135)
Anzeigendisposition: Magdalena Lerch (-291), (Fax -328)
Digitale Anzeigenannahme: Thomas Wilms, leitend (-604), Manfred Aumaier (-602), Andreas Mallin (-603), Martin Mantel (-780)

Anzeigenpreise: Es gilt die Anzeigenpreisliste 19 (1.10.2001).
Fließsatzanzeigen nach Zeilen:
Private Kleinanzeigen 4,00 Euro je Zeile (inkl. ges. MwSt.). **Gewerbliche Kleinanzeigen:** 13,00 Euro je Zeile zuzügl. ges. MwSt. / Chiffregebühr 5,00 Euro
Bankverbindungen: Hypovereinsbank München, Konto 322 460 95, BLZ 700 202 70; Postbank München, Konto 220 977-800, BLZ 700 100 80
Anschrift für Anzeigen: siehe Anschrift des Verlags
Erfüllungsort, Gerichtsstand: München
IGS Anzeigenverkaufsleitung für ausländische Publikationen: Tina Ölschläger (-116);
für inländische Publikationen: Peter L.Townsend (Leitung) (-299)
Verlagsrepräsentanten für Anzeigen Frankreich: F. Bonnin, 5 Rue Chantecoq, 92808 Puteaux, Tel.: 0033-1-4197-0, Fax 0033-1-4197-6202. **NL:** Florence Schmit, Richard Holkade 8, 2033 Haarlem, Tel.: 0031-23-5461090. **Großbritannien:** Shane Hannam, 29/31 Kingston Road, GB-Staines, Middlesex TW 18 4QG, Tel.: +(44) 1-784210210. **USA East:** Chip Zaborowski, 500 Old Connecticut Path, P.O. Box 9377, Framingham, MA 01701-9377, Tel.: 001-508-87907 00. **USA West:** Larry Arthur, 501 Second Street, S. 114, San Francisco, CA 94107, Tel.: 001-415-2434141. **Taiwan:** The Infopro Group, Sophia Yu, 8F, 131 Sec 3 Nanking E Road, Tel.: 00886-2-2715-3000. **Japan:** Noriko Nozaki, 8th Floor 3-4-5, Hongo Bunkyo-Ku, Tokio 113-0033, Japan, Tel. 0081-3-5800-3734. **Singapur:** J. Yu, No. 80 Marine Parade Road, #17-01A Parkway Parade, S-449269, Tel.: 0065-3458383. **Hongkong:** V. Chan, S.1707, K.Wah Centre, 191 North Point, Tel.: 00852-2861 3238. **Korea:** C.H. Park, Rm. 1806/7, Golden Tower 191, 2-ka, Choongjungro, Seodaemun-ku, Seoul, Tel.: 0082-2364-4182/3
Vertriebsleitung: Josef Kreitmair (-243)
Leitung Vertriebsmarketing: Peter Priewasser (-154)
Vertrieb Handelsauflage: MZV Moderner Zeitschriften Vertrieb GmbH, Breslauer Straße 5, 85386 Eching, Tel. 089/31906-0, Fax 089/31906-113, E-Mail: **mzv@mzv.de**, Internet: **www.mzv.de**
Erscheinungsweise: Das Spezial 2/2002 ist ein Special der PC-WELT.

Produktion: Heinz Zimmermann (Leitung)
Druck: Mayr Miesbach
Am Windfeld 15
83714 Miesbach
Tel. 08025/294-267
Haftung: Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Die Veröffentlichungen in der PC-WELT erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Auch werden Warennamen ohne Gewährleistung einer freien Verwendung benützt.
Copyright: IDG Magazine Verlag GmbH, Leopoldstraße 252b, 80807 München, Tel. 089/36086-02, Fax 089/36086-267
Verlag: IDG Magazine Verlag GmbH, Leopoldstraße 252b, 80807 München, Tel. 089/36086-02, Fax 089/36086-267
Geschäftsführer: York von Heimburg
Verlagsleitung (Mitglied der Geschäftsleitung): Stephan Scherzer

Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Alleiniger Gesellschafter der IDG Magazine Verlag GmbH ist die **IDG Communications Verlag AG,** München, eine 100%ige Tochter der IDG Inc., Boston, Mass., USA.

Vorstand: Keith Arnot, Kelly P. Conlin, York von Heimburg, Ralph Peter Rauchfuss
Aufsichtsratsvorsitzender: Pat McGovern

Die PC-WELT wird auf Recyclingpapier gedruckt (100 Prozent Altpapier).

Inserentenverzeichnis

Windows-Bordmittel gegen Dialer einsetzen

Kein Klick ins Unglück

Schon manch unvorsichtiger Surfer hat seine Blauäugigkeit mit einer horrend hohen Telefonrechnung bezahlt. Dabei schützen schon Windows-Bordmittel vor den 0190-Dialern.

▸Auf reißerischen Erotik-Websites, auf Portalen rund um das Thema Filesharing oder auf Homepages der Cracker- und Raubkopier-Szene – an vielen Orten im Internet lauern 0190-Dialer auf ihre Opfer, die nur ein Ziel kennen: das Aufbauen von Internet-Verbindungen über eine 0190-Rufnummer. Hier beträgt der Minutenpreis über eine mit 0190-8 beginnende Nummer satte 1,86 Euro. Und da beim täglichen Surfen eher Stunden als Minuten online verbracht werden, kann am Monatsende leicht ein erkleckliches Sümmchen zusammenkommen.

Doch trotz der latenten Gefahr sind Sie diesem Treiben nicht schutzlos ausgeliefert. Auf den folgenden beiden Seiten zeigen wir die wichtigsten Kniffe, mit denen Sie 0190-Dialern die Tür zu Ihrem Rechner versperren und eventuell schon aktive Störenfriede mit den Windows-Bordwerkzeugen entdecken und entfernen.

Eines vorweg: Kein 0190-Dialer installiert sich auf einem Rechner, ohne dass der Benutzer zumindest eine Dialogbox bestätigt hat. Und genau an dieser Stelle liegt auch der Ansatzpunkt für den einfachsten Schutzmechanismus.

Gesunder Menschenverstand ist oberste Surferpflicht

Bevor Sie sich mit Anti-Dialer-Software (auf das besonders empfehlenswerte Yaw 3.01 gehen wir ab ▷ Seite 110 ein), speziellen Security-Tools (Firewalls nehmen wir ab ▷ Seite 50 unter die Lupe) und Windows-Einstellungen auseinandersetzen, sollten Sie sich zunächst einmal vor Augen halten, wie sich ein 0190-Dialer überhaupt in ein System einnistet.

Der mit Abstand häufigste Weg besteht darin, auf einen angeblich hilfreichen Link zu klicken und anschließend eine Dialogbox mit „Ja“ zu bestätigen. Der zweite Klick führt dann meist direkt ins Unglück, sprich: Die Dialer-Software wird auf den PC des Anwenders überspielt oder – falls es sich um eine ActiveX-Komponente handelt – gleich installiert. Mit solchen Bauernfängereien wird mittlerweile immer öfter auch unter dem Deckmäntelchen der PC-Sicherheit geneppt. Vor allem die angebliche Sicherheitslücke Ihres Rechners – auf der besuchten Website wird Ihnen über einen ungefährlichen Systemaufruf die exakte Ordnerstruktur Ihrer System-Festplatte präsentiert – wird von dubiosen Site-Betreibern dazu genutzt, um 0190-Dialer an den Mann zu bringen. Im Klartext bedeutet dies, dass dem Anwender ein teures Programm untergeschoben wird, um ein gar nicht existentes Sicherheitsrisiko zu eliminieren.

Um sich vor solch billigen Tricks zu schützen, reicht es in den meisten Fällen aus, die im Download-Dialog angegebenen Informationen aufmerksam durchzulesen. Bei Dateinamen wie „Mega-Dialer.exe“ ist der Fall schnell klar; aber auch unverfängliche Bezeichnungen wie „Speedburst.exe“ oder „X-Diver.exe“ sollten nicht zuletzt wegen der Datei-Endung „.EXE“ zu erhöhter Wachsamkeit führen.

Auch wenn es Boulevardpresse und einschlägige TV-Magazine anders erklären: Als Mailanhänge verbreitete 0190-Dialer sind zwar keine Fiktion mehr; im

Bauernfängerei: Ein vorgebliches Sicherheitsleck des Anwender-Rechners wird im Browser präsentiert und kann angeblich nur durch das „kostenlose Zusatztool“ in Form eines 0190-Dialers geschlossen werden

Info: Schutz vor Dialern

Mit zwei, drei unachtsamen Klicks ist ein Dialer installiert, der Sie fortan über eine teure 0190-Nummer ins Internet bringt. Doch bieten einige wenige Einstellungen und Maßnahmen ausreichend Schutz.

Vergleich zu ungewollt erhaltenen Viren und Würmern ist die Häufigkeit jedoch sehr gering. Allerdings sorgte vor wenigen Monaten ein Fall für Aufsehen, bei dem eine angeblich vom T-Online-Support verschickte Mail als Transportmittel für einen 0190-Dialer verwendet wurde.

Ausgangspunkt: Das Windows-DFÜ-Netzwerk

Haben Sie vor lauter Pop-up-Fenstern und verwirrenden Animationen doch einen ominösen Download gestartet, ist noch nichts verloren. Als erstes sollten Sie einen Blick in das DFÜ-Netzwerk werfen, nach unbekannten Einträgen Ausschau halten und diese ohne Umschweife löschen. Mit einem rechten Mausklick auf das entsprechende Icon und Auswahl des Kontextbefehls „Eigenschaften“ erkennen Sie auf der Registerkarte „Allgemein“ anhand der eingetragenen Rufnummer auf einen Blick, ob es sich um einen 0190-Dialer handelt oder nicht. Achten Sie auch auf getarnte Telefonnummern der Form „0103301908“, die ebenfalls zur Kostenfalle werden können. Die Netzvorwahl 01033 besagt nichts anderes, als dass Sie über das Telefonnetz der Deutschen Telekom anrufen. Das Gleiche gilt übrigens für alle Rufnummern, die mit „010“ beginnen. Ein oft vergessener Schutzmechanismus für Windows-98-Anwender besteht darin, die automatische Einwahl ohne Benutzerbestätigung auszuhebeln. Dazu wählen Sie im System-Ordner „DFÜ-Netzwerk“ im Menü „Verbindungen“ den Befehl „Einstellungen“ und markieren auf der Registerkarte „Allgemein“ die Option „Verwendung des DFÜ-Netzwerks bestätigen“. Nach einem abschließenden Klick auf „OK“ müssen Sie vor jeder Einwahl in das Internet eine Dialogbox bestätigen, aus der sowohl die angewählte Rufnummer als auch der Name der Verbindung ersichtlich sind.

Aufmerksam: Ist die DFÜ-Netzwerkeinstellung „Verwendung des DFÜ-Netzwerks bestätigen“ aktiv, kann sich kein 0190-Dialer ungefragt mit einer teuren Rufnummer verbinden

Auch das Start-Menü muss geprüft werden

Da sich besonders hartnäckige Vertreter der Dialer-Zunft gar nicht im DFÜ-Netzwerk verewigen, kommen Sie nicht darum herum, auch die Autostart-Gruppe zu inspizieren. Dazu wählen Sie zunächst in der Programmgruppe „Zubehör“ das Hilfsprogramm „Systeminformationen“ aus dem Unterordner „Systemprogramme“ aus. Im Menü „Extras“ klicken Sie auf den Befehl „Systemkonfigurationsprogramm“ und aktivieren die Registerkarte „Autostart“. Treffen Sie hier auf verdächtige Einträge wie „Fairdailer“, „Aconti“ oder „Stardialer“, sollten Sie diese umgehend deaktivieren und den Rechner anschließend neu starten.

Beliebtes Angriffsziel: Microsoft Internet Explorer

Auch der Internet Explorer ist nicht resistent gegen Angriffe aus dem Internet und öffnet über eine standardmäßig vorgegebene Einstellung manchen 0190-Dialern Tür und Tor. Dabei sorgt bereits ein kleiner Eingriff unter „Extras, Internetoptionen“ dafür, dass aktive Scripts ausgehebelt werden. Auf der Registerkarte „Sicherheit“ markieren Sie den Eintrag „Internet“ und klicken auf den Button „Stufe anpassen“. Unter „ActiveX-Steuerelemente und Plugins“ setzen erfahrene PC-Besitzer alle Optionen auf „Benutzerdefiniert“; sicherheitsbewusste Anwender entscheiden sich gleich für „Deaktivieren“. Wer noch einen Schritt weiter gehen möchte, nutzt einen alternativen Browser, denn Netscape (**www.netscape.de**, Download 27 MB, ◉ auf Heft-CD), Opera (**www.opera.de**, Download 11 MB, ◉ auf Heft-CD) und Mozilla (**www.mozilla.org**, englischsprachiger Download 11 MB, ◉ auf Heft-CD) verzichten auf Active X.

Stefan Forster

Telefonrechnung zu hoch – was tun?

Selbst wenn sich ein 0190-Dialer in Ihrem System eingenistet und die Telefonrechnung in ungeahnte Höhen getrieben hat, ist das Geld noch nicht verloren. Aufgrund der unsicheren Rechtslage und fehlender Grundsatzurteile stellen die folgenden Ratschläge nicht mehr als einen bloßen Leitfaden für 0190-Geschädigte dar. Dialer-Opfer finden weitere Hinweise etwa auf der Website der Rechtsanwälte Weber & Partner (**www.dialerundrecht.de**).

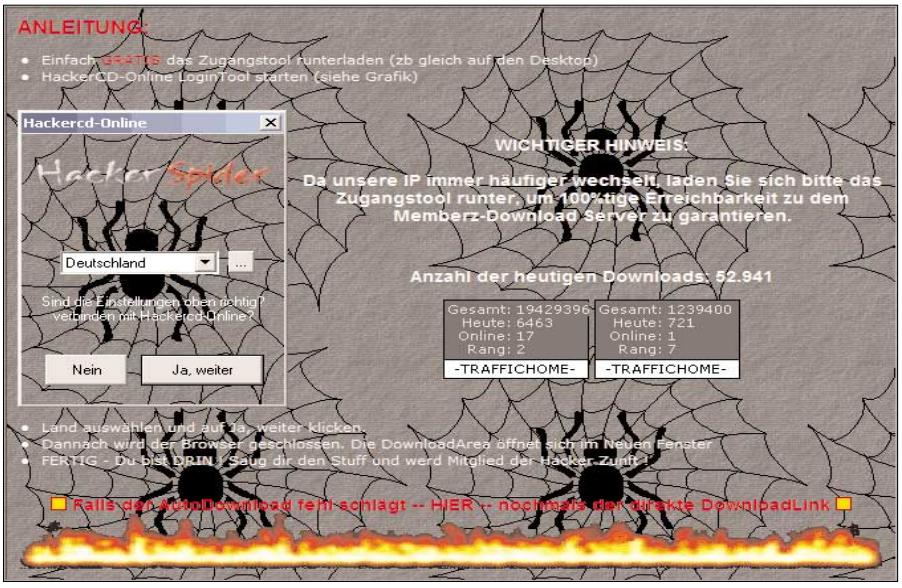
Der erste Schritt besteht darin, die fragliche Telefonrechnung schriftlich anzufechten, die automatisch abgebuchte Telefonrechnung auf Ihr Konto rückbuchen zu lassen und den Ihrer Meinung nach tatsächlich vertelefonierten Betrag entsprechend dem monatlichen Durchschnitt zu überweisen. Als Nächstes sollten Sie sich mit der Verbraucherschutzzentrale sowie der Freiwilligen Selbstkontrolle Telefonmehrwertdienste (**www.fst-ev.org**) in Verbindung setzen. Je mehr Informationen (Name des Dialers, Hersteller, Website) Sie dabei parat haben, desto schneller wird Ihre Beschwerde bearbeitet. Als letzter Schritt bleibt nur noch der Weg zum nächsten Polizeirevier, um eine formale Anzeige zu erstatten. In diesem Fall müssen Sie Ihren PC möglicherweise der Polizei übergeben, damit die Beamten eine Spurensicherung durchführen können.

Tools gegen 0190-Dialer

Schluss mit 0190-Terror

Neben gesundem Menschenverstand und einem perfekt konfigurierten System beugen auch Anti-Dialer einer horrenden Telefonrechnung vor. Wir zeigen, welche Tools auf den PC gehören.

▸Nepper, Schlepper und Bauernfänger treiben nicht nur in der realen Welt ihr Unwesen. Auch – oder gerade – das Internet stellt eine ideale Spielwiese dar, um unerfahrenen und unvorsichtigen Surfern das Geld aus der Tasche zu ziehen. Stark im Trend liegen hier Dialer, die als umstrittene Ergänzung zum Windows DFÜ-Netzwerk arbeiten und den Anwender mit einer teuren 0190-Servicenummer verbinden. Versteckte Dialer wählen sich ohne Benutzereingriffe über 0190-Nummern ins Internet ein; angebliche Support-Mitarbeiter verschicken Dialer per Mail; einmal über einen Dialer eingewählt, und schon sind bis zu 900 Euro weg. Allerdings sind Sie dem Treiben nicht vollkommen schutzlos ausgeliefert.



Wer's glaubt, wird selig: Das Einzige, das ein Besucher auf dieser Homepage für optimale Rechner-Sicherheit vorfindet, sind ein 0190-Dialer und naive Begründungen, die seinen Einsatz rechtfertigen sollen

Gefahrenquellen: ISDN-Adapter und unbedachte Klicks

Wer seinen PC vor Angriffen aus dem Internet im Allgemeinen und heimtückischen 0190-Dialern im Speziellen schützen möchte, darf sich nicht allein auf seinen gesunden Menschenverstand und die Windows-Bordwerkzeuge verlassen. Zum einen ist nicht einmal der absolute Profi-Anwender vor einem versehentlichen Klick auf die falsche Schaltfläche gefeit; zum anderen werden sehr viele Privatrechner von mehreren Personen genutzt. Und sobald ein unerfahrener – zumeist jugendlicher – Anwender in die bunte Welt des Internets eintaucht, steigt die Gefahr, sich einen 0190-Dialer einzufangen, rapide an. Und nicht einmal stolze DSL-Besitzer dürfen sich in Sicherheit wiegen, sofern sie noch einen ISDN-Adapter oder ein Modem am Rechner angestöpselt haben. Denn während DSL-Anschlüsse nicht von einem Dialer missbraucht werden können, stellen die herkömmlichen Zugänge potenzielle Angriffsziele dar. Und auch der Einsatz einer Desktop-Firewall läuft hier ins Leere, da solche Programme ihre Kontrolltätigkeit erst nach dem Zustandekommen einer Internet-Verbindung aufnehmen.

Sicher ist sicher: Aufbau mehrerer Verteidigungslinien

Damit Sie am Monatsende nicht von einer horrenden Telefonrechnung überrascht werden, empfiehlt Ihnen die PC-WELT den traditionellen Aufbau mehrerer Sicherheitsstufen. Neben dem obligatorischen Virenscanner ist für alle Modem- und ISDN-Surfer eine intelligente Anti-Dialer-Software unumgänglich.

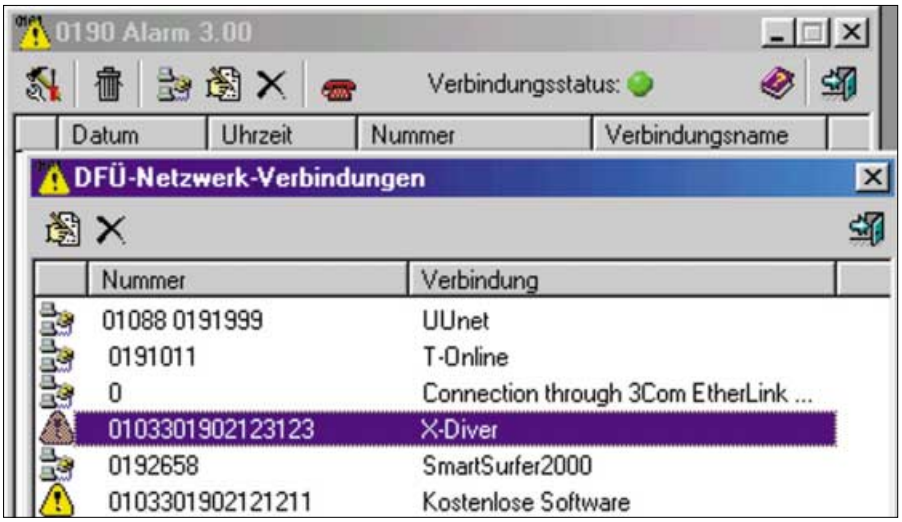
Je nach Funktionsumfang überwachen solche Programme nicht nur das DFÜ-Netzwerk, sondern auch die Capi-, Tapi- und COM-Schnittstellen, um alle von 0190-Dialern genutzten Angriffsziele im Blick zu haben. Darüber hinaus werden aber auch Festplatten, Arbeitsspeicher sowie die Windows-Registry auf der Suche nach verräterischen Dateien und Einträgen durchstöbert. Das einzige Problem: Ähnlich wie bei den Virenscannern ist ein regelmäßiges Update Pflicht, da nur diese Aktualisierungen wirkungsvollen Schutz vor den neuesten 0190-Nepps gewährleisten. Schließlich sind sich die Dialer-Hersteller dieser „Gefahr" bewusst und passen ihre „Produkte" den veränderten Gegebenheiten an. Das Ganze erinnert ein wenig an den Kampf zwischen Virenprogrammierern und Herstellern

Info: Dialer-Abwehr

Anti-Dialer-Programme setzen an mehreren Stellen an und versprechen wirkungsvollen Schutz. Allerdings unterscheiden sich die Tools in Sachen Funktionsumfang und Benutzerführung zum Teil drastisch voneinander.

von Antiviren-Software — die eine Gruppe entwickelt einen neuen Schädling, die andere Seite stellt binnen Stunden das passende Gegenmittel zur Verfügung.

Angesichts dieser Analogie stellt sich die berechtigte Frage, warum Virenscanner eigentlich nicht auch über ein Anti-Dialer-Feature verfügen. Die Antwort auf diese Frage hat ein Richter Ende Mai gegeben: H+B EDV, Hersteller des Virenwächters Antivir (**www.antivir.de**), darf 0190-Dialer „aus wettbewerbsrechtlichen Gründen" nicht mehr als Viren bezeichnen. Der Grund: Eine Reihe von Dialer-Herstellern ist gerichtlich gegen diese Definition vorgegangen, und der Richter hat zu ihren Gunsten entschieden.



Alles im Blick: 0190 Alarm 3.00 kennzeichnet alle verdächtigen Einträge des DFÜ-Netzwerks mit einem Ausrufezeichen. Alle verdächtigen Einträge können mit einem Klick entfernt werden

Welches Tool bietet maximalen Schutz?

Angesichts der immer größer werdenden Dialer-Gefahr ist es kein Wunder, dass der sicherheitsbewusste PC-Besitzer aus einer Vielzahl von Anti-Dialer-Programmen wählen kann. Doch was macht ein gutes Anti-Dialer-Tool eigentlich aus? Abgesehen von den ganz persönlichen Vorlieben des einzelnen Nutzers haben sich eine Handvoll Funktionen herauskristallisiert, ohne die kein leistungsfähiges Schutzprogramm auskommt. Auf den folgenden Seiten stellen wir Ihnen die Stärken und Schwächen von insgesamt sieben Anti-Dialer-Tools aus der Free- und Shareware-Szene vor. Übrigens finden Sie fast alle hier vorgestellten Programme auch ◉ auf Heft-CD.

0190 Alarm 3.00

Zu den Vorzügen von 0190 Alarm 3.00 (◉ auf Heft-CD oder unter **www.onlinetimer.de/others.html**) für Windows 95/98/ME sowie XP gehören zweifelsohne die vielfältigen Konfigurationsmöglichkeiten. Angefangen bei der Autostartoption (sehr zu empfehlen) über die Wahl der durchzuführenden Aktion bei Entdeckung einer verdächtigen Rufnummer (Verbindung trennen oder nachfragen) bis hin zur optionalen Einbindung einer Sound-Datei — das kostenlose Programm hinterlässt einen guten Eindruck.

Die Schutzfunktionen greifen bereits nach der Installation, da sofort die Telefonnummern der im DFÜ-Netzwerk eingetragenen Verbindungen überprüft werden. Vorkonfiguriert sind die Nummernblöcke 0190, 0193 und 0900, eine beliebige Anzahl weiterer Rufnummern können Sie eingeben. Wie auch das weiter unten vorgestellte Tool 0190-Killer 2.0 mäkelt allerdings auch 0190 Alarm 3.00 an der DSL-Verbindung herum, schlägt aber richtigerweise vor, die Rufnummer „0" zur Liste der fortan zu ignorierenden Telefonnummern hinzuzufügen. Jede DFÜ-Netzwerkverbindung lässt sich direkt aus dem Programm heraus editieren.

0190-Killer 2.0

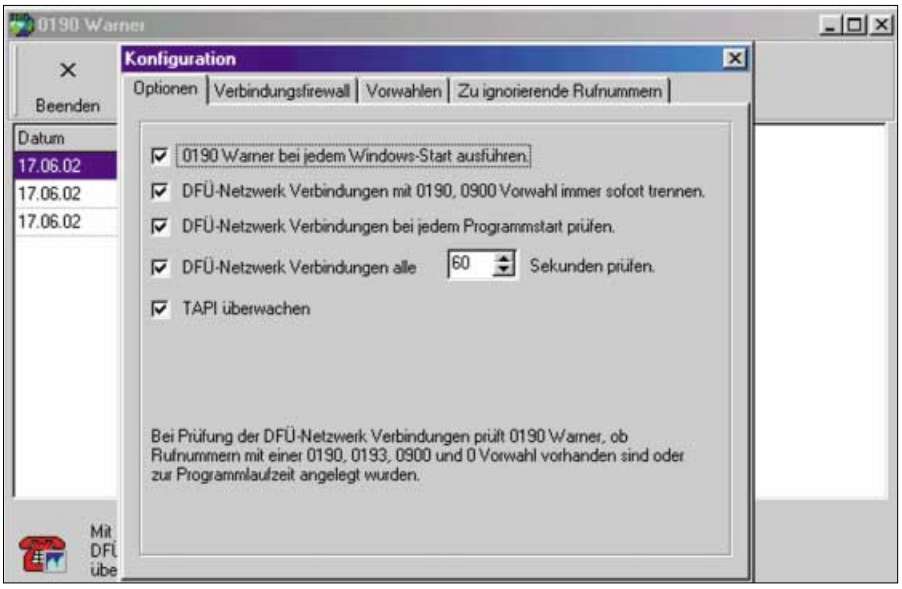
Der 0190-Killer für Windows 95/98/ME, 2000 und XP (◉ auf Heft-CD oder unter **www.hudec-soft.de/0190killer/**) wird nach dem Shareware-Prinzip vertrieben, so dass Sie

Checkliste: Zehn Regeln für einen Dialer-freien PC

Beim Schutz vor 0190-Dialern spielen mehrere Faktoren eine Rolle. Angefangen bei — trotz der Offensichtlichkeit — oftmals vergessenen Verhaltensregeln über den Einsatz der richtigen Tools bis hin zum Wissen um die Funktionsweise dieser ungebetenen PC-Gäste — mit der folgenden Checkliste geben wir Ihnen einen schnellen Überblick über die Grundregeln, die jeder ambitionierte Rechner-Besitzer kennen und befolgen sollte.

1. Setzen Sie eine leistungsfähige Anti-Dialer-Software ein, und aktualisieren Sie das Programm regelmäßig.
2. Klicken Sie nicht jedes Pop-up-Banner an, und glauben Sie nicht alles, was Ihnen eine Website verspricht.
3. Deaktivieren Sie die automatische Einwahl des DFÜ-Netzwerks, um eine ungefragte Einwahl zu unterbinden.
4. Passen Sie die Sicherheitseinstellungen des Internet Explorers an. Lieber eine Dialogbox mehr bestätigen als sich einen Dialer einfangen.
5. Klären Sie Ihre PC-Mitbenutzer über die potenziellen Gefahren auf.
6. Überprüfen Sie regelmäßig die Einträge im Autostart-Menü und in der Windows-Registry.
7. Kontrollieren Sie das DFÜ-Netzwerk regelmäßig auf neue Verbindungen, und entfernen Sie alle unbekannten Einträge.
8. Achten Sie auf unbekannte Symbole im Start-Menü, auf dem Desktop, in der Taskleiste sowie im Systray neben der Windows-Uhr.
9. DSL-Anwender sollten die ISDN-Karte oder das ISDN-Modem nur bei Bedarf mit der Telefonleitung verbinden.
10. Ganz gleich wer der Absender einer unaufgeforderten Mail mit unbekanntem Datei-Anhang zu sein scheint — löschen Sie die Anlagen umgehend.

nach Ablauf der 30 Tage langen Testperiode 6 Euro bezahlen müssen. Sehr guter Hinweis: Nach abgeschlossener Installation macht Sie das Programm darauf aufmerksam, dass der Einsatz nicht nötig ist, sofern ausschließlich ein Internet-Zugang per DSL genutzt wird. Der 0190-Killer entdeckte im Test alle potenziell gefährlichen Einträge im DFÜ-Netzwerk und ließ Einwahlverbindungen zu Providern wie Uunet und T-Online anstandslos zu. Und selbst der häufig genutzte Trick, eine 0190-Rufnummer durch die zusätzliche Angabe der Netzbetreibervorwahl (bei der Deutschen Telekom ist das die 01033) zu verschleiern, wurde erkannt und durch eine blinkende Warnmeldung angezeigt. Sehr wichtige Zusatzfunktion: Alle Aktionen werden automatisch in eine Protokolldatei geschrieben – so haben Sie stets alle Einwahlversuche im Blick.



Kennt keine Gnade: Auf Wunsch beendet der 0190 Warner 2.12 alle ominösen Verbindungen ohne weitere Nachfrage, was für größtmöglichen Schutz vor teuren Dialern sorgt

0190 Warner 2.12

Das kostenlose Überwachungs-Tool 0190 Warner 2.12 (unter **www.wt-rate.de/freeware1.htm** oder ◉ auf Heft-CD) für Windows 95/98/ME und XP testet die in den jeweiligen DFÜ-Netzwerkverbindungen eingetragenen Telefonnummern und greift zudem auch kurz vor dem Wählvorgang regulierend ein, um auch diejenigen Dialer zu entdecken, die sich nicht im DFÜ-Netzwerk verewigen. Zudem können Sie optional auch alle Zugriffe auf die Capi-Schnittstelle überwachen lassen.

Doch auch ohne diesen intelligenten Zusatzschutz ist der Sicherheitsfaktor hoch, da das Tool die gängigen Rufnummern erkennt und sich auch nicht von einer Netzvorwahl wie 01033 aus dem Konzept bringen lässt. Zudem können Sie die Liste der gesperrten Nummern um eigene Einträge erweitern und auch festlegen, in welchen Intervallen das DFÜ-Netzwerk nach verdächtigen Verbindungen durchsucht werden soll.

Dial Guard 1.62

Das englischsprachige, recht schlicht gehaltene Dial Guard 1.62 für Windows 95/98/ME, NT 4, 2000 und XP (unter **www.dialguard.com/eng/** oder ◉ auf Heft-CD, Registriergebühr: 20 Euro) kann 14 Tage lang kostenlos und ohne jegliche Einschränkung getestet werden. Nach der Installation müssen Sie selbst festlegen, welche DFÜ-Netzwerkverbindungen die Telefonleitung benutzen dürfen. Zudem müssen auch alle Rufnummern vom Anwender selbst eingegeben werden.

Hierbei unterscheidet das Tool zwischen erlaubten Telefonnummern („Authorized Numbers“) und Vorwahlen („Allow these prefixes“) und niemals zu verwendenden Zahlenfolgen („Never allow calls to numbers beginning with“). Erfahrenen Anwendern kommt dies sehr entgegen, da sie dadurch von permanenten Falschmeldungen verschont bleiben und auch vor – hierzulande zugegebenermaßen selten anzutreffenden – Dialern geschützt sind, die zwar keine 0190-Nummer anwählen, dafür aber Ferngespräche zum Beispiel mit den Cook-Inseln oder Vanuatu führen.

Um auch dann für maximalen Schutz zu sorgen, wenn mehrere Personen einen Rechner nutzen, kann der Einstellungsdialog durch ein Passwort gesichert werden; alle Programmeingriffe werden automatisch in einer Protokolldatei gesichert.

Pop Up Killer & Dialer Detector 2.02

Wie es der Programmname bereits verrät, handelt es sich bei diesem Shareware-Tool für Windows 95/98/ME und XP (◉ auf Heft-CD oder Download unter **www.boesherz-online.de**, Registriergebühr: 7 Euro) um eine Mischung aus Werbeblocker und Anti-Dialer-Tool. Letztere Funktion umfasst die regelmäßige Überprüfung des DFÜ-Netzwerks auf verdächtige Einträge sowie die Warnung vor dem Herstellen verdächtiger Verbindungen. Wie oft dabei nach ominösen Einträgen gesucht wird, lässt sich exakt einstellen; eine eigenhändige Erweiterung der unerwünschten Rufnummern ist ebenfalls möglich. Ein großes Plus: Der Pop Up Killer & Dialer Detector 2.02 ist bereits jetzt in der Lage, 0900-Rufnummern (werden die 0190-Dienste ablösen) zu erkennen und abzublocken.

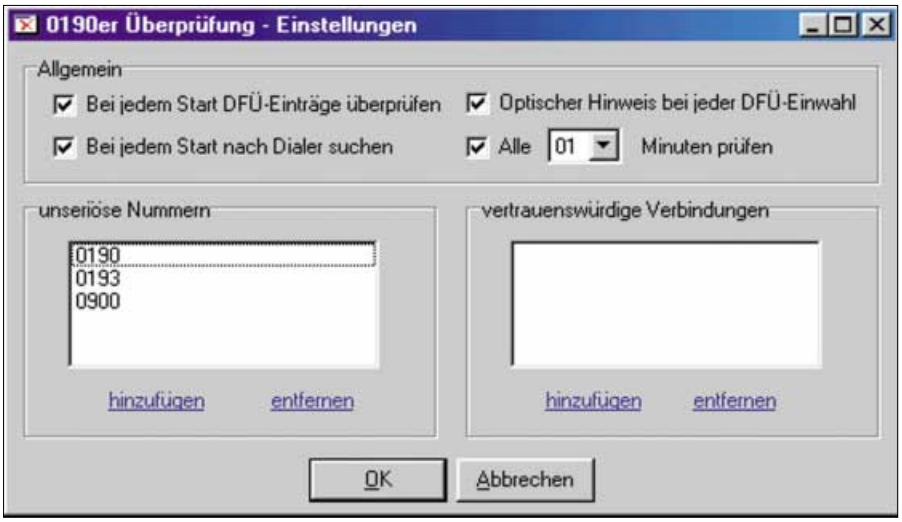
Die auf unserem Testrechner eingespielten Dialer wurden allesamt erkannt; eine Maskierung mittels vorgeschaltener Netzbetreiberrufnummer konnte das Programm nicht überlisten. Zwei getrennte Protokolldateien (jeweils für abgeblockte Pop-up-Fenster und Einwahlversuche) informieren über die durchgeführten Aktionen.

Smart Surfer 2.30

Das von den Betreibern des großen deutschsprachigen Internet-Portals Web.de kostenlos zur Verfügung gestellte Anti-Dialer-Tool Smart Surfer 2.30 (◉ auf Heft-CD, für Windows 95/98/ME und XP, neueste Version unter **http://smartsurfer.web.de**) dient in erster Linie als eine Art Least-Cost-Router, der Ihnen die jeweils günstigste Internet-Verbindung vorschlägt und zudem automatisch ein eventuell vorhandenes Web.de-Mailkonto abfragt.

Dementsprechend werden Sie während der Installation nach bevorzugtem Gerät, Wähl-String und Zugangsdaten gefragt.

Ist der Einrichtungsvorgang einmal überstanden, kommt die Anti-0190-Funktion ins Spiel und sucht sofort nach verdächtigen Einträgen im DFÜ-Netzwerk. Im Test meldete es alle von uns selbst eingespielten 0190-Dialer, selbst bei Vorschaltung einer Netzbetreibervorwahl. Nur das Löschen der beanstandeten Verbindungen muss in Eigenregie erfolgen.



Für die Zukunft gerüstet: Als eines von wenigen Programmen kennt der Pop Up Killer & Dialer Detector 2.02 bereits 0900-Rufnummern, die über kurz oder lang die 0190-Dialer ablösen werden

Yaw 3.01

Trotz des etwas seltsamen Programmnamens (Yaw steht für „Yet Another Warner", salopp übersetzt bedeutet dies „nur ein weiterer 0190-Warner") gehört die Freeware Yaw 3.01 (◉ auf Heft-CD oder unter **www.trojaner-info.de/programme.shtml**) für Windows 95/98/ME, 2000 und XP zur absoluten Referenzklasse. Dieser gute Ruf hängt in erster Linie damit zusammen, dass der Herausgeber gleichzeitig eine der besten deutschen Websites (Trojaner-Info, **www.dialerhilfe.de**) zum Thema Security betreibt und somit genau weiß, worauf es ankommt.

So beschränkt sich das Tool nicht auf die Überwachung von DFÜ-Netzwerk sowie Capi- und Tapi-Schnittstelle, es fahndet auch auf lokalen Datenträgern und sogar im Arbeitsspeicher nach verdächtigen Programmen. Dabei kommen – ähnlich wie bei Virenscannern – spezielle Signaturen (in der aktuellen Version sind 810 solcher Muster implementiert) sowie eine heuristische Suchroutine zum Einsatz. Mit letzterer ist es sogar möglich, bisher noch unbekannte Dialer aufzuspüren und unschädlich zu machen.

Stefan Forster

Mit Yaw 3.01 zum Dialer-freien Rechner

Nach der einfachen Installation und dem ersten Programmstart finden Sie sich in der Reportdatei des Anti-Dialer-Tools wieder, in der alle durchgeführten Aktionen fein säuberlich aufgelistet sind. Zur besseren Übersicht werden abgeblockte Einwahlversuche farblich hervorgehoben.

Ihre erste Aufgabe besteht darin, nach einem neuen Datenbank-Update zu suchen. Dazu wechseln Sie zur Registerkarte „Hilfe und Updates" und klicken auf die Schaltfläche „Auf Updates prüfen". Ist der Button nicht aktiv, sind die Dialer-Signaturen auf dem neuesten Stand.

Zahlreiche Sicherheitsmechanismen: Yaw 3.01 minimiert die Dialer-Gefahr

Die weitere Konfiguration wird auf der Registerkarte „Einstellungen" durchgeführt. Hier sind vor allem die Optionen „YAW automatisch mit Windows starten", „DFÜ-Netzwerk permanent überwachen" und „Den Speicher auf Dialer überwachen" zu aktivieren, damit die maximale Sicherheitsstufe erreicht wird. Falls die Ressourcen Ihres Rechners begrenzt sind, können Sie zur Verbesserung der Leistung die beiden standardmäßig auf 1000 Millisekunden eingestellten Prüfintervalle für DFÜ-Netzwerk und Speicher auf einen höheren Wert einstellen.

Den Zugriff auf die im DFÜ-Netzwerk abgelegten Verbindungen erledigen Sie über das gleichnamige Register. Ein Klick mit der rechten Maustaste auf einen bestimmten Eintrag öffnet ein Kontextmenü, das Ihnen Optionen wie „Editieren", „Verbinden" und „Löschen" bereitstellt. Das ist sehr bedienerfreundlich, denn Sie müssen beim Bearbeiten einer Verbindung nicht erst das DFÜ-Netzwerk öffnen.

Haben Sie das Gefühl, dass sich trotz aller Schutzvorrichtungen doch ein Dialer auf Ihrem PC eingenistet hat, können Sie das Programm zu einer umfangreichen Suche veranlassen. Ein Klick auf die Registerkarte „Suche nach Dialern" öffnet einen Dialog, in dem Sie lokale, austauschbare und sogar Netzlaufwerke überprüfen können. Besonders vorsichtige Zeitgenossen markieren vor dem Scanvorgang auf der Registerkarte „Einstellungen" zusätzlich noch das Optionsfeld „Heuristik auch beim Laufwerksscan aktivieren" und starten die Suche nach verdächtigen Dateien mit „Scan starten". Dann ist Yaw sogar in der Lage, bisher unbekannte Dialer zu finden.

Wer suchet, der findet: Yaw 3.01 scannt auf Wunsch sogar die Festplatte nach Dialern

Die wichtigsten Verschlüsselungsverfahren

Schlüsselsuche

Angesichts der zahlreichen Verschlüsselungsmethoden hängt die Auswahl des Verfahrens von drei Faktoren ab: Sicherheit, Verschlüsselungsgeschwindigkeit und Einsatzgebiet.

Ein verschlüsseltes Dokument ist nur so sicher wie der verwendete Krypto-Algorithmus. Und dessen Qualität steht und fällt wiederum mit der Länge des Schlüssels, der sowohl beim Codieren als auch beim Decodieren zum Einsatz kommt. Angesichts dieses – stark vereinfachten – Grundprinzips stellt sich die berechtigte Frage, warum man nicht ausschließlich Schlüssel verwendet, deren Längen in Bereichen größer 10^{1000} angesiedelt sind. Die Antwort ist ganz einfach: Rechenzeit.

Denn je länger ein Schlüssel ist, desto langsamer laufen Ver- und Entschlüsselung ab. Und was bei Mails, die mittels Public Key Algorithmen codiert werden, noch zu verschmerzen ist, kommt für Echtzeitverschlüsselung nicht in Frage, da hier selbst im Nanosekundenbereich liegende Verzögerungen unerwünscht sind. Dementsprechend haben sich die Verschlüsselungsverfahren in die beiden Richtungen symmetrische (Secret-Key-Verfahren) sowie asymmetrische Verschlüsselung (Public-Key-Verfahren) entwickelt. Dazwischen gibt es noch die so genannten hybriden Verschlüsselungsverfahren, also Algorithmen, die beide Formen der Kryptografie in sich vereinen. Im folgenden Artikel stellen wir Ihnen die jeweils wichtigsten Vertreter vor und erklären, wie sich die einzelnen Verfahren unterscheiden; einen Workshop zu PGP finden Sie ab ▷ Seite 124, und die wichtigsten Krypto-Tools bringen wir Ihnen ab ▷ Seite 128 näher.

Info: Krypto-Verfahren

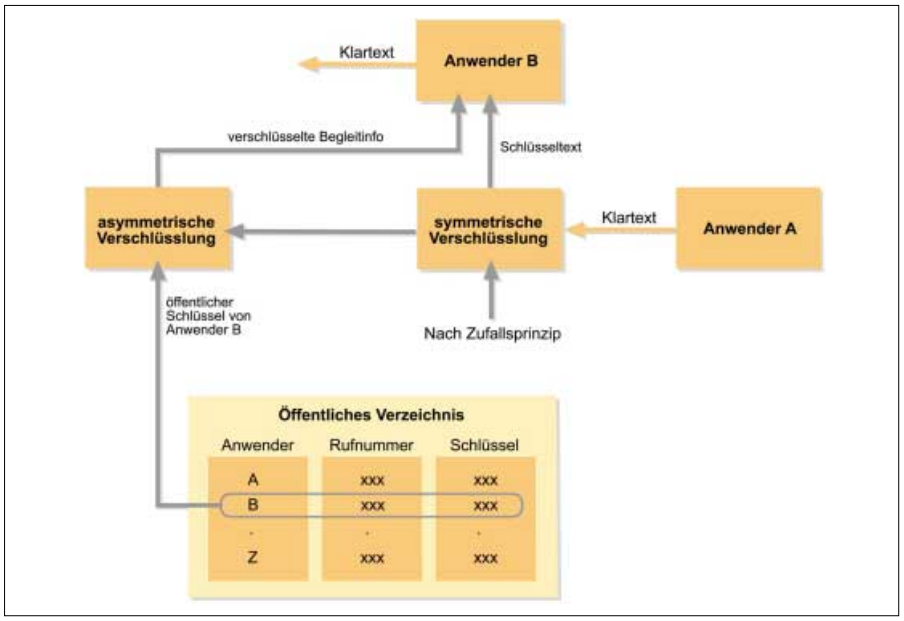
Ob symmetrische, asymmetrische oder gar hybride Verschlüsselung – wer lokale Daten und Mailnachrichten vor unbefugten Zugriffen schützen will, hat auf den ersten Blick die Qual der Wahl. De facto ist die richtige Wahl einfach, da nicht jeder Algorithmus für alle denkbaren Anwendungsfälle geeignet ist.

Verschlüsselung: Symmetrisch oder asymmetrisch?

Der signifikante Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung lässt sich anhand des Umgangs mit den beiden zum Ver- und Entschlüsseln benötigten Schlüsseln verdeutlichen. Symmetrische Algorithmen wie beispielsweise AES/Rijndael, Blowfish und Cast setzen entweder einen identischen Schlüssel zum De- und Encodieren von Daten ein oder erlauben es, den Chiffrierschlüssel aus dem Dechiffrierschlüssel abzuleiten (und umgekehrt). Dies hat den Vorteil, dass die Anwender nicht mit

mehreren Schlüsselpaaren hantieren müssen. Um Missbrauch vorzubeugen, empfehlen alle Hersteller, den Schlüsseltausch persönlich vorzunehmen – bei internationalen Kontakten ein Ding der Unmöglichkeit. Aus genau diesem Grund werden symmetrische Algorithmen nahezu ausschließlich zur Verschlüsselung lokaler Daten verwendet.

Asymmetrische Verfahren (RSA und ECC) unterscheiden hingegen strikt zwischen privatem und öffentlichem Schlüssel. Das grundlegende Funktionsprinzip sieht so aus: Der Absender einer Nachricht codiert den Text mit Hilfe des öffentlichen Schlüssels (Public Key) des Empfängers und versendet die chiffrierte Nachricht per Mail. Der Adressat verwendet beim Dechiffrieren seinen ganz persönlichen, privaten Schlüssel (Private Key). So lässt sich auch dann sicher kommunizieren, wenn die benötigten Schlüssel nicht persönlich ausgetauscht wurden – ideal, um Mails zu schützen. Die folgenden Abschnitte geben einen Überblick über Vor- und Nachteile populärer Verschlüsselungsverfahren.



Zwei Passwörter im Einsatz: Bei der asymmetrischen Verschlüsselung verwendet Anwender A das öffentliche Kennwort von Anwender B zum Verschlüsseln. Letzterer entschlüsselt mit seinem privaten Key

Frei verfügbar: Blowfish/Twofish

Der vom US-Unternehmen Counterpane Labs (**www.counterpane.com**) im Jahre 1993 erstmals vorgestellte Blowfish-Algorithmus benutzt bei der symmetrischen Verschlüsselung der jeweils 64 Bit großen Datenblöcke variable Schlüssellängen zwischen 32 und 448 Bit. Dadurch lässt er sich exakt an die jeweilige Benutzerumgebung anpassen. Da die Verwendung des nicht durch ein Patent geschützten Algorithmus keine Lizenzgebühren kostet, setzen weit über 150 Security-Produkte wie Drive Crypt, 1 Passwort Pro und Gnu-PGP auf diese Methode.

Die direkte Weiterentwicklung von Blowfish ist Twofish. Dieser Algorithmus gehört zu den fünf Verfahren, die es bei der vom National Institute of Standards and Technology (NIST; **www.nist.gov**) durchgeführten Suche nach einem neuen Krypto-Standard bis in die Endausscheidung geschafft haben. Zu den Vorzügen von Twofish gehören eine verdoppelte Blockgröße (128 anstatt 64 Bit), variierende Schlüssellängen von 128, 192 und 256 Bit und ein beachtliches Verschlüsselungstempo. Und da auch dieser Algorithmus frei verwendbar ist, wird Twofish sowohl bei Verschlüsselungs-Software als auch in Hardware-basierten Systemen wie Smartcards eingesetzt.

Der Außenseiter: Cast 128/256

Wie bei Blowfish handelt es sich auch bei dem von Carlisle Adams entwickelten Verfahren Cast 128 (**www.entrust.com**) um eine Verschlüsselung, bei der 64 Bit große Datenblöcke mit einem symmetrischen Schlüssel (maximale Länge 128 Bit) codiert werden. Bei der Verschlüsselung werden im Gegensatz zum Data Encryption Standard DES keine Permutationen (siehe unten), sondern Additionen und Substraktionen durchgeführt. Dies hat den großen Nachteil, dass die Geschwindigkeit bei weitem nicht so hoch ist – ein Einsatz in zeitkritischen Systemen also

Info: Symmetrische Verschlüsselungsverfahren

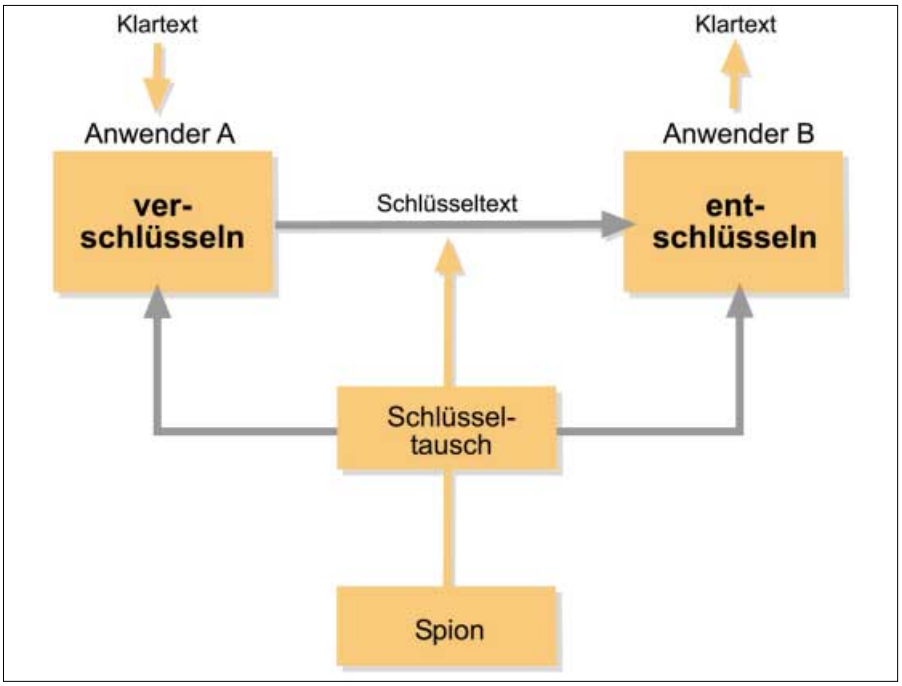
Um Ihnen einen Überblick über die unterschiedlichen Blockgrößen und Schlüssellängen der wichtigsten symmetrischen Verschlüsselungsverfahren zu geben, listen wir in der folgenden Tabelle die Eckdaten von 16 Algorithmen auf.

Verfahren	Blockgröße(n)	Schlüssellänge(n)
Advanced Encryption Standard AES (Rijndael)	128, 192 und 256 Bit	128, 192 und 256 Bit
Blowfish	64 Bit	32–448 Bit
Cast 128	64 Bit	128 Bit
Cast 256	64 Bit	256 Bit
Data Encryption Standard DES	64 Bit	56 Bit
Fast Encryption Algorithm Feal	64 Bit	64 Bit
International Data Encryption Algorithm Idea	64 Bit	128 Bit
Mars	128 Bit	128, 192 und 256 Bit
RC2	64 Bit	40 Bit
RC4	keine Angaben	128 Bit
RC5/RC6	32, 64 und 128 Bit	maximal 2040 Bit
Secure And Fast Encryption Routine Safer	64 Bit	64 Bit
Serpent	128 Bit	128, 192 und 256 Bit
Skipjack	64 Bit	80 Bit
Triple DES	64 Bit	168 Bit
Twofish	128 Bit	128, 192 und 256 Bit

nicht in Frage kommt. Bei Anwendungen, bei denen die Arbeitsgeschwindigkeit hingegen eine sekundäre Rolle spielt, wird Cast 128 gerne eingesetzt. Das mit einem symmetrischen Schlüssel von 256 Bit ausgestattete Verschlüsselungsverfahren Cast 256 wurde speziell für die Ausschreibung im Rahmen des Advanced Encryption Standard AES angepasst. Aufgrund der Geschwindigkeitsproblematik wurde Cast 256 allerdings bereits in der zweiten Entscheidungsrunde aussortiert.

Der Oldie: DES – Data Encryption Standard – und Triple DES

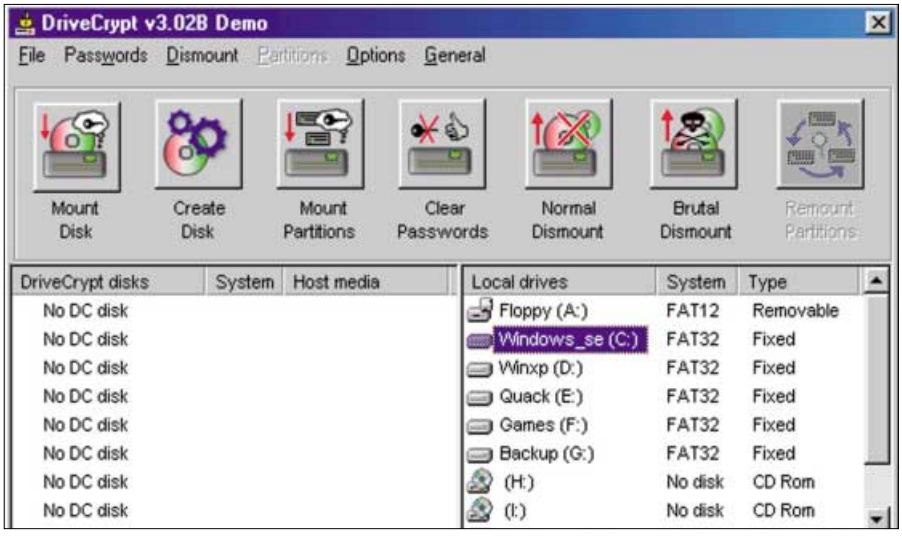
Das mit einer Schlüssellänge von 56 Bit arbeitende, symmetrische Verschlüsselungsverfahren gilt als Vorreiter des heutzutage gültigen Standards AES. Bereits Mitte der 1970er Jahre wurde DES von den staatlichen Stellen in den USA zum Verschlüsseln wichtiger Nachrichten verwendet. Der Algorithmus arbeitet mit der so genannten Produktverschlüsselung, bei der die eigentliche Verschlüsselung der 64 Bit großen Blöcke durch Substitution und Transposition (zusammen als Permutation bezeichnet) erzeugt wird. Doch die zunehmende Rechenleistung von Workstations und dann auch von PCs machte dem DES-Verfahren zu schaffen, und nach der ersten erfolgreichen Brute-Force-Attacke im Jahre 1999 war es mit der Sicherheit vorbei. So taugt DES heute höchstens noch als Anschauungsobjekt für angehende Mathematiker, Informatiker und Kryptologen. Die direkte Weiterentwicklung namens Triple DES setzt auf eine Schlüssellänge von 168 Bit (eben dreimal 56 Bit) und ist auch heute noch im Einsatz.



Nur ein Kennwort: Da Absender und Empfänger bei der symmetrischen Methode mit ein und demselben Passwort arbeiten, können Datenspione die Übermittlung des Schlüssels leichter abhören

Der Emporkömmling: AES – Advanced Encryption Standard

Das US-amerikanische National Institute of Standards and Technology veröffentlichte im Jahre 1997 eine Ausschreibung, um einen Nachfolger für das veraltete Verschlüsselungsverfahren DES zu finden. Das wichtigste Kriterium für den bereits vorab als Advanced Encryption Standard AES bezeichneten Algorithmus: Es mussten die Schlüssellängen 128, 192 und 256 Bit unterstützt werden. Nach diversen Ausleseverfahren kamen am Ende fünf Kandidaten (Mars, RC6, Serpent, Twofish und Rijndael) in die engere Wahl (Details dazu gibt es auf **http://csrc.nist.gov/encryption/aes/round2/r2algs-code.html**). Das Rennen machte dann der von Joan Daemen und Vincent Rijmen entwickelte Rijndael-Algorithmus (**www.esat.kuleuven.ac.be/~rijmen/rijndael/**), der seit dem 26. November 2001 als neuer Verschlüsselungsstandard von allen US-Regierungsstellen verwendet wird. AES/Rijndael basiert wie der Vorgänger DES auf der symmetrischen Verschlüsselung, setzt zusätzlich aber variable Block- und Schlüssellängen ein. Zurzeit werden sowohl bei den Schlüsseln als auch bei den Blöcken die Längen 128, 192 und 256 Bit unterstützt, die beliebige Kombination der einzelnen Längen ist ebenfalls möglich.



Sehr gerne eingesetzt: Da die Verwendung des Blowfish-Verfahrens kostenlos ist, setzen viele Krypto-Tools (hier Drive Crypt) auf die Qualitäten dieser Verschlüsselungsmethode

Militärgeprüft: RSA – Rivest-Shamir-Adleman

Das von Rivest, Shamir und Adleman entwickelte Public-Key-Verfahren RSA (**www.rsasecurity.com**) stellt so etwas wie den Standard der asymmetrischen Verschlüsselung dar und wird weltweit am häufigsten eingesetzt. Wie bei allen Methoden, bei der der Schlüssel öffentlich zugänglich ist, steht und fällt die Sicherheit mit

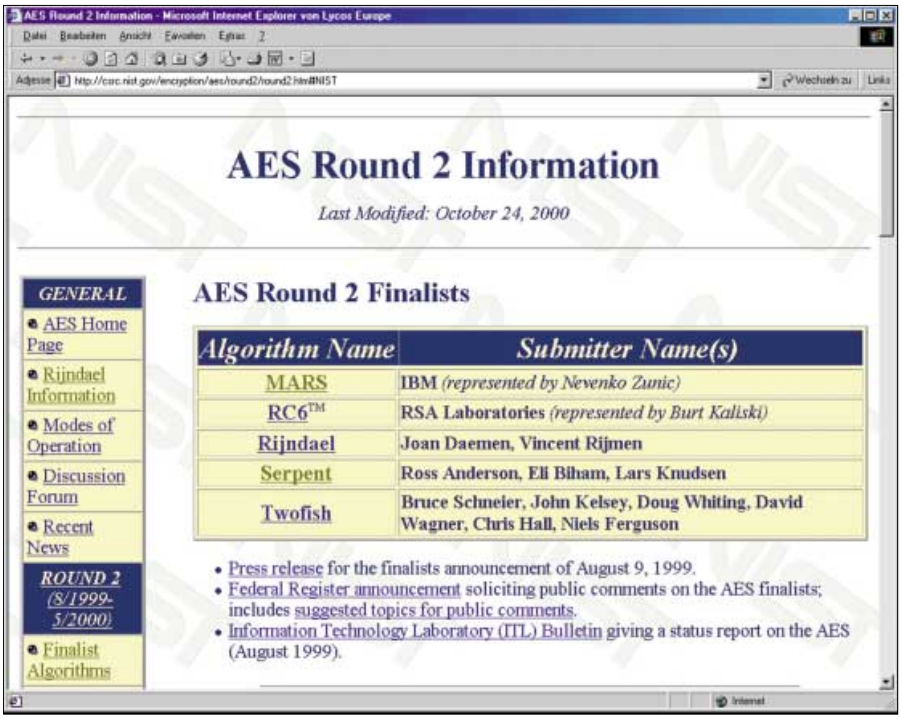
der Länge des Public Keys, der bei RSA durch eine sehr große, mindestens 200-stellige Primzahl dargestellt wird. Und diese in Bit angegebene Länge hängt wiederum davon ab, wie sensitiv die zu verschlüsselnden Daten sind. Während etwa im privaten Mailverkehr eine Schlüssellänge von 384 Bit völlig ausreichend ist, sollten geschäftliche Unterlagen mit 512 Bit codiert werden. Handelt es sich hingegen um streng geheime Daten wie diplomatische Depeschen oder militärische Informationen, sind Schlüssellängen von 1792 beziehungsweise 2048 Bit angebracht. Das deutsche Bundesamt für Sicherheit in der Informationstechnik BSI (**www.bsi.bund.de/esig/faq/practice.htm**) empfiehlt übrigens Schlüssellängen zwischen 1024 und 2048 Bit.

Für Karten: ECC - Ecliptic Curve Cryptography

Die im Jahre 1985 von Victor Miller und Neil Koblotz entwickelte Ecliptic Curve Cryptography ECC (**www.certicom.com/resources/ecc/ecc.html**) setzt als asymmetrisches Verschlüsselungsverfahren auf ein Schlüsselpaar aus privatem und öffentlichem Schlüssel. Bei der Verschlüsselung kommen anders als bei RSA aber keine Primzahlen, sondern elliptische Kurven (so genannte diskrete Logarithmen) zum Einsatz. Die Verwendung dieser mathematischen Funktionen hat den Vorteil, dass vergleichsweise kleine Schlüssel eingesetzt werden können, ohne dass die Sicherheit der codierten Nachrichten beeinträchtigt wird. Dafür steigt aber der Rechenaufwand an, was wiederum die Arbeitsgeschwindigkeit schmälert. Somit setzen die inzwischen mehr als 200 Lizenznehmer das ECC-Verfahren primär als Hardware-basierten Schutzmechanismus in Smartcards ein.

Hybride Verfahren zur Mailverschlüsselung

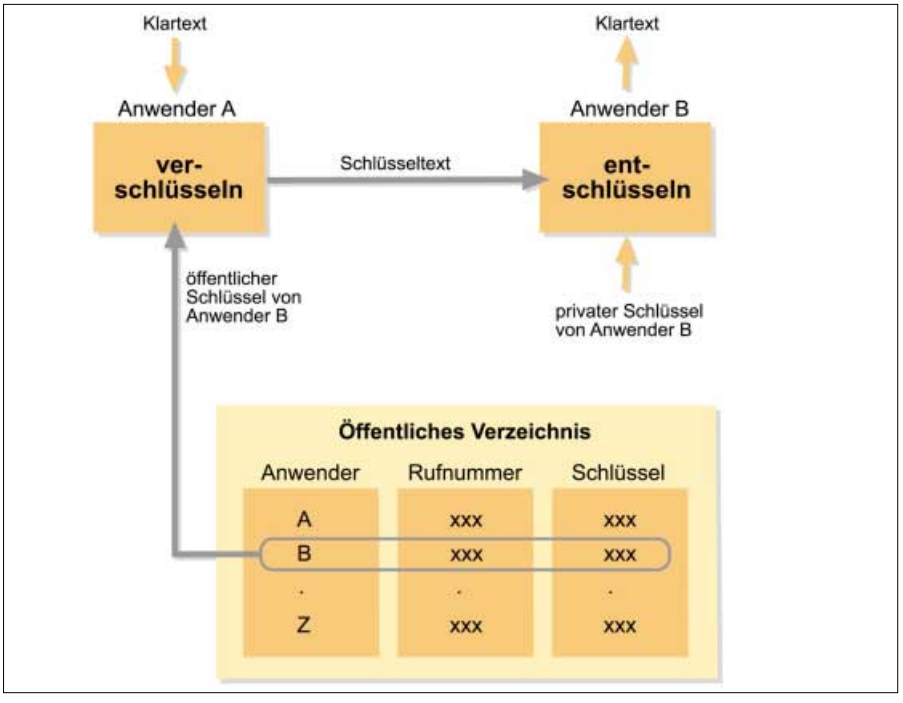
Hybride Verschlüsselungsalgorithmen, wie sie beispielsweise von Pretty Good Privacy PGP und Gnu-PGP genutzt werden, greifen beim Chiffrieren von Daten sowohl auf eine symmetrische Verschlüsselung als auch auf ein asymmetrisches Public-Key-Verfahren zurück. Der eigentliche Nachrichtentext wird zunächst mit einem symmetrischen, von



Fünf AES-Anwärter: Aus den fünf verbliebenen Kandidaten ging in der Finalrunde der Rijndael-Algorithmus als Sieger und damit als Advanced Encryption Standard hervor

einem Zufallsgenerator erzeugten Sitzungsschlüssel codiert. Dieser geheime Sitzungsschlüssel wird im zweiten Schritt mit dem öffentlich zugänglichen Schlüssel des Empfängers verschlüsselt. Danach werden der mit dem öffentlichen Schlüssel des Empfängers verschlüsselte Sitzungsschlüssel und die symmetrisch verschlüsselte Nachricht automatisch zusammengefasst. Der geheime Schlüssel des Empfängers wird zum Entschlüsseln des Sitzungsschlüssels verwendet, mit dem wiederum der ursprüngliche Nachrichtentext decodiert wird. PGP setzt hier gleich vier Verschlüsselungsverfahren (Idea, Triple DES, RSA und El Gamal) ein.

Stefan Forster



Kombination zweier Verfahren: Per Zufall wird bei Anwender A ein symmetrischer Schlüssel erzeugt, der mit dem öffentlichen Key von Anwender B verschlüsselt wird und zusammen mit dem Dokument verschickt wird

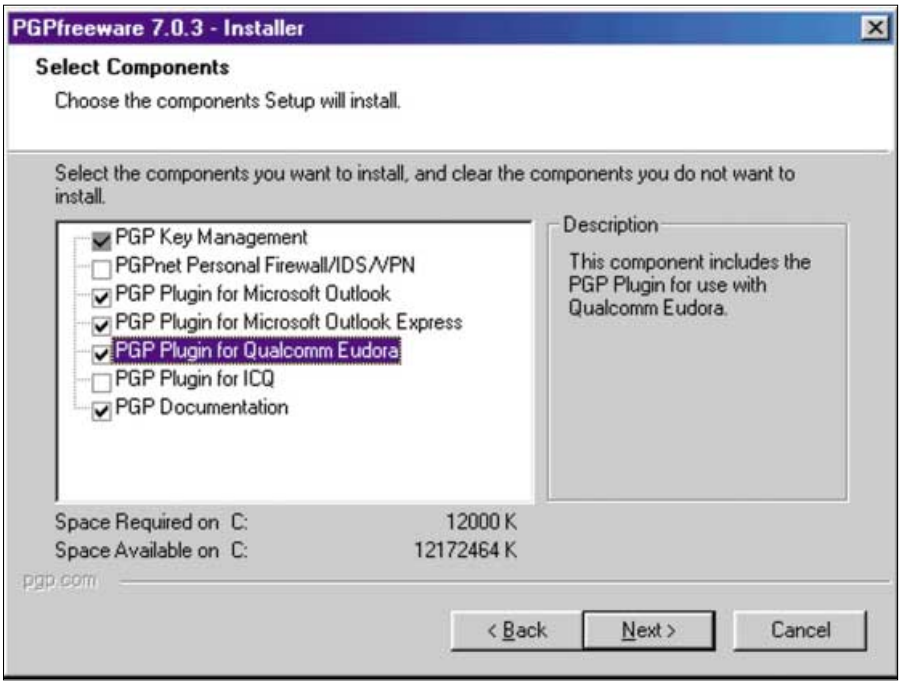
Nachrichten sichern mit PGP

E-Mail unknackbar

Wer seine Mails mit PGP verschlüsselt, muss sich keine Sorgen mehr um das digitale Briefgeheimnis machen, da solcherart chiffrierte Nachrichten als nahezu unknackbar gelten.

Die vom US-Amerikaner Phil Zimmermann entwickelte Freeware Pretty Good Privacy (PGP; Version 7.0.3 auf Heft-CD) ist seit Jahren erste Wahl in Sachen Verschlüsselung. Die Software kann auch auf eine bewegte Geschichte zurückblicken. So war es bis vor wenigen Jahren aufgrund rigider Exportbeschränkungen untersagt, funktionsfähige PGP-Versionen mit einer Schlüssellänge größer 64 Bit aus den USA auszuführen. Um diese Hürde zu umgehen, wurde der 6000 Seiten umfassende Quelltext ausgedruckt, in Europa von Hand eingescannt, und der so „neu geschriebene" Code wurde kompiliert (**www.pgpi.org/pgpi/project/scanning/**). Seit der Freigabe im Jahre 1999 kann sich jeder Interessierte die jeweils aktuellste Version direkt von der internationalen PGP-Website (**www.pgpi.org**) herunterladen und installieren.

Achtung: McAfee respektive die Muttergesellschaft Network Associates (**www.nai.com**) hat die Weiterentwicklung von Pretty Good Privacy aufgrund des kommerziellen Misserfolgs eingestellt, der Support wird noch bis Ende des Jahres aufrechterhalten.



Offen für die Zusammenarbeit: PGP 7.0.3 arbeitet standardmäßig bereits mit den wichtigsten Mail-Clients wie Microsoft Outlook und sogar mit dem Instant Messenger ICQ zusammen

Info: Sicher mit PGP

Das Krypto-Tool Pretty Good Privacy (PGP) stellt seit Jahren den Standard in Sachen Mailverschlüsselung dar. Einzig die Tatsache, dass die Handhabung selbst fortgeschrittene PC-Besitzer zum Lesen der Hilfedatei zwingt, steht einer regelmäßigen Nutzung im Wege. Dabei hat die aktuelle Version 7.0.3 nichts mehr mit den komplexen DOS-Anwendungen früherer Tage gemeinsam. Lesen Sie, wie Sie mit PGP arbeiten.

Sicherheitsauguren weisen darauf hin, dass der Quelltext der PGP-Versionen ab 6.5.8 nicht mehr offengelegt wurde. Dieser Umstand lässt in den Augen von Verschwörungstheoretikern darauf schließen, dass NAI ein so genanntes Backdoor-Programm eingebaut hat, über das die üblichen Verdächtigen FBI, CIA und NSA verschlüsselte Nachrichten ausspionieren können.

Installation des Verschlüsselungs-Tools

Obwohl die aktuellen Distributionen nur wenig mit den früheren, ausschließlich per Kommandozeilenparameter zu bedienenden Versionen gemeinsam haben, sind während der Installation einige Hürden zu nehmen. Und da die aktuellste Variante momentan nur in einer englischsprachigen Version angeboten wird, gehen wir detailliert auf die sach- und fachgerechte Installation ein. Bevor Sie aber mit dem Verschlüsselungsprogramm arbeiten, ist es empfehlenswert, zwei aktuelle Patches für Windows 95/98/ME, NT 4 und 2000 einzuspielen (**www.pgpi.org/products/pgp/versions/freeware/win32/7.0.3/**), die ein seit März 2001 bekanntes Sicherheitsproblem beheben.

Schon während des Installationsvorgangs werden Sie gefragt, ob Sie bereits über einen PGP-Schlüsselbund („PGP keyring") verfügen, den Sie auch weiterhin verwenden möchten. Ist das nicht der Fall – und davon gehen wir in diesem Workshop aus – entscheiden Sie sich für die Option „No, I'm a New User", klicken auf „Next" und geben den Pfad zum gewünschten Installationsverzeichnis ein. Im nächsten Schritt werden die einzu-

spielenden Komponenten ausgewählt, wobei die Installationsroutine automatisch die auf dem PC vorhandenen Mail-Clients identifiziert und die entsprechenden Plug-ins markiert. Optional dazu können Sie die Verschlüsselungs-Software aber auch zusammen mit dem Instant-Messaging-Programm ICQ nutzen. Die Installation des Moduls „PGP Net Personal Firewall“ ist nicht ratsam, da dieses Security-Tool nicht ausgereift ist.

Wichtig: Eingabe der globalen Schlüsselparameter

Die grundlegende Einrichtung erfolgt noch während der Installation. Im Dialog „PGP Key Generation Wizard“ klicken Sie auf die Schaltfläche „Expert“, um bei der Definition der Parameter eine größere Auswahl zu haben. Tippen Sie Namen und Mailadresse in die entsprechenden Felder ein, und wählen Sie dann den gewünschten Verschlüsselungsalgorithmus. Zur Auswahl stehen „Diffie-Hellman/DSS“, „RSA“ und „RSA Legacy“ (auf Deutsch: originärer RSA-Algorithmus). Der Unterschied zwischen beiden letztgenannten Verfahren besteht darin, dass das reine RSA-Verfahren nicht mit älteren PGP-Versionen zusammenarbeitet. Bei der Schlüssellänge gilt die Faustregel, nach der ein längerer Schlüssel zwar sicherer ist, dafür aber Abstriche bei der Arbeitsgeschwindigkeit hinzunehmen sind.

Wir entscheiden uns für das Krypro-Verfahren „RSA“ mit einer Schlüssellänge von „2048“ Bit und einem Verfallsdatum („Key expiration“) von 12 Monaten. Nach Ablauf dieses Datums verliert der öffentliche Schlüssel („Public Key“) seine Gültigkeit und kann nicht mehr zum Verschlüsseln verwendet werden. Doch als Hilfsmittel zur Überprüfung der digitalen Unterschrift kann dieser entwertete Schlüssel nach wie vor genutzt werden. Auf den privaten Schlüssel („Private Key“) übertragen bedeutet dies, dass mit Hilfe eines veralteten Schlüssels Nachrichten zwar dechiffriert, aber nicht mehr unterzeichnet werden können.

Nach einem Klick auf „Weiter“ geht es an die Definition des Passworts, mit dem der von Ihnen verwendete private Schlüssel vor unbefugten Zugriffen geschützt wird. Das Programm weist Sie darauf hin, dass das Passwort aus mindestens acht Zeichen bestehen soll und keinesfalls aufgeschrieben oder sonst wie gespeichert werden darf. Der blaue Fortschrittsbalken

Keine Gewissensfrage: Als Verschlüsselungsmethode stehen RSA und Diffie-Hellman/DSS bereit

macht Sie während der Eingabe übrigens auf die Knack-Sicherheit des eingegebenen Codes aufmerksam. Mit „Weiter“ veranlassen Sie das Programm dazu, Schlüssel und Unterschlüssel zu generieren. Mit „Fertigstellen“ schließen Sie den Wizard und starten dann den Rechner neu.

Schlüssel generieren: Auch in Extra-Komponente möglich

Die Generierung eines Schlüsselpaares kann aber auch direkt in der Programmkomponente „PGP Keys“ durchgeführt werden. Hierzu wählen Sie im Menü „Keys“ den Befehl „New Keys“ und folgen den Anweisungen des „PGP Key Generation Wizard“.

Achtung: Auch wenn die Generierung neuer Schlüsselpaare im Handumdrehen erledigt ist, sollte Sie das nicht dazu verleiten, gleich einen ganzen Schwung neuer Keys anzulegen. Denn das Grundprinzip der Public-Key-Verschlüsselung basiert auf der Eindeutigkeit, Identifizierbarkeit und Vertrauenswürdigkeit des Schlüsselbesitzers, mehrere Schlüsselpaare sind diesbezüglich kontraproduktiv. Erschwerend kommt hier die Tatsache hinzu, dass Sie sich für jedes Schlüsselpaar ein neues Passwort merken müssen.

Programmoptionen: Geschickt auswählen und anpassen

Das PGP-Kontrollmenü erreichen Sie über das Taskleisten-Icon und den Befehl „Options“. Aktivieren Sie die Registerkarte „Advanced“, und überprüfen Sie, ob die Option „Automatic keyring backup when PGP keys closes“ aktiviert ist. Dieses Backup ist deswegen wichtig, damit Ihr Schlüsselring im Falle eines Festplatten-

Diese Mailprogramme arbeiten mit PGP 7

Da nicht jeder Anwender mit Microsoft Outlook Express arbeitet, listen wir in der folgenden Aufstellung die gängigsten Mailprogramme auf, die PGP 7 entweder standardmäßig unterstützen oder die zumindest mit Hilfe eines Plug-ins zur Zusammenarbeit bewegt werden können.

Programm	Version	Hersteller	PGP-Unterstützung	Web-Adresse
Eudora	4.x	Qualcomm	standardmäßig	www.eudora.com
Eudora	5.x	Qualcomm	standardmäßig	www.eudora.com
Lotus Notes	4.5x	Lotus	standardmäßig	www.lotus.com
Lotus Notes	4.6x	Lotus	standardmäßig	www.lotus.com
Lotus Notes	R5	Lotus	standardmäßig	www.lotus.com
Netscape Messenger	4.5 bis 4.7.9	Netscape	Plug-in erforderlich	http://bear-software.freeservers.com/downloads.html
Outlook Express	4.x	Microsoft	standardmäßig	www.microsoft.de
Outlook Express	5.x	Microsoft	standardmäßig	www.microsoft.de
Outlook	97	Microsoft	standardmäßig	www.microsoft.de
Outlook	98	Microsoft	standardmäßig	www.microsoft.de
Outlook	2000	Microsoft	standardmäßig	www.microsoft.de
Outlook	XP	Microsoft	standardmäßig	www.microsoft.de
Pegasus Mail	4.0x	David Harris	Plug-in erforderlich	www.pmpgp.de/pmpgp/anleitung.htm
Pegasus Mail	3.x	David Harris	Plug-in erforderlich	http://community.wow.net/grt/qdpgp.html

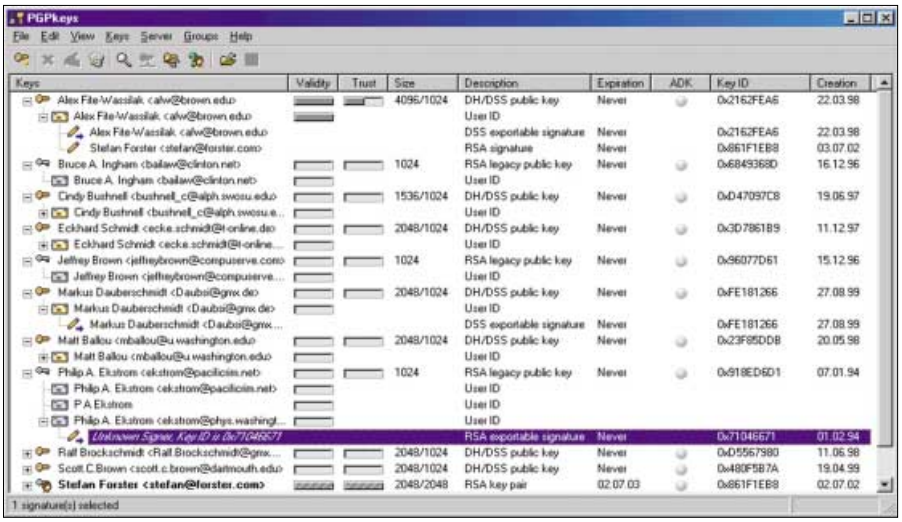
defekts oder Virenbefalls nicht verloren geht. Standardmäßig ist hier die Einstellung „Backup to keyring folder“ vorgegeben (die Sicherheitskopie wird im gleichen Verzeichnis wie der Schlüsselring gespeichert); weitaus sicherer ist es, das Backup auf einer anderen Partition oder gleich auf Diskette anzulegen. Falls gewünscht, können Sie das vorgegebene Standardverzeichnis – „C:\Eigene Dateien\PGP“ – für den öffentlichen (PUBRING.PKR) und privaten Schlüsselring (SECRING.PKR) jederzeit über das Register „Files“ an die eigenen Wünsche anpassen. Ein zusätzlicher Verschleierungstrick: Kopieren Sie die Datei SECRING.PKR in das Windows-Verzeichnis, und benennen Sie sie zur Tarnung um.

Die unter „Encryption“ zur Verfügung stehenden symmetrischen Verschlüsselungsverfahren haben nichts mit dem Codieren der eigentlichen Nachrichten zu tun, sondern kommen ausschließlich bei der Verschlüsselung Ihrer PGP-Schlüssel zum Einsatz. Ebenfalls im Register „Advanced“ sind bei „Trust Model“ zwei Optionen untergebracht, die sich um die grafische Darstellung der öffentlichen Schlüssel im Keyring kümmern. Ist das Feature „Display marginal validity level“ nicht aktiv, werden Schlüssel entweder als gültig („valid“) oder ungültig („invalid“) abgetan und durch ein grünes oder rotes Icon gekennzeichnet. Bei aktivierter Option zeigt das Programm hingegen die Vertrauenswürdigkeit an. Analog dazu können Sie nicht 100 Prozent sichere Schlüssel durch Auswahl des Befehls „Treat marginally valid keys as invalid“ automatisch als ungültig kennzeichnen.

Eudora: PGP leistet auch hier ganze Arbeit

Wer mit dem Mail-Client Eudora arbeitet, findet auf der Registerkarte „Email“ eine ganze Reihe zusätzlicher Optionen, die ausschließlich auf dieses Programm zugeschnitten sind. Beispielsweise bewirkt die Aktivierung der Option „Use PGP/MIME when sending email“ eine automatische Verschlüsselung aller Mails und Datei-Anlagen. Dieser Automatismus erhöht zwar die Sicherheit, kann aber bei Empfängern, die nicht mit dem Eudora-Mailer arbeiten oder ein anderes, zum Standard PGP/MIME inkompatibles Programm einsetzen, zu Verwirrung führen. Das Gleiche gilt übrigens auch für die Funktion „Sign new messages by default“. Weitaus besser ist es, sich für die zweite Eudora-typische Option „Encrypt new messages by default“ zu entscheiden, da auch dies eine automatische Codierung aller ausgehenden Mails und Anlagen bewirkt. Der Befehl „Automatically decrypt/verify when opening messages“ sollte unabhängig vom verwendeten Mail-Client aktiviert werden, da die automatische Dechiffrierung den Arbeitsaufwand minimiert.

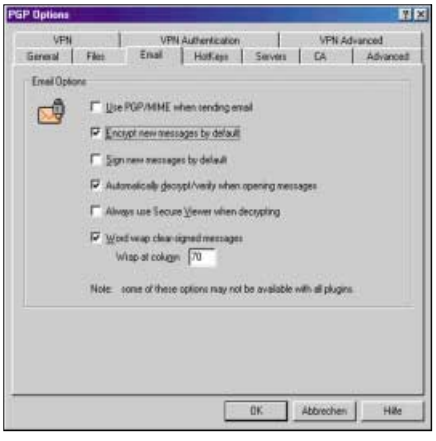
Speziell auf Profi-Anwender, die tagtäglich mit streng geheimen Dokumenten hantieren, ist das Sicherheits-Feature „Always use Secure Viewer when decrypting“ zugeschnitten. Hierbei werden die entschlüsselten Nachrichten in einem Extra-Fenster, unter Verwendung einer ganz speziellen Schriftart, angezeigt. Dieser Font ist so konzipiert, dass die Klartextmeldungen nicht durch „Tempest“-Attacken („Abhören“ der elektromagnetischen Signale, die von Monitor und Tastatur abgestrahlt werden) in Erfahrung gebracht werden können. Der große Nachteil: Es gibt keinerlei Möglichkeit, die dechiffrierten Nachrichtentexte in unverschlüsselter Form zu speichern.



Virtueller Schlüsselbund: In Ihrem Public Keyring sind alle vom Online-Server heruntergeladenen öffentlichen PGP-Schlüssel lokal auf Ihrem PC zusammengefasst und gespeichert

Gute Ordnung: So verwalten Sie Ihre Schlüsselringe

Ein Klick auf das Tray-Icon öffnet das PGP-Menü, in dem Sie den Befehl „PGP Keys“ wählen, um die Schlüsselverwaltung aufzurufen. Haben Sie schon während der Installation einen Schlüssel definiert, ist dieser neben einer Reihe von Beispielschlüsseln bereits aufgelistet. Löschen Sie zunächst die allesamt veralteten Test-Keys, um die Übersichtlichkeit zu erhöhen. Der nächste logische Schritt besteht darin, Ihren öffentlichen Schlüssel auf einem Key-Server abzulegen, damit dieser von anderen PGP-Nutzern in ihre Schlüsselringe aufgenommen werden kann. Dazu klicken Sie den Schlüsseleintrag mit der rechten Maustaste an, wählen den Kontextbefehl „Send to“ und wählen einen Server aus der Liste aus. Die Bildschirmmeldung „Key(s) successfully uploaded to server“ zeigt die erfolgreiche Übertragung an. Alternativ ist es beispielsweise auch möglich, den Schlüssel in einer Datei abzulegen und diese an jede Mailnachricht anzuhängen, den Code mit Hilfe der Zwischenablage in den Nachrichtentext zu kopieren oder den Private Key per Drag & Drop direkt in die gewünschte Applikation zu ziehen.



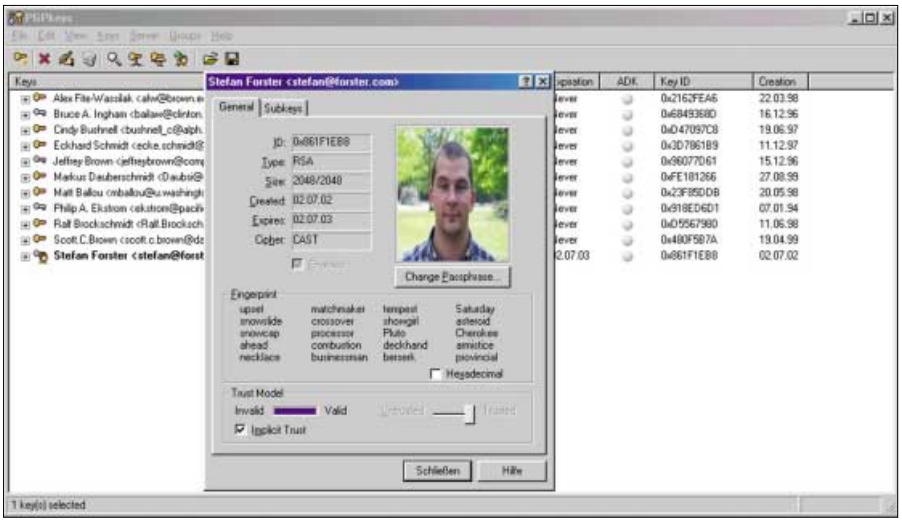
Maßgeschneiderte Nachrichtensicherheit: Mit den Mailoptionen passen Sie PGP-Plug-ins an

Private Schlüssel: Erst damit können Sie Mails lesen

Nachdem Sie Ihren öffentlichen Schlüssel auf einem Key-Server abgelegt haben, geht es darum, die Private Keys anderer PGP-Nutzer zu importieren. Und auch hier stehen Ihnen gleich mehrere Optionen zur Auswahl. Die mit Abstand am häufigsten genutzte Methode besteht darin, bereits auf Key-Servern veröffentlichte Schlüssel herunterzuladen. Dazu klicken Sie im Menü „Server“ auf den Befehl „Search“. In das Feld „User ID“ können Sie entweder den Benutzernamen oder die Mailadresse des gesuchten Teilnehmers eingeben, weitere Suchkriterien aktivieren Sie durch Klicks auf „More Choices“. Mit „Search“ starten Sie die Suche. Um einen Public Key an Ihren Schlüsselbund zu hängen, klicken Sie mit der rechten Maustaste auf den Eintrag und wählen den Befehl „Import to Local Keyring“. Darüber hinaus ist es aber auch möglich, öffentliche Schlüssel aus Mails und Schlüsseldateien zu importieren oder in Textform zugestellte Keys in die Zwischenablage zu kopieren und über die Befehlskette „Clipboard, Decrypt & Verify“ zu übernehmen.

Gültigkeit: Erst eine Prüfung sorgt für Sicherheit

Zum Abschluss der Konfiguration steht die Gültigkeitsüberprüfung der vom Key-Server heruntergeladenen Schlüssel an. Um sicherzugehen, dass ein öffentlicher Schlüssel auch tatsächlich echt ist, klicken Sie den Eintrag mit der rechten Maustaste an und wählen „Key Properties“. Im Register „General“ finden Sie unter „Fingerprint“ eine Liste mit 20 nach dem Zufallsprinzip zusammengestellten Wörtern, mit deren Hilfe Sie die Echtheit bestätigen können. Dazu müssen Sie mit der Gegenstelle Kontakt aufnehmen und die Übereinstimmung überprüfen. Ist dieser Weg nicht möglich, können Sie sich auch an unabhängige deutsche Zertifizierungsstellen wie DFN-PCA (**www.dfn-pca.de/certify/**), die Gesellschaft zur Förderung kommunikativer Medien (**www.mayn.de/dienste/ca/**) und die Arbeitsgruppe Zertifikationsinfrastruktur (**www.in-ca.individual.net**) wenden. Eine Liste internationaler Anlaufstellen finden Sie unter **www.pki-page.org**.



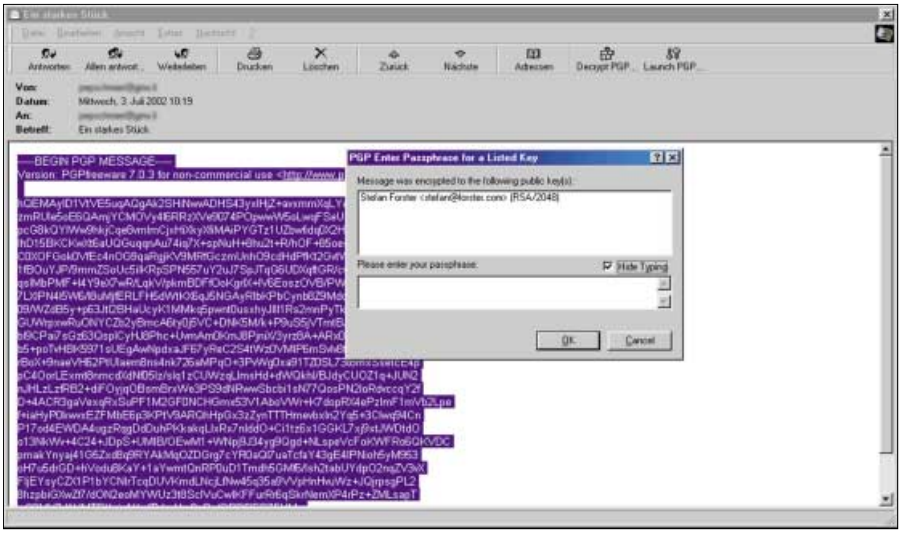
Nicht ohne Fingerabdruck: Die unter „Fingerprint“ angegebenen 20 Wörter dienen der eindeutigen Kennzeichnung eines Public Keys und helfen bei dessen Überprüfung

Mails verschlüsseln, dechiffrieren und signieren

In Outlook Express klicken Sie wie gewohnt auf das Icon „Neue E-Mail“, geben die Kontaktparameter ein, schreiben den Nachrichtentext und klicken dann auf die neue Menüschaltfläche „Encrypt Message (PGP)“. Ist der Empfänger der Mail nicht eindeutig einem Eintrag Ihres Schlüsselrings zuzuweisen, öffnet sich das entsprechende Auswahlfenster vor dem Versenden. Erhalten Sie eine chiffrierte Mail, ist die Decodierung ebenso einfach: Ein Doppelklick auf die Betreffzeile öffnet das Nachrichtenfenster, dessen Inhalt automatisch entschlüsselt wird – sofern Sie unseren Tipp befolgt und die entsprechende Option aktiviert haben. Sie müssen dazu lediglich Ihr persönliches Passwort eingeben. Ähnlich komfortabel verläuft aber auch das Signieren von Mails: einfach eine neue Mailnachricht schreiben, das Menü-Icon „Sign Message (PGP)“ wählen, auf „Senden“ klicken und Ihr Passwort eingeben. Die Verifizierung eintreffender Nachrichten, die von den Absendern signiert wurden, erfolgt vollautomatisch.

Darüber hinaus ist es aber problemlos möglich, lokale Daten, den Inhalt des gerade aktiven Programmfensters und auch die Zwischenablage mit zwei Mausklicks zu verschlüsseln oder mit einer Signatur zu versehen. Die Befehle lassen sich über die Programmkomponente „PGP Tools“ aufrufen. Somit ist sichergestellt, dass Sie jederzeit auf die Features der Verschlüsselungs-Software zugreifen können.

Stefan Forster



Keine Hexerei: Nach Eingabe der bei der Schlüsselgenerierung gewählten Passphrase wird der verschlüsselte Nachrichtentext decodiert, anschließend wird er angezeigt und kann kopiert werden

So verbergen Sie Ihre Daten vor neugierigen Blicken

Augenklappen

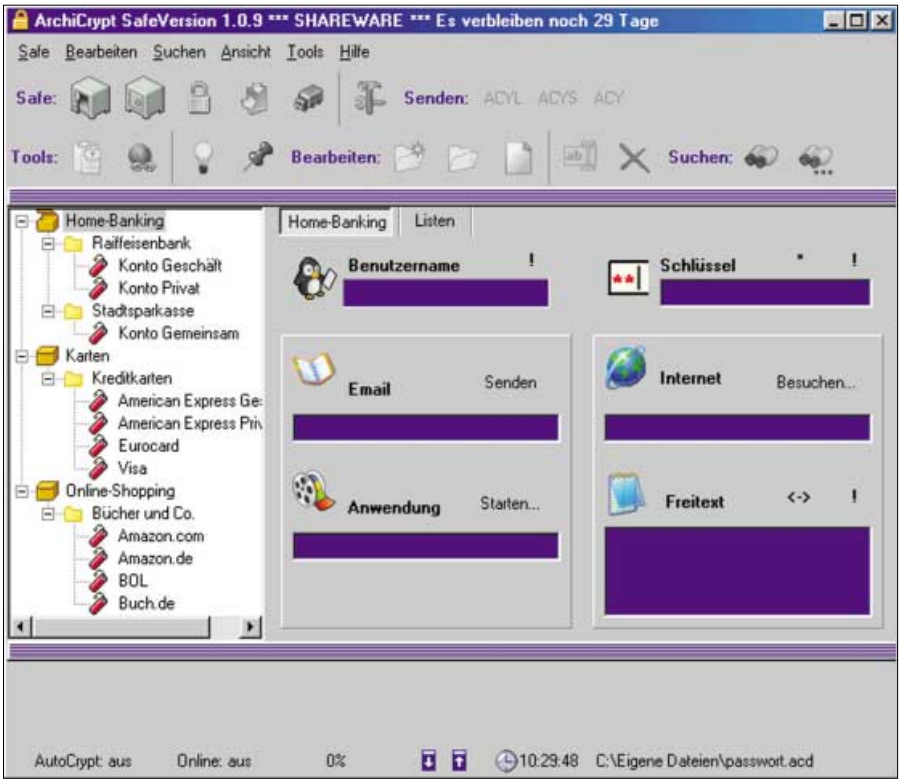
Ganz gleich ob Ihr PC von mehreren Personen genutzt wird oder Sie Ihre Daten vor Angreifern aus dem Internet schützen wollen – Sie brauchen die richtigen Verschlüsselungs-Tools.

▸Alle auf dem PC abgelegten Daten können – genügend kriminelle Energie und ein fundiertes Wissen vorausgesetzt – ausspioniert werden. Ob der Datendieb dabei in Ihrem Bürostuhl sitzt und auf Ihr neues TFT-Display blickt oder ob er sich über ein Sicherheitsloch Fernzugriff auf Ihren PC verschafft hat, ist sekundär.

Die Höhe der durch solche Zugriffe entstandenen Schäden hängt einzig und allein davon ab, welche Daten gestohlen oder ausspioniert wurden. Somit ist es klar, dass dieses Problem nicht nur rein geschäftlich genutzte Rechner betrifft, auf denen sich wichtige bis absolut geheime Daten befinden. Schließlich spielt es keine Rolle, ob ein Rechtsanwalt Notizen zu einem Erbrechtsverfahren auf seinem Notebook speichert, ein kaufmännischer Angestellter zu Hause Budgetberechnungen anstellt oder eine Personalsachbearbeiterin Arbeitsverträge per Mail versendet. Notebooks können gestohlen und ihr Inhalt dann ausgewertet, Privat-Rechner gehackt und Mails von fremden Personen gelesen werden.

Wirklich sicheren Schutz vor solchen Gefahren bieten spezielle Verschlüsselungs-Tools. Die Spanne der angebotenen Programme reicht von einfach gestrickten Lösungen zum Schutz häufig benötigter Passwörter über intelligente Stealth-Werkzeuge, mit deren Hilfe sich Verzeichnisse, Dateien und Mails verstecken oder codieren lassen, bis hin zu – laut Hersteller – unknackbaren Software-Paketen, die die Inhalte von Festplatten in Echtzeit ver- und entschlüsseln.

Bei der Auswahl der vorgestellten Programme haben wir in erster Linie auf die beiden wichtigen Kriterien Preis und Verfügbarkeit einer Demoversion geachtet. So können Sie sich die Tools in Ruhe ansehen, sich nach einer Testphase für Ihren Favoriten entscheiden und gleich mit dem Aufbau einer effizienten Abwehrstrategie beginnen. Achten Sie allerdings darauf, dass Sie beim Testen keine echten Daten, sondern wirklich nur Dummy-Dateien verwenden. Die beiden Themen Verschlüsselungsverfahren (▷Seite 120) und E-Mail-Sicherheit (▷Seite 124) werden in gesonderten Artikeln behandelt.



Passwortverwaltung mit Pep: Die Shareware Crypt Safe 1.0.9 beschränkt sich nicht auf das Speichern von Kennwörtern, sondern bietet auch eine integrierte Verschlüsselung

Info: Verschlüsselung

Dass die Verschlüsselung nicht zwangsläufig nur bei der Mailkorrespondenz zum Einsatz kommt, ist allgemein bekannt. Allerdings wissen nicht alle PC-Besitzer, welche Möglichkeiten ihnen offen stehen, um die auf dem eigenen PC abgelegten Daten vor den Augen Unbefugter zu schützen. Wir liefern Ihnen die nötigen Infos – und viele Tools ◉ auf Heft-CD.

So schützen Sie Ihre Passwörter

Ob Home-Banking, Online-Shopping oder Web-Mails – sehr viele der täglich angesteuerten Internet-Seiten verlangen nach Passwort und Benutzerkennung. Wer hier den Überblick behalten und die sensitiven Daten gleichzeitig vor neugierigen Blicken schützen möchte, kommt nicht um den Einsatz eines Tools zur Verwaltung von Passwörtern herum.

1 Passwort Pro 3.0

Das auch in einer nicht ganz so leistungsfähigen Freeware-Version angebotene 1 Passwort Pro 3.0 für Windows 95/98/ME, NT 4, 2000 und XP (512 KB, **www.1pw.de** oder ◉ auf Heft-CD, Registriergebühr: 5 Euro) glänzt durch die Verwendung von gleich sechs Verschlüsselungsverfahren mit unterschiedlichen Schlüssellängen. Ob Blowfish (mit einer maximalen Schlüssellänge von 448 Bit), Gost (256 Bit) oder RC2 (1024 Bit) – der Programmierer weist auf seiner Website darauf hin, dass noch keiner der eingesetzten Algorithmen jemals geknackt wurde.

Die so geschützten Passwörter können in beliebig viele Rubriken unterteilt, in eines von vier Formaten (CSV, TXT, XML und HTML) exportiert und zudem in einer Backup-Datei gesichert werden. Praktisch: Das Tool lässt sich von mehreren Benutzern verwenden, wobei die einzelnen Passwortlisten wiederum durch ein Kennwort vor Missbrauch geschützt sind.

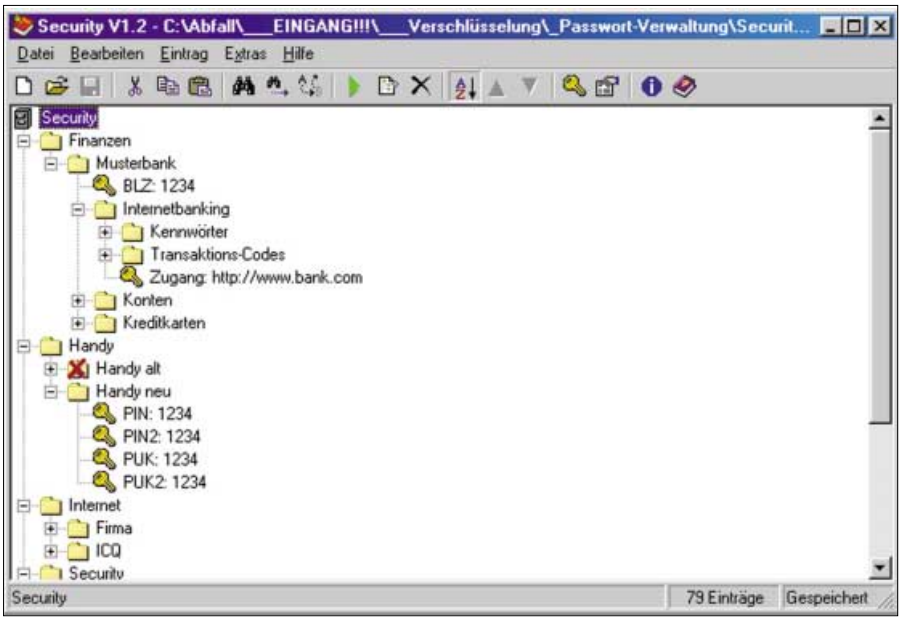
Archi Crypt Safe 1.0.9

Im Gegensatz zu nahezu allen anderen hier vorgestellten Passwortmanagern versteht sich Archi Crypt Safe 1.0.9 für Windows 98/ME, 2000 und XP (3,42 MB, **www.archicrypt.com/textACS.htm**, ◉ auf Heft-CD, Registriergebühr: 17 Euro) als Kombination aus Datensafe und Kennwort-Verwaltung. Alle gespeicherten Daten werden nach dem aktuellen Advanced Encryption Standard (AES) mit 256 Bit verschlüsselt; der Zugangsschutz zum Programm kann entweder per Key Disk oder durch ein herkömmliches Passwort geregelt werden. Hier können Sie auf den integrierten Generator zugreifen, mit dessen Hilfe Sie unknackbare Zugangscodes generieren. Ein weiteres Plus des Programms: Da sich beliebig viele Passwort-Safes anlegen lassen, eignet sich das Tool besonders für den Einsatz auf Rechnern, die abwechselnd von mehreren Personen genutzt werden.

Passwort Keeper 1.14

Das selbst unter einem älteren Betriebssystem im frischen XP-Look erstrahlende Passwort Keeper 1.14 für Windows 98/ME, 2000 und XP (2,11 MB, ◉ auf Heft-CD und unter **www.ag-software.de**, Registriergebühr: 10 Euro) ist aufgrund des überschaubaren Funktionsumfangs sehr einfach zu bedienen. Einfach Benutzername, Kennwort und eventuelle Notizen eingeben – schon werden die Zugangsdaten in der Datenbank abgelegt. Auf Seiten der Verschlüsselungsmethode kommen die beiden Algorithmen Blowfish (chiffriert die Datenbank) und SHA 1 (zuständig für das Programmpasswort) zum Einsatz.

Komplettiert wird der Funktionsumfang durch einen Passwortgenerator, der auf Knopfdruck ein bis zu 25 Zeichen langes Kennwort generiert. Eine Professional-Variante von Password Keeper ist in Planung, stand aber zu Redaktionsschluss noch nicht zur Verfügung.



Handlich und kostenlos: Mit der Freeware Security 1.2 lassen sich beliebig viele Passwörter einfach und komfortabel in einer übersichtlichen Bedienerführung verwalten und zuordnen

Security 1.2

Das unter der Freeware-Lizenz kostenlos vertriebene Security 1.2 für Windows 95/98/ME, NT 4, 2000 und XP (709 KB, **www.schmidtsoft.com/dt.htm**) greift bei der Verschlüsselung auf eine proprietäre Lösung zurück. Diese zeichnet sich vor allem durch die Tatsache aus, dass bei jedem neuen Eintrag ein neuer Schlüssel verwendet wird.

Die einzelnen Kombinationen aus Benutzername und Passwort werden in einer Baumstruktur gespeichert, was die Übersichtlichkeit erhöht. Ebenso gelungen: Da keine Installation nötig ist, können Sie Programm und Datenbank problemlos auf mehreren Rechnern nutzen. Alternativ dazu ist es aber auch möglich, die Einträge in eines von fünf Formaten zu exportieren.

Dateien vor neugierigen Augen verstecken

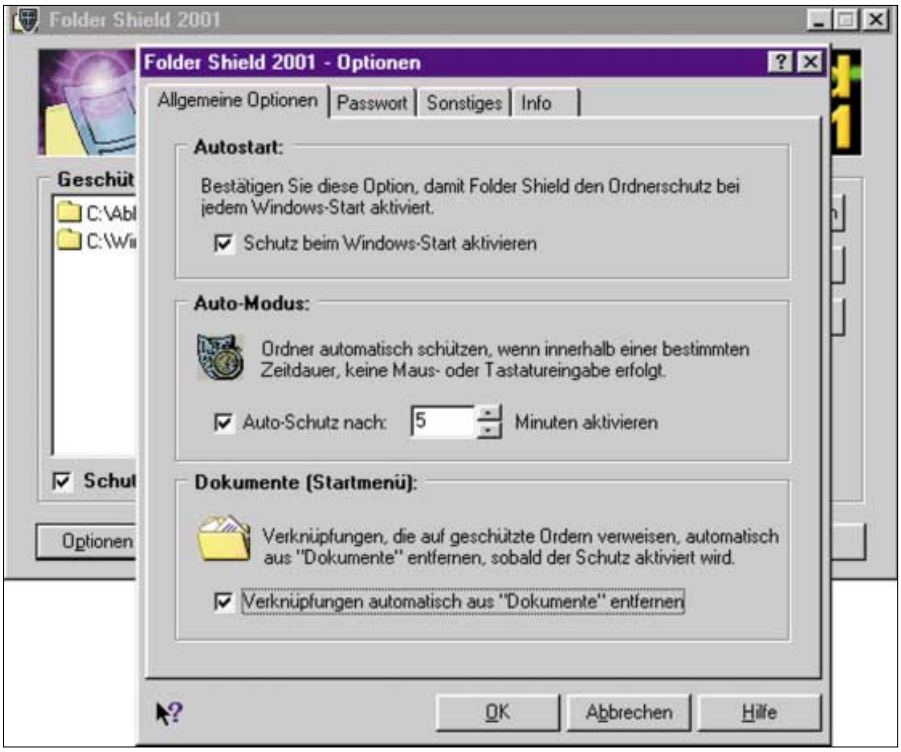
Das Verstecken von Dateien oder ganzen Verzeichnissen ist ein probates Mittel, um neugierige Schnüffler ins Leere laufen zu lassen. Denn wo keine Ordner mit aussagekräftigen Bezeichnungen wie „Steuererklärung“, „Rechnungen“ oder „Tagebuch“ zu finden sind, lohnt eine weitere Suche scheinbar kaum. Somit ist es nicht überraschend, dass es gleich mehrere ausgezeichnete Programme gibt, die sich dem Verstecken von Daten und Verzeichnissen verschrieben haben. Für welche der im Folgenden vorgestellten Lösungen Sie sich schlussendlich entscheiden, hängt im Grunde genommen nur von drei Faktoren ab: Sprache des Programms, Bedienkomfort und natürlich Verkaufspreis.

Camouflage 1.2.1

Nach der Installation der englischsprachigen Freeware Camouflage 1.2.1 für Windows 95/98/ME, NT 4 und 2000 (2,59 MB, **www.camouflagesoftware.com** und ◉ auf Heft-CD) empfiehlt es sich, zunächst einmal die im Kontextmenü der rechten Maustaste verankerten Befehle „Camouflage“ (Verstecken) und „Uncamouflage“

(Wiederherstellen) nach eigenem Gusto zu verändern. Die Wortwahl passt übrigens perfekt zum Grundprinzip, da Sie mit diesem Tool Daten nicht etwa nur unsichtbar machen, sondern in anderen Dateien verstecken und zusätzlich per Passwort schützen.

So ist es zum Beispiel problemlos möglich, eine Grafik unbemerkt in ein Word-Dokument einzubinden, ohne dass die Eigenschaften (nur Lesen) des Textes negativ beeinflusst werden. Und nicht einmal die Verschachtelung mehrerer getarnter Dateien ineinander stellt eine wesentliche Hürde dar. Um die Träger versteckter Dateien vor einer versehentlichen Änderung zu schützen, können Sie diese mit einem Schreibschutz versehen.



Sehr umsichtig: Folder Shield 2001 1.2 denkt sogar an die Windows-Verweise auf Dateien, die in versteckten Ordnern untergebracht sind, und entfernt diese auf Wunsch automatisch

Folder Shield 2001 1.2

Eines der einfacheren Programme, mit dem Sie Ordner und die darin abgelegten Dateien verbergen können, nennt sich Folder Shield 2001 1.2 für Windows 95/98/ME, NT 4, 2000 und XP (955 KB, Download unter **www.baxbex.de** und ◉ auf Heft-CD, Registriergebühr: rund 25 Euro). Nach der problemlosen Einrichtung legen Sie in einem übersichtlichen Konfigurationsdialog fest, welche Windows-Verzeichnisse versteckt werden sollen. Zudem können Sie die Zugriffe auf die Windows-Registry und das beim Booten per <F8>-Taste aktivierte Start-Menü sperren und automatisch alle im Start-Menü unter „Dokumente“ auftauchenden Verweise auf geschützte Dateien löschen. Der hiermit realisierte Schutzmechanismus funktioniert auch im DOS-Modus beziehungsweise in einer DOS-Box. Und damit Sie bei der täglichen Arbeit nicht erst das Programm über das Start-Menü aufrufen müssen, können Sie zum Starten einen Shortcut definieren.

Magic Folders 1.8.1

Der englischsprachige Klassiker Magic Folders 1.8.1 für Windows 95/98/ME (253 KB, **www.pc-magic.com/dl.htm#mf**, Registriergebühr: 30 US-Dollar) gehört bereits seit Jahren zur Grundausstattung aller übervorsichtigen PC-Besitzer, da sich mit diesem Tool beliebige Ordner und deren Inhalte unsichtbar machen lassen. Der Schutzmechanismus greift bereits während der Installation, bei der Sie aufgefordert werden, die in der AUTOEXEC.BAT und im Start-Menü angelegten Programmeinträge nach Belieben zu verändern. Auf diese Weise wird dann aus Magic Folders beispielsweise Powerpoint 95 oder ein anderes unverfängliches Programm. Zusätzlich dazu können Sie auch eine Tastenkombination definieren, mit der sich der passwortgeschützte Konfigurationsdialog schnell aufrufen lässt. Die eigentliche Einstellung ist sehr einfach, da Sie nur die zu versteckenden Ordner (der Schutz funktioniert auch im DOS-Modus) auswählen und auf den Button „Make folders Invisible“ klicken müssen. Als Dreingabe gibt es eine rudimentäre Passwortverwaltung. Seit kurzem wird auch eine Version für Win 2000 und XP angeboten; eine Version mit integrierter Verschlüsselung (Encrypted Magic Folders, Registriergebühr: 60 US-Dollar) steht ebenfalls zur Verfügung.

Password Protection System Plus 1.54

Obwohl es sich beim englischsprachigen Password Protection System Plus 1.54 für Windows 95/98/ME, 2000 und XP (1,88 MB, ◉ auf Heft-CD und unter **www.necrocosm.com/ppsplus/index.html**, Registriergebühr: 20 US-Dollar) im Grunde genommen nicht um ein Tool zum Verstecken von Ordnern und Dateien handelt, sollte es zur Grundausstattung aller sicherheitsbewussten Anwender gehören. Warum? Ganz einfach: Mit Hilfe dieser Shareware können Sie jede beliebige EXE-Datei mit einem Passwort versehen und somit vor unbefugten Zugriffen schützen.

Ein weiteres intelligentes Feature: Sie können sogar eine Zeitspanne definieren, während der der Aufruf einer ausführenden Datei schlichtweg verboten ist. Auf diese Art und Weise ist es beispielsweise möglich, die Ausführung bestimmter Programme während Ihrer Abwesenheit komplett zu sperren. Darüber hinaus ist das Tool aber auch in der Lage, beliebige Dateien und Ordner zu verschlüsseln und mit einem zusätzlichen Kennwortschutz zu versehen.

Kryptografie schützt lokale Daten und Mails

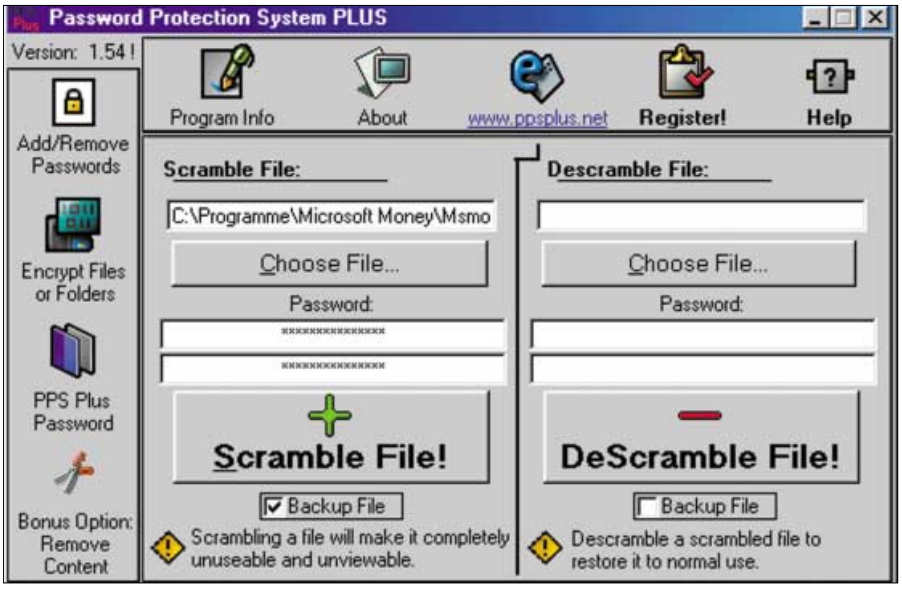
Wo das bloße Verstecken von Dateien und Ordnern keinen ausreichenden Schutz bietet, müssen die Anwender härtere Schutzmaßnahmen ergreifen. An erster Stelle steht hier der Einsatz spezieller Kryptografie-Tools, mit denen Sie lokale

Dateien verschlüsseln, damit unbefugte Personen ohne das richtige Passwort nicht mehr an die Inhalte herankommen. Und was bei Daten, die auf dem eigenen Rechner abgelegt sind, empfehlenswert ist, gehört bei der Mailkommunikation zum unumgänglichen Pflichtprogramm. Denn wo private und geschäftliche Korrespondenz über die unsicheren Leitungen des Internets verschickt werden, schlagen Sie eventuellen Datenschnüfflern durch die Verwendung eines Krypto-Tools ein Schnippchen. In diesem Zusammenhang ist bei der Wahl des Verschlüsselungsprogramms vor allem darauf zu achten, in welchem Format die chiffrierten Nachrichten versendet werden und ob die Gegenseite zum Entschlüsseln das gleiche Programm einsetzen muss oder ob das von Ihnen festgelegte Passwort zum Dechiffrieren beim Empfänger ausreicht.

Das Schließfach 2.0

Der Name ist Programm, da sich der Funktionsumfang von „Das Schließfach" 2.0 für Windows 95/98/ME, NT 4, 2000 und XP (376 KB, **www.cadkas.de/cgi-bin/lang.cgi** und ◉ auf Heft-CD, Registriergebühr: 9 Euro) auf das Verschlüsseln von Windows-Verzeichnissen beschränkt. Über den dabei verwendeten Algorithmus schweigt sich der Programmautor allerdings aus.

Die Ver- und Entschlüsselung von Dateien und Verzeichnissen ist überaus einfach, da die einzelnen Funktionen über zwei Registerkarten zugänglich sind. Sie markieren einfach den gewünschten Ordner, klicken auf die Schaltfläche „Go!" und bestätigen noch eine Warnmeldung, bevor die Inhalte „weggeschlossen" werden. Die auf diese Weise codierten Inhalte werden zusätzlich durch ein frei wählbares Passwort geschützt. Ihre letzte Aufgabe besteht darin, die Originaldateien zu löschen. Dies ist deswegen erforderlich, weil das Programm alle verschlüsselten Inhalte ausschließlich als Kopie speichert. Das Wiederherstellen codierter Inhalte ist ebenso einfach: gewünschte Datei (erkennbar an der Endung KRY) markieren und mit „Go!" öffnen. Und falls Sie sich nicht sicher sind, in welchem „Schließfach" Sie einen bestimmten Ordner weggesperrt haben, zeigt Ihnen das Programm auf Wunsch eine Vorschau auf die Inhalte an.



Stopp, Zugriff verboten! Wer seine EXE-Dateien mit dem Password Protection System Plus 1.54 schützt, verhindert verbotene Programmaufrufe von unbefugten Anwendern

Safeguard Private Crypto 2.01.1

Die Freeware Safeguard Private Crypto 2.01.1 für Windows 95/98/ME, NT 4, 2000 und XP (4,22 MB, **www.utimaco.de/privatecrypto/ger_privatecrypto.html**) verschlüsselt Ordnerinhalte nach dem AES-Algorithmus. Dabei kommt ein Schlüssel zum Einsatz, der auf dem vom Anwender eingegebenen Passwort basiert und somit eindeutig ist. Diese Methode führt dazu, dass der Empfänger der verschlüsselten Datei, die auf Wunsch auch gepackt (ZIP-Verfahren) und in ein selbstextrahierendes Archiv umgewandelt werden kann, lediglich das von Ihnen gewählte Passwort benötigt, um die Dechiffrierung durchzuführen.

Durch die Integration in das Kontextmenü der rechten Maustaste stehen Ihnen die wichtigsten Befehle (beispielsweise „Verschlüsseln", „Verschlüsseln & Senden" und „Entschlüsseln") jederzeit zur Verfügung, und Sie müssen beim Ver- und Entschlüsseln von Daten und Dateien nicht erst das Programm aufrufen. Aber auch in Sachen E-Mail-Sicherheit macht das Tool einen guten Eindruck, da es die verschlüsselten Dateien auf Wunsch automatisch an den standardmäßig im System verankerten Mail-Client (zum Beispiel Microsoft Outlook, Lotus Notes oder Eudora Pro) übergibt. Außerdem verfügt Safeguard Private Crypto auch über eine sichere Löschfunktion, mit der sich nicht mehr benötigte Dateien rückstandsfrei von der Festplatte putzen lassen.

Shy File 5

Das brandaktuelle Shy File 5.0 für Windows 95/98/ME, 2000 und XP (1,79 MB, **www.shyfile.net**, ◉ auf Heft-CD, Registriergebühr: rund 75 Euro) ist ein Verschlüsselungswerkzeug, dass beliebige Daten in Echtzeit (maximale Verschlüsselungstiefe: 6144 Bit) chiffriert. Dabei werden keine Public Keys, sondern symmetrische Schlüssel verwendet, womit die eigentliche Kommunikation unabhängig von jedweden Zertifizierungsstellen ist. Da Shy File einen eigenen Zufallsgenerator verwendet, mit dem die veschlüsselten Nachrichten während der eigentlichen Codierung zusätzlich um sinnlosen Datenmüll erweitert werden, müssen Sie nach dem erstmaligen Programmstart 254 beliebige Zeichen eintippen.

Die Verschlüsselung läuft nach folgendem Muster ab: Zunächst wird ein Schlüssel definiert, der beim anschließenden Codieren Verwendung findet. Dann wird der Text entweder direkt in das Eingabefenster getippt oder über die Windows-Zwischenablage eingefügt. Alternativ dazu öffnen Sie mit einem Klick auf „Kodiere" ein Datei-Auswahlmenü, in dem Sie die zu verschlüsselnde Komponente markieren. Handelt es sich dabei um eine reine Textdatei, kann der Empfänger diese – den richtigen Schlüssel vorausgesetzt – direkt im Browser betrachten; bei binären Anlagen muss die Gegenseite hingegen das gleiche Programm auf dem Rechner haben. ▶

Steganos Crypt & Go 1.62

Profi-Anwender und Gewerbetreibende, die auf der Suche nach dem maximalen Schutz sind und bereit sind, dafür viel Geld auszugeben, sollten sich die Testversion von Steganos Crypt & Go 1.62 für Windows 95/98/ME, NT 4, 2000 und XP (auf Heft-CD und unter **www.steganos.com/de/cng/index.htm**, 5 MB, Preis: 139 Euro) installieren. Das Verschlüsselungswerkzeug codiert Daten und Dateien nach dem international anerkannten AES-Standard mit 128 Bit und komprimiert die gesicherten Archive entweder als selbstextrahierende EXE-Dateien oder nach dem Microsoft-Standard CAB. Letzteres Format wird in erster Linie dazu verwendet, um chiffrierte Dateien per Mail zu versenden; ein spezielles Plug-in für Microsoft Outlook gehört zum Lieferumfang des Programms. Sehr hilfreich: Die wichtigsten Befehle zum Ver- und Entschlüsseln lassen sich direkt über das Kontextmenü der rechten Maustaste auswählen.

Die professionelle, auf den gewerblichen Nutzer zielende Ausrichtung zeigt sich aber auch bei den vielfältigen weiterführenden Optionen. So ist es beispielsweise möglich, die mit Crypt & Go erzeugten Archive um eigene Logos (nur im Format BMP), Textnachrichten, Hyperlinks und sogar um die Lizenzbedingungen zu erweitern – vorbildlich.

Ultimativer Schutz: Festpatte verschlüsseln

Die mit Abstand sicherste Methode zum Schutz der eigenen Dateien besteht darin, einzelne Bereiche der Festplatte zu verschlüsseln oder Dokumente in speziellen Hochsicherheits-Bereichen abzulegen. Wird dann etwa eine Word-Datei aufgerufen, übernimmt das Krypto-Tool die Kontrolle über einen bestimmten Speicherraum des RAM und dechiffriert die Datei oder Teile davon in Echtzeit. Zusätzlich dazu wird auch ein Passwortschutz verwendet, moderne Programme unterstützen sogar die Hardware-basierte Authentifizierung mittels Smartcard, Fingerabdruck oder USB-Key. Somit sind die nach diesem Verfahren geschützten Daten nahezu „unknackbar".

Der einzige Nachteil dieser Variante besteht darin, dass sich ein permanent im Hintergrund laufender Verschlüsselungsalgorithmus negativ auf die Systemleistung auswirkt, das heißt: Er kann einen ohnehin schon am Limit arbeitenden Rechner im Extremfall zum Absturz bringen.

Verschlüsseln und per Mail versenden: Das kostenlose Programm Safeguard Private Crypto 2.01.1 leitet codierte Dateien auf Wunsch direkt an den Mail-Client weiter, der diese dann verschickt

Archi Crypt Live 2.3.9

Aufgrund der Kombination aus eingängiger Benutzerführung und übersichtlichem Funktionsumfang ist Archi Crypt Live 2.3.9 für Windows 98/ME, 2000 und XP (2,5 MB, auf Heft-CD und unter **www.archicrypt.com/go.htm**, Registriergebühr: 35 Euro) ideal für sicherheitsbewusste Anwender, die nicht zu tief in die Materie einsteigen möchten.

Wie die weitaus teureren Vollprodukte verschlüsselt auch das deutschsprachige Tool in Echtzeit; die Codierung der Daten erfolgt entweder per AES- (mit 256 Bit) oder Blowfish-Algorithmus (128 Bit). Bei der lediglich drei Arbeitsschritte (Verzeichnisauswahl, Größe des Laufwerks und Verschlüsselungsmethode) umfassenden Einrichtung der virtuellen Laufwerke kommt ein Assistent zum Einsatz. Maximal werden acht verschlüsselte Laufwerke mit einer Kapazität von bis zu zwei GB (in der Demoversion auf 20 MB beschränkt) angelegt und mit Hilfe des Windows-Explorers verwaltet. Die verwendeten Laufwerksbuchstaben können Sie nach eigenem Gusto vergeben; frei definierbare Tastenkombinationen erlauben Ihnen schnellen Zugriff auf die drei wichtigsten Funktionen „Laufwerk schließen", „Inhalte anzeigen" und „Programm beenden".

Drive Crypt 3.0.2b

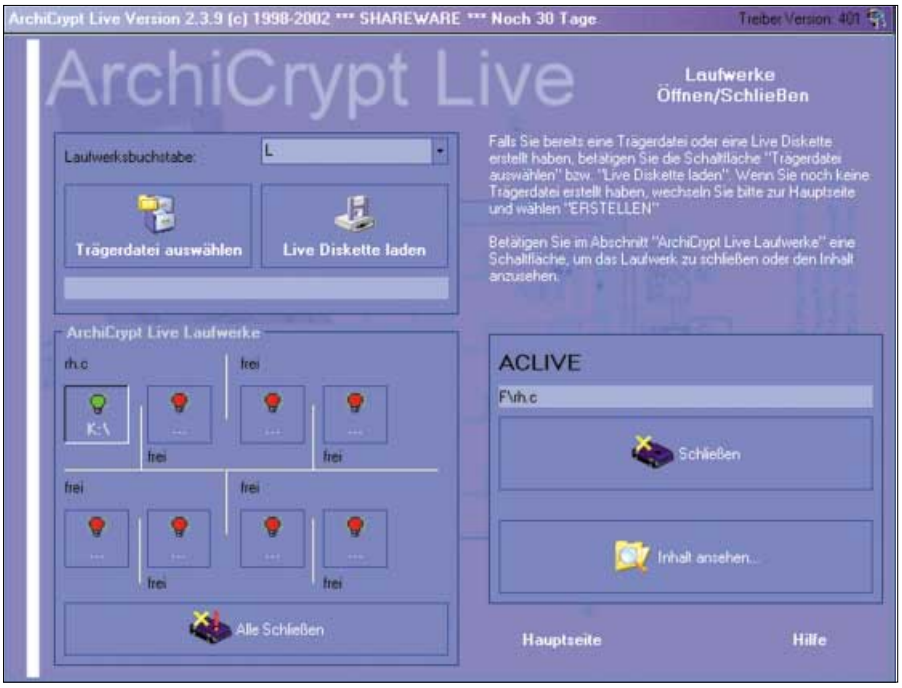
Das laut Herstellerangaben unter anderem von Scotland Yard eingesetzte, englischsprachige Drive Crypt 3.0.2 für Windows 95/98/ME, NT 4, 2000 und XP (2,19 MB, **www.securstar.de/drivecrypt.html**, Preis: rund 40 US-Dollar) ver- und entschlüsselt Daten in Echtzeit und bietet somit umfassenden Schutz. Dabei setzt das Programm gleich auf mehrere Algorithmen wie AES, Blowfish und Triple DES; die maximale Verschlüsselungstiefe beträgt 256 Bit. Der Clou: Um die Ressourcen des Systems so wenig wie möglich zu belasten, verschlüsselt das Programm nicht die komplette in den Speicher geladene Datei, sondern beschränkt sich auf den gerade genutzten Part. Dies wirkt sich positiv auf die Arbeitsgeschwindigkeit aus.

Auf Seiten der Schutzmechanismen stehen Ihnen zwei Varianten zur Auswahl. Entweder Sie verschlüsseln eine komplette Partition beziehungsweise Platte, oder Sie legen so genannte Container an, die vom Betriebssystem wie her-

kömmliche Wechsellaufwerke behandelt werden. Dateisystem (FAT16, FAT32 und NTFS) und Speicherplatz sind dabei frei wählbar; die maximale Dateigröße der einzelnen Container beträgt 4 (unter FAT32) beziehungsweise 64 GB (NTFS).

Strong Disk Pro 2.9

Das Programm Strong Disk Pro 2.9 für Windows 95/98/ME, NT 4, 2000 und XP (Demoversion unter **www.strongdisk.de** und ◉ auf Heft-CD, 1,1 MB, Preis: 100 Euro) hat bereits seit Jahren viel Anhänger. Als Verschlüsselungs-Algorithmus kommen die bewährten Verfahren Triple DES (maximale Schlüssellänge 112 Bit), Cast 128 (128 Bit), Safer (64 Bit) und Blowfish (128 Bit) zum Einsatz. Die Handhabung stellt keine große Herausforderung dar, da Sie nach dem Programmstart einfach auf den Button „Erstellen“ klicken, um von einem Assistenten durch den Einrichtungsvorgang (Laufwerksauswahl, gewünschte Größe und Dateisystem sowie Verschlüsselungsverfahren) geleitet zu werden. Das Krypto-Laufwerk erhält automatisch den Buchstaben „Z“. Allerdings kann diese Einstellung nach der Einrichtung geändert werden. Ausgezeichnetes Zusatz-Feature: Das absolute Profi-Programm beschränkt sich nicht auf den Schutz per Passwort beziehungsweise externe Schlüsseldatei, sondern unterstützt auch einen Hardware-seitigen Schutzmechanismus per elektronischem Schlüssel (I-Button Touch Memory sowie I-Key USB Token).



Einfach und dennoch sicher: Mit Archi Crypt Live 2.3.9 erzeugen und verwalten Sie bis zu acht verschlüsselte Laufwerke mit maximalen Kapazitäten von 2 GB pro Datenträger

Stefan Forster

Steganos Security Suite 4: Komplettlösung für den Datenschutz

Anwender, die sich beim Schutz der eigenen Dateien nicht auf eine bestimmte Strategie verlassen möchten, sondern gleich mehrere Verfahren einsetzen wollen, kommen nicht um den Kauf einer Komplettlösung herum. Solche Sammlungen diverser Sicherheits-Tools haben den nicht zu unterschätzenden Vorteil, dass die einzelnen Komponenten perfekt aufeinander abgestimmt sind – störende Interferenzen sind also nahezu ausgeschlossen.

Die seit Jahren zu den absoluten Dauerbrennern zählende Steganos Security Suite Version 4.13 für Windows 95/98/ME, NT 4, 2000 und XP; 8,3 MB, **www.steganos.com** und ◉ auf Heft-CD, Preis: rund 50 Euro) vereinigt sieben Sicherheitsapplikationen unter einer ansprechend gestalteten Bedienerführung. Angefangen bei der Verschlüsselung von Mails nebst dazugehörigen Anlagen über das rückstandsfreie Löschen nicht mehr benötigter Dateien bis hin zur bequemen Verwaltung von Passwörtern – mehr Features bietet kein zweites Programm auf diesem Sektor. Fortgeschrittene Anwender freuen sich über den integrierten Datensafe, der alle Inhalte (maximal 1 GB) on the fly nach dem AES-Standard verschlüsselt und die Datenkonsistenz selbst bei einem Absturz des Rechners gewährleistet. Die Einrichtung erfolgt mit Unterstützung eines Assistenten.

Ebenfalls wichtig: Bei der Datenvernichtung stehen die beiden Optionen „Vollständiges Überschreiben“ und „Mehrfaches Überschreiben“ zur Auswahl. Mit ersterer Methode geht die Entfernung zwar schneller vonstatten, sie ist aber bei weitem nicht so sicher wie die zweite Variante.

Der Zugriff auf die einzelnen Komponenten gestaltet sich trotz der professionellen Ausrichtung sehr einfach, da die übersichtliche Benutzerführung auch von unerfahrenen PC-Besitzern sehr schnell durchschaut ist. Darüber hinaus lassen sich die wichtigsten Befehle – zum Beispiel „Verschlüsseln“, „Verstecken“ und „Vernichten“ – auch ganz bequem über das Kontextmenü der rechten Maustaste aufrufen. Und dies funktioniert nicht nur im Windows-Explorer, sondern auch direkt auf dem Desktop.

Lediglich die Tatsache, dass die Mailverschlüsselung nicht direkt im bevorzugten Mail-Client durchgeführt werden kann, schmälert den Nutzwert der ansonsten hervorragenden Security Suite ein wenig. Aber das lässt sich verschmerzen.

Rundum-Schutz für alle PC-Besitzer: Die Steganos Security Suite 4 stopft alle Sicherheitslöcher