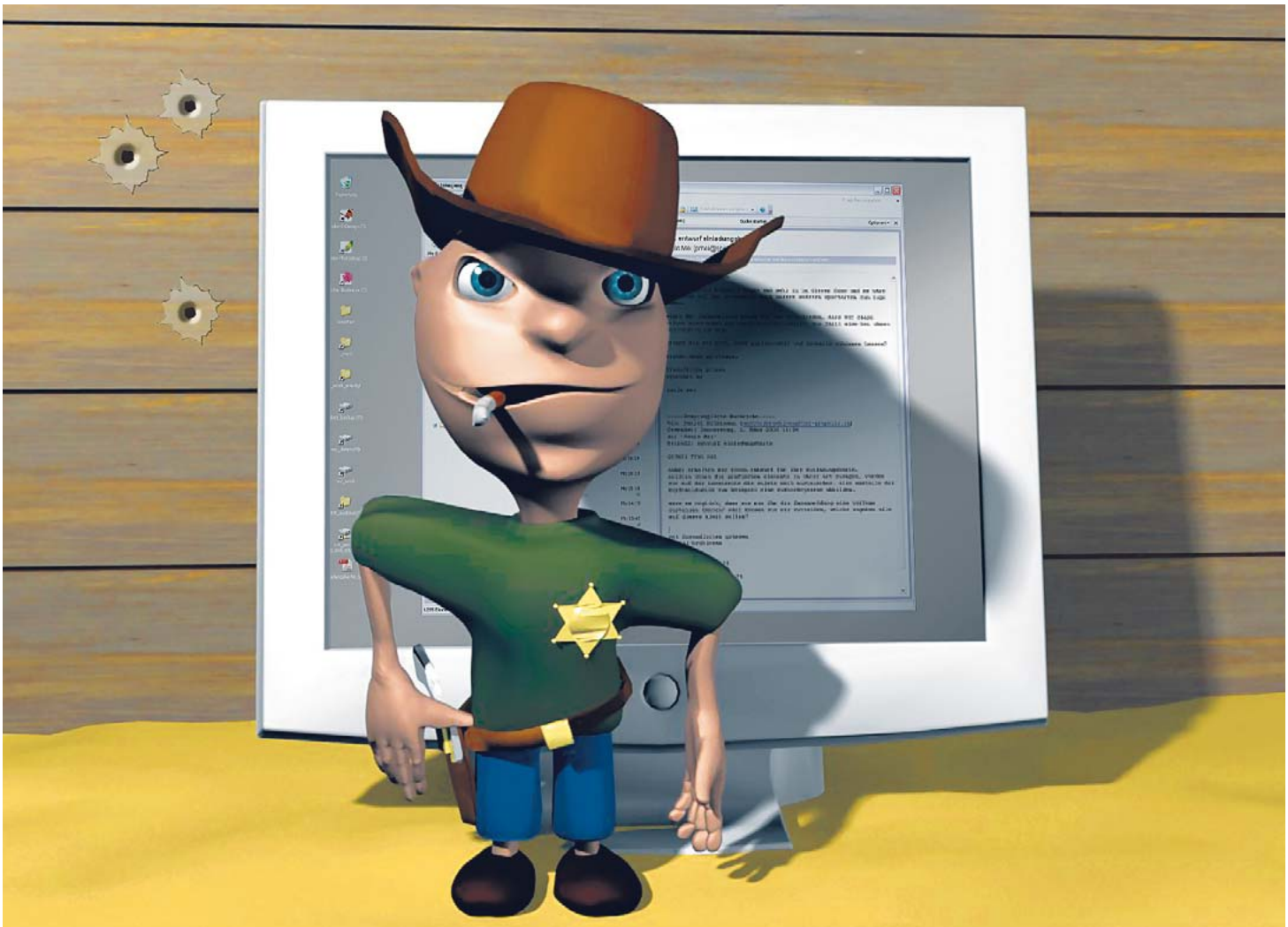


Finger weg!

Von ActiveX bis Zombie-PC: die gefährlichsten Computerbedrohungen und wichtigsten Sicherheitsbegriffe – mit vielen nützlichen Tipps zu Ihrem Schutz.

von Sascha Zäch

Das Internet ist ein Minenfeld: Überall lauern Gefahren. Doch mit etwas Vorsicht und einigen Abwehrmassnahmen kommen Sie gut über die Runden. 26 Sicherheitstipps – für jeden Buchstaben des Alphabets einen.

ActiveX

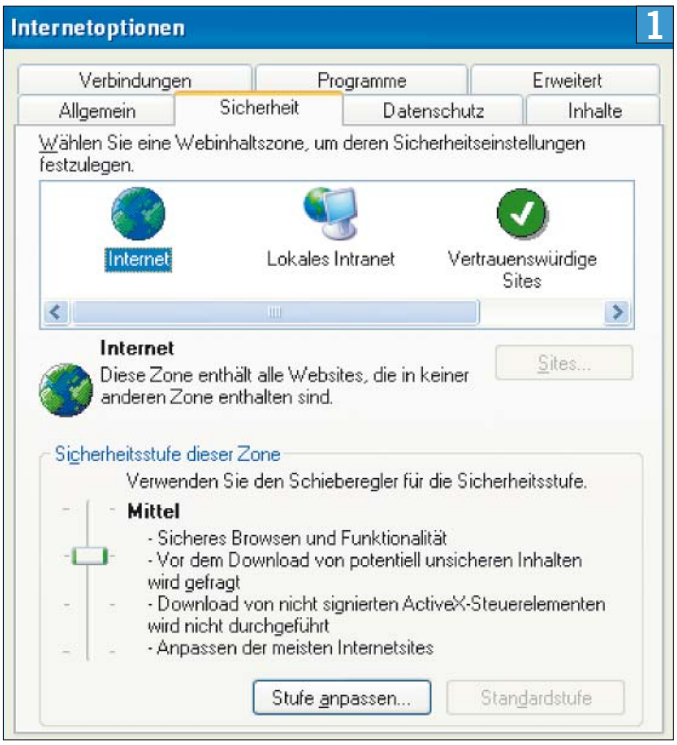
Wenn Sie die Microsoft-Update-Seite besuchen (http://update.microsoft.com), prüft diese automatisch, ob Ihr Windows-System auf dem neusten Stand ist. Möglich macht das ActiveX. Dank der von Microsoft entwickelten Technologie lassen sich Programme und interaktive Inhalte direkt auf Webseiten ausführen. Da sie von den Windows-Machern stammt, wird ActiveX nur vom Internet Explorer unterstützt. Andere Webbrowser verwenden stattdessen JavaScript. Beides sind im Grunde sehr nützliche Technologien. Das Problem: Sowohl ActiveX als auch JavaScript werden von Kriminellen immer wieder missbraucht, um bösartigen Code einzuschleusen.

So schützen Sie sich: Erlauben Sie ActiveX und JavaScript nur auf Webseiten, denen Sie vertrauen. Surfen Sie unter Windows XP mit Service Pack 2, sind die Einstellungen im Internet Explorer bereits sehr streng.

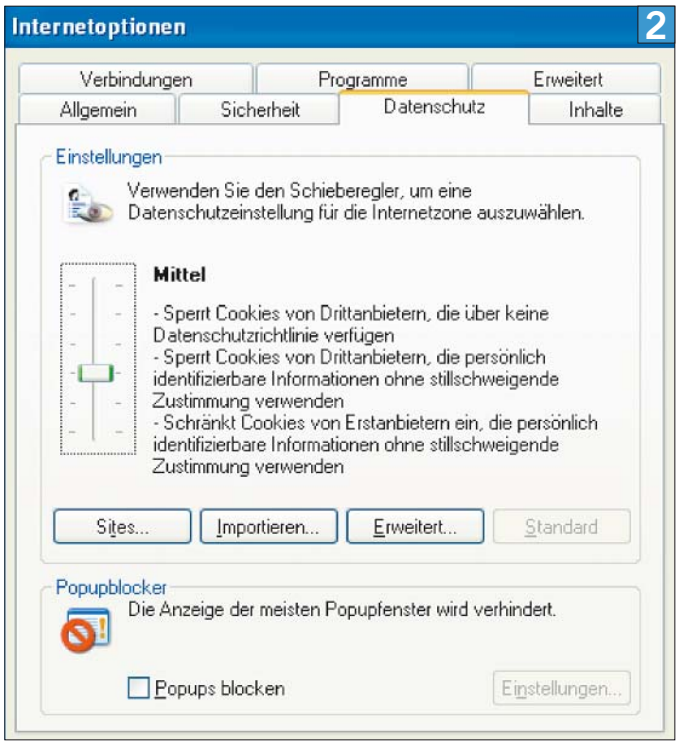
Als zusätzliche Sicherheit empfehlen wir, für die Zone «Internet» die Option «ActiveX-Steuerelemente ausführen, die für Scripting sicher sind» auf Eingabeaufforderung zu stellen. Wählen Sie dazu unter Extras/Internetoptionen/Sicherheit die Zone «Internet» aus und klicken Sie auf Stufe anpassen, Screen 1.

Nerven Sie die ständigen Eingabeaufforderungen und Warnungen bei häufig besuchten

ILLUSTRATION TOM HÜBSCHER, TNT-GRAPHICS



Im Internet Explorer sollten Sie die Regeln für die Zone «Internet» verschärfen



In diesem Fenster bringen Sie dem Internet Explorer bei, wie er Cookies behandeln soll

Seiten? Dann fügen Sie deren Internetadresse unter Extras/Internetoptionen/Sicherheit/Vertrauenswürdige Sites/Sites hinzu. Nun gelten diese Seiten und ihre Inhalte als sicher. Arbeiten Sie mit einem anderen Windows-System, müssen Sie weitere Sicherheitseinstellungen im Internet Explorer anpassen. Eine genaue Anleitung finden Sie im Artikel «Sicher und voll funktionsfähig», PCtipp 2/2004, Seite 71, oder auf www.pctipp.ch mit WEBCODE **pdf040271**.

Wer mit Firefox oder Opera unterwegs ist, konfiguriert das Ausführen von JavaScript unter Extras/Einstellungen/Inhalt bzw. Extras/Einstellungen/Erweitert/Inhalt/Darstellung.

Biometrie

Dieser Begriff bedeutet wörtlich «Vermessung von Leben». Biometrie dient dazu, Menschen anhand typischer Merkmale eindeutig zu identifizieren. Das können etwa Fingerabdruck, Gesicht, Stimme oder die Beschaffenheit der Iris sein. Es gibt schon heute Notebooks oder externe Festplatten, die erst nach einem Fingerabdruck-Scan zugänglich sind.

Cookie

Im Gegensatz zu ihren realen Pendants haben die virtuellen Cookies (zu Deutsch «Kekse») nichts mit Essen zu tun. Es handelt sich um kleine Textdateien, die auf Webseiten versteckt sind und Informationen über die Besucher sammeln. Dadurch ist es möglich, einen Anwender beim nächsten Besuch zu erkennen, um ihn z. B. persönlich zu begrüssen. Leider lassen sich Cookies auch dazu missbrauchen, ausführliche Benutzerprofile zu erstellen.

So schützen Sie sich: Cookies können Sie sperren. Damit verzichten Sie allerdings auch auf einige nützliche Funktionen. Im Internet Explorer entfernen Sie bereits vorhandene Cookies über Extras/Internetoptionen/Allgemein/Cookies löschen. Zusätzlich lässt sich im Register Datenschutz genau einstellen, wie das Programm mit Cookies umgehen soll, Screen 2. Ähnliche Optionen bieten auch Firefox und Opera, und zwar unter Extras/Einstellungen/Datenschutz/Cookies bzw. Extras/Einstellungen/Erweitert/Cookies.

Denial of Service (DoS)

Dieser Begriff heisst wörtlich übersetzt «Dienstverweigerung». Er steht für eine bekannte Angriffsmethode. Bei einer DoS-Attacke wird ein Netzwerk so lange mit unnützem Datenverkehr überflutet, bis gewisse (oder alle) Dienste lahm gelegt sind. So ist es möglich, ganze Webserver in die Knie zu zwingen. Geschieht dies mit Hilfe mehrerer Rechner (z. B. → Zombie-PCs), spricht man auch von einem DDoS-Angriff (Distributed Denial of Service).

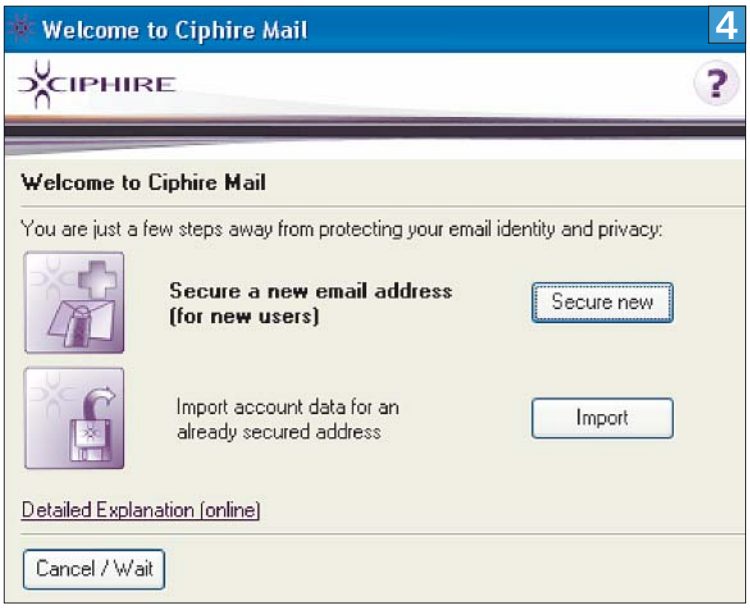
So schützen Sie sich: DoS-Angriffe zielen selten auf Privatanwender, sondern meist auf Firmen. Der beste Schutz sind → Firewalls. Diese verfügen meist über spezielle Technologien zur Abwehr von DoS-Attacken.

Eingeschränkte Rechte

Eine der besten Sicherheitsvorkehrungen ist das Arbeiten mit eingeschränkten Windows-Rechten. Dann lassen sich Programme nur noch bedienen, aber nicht mehr installieren. Damit haben → Viren und andere Schädlinge keine Chance mehr, sich heimlich auf dem Rechner einzunisten.

So schützen Sie sich: Erstellen Sie ein neues Benutzerkonto mit eingeschränkten Rechten, siehe auch «Eingeschränkt sicher», S. 37. Dieses verwenden Sie zum täglichen Arbeiten. Dazu wählen Sie in Windows XP unter Start/Systemsteuerung/Benutzerkonten die Option Neues Konto erstellen. Tippen Sie einen Namen ein und selektieren Sie im folgenden Bildschirm den Kontotyp Eingeschränkt, Screen 3. Während des nächsten Aufstartens erscheint das neue Konto bei der Windows-Anmeldung. Weitere nützliche Tipps im Umgang mit eingeschränkten Benutzerkonten finden Sie in «Zugangskontrolle», PCtipp 11/2004, S. 40 (WEBCODE **pdf041140**). ▶

Dank eingeschränkter Benutzerrechte können sich Schädlinge nicht mehr heimlich installieren



4 **Ciphire Mail schützt Ihre Nachrichten vor den Augen Dritter**

Firewall

Eine Firewall (zu Deutsch «Brandmauer») legt fest, welche Programme über welche → Offenen Ports zwischen dem Internet und Ihrem PC kommunizieren dürfen. Sie funktioniert wie eine Art Grenzwächter. Eingehende und ausgehende Daten werden kontrolliert und abgeblockt, falls sie nicht vom PC ins Internet oder umgekehrt fliessen dürfen. Damit verhindern Sie, dass schädliche Programme unbemerkt Daten ins Internet senden oder von dort herunterladen. Ausserdem bietet eine Firewall Schutz vor Hackerangriffen. Sie kann jedoch keine Vireninfektion verhindern. Wenn Sie einen → Virus per E-Mail herunterladen und ausführen, befällt er trotz Firewall den Rechner. Sie brauchen also noch ein Antivirenprogramm. Firewalls gibt es sowohl in Software- als auch Hardware-Ausführung, wobei Letztere die bessere Sicherheit bietet. Eine genaue Anleitung zur Konfiguration von Firewalls lesen Sie in «Abwehrschlacht», PCtipp 1/2006, S. 26 (WEBCODE pdf060126).

Geheimtext

Nicht jede Information ist für die Augen Dritter bestimmt. Wie soll man jedoch verhindern, dass andere ein heikles Geschäftsdokument unbefugt lesen können?

So schützen Sie sich: Die beste Lösung heisst Verschlüsseln: Dabei werden normal lesbare Informationen in ein unverständliches Zeichenwirrwarr umgewandelt. Ein solcher Geheimtext ist nur für den verständlich, der die Verschlüsselungsmethode kennt.

Im Web gibt es viele kostenlose Programme, mit denen sich E-Mails, einzelne Dateien, ganze Harddisk-Bereiche oder sogar komplette Festplatten verschlüsseln lassen. Zwei besonders empfehlenswerte Vertreter dieser Zunft sind Ciphire Mail (WEBCODE 32221), Screen 4, und TrueCrypt (WEBCODE 32706). In «Nur für Ihre Augen», PCtipp 5/2006, Seite 46 (WEBCODE pdf060546), sind beide genau beschrieben.

Hoax

«Hallo zusammen, es gibt einen neuen Virus, der sich übers Adressbuch verschickt und der nicht von allen Virenprogrammen erkannt wird. Er soll 14 Tage nach der Infektion aufwachen und ist leicht zu entfernen: Suche auf der Festplatte nach der Datei jdbgmgr.exe und lösche diese. Wenn du die Datei auf dem Rechner gefunden hast, bitte diese E-Mail an alle Kontakte im Adressbuch versenden, weil der Virus über das Adressbuch verbreitet wird.» Solche oder ähnliche Warnungen von Unbekannten und Freunden trudeln in regelmässigen Abständen im E-Mail-Postfach ein. Es handelt sich um nichts anderes als einen üblen Scherz (engl. «Hoax»). Befolgten Sie obigen Rat, würden Sie eine harmlose Programmdatei löschen, die auf fast jedem Windows-PC zu finden ist. Leider gibt es viele Anwender, die auf solche Hoaxes hereinfallen und sie weiterleiten. Dadurch verbreiten sich diese wie Kettenbriefe und tauchen immer wieder auf.

So schützen Sie sich: Seien Sie misstrauisch, wenn Sie eine E-Mail erhalten, die Sie «an möglichst viele Leute» weiterleiten sollen. Das ist ein typisches Merkmal von Hoaxes. Charakteristisch sind auch Betreffzeilen mit Warnungen vor Viren oder anderen Gefahren. Zudem beziehen sich die Scherzmails häufig auf namhafte Firmen und Organisationen, um ihre Glaubwürdigkeit zu untermauern. Einen Hoax sollten Sie immer löschen und niemals weiterleiten. Nur so kann ihre Verbreitung eingedämmt werden. Sind Sie nicht sicher, ob Sie einen Hoax erhalten haben? Dann ist www.tu-berlin.de/www/software/hoax.shtml die richtige Adresse. Die Seite enthält nützliche Hintergrundinformationen und eine ausführliche Hoax-Datenbank.

IP-Adresse

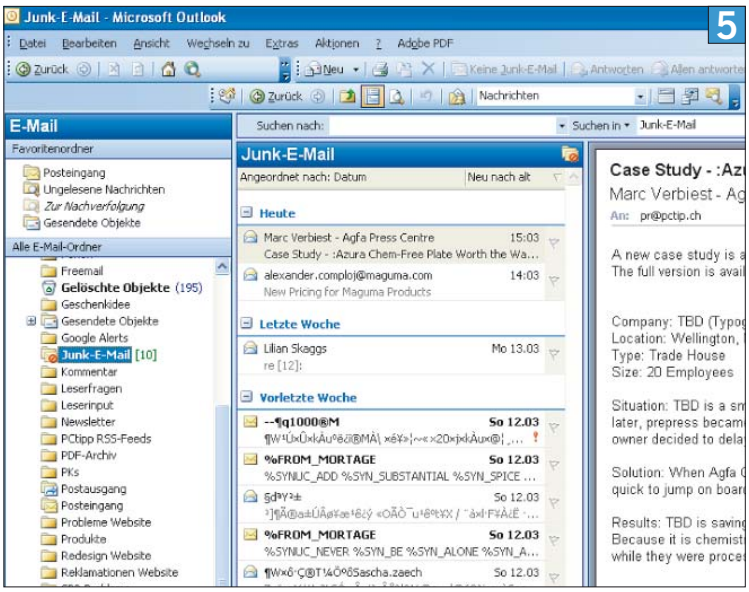
Jeder PC braucht für die Einwahl ins Internet eine eindeutige IP-Adresse (Internet-Protokoll-Adresse). Sie ist sozusagen sein Ausweis, damit ihn andere Rechner identifizieren können. Die IP-Adresse besteht aus vier maximal dreistelligen Zahlen, die durch einen Punkt getrennt sind. Die Werte liegen zwischen 0 und 255. Der Webserver des PCtipp hat z. B. die IP-Adresse 195.141.85.5.

Es gibt dynamische und statische IPs. Erstere ändern bei praktisch jeder Online-Sitzung. Die meisten Privatanwender sind mit einer dynamischen IP unterwegs. Statische IP-Adressen bleiben hingegen immer gleich. Ein typischer Anwendungszweck sind etwa Webserver. Durch seine IP-Adresse ist jeder PC eindeutig identifizierbar, was unter Umständen nicht erwünscht ist.

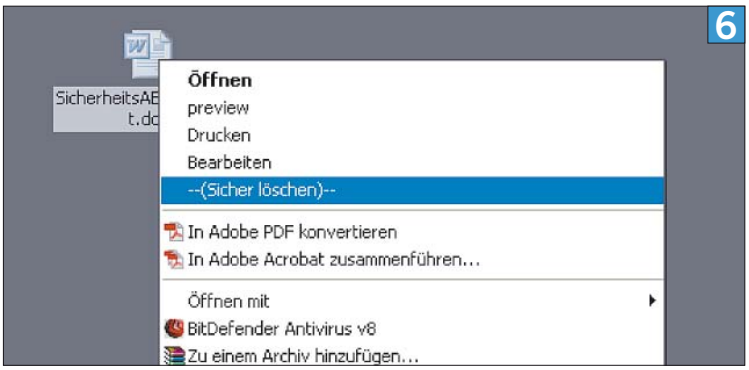
So schützen Sie sich: Möchten Sie lieber unerkannt im Web surfen? Dann helfen so genannte Anonymisierungsdienste weiter. Mehr dazu in «Identitätskrise», PCtipp 3/2006, S. 31 (WEBCODE pdf060328).

Junkmail

Junk bedeutet auf Deutsch so viel wie Müll oder Abfall. Genau dort gehören die zahlreichen unerwünschten Werbemails (auch Spam genannt)



5 **Junkmail-Filter helfen beim Aussortieren von unerwünschten Werbemails**



6 **Nur mit einem Spezialprogramm wie Easy Eraser lassen sich Daten restlos von der Festplatte löschen**

hin, die täglich in unseren virtuellen Postfächern landen. Sie belasten nicht nur den Internetverkehr, sondern machen die Arbeit im Mailprogramm zu einem Klick-und-Lösch-Spiessrutenlauf. Zudem handelt es sich meist um unseriöse oder überteuerte Angebote.

So schützen Sie sich: Ein wirklich effizientes Mittel gegen Spam lässt leider noch auf sich warten. Die bislang beste Lösung ist ein Junkmail-Filter. Er sortiert die lästigen Werbenachrichten aus und verfrachtet sie in einen speziellen Ordner (meist mit «Junk» oder «Spam» bezeichnet). Mailprogramme wie Outlook oder Thunderbird (WEBCODE **27440**) verfügen über einen integrierten Filter, **Screen 5**, ebenso wie einige Maildienste.

Für andere Anwendungen gibt es kostenlose Filter-Software wie Spamihilator (WEBCODE **24327**). Eine genaue Beschreibung zu diesem Programm finden Sie in «Der Spam-Killer», PCtipp 5/2005, S. 26 (WEBCODE **pdf050526**).

Als Anwender haben Sie zudem noch eine zweite Möglichkeit, die Spam-Plage zu vermindern: Kaufen Sie nie Produkte, die in unangeforderten E-Mails angepriesen werden. Dadurch verliert der ganze Massenmailversand seine Attraktivität.

Keylogger

So genannte Keylogger (zu Deutsch etwa «Tastaturaufzeichner») sind äusserst unangenehme Zeitgenossen und gehören zur Familie der Spyware. Die kleinen Spione überwachen Tastatureingaben und leiten diese an Dritte weiter. Der Zweck ist klar: Die Autoren von Keyloggern hoffen, an wertvolle Passwörter und Benutzerdaten zu kommen.

So schützen Sie sich: Den frechen Tastaturspionen kann auf zwei Arten der Garaus gemacht werden. Die erste Schutzmöglichkeit sind Antispyware-Programme wie Spybot oder Ad-Aware. Mehr dazu unter → **Spyware**. Zweitens: Hilfe bieten auch Antivirenanwendungen. Sie schlagen Alarm, wenn sich ein Keylogger auf der Festplatte einnisten will.

Löschen

Ein Dokument auf einem Windows-PC zu löschen, ist simpel. Man wirft es in den virtuellen Papierkorb und leert diesen. Schon befindet sich das Dokument in den ewigen Jagdgründen. Schön wärs! Leider schlummert die Datei noch immer friedlich auf der Harddisk und kann mit spezieller Software schnell wiederbelebt werden. Windows löscht nur die Verknüpfung zur Datei. Erst mit der Zeit wird diese mit neuen Daten überschrieben. Das kann bei heiklen Dokumenten fatal sein. Schon auf manchem Occasions-Rechner kamen Daten zum Vorschein, welche die früheren Besitzer längst gelöscht glaubten.

So schützen Sie sich: Möchten Sie eine Datei richtig von der Festplatte entfernen, brauchen Sie spezielle Software. Glücklicherweise gibt es die auch gratis. Empfehlenswert ist etwa Easy Eraser (WEBCODE **32438**), **Screen 6**.

Das Programm klinkt sich nach der Installation ins Kontextmenü ein. Wenn Sie eine Datei mit der rechten Maustaste anklicken, erscheint neu die Option SICHER LÖSCHEN. Wählen Sie diese, werden die entsprechenden Datenblöcke mehrere Male mit zufälligen Mustern überschrieben und damit für immer unlesbar gemacht.

Man-In-The-Middle

Zu Deutsch bedeutet dieser Begriff so viel wie «Mann in der Mitte». Das klingt nicht nur wie der Titel eines Agentenromans, sondern meint auch eine besondere Form der Spionage. Unter Man-In-The-Middle versteht man eine Person, welche die Verbindung zwischen Ihrem PC und dem Server abhorcht oder sogar manipuliert.

So schützen Sie sich: Für Privatanwender stellen Man-In-The-Middle-Angriffe keine grosse Bedrohung dar. Sie sind mit einem hohen Aufwand verbunden und lohnen sich deshalb nur bei entsprechenden Zielen. Für Firmen bietet das Verwenden verschlüsselter → **Geheimtexte** den effektivsten Schutz.

NTFS-Streams

Windows XP, NT, 2000 und Server 2003 verwenden ein Dateisystem namens NTFS. Dieses unterstützt so genannte Alternate Data Streams (ADS). Damit lassen sich Informationen in versteckten Dateien speichern, die mit einer normal sichtbaren Datei verknüpft sind. Eine typische Anwendung sind etwa die Miniaturbilder für die Windows-Vorschau. NTFS-Streams weisen mehrere gefährliche Eigenschaften auf: Sie lassen sich mit Windows-eigenen Mitteln nur schwer anzeigen. Zudem können sie ausführbare Dateien enthalten. Dies ist leider auch Virenprogrammierern nicht entgangen. Es existieren Schädlinge, die NTFS-Streams missbrauchen. Einer der bekanntesten ist der → **Wurm** W32.Dumaru. ▶

So schützen Sie sich: Obwohl die Gefahr bekannt ist, schützen leider noch immer nicht alle Antivirenprogramme konsequent vor Schädlingen in NTFS-Streams. Ein paar Produkte haben sich aber in Tests mehrfach bewährt, dazu zählen AntiVirenKit von G Data, VirusScan von McAfee und Anti-Virus von Kaspersky. Auch die kostenlose Schutz-Software AntiVir (WEBCODE 21192) überwacht laut Hersteller die (fast) unsichtbaren Datenströme.

Offene Ports

Windows verfügt über viele Netzwerkdienste, die mit anderen Rechnern oder Programmen im Internet kommunizieren. Dies tun sie über so genannte Ports (engl. für Kanal). Das Problem: Diese Ports sind in Windows standardmässig geöffnet (ausser bei Windows XP SP2 und Windows Server 2003 SP1). Entdecken Angreifer Lücken im Betriebssystem oder in einem Programm, können sie über die offenen Ports eindringen. Dies tat etwa der berüchtigte Blaster-Wurm, der innert kurzer Zeit zahlreiche Rechner infizierte.

So schützen Sie sich: Schliessen Sie alle Ports, die nicht benötigt werden. Am einfachsten geht dies mit einer → Firewall. Sie macht erst einmal alle Luken dicht. Danach können Sie genau bestimmen, welche Programme über welche Ports ins Internet dürfen. Dies klingt komplizierter, als es ist. Die meisten Firewalls bieten dazu sehr benutzerfreundliche Funktionen an. Windows XP SP2 und Windows Server 2003 SP1 sind übrigens mit einer Firewall ausgerüstet, die standardmässig aktiviert ist, Screen 7.

Eine ausführliche Anleitung zur Konfiguration von Firewalls lesen Sie in «Abwehrschlacht», PCtipp 1/2006, S. 26 (WEBCODE pdf060126).

Phishing

Eine Form des Internettrickbetrugs, die in den letzten Monaten stark zugenommen hat. Der Begriff ist ein Kunstwort, das sich aus «Passwort» und dem englischen «fishing» (zu Deutsch «fischen») zusammensetzt. Damit ist die Bedeutung schön umrissen: Mittels Phishing versuchen Betrüger, Passwörter und Zugangsdaten zu ergaunern. Dazu verschicken sie E-Mails, die vorgeben, von einem seriösen Anbieter (z. B. einer Bank) zu stammen. Darin wird der Empfänger aufgefordert, seine Kontodaten zu aktualisieren. Er solle dazu auf einen Link klicken. Anschliessend wird das Opfer auf eine falsche Webseite umgeleitet, die dem Original bis aufs Haar gleicht.

So schützen Sie sich: Das beste Mittel gegen Phishing ist eine gesunde Portion Misstrauen. Seriöse Anbieter fordern ihre Kunden niemals dazu auf, Kontodaten per E-Mail-Link zu aktualisieren. Die Absenderadresse («From») weicht bei Phishingmails oft nicht mal vom Original ab, da sie sich beliebig fälschen lässt. Gleiches gilt für die enthaltenen Links. Die wirkliche Link-Adresse sehen Sie, wenn Sie sich den Mailquelltext anzeigen lassen. In Outlook klicken Sie dazu mit der rechten Maustaste auf die Nachricht und wählen QUELLTEXT ANZEIGEN. Oft haben Phishingmails zudem eine unpersönliche Anrede (z. B. «Liebes eBay-Mitglied»).

Eine weitere Hilfe: Mehrere Software-Firmen bieten so genannte Anti-Phishing-Toolbars an, z. B. Star Finanz (www.starmoney.de/index.php?toolbar). Diese klinken sich in den Webbrowser ein und zeigen an, wie sicher eine bestimmte Webseite ist. In kommenden Browser-Generationen wie dem Internet Explorer 7 und Firefox 2.0 soll eine solche Funktion standardmässig enthalten sein.

Windows XP ist bereits mit einer einfachen Firewall ausgerüstet

Quellcode

Als Quellcode bezeichnet man den für Menschen lesbaren Text, in dem ein Programm geschrieben wird. Er besteht aus einer Reihe von Befehlen, die in einer bestimmten Programmiersprache verfasst sind. Würde man einen Computer direkt mit dem Quellcode füttern, verstünde er nur Bahnhof. Deshalb muss er in eine Maschinensprache übersetzt werden. Diesen Vorgang nennt man in der Informatik «kompilieren». Geschieht dies direkt beim Ausführen des Codes, spricht man von «interpretieren». Bekommt ein Angreifer den Quellcode eines Programms in die Hände, ist es für ihn viel leichter, mögliche Sicherheitslücken zu finden. Der kompilierte bzw. interpretierte Code ist für Menschen hingegen unverständlich.

So schützen Sie sich: Als Heimanwender haben Sie keine Möglichkeit, sich gegen den Missbrauch des Quellcodes zu schützen. Die Hersteller müssen dessen Diebstahl verhindern.

Rootkit

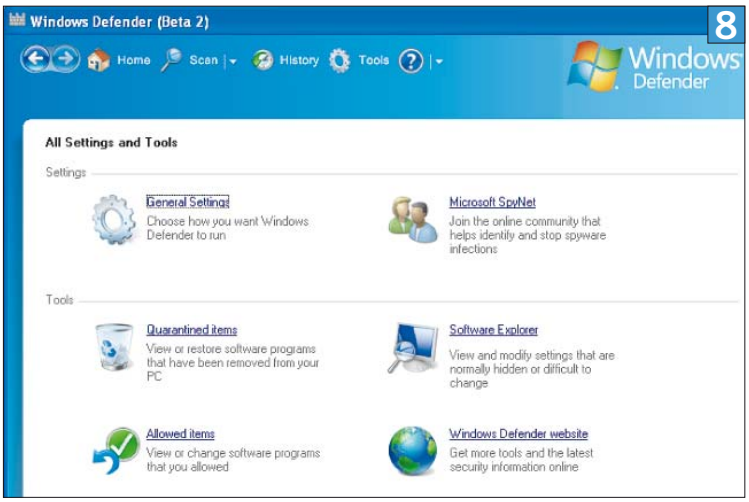
Tarnkappen gibt es nicht nur im Märchen: Dank so genannter Rootkits lassen sich auch Dateien, Ordner, Registry-Einträge, laufende Prozesse oder sogar Benutzerkonten tief im Betriebssystem verstecken. Mit Windows-eigenen Mitteln sind die verborgenen Daten nicht erkennbar. Auch viele Antivirenprogramme können sie nicht mehr aufspüren. Kein Wunder also, dass sich Rootkits gerade bei Virenschreibern grosser Beliebtheit erfreuen. Der Begriff stammt übrigens aus der Unix-Szene und lässt sich etwa mit «Administratorwerkzeugkasten» übersetzen.

So schützen Sie sich: Die meisten Virenscanner sind heute noch nicht in der Lage, von Rootkits versteckte Daten aufzuspüren. Es gibt aber Anwendungen, die den Tarnkappenprogrammen das Handwerk legen können. Dazu zählt z. B. der kostenlose Rootkit Revealer von Sysinternals (www.sysinternals.com/Utilities/RootkitRevealer.html). Er hat jedoch noch kleinere Schwächen und listet teilweise Elemente auf, die nicht verborgen sind. Zudem kann er keine Rootkits löschen.

Anders die Software BlackLight von F-Secure: Sie spürt die Unsichtbarmacher nicht nur auf, sondern entfernt sie auch. BlackLight ist leider nur als Bestandteil von F-Secures Internet Security 2006 erhältlich (www.f-secure.de/blacklight). Weitere nützliche Infos über Rootkits finden Sie in «Ihr PC – ein Zombie?», PCtipp 4/2006, S. 30 (WEBCODE pdf060430).

Spyware

Der Begriff ist eine Zusammensetzung aus den englischen Wörtern «spy» (zu Deutsch «Spion») und «Software». Die schädlichen Programme installieren sich oft heimlich, indem sie Lücken im Webbrowser (vor allem Internet Explorer) ausnutzen oder mit anderen Anwendungen installiert werden. Anschliessend erfassen sie die Surfgewohnheiten des Benutzers, senden diese ohne dessen Wissen an Dritte und blenden entsprechende Werbung ein. Besonders schlimme Exemplare ändern zusätzlich Browser-Einstel-



8

Auch Microsoft hat einen Antispyware-Jäger in der Mache. Er soll Bestandteil des kommenden Windows Vista werden

lungen oder zeichnen gar Tastatureingaben auf. Für die Tastaturspione wird der englische Begriff → Keylogger verwendet.

Spyware wird oft mit Adware gleichgesetzt. Letztere ist jedoch völlig harmlos. Sie blendet Werbung ein, aber ohne den Nutzer auszuspionieren. Hersteller nutzen diese Methode, um kostenlose Programme zu finanzieren. So war etwa der norwegische Webbrowser Opera lange Zeit Adware.

So schützen Sie sich: Einige Virenschutzprogramme können Spyware erkennen und entfernen, dazu gehört z. B. Kasperskys Anti-Virus. Noch effizienter sind spezielle Antispyware-Jäger. Diese sind nur aufs Entdecken und Entfernen der lästigen Festplattenspione abgerichtet. Zu den besten kostenlosen Antispyware-Anwendungen zählen Spybot Search & Destroy (WEBCODE **25550**) und Ad-Aware SE (WEBCODE **17579**). In der nächsten Windows-Version Vista wird zudem schon ein Spyware-Killer enthalten sein, und zwar Microsofts Windows Defender (WEBCODE **29358**). Dieser befindet sich zurzeit noch in der Testphase, funktioniert aber bereits sehr gut, **Screen 8**. Weitere nützliche Tipps zu Spyware gibts in «Spionagejagd», PCtipp 6/2005, S. 28 (WEBCODE **pdf050628**).

Trojaner

In der Computerwelt haben Trojaner gar nichts Heldenhaftes an sich. Das Wort steht vielmehr als Kurzform für Trojanisches Pferd; meint also das sagenhafte Holzpferd, das zum Untergang Trojas geführt hat. Genauso hinterlistig sind auch seine virtuellen Nacheiferer. Sie tarnen sich als harmlose Programme, um sich auf die Festplatte zu schmuggeln. Dort richten sie dann heimlich Schaden an, indem sie bestimmte → Ports öffnen, damit Angreifer übers Internet auf den Computer zugreifen können. Andere schnüffeln Benutzerpasswörter aus.

So schützen Sie sich: Mit einem Antivirenprogramm können Sie die gängigsten Trojaner abwehren. Wichtig ist dabei, dass der Virenschutz immer auf dem neusten Stand gehalten wird. Installieren Sie zudem keine Programme aus unbekannten oder unseriösen Quellen. Damit lässt sich die Gefahr einer Trojanerinfektion schon beträchtlich vermindern. ▶

Ständige Updates sind für die Sicherheit genauso wichtig wie ein guter Virenschutz

Update

Als Update bezeichnet man eine Software-Aktualisierung. Anders als das so genannte Upgrade bringt es keine grossen Neuerungen, sondern nur kleinere Verbesserungen sowie Fehlerkorrekturen oder Sicherheitsoptimierungen (für Letztere wird auch der Begriff Patch verwendet). Dennoch sind Updates für die Computersicherheit enorm wichtig. Die Sicherheitslücken, die sie schliessen, werden oft schon kurze Zeit nach der Entdeckung ausgenutzt. Deshalb sollten Sie alle installierten Programme regelmässig mit Updates aktualisieren, Screen 9, siehe auch den Bericht S. 6.

Virus

Die virtuellen Viren sind fast ebenso verheerend wie ihre realen Pendants. Sie führen Veränderungen am Betriebssystem oder an der Software durch, die im schlimmsten Fall das System unbrauchbar machen. Rettung bietet nur noch eine komplette Neuinstallation. Im Gegensatz zu anderen Schädlingen wie → Computerwürmern oder → Trojanern bauen sich Viren in eine oder mehrere vorhandene Dateien ein. Sie brauchen also einen Wirt. Dabei sind sie nicht wählerisch: Als Träger kann jede Art von ausführbarer Datei herhalten (z. B. EXE). Wird diese gestartet, lädt sie automatisch auch den Virencode mit. Der Schädling kann anschliessend mit seinen Schadfunktionen beginnen oder sich weiter verbreiten.

So schützen Sie sich: Eine Antiviren-Software ist für jeden PC ein Muss. Sie schützt nicht nur vor Viren, sondern auch vor verwandten Schädlingen wie → Würmern und → Trojanern. Wichtig ist, dass der Virenschutz ständig aktualisiert wird. Nur so kann er ganz neue Übeltäter aufspüren und beseitigen. Begegnen Sie zudem Dateien und Programmen aus unbekannten Quellen mit genügend Misstrauen. Egal, ob diese per Mail, CD/DVD oder aus dem Web kommen: Machen Sie vor dem Ausführen immer zuerst einen Virenscan.

Würmer

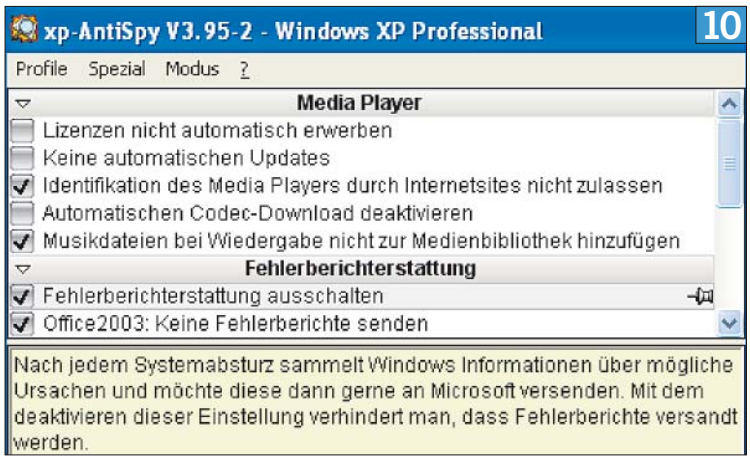
Anders als → Viren infizieren Computerwürmer keine bestehenden Dateien. Sie legen vielmehr eigene Dateien an oder überschreiben bereits vorhandene. Zudem können sich die Schädlinge selbstständig und auf verschiedenste Arten verbreiten. Typische Wege sind etwa E-Mail, Instant Messenger, Funkverbindung oder Netzwerk. Deswegen sind heute Computerwürmer viel häufiger als als ihre Artgenossen, die Viren.

So schützen Sie sich: Wie gegen Viren sind Antivirenprogramme auch gegen Wurmbefall das beste Mittel. Genauso wichtig ist die gebotene Vorsicht beim Öffnen von Mailattachments und unbekannten Programmen. Halten Sie zudem Ihre Software per → Update-Funktion auf dem neusten Stand. Es gibt mehr als einen Wurm, der sich über bekannte Sicherheitslücken (z. B. in Windows) auf die Systeme geschlichen hat.

XP-AntiSpy

Windows ist von Haus aus eine Quasseltante. Das System unterhält sich ständig mit den Microsoft-Servern, um verschiedenste Daten zu übermitteln. Die Fehlermeldungen nach einem Software-Absturz sind nur die Spitze des Eisbergs. Auch Programme wie der Internet Explorer und der Windows Media Player «plaudern» munter mit den Microsoft-Servern.

So schützen Sie sich: Stört Sie diese Geschwätzigkeit, hilft die Software XP-AntiSpy (WEBCODE 19905), Screen 10. Das Programm hindert Windows am unerlaubten Senden von Daten an Microsoft. Ausserdem deaktivieren Sie mit der Software die lästigen Windows-Ballontipps und kritische Script-Sprachen wie → ActiveX. Eine empfehlenswerte Alternative zu XP-AntiSpy ist das ebenfalls kostenlose Xpy (WEBCODE 30002).



Mit XP-AntiSpy verpassen Sie dem geschwätzigen Windows einen Maulkorb

YAW

Früher war nicht immer alles besser. Noch vor zwei Jahren gehörte so genannte Dialer-Software zu den schlimmsten Plagen. Bösartige Exemplare installierten sich heimlich auf dem PC und wählten anschliessend automatisch teure Telefonnummern.

So schützen Sie sich: Schutz gegen die Abzockprogramme bot die Software YAW (Yet Another Warner). Sie blockierte Anrufe auf teure 0900er-Nummern. Heute trägt YAW den Namen a-squared (WEBCODE 30462) und hilft auch gegen Übeltäter wie → Würmer, → Trojaner und → Spyware. Dieser Wandel hat seinen Grund: Dialer sind heute bedeutungslos. Bereits 2004 hat das Schweizer Bakom (Bundesamt für Kommunikation) die Einwahlprogramme für 0900er-Nummern verboten. Zudem funktionieren sie nur mit analogen und ISDN-Modems. Der heutige Breitband-Boom hat den Dialern also zusätzlich einen Todesstoss versetzt.

Zombie-PC

Was nach einem billigen Horrorstreifen klingt, ist für heutige PC-Anwender eine der grössten Bedrohungen. Immer öfter versuchen Online-Gauner mittels → Rootkits, → Würmern und → Trojanern, fremde Rechner unter ihre Kontrolle zu bringen. Gelingt dies, mutieren die Maschinen zu so genannten Zombie-PCs. Diese lassen sich fernsteuern, um z. B. → Junkmails zu verschicken, → DDoS-Angriffe zu starten oder Computerschädlinge zu verbreiten. Es gibt bereits Netzwerke mit über einer Million solcher Zombie-PCs (in der Fachsprache auch Botnetze genannt).

So schützen Sie sich: Je nach Infektionsart sind Virenscanner nicht immer in der Lage, aus einem Zombie-PC wieder einen normalen Rechner zu machen. Selbst bei erfolgreicher Beseitigung der schädlichen Dateien können offene Hintertüren oder andere Risiken auf der Festplatte schlummern. Am besten befördern Sie deshalb das Zombie-System ganz ins Jenseits, indem Sie die wichtigsten Daten sichern, anschliessend die Festplatte komplett formatieren und das Betriebssystem sowie die Software neu installieren. Weitere wichtige Tipps zum Thema gibts in «Ihr PC – ein Zombie?», PCtipp 4/2006, S. 30 (WEBCODE pdf060430). ■