SECURITY

CHIP

SO GEHT'S: W-LAN abschotten

Nachbarn aussperren, Geld sparen, Netz knacken & schützen

Rettungs-CD

VOLLVERSION

O&O DiskRecovery

DiskRecovery 3.0 PE

Nr. 1 der Datenretter
& viele weitere Tools

SECURITY

€ 9,95

Österreich, Niederlande, Belgien, Luxemburg: € 11,50
Schweiz: sfr 19,50

Ein Sonderheft von CHIP
Ausgabe 02/07

So sicher ist Ihr PC wirklich

Alle Lücken finden & schließen

Schützen: PC absichern
Viren & Rootkits loswerden, Komplettschutz installieren

Verstecken: Mailen & Surfen
Verschlüsselt mailen, unerkannt surfen, sicher browsen

Retten: Daten schützen
Nie mehr Datenverlust: Perfektes Backup, geniale Rettung

NEU: Geheime Registry-Tricks für XP

DT-Control

Zusätzlich auf CD

Vollversion 2
ArchiCrypt Live 4

Profi-Tool zur Echtzeit-Verschlüsselung von Texten

Vollversion 3
Outpost Pro Firewall

Spione & Hacker zuverlässig abwehren

6-Monats-Lizenz
Anti-Malware

Schützt Ihren PC vor Dialern, Rootkits, Bots & Trojanern

Exklusiv!
50 Security-Tools

Die besten Gratis-Tools – von der Redaktion getestet

02
4 196627 899526

Vorsicht, bald hackt das BKA!

Andreas Vogelsang
Redaktionsleiter
CHIP-Sonderhefte

Liebe Leser,

dass die vereinigte Internet-Mafia ihre Hacker-, Spam- und Phishing-Attacken Monat für Monat raffinierter gestaltet, ist zwar unerfreulich, überrascht aber nicht wirklich. Eine echte Überraschung dagegen sind die ganz offen diskutierten Pläne des Bundesinnenministeriums, Sicherheitsbehörden das Hacken privater PCs zu gestatten. Mittel zum Zweck der staatlichen Schnüffelpraxis im „Kampf gegen den Terror" sollen Trojaner und das Ausnutzen von Sicherheitslücken installierter Software sein – die Internet-Mafia lässt grüßen.

Stoppen Sie die Schnüffler! Ob krimineller Hacker oder übereifriger Polizeibeamter – der Inhalt Ihrer Festplatte geht keinen etwas an. Wie Sie alle Sicherheitslücken Ihres Computers finden und dauerhaft schließen, zeigen wir Ihnen in diesem Sonderheft. Mein Tipp: Führen Sie zunächst die wichtigsten Handgriffe für eine Grundsicherung Ihres Rechners durch, die wir im Artikel ab **26** beschrieben haben – das kostet Sie maximal zehn Minuten. Anschließend analysieren Sie die Sicherheitslage Ihres PCs (Artikel ab **32** und **36**) und Ihres Netzwerks (Artikel ab **74**), entfernen die enttarnten Schadprogramme und schließen die aufgedeckten Lecks.

Schützen Sie Ihre Identität! Mails verschlüsseln, Browser absichern, anonym surfen – und ein gesundes Misstrauen gegenüber zweifelhaften Angeboten, das sind die Grundlagen für weitgehend risikofreie Internet-Aktivitäten. Wie Sie etwa beim Onlinebanking garantiert auf der sicheren Seite bleiben, zeigen wir Ihnen ab **86**. Auch das rückstandslose Löschen vertraulicher Daten ist immens wichtig für den Schutz Ihrer Privatsphäre (Artikel ab **90**).

Retten Sie Ihre Daten! Nicht nur Hacker bedrohen die Sicherheit Ihrer Daten, auch eine marode Festplatte kann unversehens zu einer mittleren Katastrophe führen. Davor bewahrt Sie eine sinnvolle Strategie der Datensicherung, die wir Ihnen ab **102** vorstellen. Und wenn schon alles verloren scheint, hilft die Vollversion des Profi-Rettungstools DiskRecovery 3.0 PE auf der Heft-CD: Mit ihr können Sie sogar beschädigte oder gelöschte Dateien retten.

Viel Spaß mit Ihrem sicheren PC!

avogelsang@chip.de

Security-Suiten im Test

8 Schützen die bekannten Suiten von Symantec, Kaspersky, McAfee & Co. auch vor den neuen Bedrohungen durch die Internet-Mafia? CHIP hat zehn Pakete aus Firewall, Virenscanner und Spamfilter getestet.

Zehn Gebote für den sicheren PC

20 CHIP hat die häufigsten Gefahrenquellen und Sicherheitsrisiken bei der Kommunikation mit der Außenwelt via PC zusammengestellt – und zeigt, wie Sie diese Risiken ohne viel Aufwand minimieren.

E-Mails verschlüsseln

52 Wenn Sie sicher sein wollen, dass nur der Empfänger Ihre Nachrichten und Datei-Anhänge lesen kann, sollten Sie sie verschlüsseln – beispielsweise mit dem Open-Source-Tool Gpg4win. CHIP zeigt, wie Sie Ihre Mails chiffrieren.

AKTUELL

PC SICHER MACHEN

SICHER MAILEN & SURFEN

SPECIAL W-LAN

DATEN SCHÜTZEN

HEFT-CD

RUBRIKEN

Der große W-LAN-Check

74 Professionelle Tools wie NetStumbler und Nessus zeigen gnadenlos alle Schwachstellen eines drahtlosen Netzwerks auf. Erst wenn Sie die Lecks Ihres W-LAN kennen, sind gezielte Schutzmaßnahmen möglich.

Sicheres Onlinebanking

86 Trotz zunehmender Phishing-Attacken können Sie Onlinebanking ruhigen Gewissens nutzen, wenn Sie einige Grundregeln beachten. CHIP hat sie zusammengestellt – und sagt Ihnen auch, was Sie besser nie tun sollten.

Auf Heft-CD

Vier Vollversionen – DiskRecovery 3.0 PE, ArchiCrypt Live 4, Outpost Firewall Pro 3.0 und a-squared Anti-Malware –, die 50 besten Freeware-Tools zum Thema Security und das CHIP-Sicherheitspaket zum Nulltarif sind die Highlights der Heft-CD. Mehr zu den Programmen erfahren Sie ab 42 bis 51, Workshops zu den Vollversionen finden Sie ab 44 und ab 110.

Windows Vista: Vom Start weg mit Viren verseucht

Glaubt man Microsoft, ist Vista das sicherste Betriebssystem aller Zeiten. Sicherheitsexperten sehen das allerdings ganz anders – aus gutem Grund.

Wenn Vista am 30. Januar endlich auch für Endkunden auf den Markt kommt, ist nur eines sicher: Mindestens drei der aktuellen Top-10-Viren laufen auch unter dem neuen Microsoft-Betriebssystem.

Die Viren Stratio-Zip, Netsky-P und MyDoom-O sind derzeit für rund 40 Prozent aller Infektionen verantwortlich. Netsky-P beispielsweise ermöglicht dem Angreifer, fremde E-Mail-Adressen für Spamattacken zu missbrauchen. Alle seine Nachrichten verschickt der Hacker dann im Namen des Opfers. Ähnlich funktioniert MyDoom-O: Die Malware legt im Windows-Verzeichnis die Datei „services.exe“ an, über die der Hacker auf das System zugreifen kann. Der dritte Schädling, Stratio-Zip, kommt ebenfalls per E-Mail, er infiziert allerdings per ZIP-Archiv. Das Archiv enthält den eigentlichen Virus.

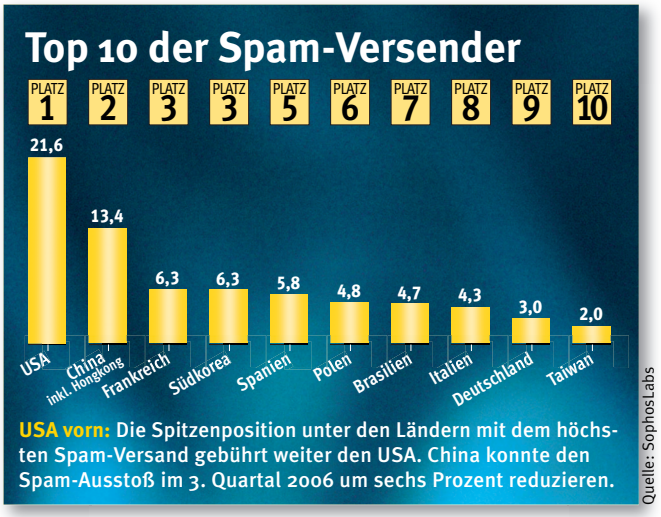
Unsicher: Das Vista-Tool Teredo übersetzt das neue Netzwerk-Protokoll IPv6 in IPv4 – die Sicherheitsfeatures bleiben auf der Strecke.

Bekannt sind diese Viren schon länger – warum also stellen die Vista-Programmierer kein Gegenmittel bereit? Insidern zufolge haben sie die Gefahr zunächst unterschätzt, und später war der Produktionsdruck zu hoch: „Jetzt noch Updates auf die Scheiben zu bringen wäre ein zu großer Aufwand, lieber behebt man das Problem später mit Sicherheits-Patches“, so ein Microsoft-Mitarbeiter.

Aber nicht nur mit Viren hat Windows Vista ein Problem. Auch bei den Netzwerkfeatures gibt es laut Antiviren-Hersteller Symantec bereits vor Erscheinen von Vista eine Sicherheitslücke – im Vista-Tool Teredo, das Befehle aus dem neuen IPv6-Netzwerk-Protokoll ins alte IPv4 übersetzt. Dazu empfängt das eingebaute Programm die Daten aus dem IPv6-Protokoll und schleust sie in den IPv4-Datenstrom. Bei diesem Vorgang gehen wichtige Sicherheitsmerkmale verloren.

Die nächste schlechte Nachricht stammt ebenfalls von einem Anti-Viren-Hersteller: Laut Trend Micro wird derzeit erstmals eine Sicherheitslücke von Vista zum Kauf angeboten – für 50 000 Dollar auf einer geheimen Webseite.

Wer wirklich auf Nummer sicher gehen will, darf sich nicht auf Microsoft verlassen. Denn auch das Vista-Tool Defender hilft nicht gegen diese Bedrohungen. Wirksamen Schutz bieten nur Security-Suiten. Welche von ihnen bereits Vista unterstützen, erfahren Sie auf **www.microsoft.com/security/part**



USA vorn: Die Spitzenposition unter den Ländern mit dem höchsten Spam-Versand gebührt weiter den USA. China konnte den Spam-Ausstoß im 3. Quartal 2006 um sechs Prozent reduzieren.

Phishing-Hochburg USA: Nahezu 30 Prozent aller Phishing-Websites werden in den Vereinigten Staaten gehostet. Anders als beim Spam-Ranking schaffte es Frankreich nicht in die Top 10.

SCHNÜFFEL-PLÄNE

Bund sucht Hacker

Nach Aussage des Grünen-Politikers Wolfgang Wieland hat die Bundesregierung bereits in vier Fällen heimliche Online-Durchsuchungen von Privat-PCs beantragt. Wieland zufolge hat der Bundesinnenminister in seinem Etat 2007 Mittel eingeplant, um Hacker einzustellen und Schnüffel-Programme zu entwickeln, berichtete der Nachrichtendienst de.internet.com am 19.12.2006.

SPYWARE-ALARM

Gefährliche Video-Codecs

Video-Downloads im Internet boomen – das wissen auch die Spyware-Hersteller. Immer öfter tauchen deshalb Webseiten auf, die User mit angeblichen Kinofilm-Downloads locken. Wer sich das Video anschauen will, muss dazu einen ebenfalls angebotenen Codec installieren.

Ähnlich wie bei „Rouge Anti-Spyware“, die sich als Spyware-Killer ausgibt, steckt hinter den Videotreibern jedoch keine legale Software, sondern hinterhältige Spyware.

Einmal installiert lässt sich die Software kaum mehr aus dem System entfernen. Die Hacker bedienen sich dazu eines Tricks: Mehrere Programme schützen sich gegenseitig. Wird der eine Prozess gekillt, startet ein andere Programm ihn kurzerhand neu – bis der User entnervt aufgibt.

SPAM-ATTACKE

Bilderspam im Aufwind

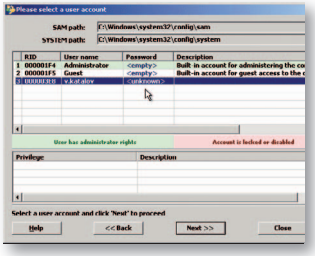
Spammer haben ein Problem. Immer bessere E-Mail-Filter blocken den allergrößten Teil der ungewollten Werbenachrichten ab. Um die Textanalyse der Antispam-Software auszutricksen, werden die Nachrichten daher häufig als Bilder verschickt.

Damit die Spamkiller nicht einfach die Bilder erkennen, wird das Bild für jede E-Mail neu generiert und mit zufälligen Inhalten gefüllt. Das aber hat zur Folge, dass die eigentliche Werbenachricht bis zur Unkenntlichkeit verdeckt wird – ein klassisches Eigentor für Spammer und Phisher.

ELCOMSOFT SYSTEM RECOVERY

Zugang zu gesperrten Rechnern wiederherstellen

Gesperrte PCs lassen sich mit dem Tool System Recovery von ElcomSoft (ESR) zum Zurücksetzen der Zugangsdaten bewegen. Dabei handelt es sich um eine Boot-Disk-Applikation, die auf Windows PE (Preinstallation Environment), einem Hardware-unabhängigen Minimal-Windows basiert.



Nach dem Hochfahren des Rechners mit System Recovery auf einer bootfähigen CD und der Wahl des Betriebssystems zeigt System Recovery alle lokalen Accounts an. Anschließend lassen sich die Passwörter zu den Accounts entfernen oder neu definieren. System Recovery kostet 300 Dollar (weitere Informationen gibt es unter **www.elcomsoft.de/programme/esr.html**).

Alles neu: ESR erlaubt das Zurücksetzen der Zugangsdaten gesperrter Accounts.

TOP 10 DER MALWARE

Die aktuelle Viren-Hitliste

1. **Stratio-Zip:** Eine Familie von ZIP-Dateien, die Würmer der Stration-Familie enthält.
2. **Netsky-P:** Mailing-Wurm, der sich an auf dem PC gefundene Adressen sendet.
3. **Bagle-Zip:** Von Würmern angelegte, kennwortgeschützte Archivdateien.
4. **Zafi-B:** Wurm, der sich als zufällig benannte EXE-Datei in den Systemordner kopiert.
5. **Netsky-D:** Wurm, der sich per Mail verbreitet und die Absenderadresse fälscht.
6. **Nyxem-D:** E-Mail- und Netzwerk-Wurm für die Windows-Plattform.
7. **MyDoom-O:** Mailing-Wurm, der sich über seine eigene SMTP-Engine verschickt.
8. **Mytob-C:** Massmailing-Wurm mit IRC-Backdoor-Funktionalität.
9. **Sality-AA:** Virus, der auch als Keylogger fungiert und Tastenfolgen speichert.
10. **Zafi-D:** Wurm, der sich als „Norton Update.exe“ in den Systemordner kopiert.

Stand: 22.12.2006 Quelle: SophosLabs

SMARTPHONES

Handy-Viren auf dem Vormarsch

Der neue Schädling Symb-OS/Mobispy.A greift Symbian-Smartphones an. Er protokolliert Anruferlisten sowie SMS-Nachrichten und schickt sie an einen Hacker-Server im Internet. Der Virus setzt auf ein kommerzielles Programm, das die Nutzdaten im Netz ablegt. Zugriff hat in der Regel nur der Besitzer des Telefons, der sich anhand der Handy-Seriennummer IMEI identifiziert. Anders ist das bei der Spyware: An dieser Stelle hat nicht nur der Handy-Nutzer Zugriff, sondern auch der Hacker.

Überdies versteckt sich die Malware so auf dem infizierten Telefon, dass kein Menü-Eintrag darauf hinweist.

Wer sich vor solchen Programmen schützen will, muss einen Virenscanner installieren, den alle großen Antiviren-Hersteller anbieten.

FÜR PC & NOTEBOOK

T-Online-Paket mit VoIP-Antidialer

Zwei Lizenzen zum Preis von einer enthält die aktuelle Version des T-Online-Sicherheitspakets 2007: Es enthält die Suite Norton Internet Security 2007 sowie die T-Online-Dialerschutz-Software. Das Antidialer-Tool unterstützt als derzeit einzige Softwarelösung die Features der Internet-Telefonie (Voice over IP, VoIP).

Interessanter Mehrwert: Für beide Programme des T-Online-Sicherheitspakets stehen jeweils zwei Lizenzen zur Verfügung, sodass sich sowohl der heimische PC als auch das Notebook für unterwegs mit Security-Suite und Antidialer-Tool absichern lassen.

Besonderes Augenmerk galt der Verbesserung des Schutzes vor Phishing, Rootkits und Sicherheitslücken. Das T-Online-Sicherheitspaket 2007 kostet fünf Euro pro Monat.

SECURITY-SUITEN IM TEST

So sicher ist Ihre Firewall

Viren sind mittlerweile das kleinste Übel, das Ihren PC bedroht. Denn Internetmafia und Phisher greifen jetzt mit völlig neuen Methoden an. Schützen die bekannten Security-Suiten auch vor diesen Angriffen? CHIP hat zehn Pakete aus Firewall, Virenscanner und Spamfilter getestet.

AUF EINEN BLICK

Alle Tools auf CD

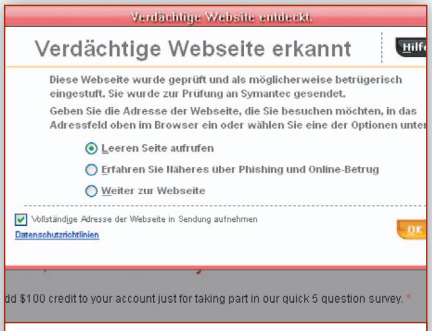
HijackThis: Findet und entfernt Browser-Hijacker ◎ Security

Killbox: Löscht zuverlässig Spyware von Ihrem System ◎ Security

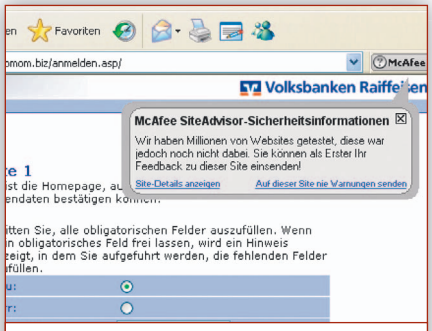
Wie kommt man an der Börse an das große Geld? Die Mitglieder einer russischen Hackertruppe haben es kürzlich vorgemacht: Sie infizierten 73 000 XP-Rechner mit dem Trojaner SpamThru – obwohl die Hälfte der Opfer das Service Pack 2 installiert hatte! Damit wären die Hacker in der Lage gewesen, eine Milliarde Spammails pro Tag zu versenden. Stattdessen nutzten sie das so rekrutierte Botnetz, um von Webseiten, die sich auf Börsennachrichten spezialisiert hatten, reihenweise die E-Mail-Adressen zu klauen. An die Empfänger schickten sie gezielte Fehlinformationen, um auf diese Weise die Börsenkurse zu manipulieren. Ein Fall, der deutlich zeigt, wie professionell die Internetmafia inzwischen ihr Geschäft betreibt.

Aber Sie können Ihren PC vor solchen Angriffen schützen – das behaupten zumindest die zehn Hersteller der aktuellen Security-Suiten. Auf den ersten Blick mag das sogar stimmen: Ein oberflächlicher

Foto: K. Satzinger; Illustration: S. Schönberger



Norton: Das Anti-Phishing-Plugin von Symantec entdeckt fast jede betrügerische Webseite.



McAfee: Keine einzige der besuchten Phishing-Seiten erkannte dagegen der McAfee SiteAdvisor.

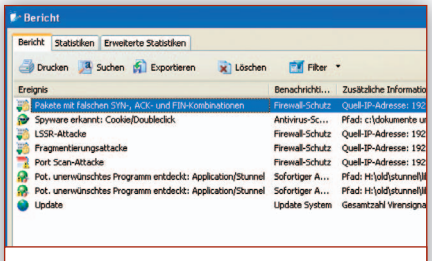
Test bescheinigt allen Sicherheitssuiten eine Erkennungsrate von 100 Prozent und kürt das Programmpaket zum Sieger, das bekannte Trojaner, Bots und Phishing-Mails erkennt.

Uns genügt das jedoch nicht. Und deshalb haben wir die Security-Suiten durch den härtesten Sicherheitstest aller Zeiten gejagt. Denn nur so zeigt sich, ob die Software selbst neue, noch unbekannte Malware erkennt – und entfernt. Das gilt auch für die berüchtigten Phishing-Fallen: Eine hohe Erkennungsrate der Betrugmails ist gut und schön, aber wenn im Browser keine Phishing-Seiten erkannt werden, dann ist der Schutz nicht komplett. Im Testlabor haben wir auch die integrierten Firewalls unter die Lupe genommen und überprüft, ob sie ernsthaften Attacken standhalten. Außerdem: Bei allem Schutz dürfen die Suiten Ihr System auf keinen Fall zu stark belasten.

VIREN, SPYWARE & CO

Kaum mehr Unterschiede dank ausgereifter Technik

Der klassische Virus kommt in freier Wildbahn kaum mehr vor – dafür stehen jetzt Trojaner, Backdoors und Bots an der Spitze der Malware-Charts. Das Antiviren-Modul ist also nach wie vor wichtiger Bestandteil einer Security-Suite – allerdings mit dem Suchfokus auf den genannten Hackerhelfern.



Panda: Die Firewall der Panda-Suite listet sämtliche aufgedeckten Angriffsversuche detailliert auf.

Bekannte Malware: An dieser Stelle schlagen sich die Security-Suiten ganz hervorragend. Alle Testkandidaten erkennen 100 Prozent der Schädlinge, die auf der Wildlist stehen, der Liste der im Internet aktiven Malware. Auch die Erkennung von Bots, Backdoors und Trojanern funktionierte bei neun von zehn Suiten gut, nur das Programm von CA patzte. Diese Ergebnisse gewichten wir jedoch weniger stark, da diese gefährlichen Hackertools glücklicherweise nur wenig verbreitet sind. Wenn Sie eine verseuchte Datei auf ein System mit aktivem Virenscanner laden, sind Sie also gut geschützt. Stoßen Sie jedoch auf einen noch unbekannten Vertreter, hilft diese Scanfunktion nicht.

Unbekannte Malware: Unser „Retrospektive-Test" prüft zusätzlich, wie gut die Heuristik der Scanner funktioniert. Für einen praxisnahen Test haben wir brandneue Malware auf Systeme ohne Virensignaturen losgelassen. Das erschreckende Ergebnis: Gerade mal 84 Prozent konnte die beste Virenscanner-Heuristik des Testfeldes – die der BitDefender-Suite – aufspüren, dicht gefolgt von McAfee mit 83 Prozent. Das traurige Schlusslicht bildet CA: Die Suite erkennt nur 63 Prozent. Wenn der PC immer sofort mit den neuesten Signatur-Updates versorgt würde, wäre das nicht so schlimm. Aber ausgerechnet bei CA dauert es bis zu 27 Stunden, bis die neue Signatur zur Verfügung steht! Vorbildlich aktualisieren Kaspersky und G Data (mit der Kaspersky Scan-Engine). Dort wartet der User maximal zwei Stunden auf die frischen Signaturen.

Aktive Spyware & Bots: Um sicherzugehen, haben wir uns einen besonders fiesen Test überlegt. Sechs ausgewählte Spyware-Programme und Bots wurden auf einem Rechner installiert, die Security-Suiten mussten sie sowohl erkennen als auch entfernen. Ein nicht ganz einfaches Unterfangen, weil sich die Malware hartnäckig dagegen wehrt. Trotzdem schaffte es Testsieger Norton, fünf Exemplare zu entfernen. Nur gegen die Spyware Purity-Scan konnte das Symantec-Paket nichts ausrichten. Das einzige Programm, das da mithalten konnte, war PC-cillin von Trend Micro. Das entfernte sogar die Registry-Einträge von vier der sechs Ein- →

KNOW-HOW

Diese Malware bedroht Ihren PC

Viren
Der Klassiker unter den Schädlingen spielt heute kaum noch eine Rolle. Er verändert andere Programme und vervielfältigt sich auf diese Weise.

Würmer
Eigenständige Programme, die sich über Sicherheitslücken in Netzwerkdiensten verbreiten und so Tausende Systeme in Rekordzeit infizieren.

Spyware und Adware
Wer die auf den ersten Blick harmlose Software installiert, wird mit Werbe-Popups (Adware) bombardiert und ausspioniert (Spyware).

Trojaner
Als harmloses Programm getarnte Malware, die schädliche Funktionen auf dem befallenen Rechner ausführt.

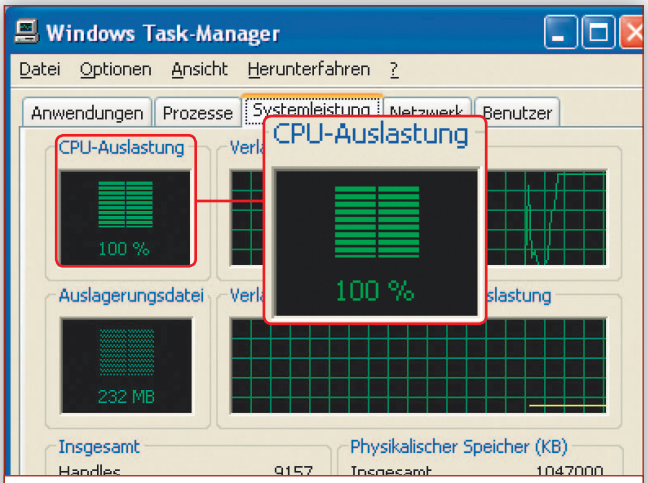
Backdoor
Ist ein Hacker in einen PC eingedrungen, installiert er als Erstes einen versteckten Zugang. Durch diese Hintertür kann er sich immer wieder ins System einklinken.

Bots
Auch diese Tools verschaffen Zugriff auf das System, sie sind aber nie allein: Hacker kontrollieren oft mehrere hundert Bot-Rechner, um Spyware oder Spam zu verbreiten.

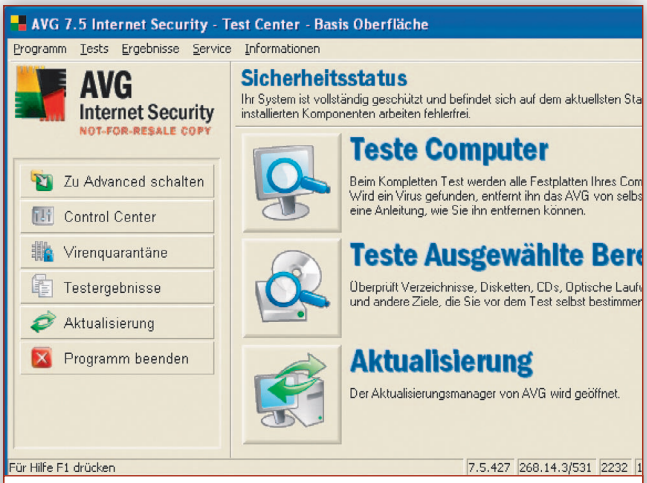
Spam
Unerwünschte Werbemails, mehr lästig als schädlich.

Phishing
Mit gefälschten E-Mails und Webseiten Passwörter oder Bankdaten klauen. Das beliebteste Ziel der Hacker: Ihr Konto abräumen oder online auf Ihre Kosten einkaufen.

Gefahren-Index von 1 (lästig, aber ungefährlich) bis 5 (extrem gefährlich).



CA Internet Security Suite: Zu viele kaputte IP-Pakete beim Denial-of-Service-Angriff überlasten die CA-Suite.



AVG Internet Security: Endlich hat jede Security-Suite eine zentrale Anlaufstelle für die Konfiguration.

dringlinge – ein Punkt, den BitDefender, F-Secure, Kaspersky und Grisoft vernachlässigen. Glücklicherweise ist das nicht gefährlich, sondern nur ärgerlich.

Boot-CD: Ebenfalls wichtig in diesem Test – was haben die verschiedenen Suiten im Notfall zu bieten? Die ideale Lösung ist eine bootfähige und aktuelle Rettungs-CD, mit der man auf Windows-Partitionen zugreifen kann. Wie das im Idealfall aussieht, zeigt der Viertplatzierte BitDefender. Die Installations-CD ist zugleich mit einem bootfähigen Knoppix ausgestattet. Damit klappen sowohl das Online-Update für aktuelle Signaturen als auch der Zugriff auf NTFS-Partitionen, die auf fast allen PCs mit Windows XP und Vista zu finden sind.

KNOW-HOW

Doppelter Schutz – doppelt so gut?

Kein Virenscanner findet 100 Prozent der Malware, keine Firewall blockt alle Angriffe, und keine Antispam-Lösung filtert sämtliche Werbemails aus. Wieso also nicht zwei Security-Suiten installieren? Wir haben es ausprobiert.

Zwei Viren-/Spyware-Scanner

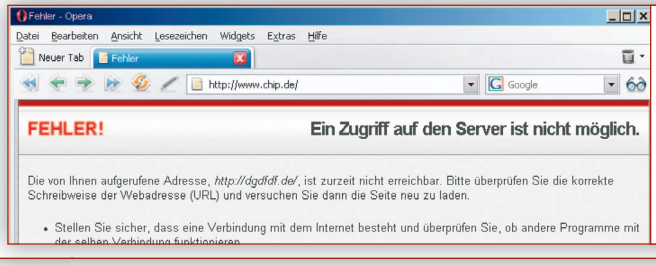
Im Prinzip eine gute Idee. Manche Hersteller setzen bereits heute auf zwei verschiedene Scan-Engines, um die Qualität der Virensuche zu verbessern. G Data etwa setzt Kaspersky und Avira ein. Jede Datei zweimal zu überprüfen kostet aber auch Zeit. G Data konnte das beheben. Wer sich jedoch sein Paket selber zusammenstellt, muss mit der doppelten Scandauer rechnen.

Zwei Antispam-Filter

An dieser Stelle gibt es keine eindeutige Antwort. Prinzipiell gilt: Doppelter Spamfilter bedeutet auch ein besser aufgeräumtes Postfach. Trotzdem schafft es manche Spammail, sich daran vorbeizumogeln. Was noch viel schlimmer ist: Manche Mailprovider haben bei POP3-Postfächern ein sehr kurzes Timeout eingestellt. Wer also zu lange nach Spam sucht, fliegt raus – noch bevor er die gewünschten E-Mails abgeholt hat.

Zwei Firewalls

Was beim Virenscanner funktioniert, klappt auch beim Netzwerkschutz? Falsch! Wer zwei Firewalls auf einem Rechner installiert, muss mit mehr Ärger und weniger Schutz rechnen, da beide gleichzeitig auf dieselben Daten zugreifen. Im schlimmsten Fall funktioniert am Ende gar nichts mehr. Außerdem haben auch Firewalls manchmal Sicherheitslücken – und Hacker dadurch doppelte Zugriffs-Chancen.



Web-Blockade: Zwei Firewalls schützen nicht – sie verhindern vielmehr den problemlosen Internetzugang.

PHISHING & SPAM

Zu wenig Schutz vor den neuen Gefahren

Wenn nur ein Promille der Empfänger auf eine Phishing-Mail hereinfällt, hat sich die Aktion für den Betrüger bereits gelohnt. Da sowohl Spam als auch Phishing genug Geld abwerfen, ist trotz verstärkter Gegenmaßnahmen die Flut betrügerischer Mails nicht zurückgegangen. Im Gegenteil, die Angriffe werden noch raffinierter und gezielter. Das heißt: Wer sich schützen will, braucht zunächst einmal einen guten Spamfilter.

E-Mail-Filter: Fast alle getesteten Suiten identifizieren mehr Phishing-Mails als Spammails. Betrügerische Nachrichten lassen sich also offenbar leichter enttarnen als Werbemails – Glück im Unglück. So erkennt zum Beispiel der Filter von F-Secure 98 Prozent aller Phishing-Nachrichten – und nur 88 Prozent der Spams. Besonders gut schlagen sich McAfee und BitDefender: Deren Filter ordnen 99 Prozent aller Phishing-Mails als solche ein. Beim Anteil der Falschmeldungen gibt es nur wenige Unterschiede: Er ist bei allen Suiten erfreulich niedrig.

Browser-Schutz: Schlimm ist, dass den meisten Suiten ein akzeptabler Phishing-Schutz im Webbrowser fehlt! Links auf Betrugsseiten werden nämlich nicht nur per Mail verschickt, sondern beispielsweise auch in Webforen gepostet. Solche Links werden dann von den meisten Security-Suiten nicht erkannt, und das Opfer tappt mit hoher Wahrscheinlichkeit in die Falle. Nur drei der zehn Sicherheitssuiten besitzen ein funktionierendes

Browser-Schutzmodul: Norton, G Data und PC-cillin.

Das allein garantiert aber noch keinen hundertprozentigen Schutz: Der Testsieger erkannte bei unseren Stichproben mit echten Phishing-Seiten alle bis auf eine, PC-cillin nur etwa 70 Prozent, und das Programm von G Data gab bei den meisten Phishing-Seiten keinen Warnhinweis aus. Weiterer Kritikpunkt: Alle Pakete arbeiten nur mit dem Internet Explorer zusammen. Wer mit Firefox oder Opera surft, hat das Nachsehen.

Außerdem sollten Sie als Nutzer einer Security-Suite mit Geduld gesegnet sein, denn ein Mehr an Sicherheit bezahlen Sie mit Leistungseinbußen: Während sich der Phishing-Filter beim Laden der Webseiten kaum bemerkbar macht, schlägt der Spamfilter mitunter heftig zu: Auf unserem Testsystem brauchte Outlook 2003 ohne vorgeschaltete Filter knapp elf Minuten zum Downloaden von 10 000 Mails. Mit aktivierten Schutzmaßnahmen blieb lediglich die Suite von CA unter 15 Minuten. Bei zwei Programmen wird der Mail-Download zur Tortur: 55 Minuten (G Data) oder gar 95 Minuten (F-Secure) sind für ein zeitsensibles Kommunikationsmittel wie E-Mail nicht tolerierbar. Die Schuld für diese extreme Verzögerung liegt allerdings nicht beim Spamfilter, sondern beim Virenschutz, der sämtliche eingehenden Mails bereits während des Empfangs prüft.

FIREWALL

Hacker und Trojaner – wer will, kommt durch

Jede Desktop-Firewall muss sich zweier Bedrohungen erwehren: Angriffe aus dem Netz und von innen – durch Malware, die Daten vom PC ins Internet sendet.

Angriff von außen: Klassische Angriffe aus dem Internet blocken alle Security-Suiten zuverlässig ab. Vor den ungezielten Angriffen der Würmer sind Sie daher mit jeder Security-Suite sicher. Mit gezielten Hackerangriffen haben allerdings die meisten Firewalls Probleme. Für einen echten Leistungstest bombardierten wir die Programme mit kaputten Netzwerkpaketen (Denial-of-Service-Attacke). Die Folge: Bei allen Angriffen stieg der Ressourcen-Verbrauch auf dem Test-PC. Bei manchen Firewalls, etwa denen von G Data und CA, war ein normales Arbeiten nicht mehr möglich. Bei zwei Testkandidaten reichten schon wenige Pakete, um die Internetverbindung unbrauchbar zu machen: Der Anti-Hacker von Kaspersky kappte die Verbindung ohne Vorwarnung, und die BitDefender-Firewall ließ gleich den ganzen PC abstürzen. Beide Bugs haben die Hersteller aufgrund unserer Hinweise mittlerweile behoben.

Angriff von innen: Sogenannte Leak-Tests sollen in Simulationen zeigen, ob ein befallener PC Code nach außen schickt. Ob die Firewall allerdings echte Schädlinge daran hindern kann, lässt sich mit diesen Tests nicht beweisen. Denn hat der Hacker erst einmal die Kontrolle über den PC, findet er immer einen Weg, die Daten ins Internet zu schmuggeln. Das Einzige, was die Firewalls richtig gut erledigen, ist das Blocken bereits bekannter Spyware.

ERGONOMIE

Performance-Killer – Sicherheit hat ihren Preis

Sicherheit kostet nicht nur Geld, sondern auch Arbeitsspeicher und Rechenzeit. Um herauszufinden, wie viele Ressourcen jede Firewall für Ihre Sicherheit verbraucht, haben wir alle Suiten unter identischen Bedingungen getestet. Ein frisches Windows XP braucht auf unserem Testrechner durchschnittlich 24 Sekunden zum Starten. Mit einer Security-Suite ist das spürbar mehr. Am genügsamsten verhält sich noch AVG: Um lediglich sieben Sekunden verlängert sich der Startvorgang. Die meisten anderen Suiten hängen rund zwanzig Sekunden an den Windows-Start an. Wirklich drastisch fällt der Zeitverlust jedoch nur bei der Suite von CA aus. Da dauert der Windows-Start fast viermal so lange: 110 Sekunden mussten wir durchschnittlich warten. An den Registry-Keys kann es allerdings nicht liegen: Denn bei CA kamen nur 203 neue hinzu. Andere Suiten – auch der Testsieger Norton – schlagen da mit deutlich mehr Einträgen zu Buche. Den größten Arbeitsspeicher-Verbrauch leistet sich F-Secure: 140 MByte RAM schluckt das Programmpaket bei einer Standard-Installation.

Ähnlich schlimm sieht es bei den Supportkosten aus: Wer kein Sicherheitsexperte ist und sich an die deutsche Telefon-Hotline wendet, muss bei manchen Herstellern tief in die Tasche greifen. Am tiefsten bei CA: 29,95 Euro kostet ein Anruf, dafür bekommt man schon fast unseren Preistipp F-Secure oder den Vorjahressieger G Data – jeweils für 40 Euro.

Wenn Sie die Anschaffung einer neuen Security-Suite planen, müssen Sie übrigens mit dem Kauf nicht auf Windows Vista warten: Alle Hersteller haben angekündigt, kurz nach dem offiziellen Release-Termin von Vista ein kostenloses Update nachzureichen. Valentin Pletzer →

G Data: Selbst verhältnismäßig harmlose Portscans quittiert die Suite von G Data mit einer Firewall-Meldung.

PROFI-TIPP

Malware im PC? Der CHIP-Notfallplan hilft

Was tun, wenn die Security-Suite doch mal versagt? Mit den Tools von der Heft-CD helfen Sie sich selbst und retten im Ernstfall zumindest Ihre Daten.

Adware-/Spyware-Abwehr

Mit diesen Tools geht's penetranter Spyware an den Kragen. HijackThis hilft beim Aufspüren, die Killbox entfernt sie. Bei unbekannten Registry- und Dateinamen stellen Sie das Protokoll in Foren wie **www.trojaner-info.de**, dort helfen Profis bei der Suche.

Rootkits entfernen

Gegen diese besonders fiese Technik zum Verstecken von Malware helfen die Tools F-Secure Blacklight und Sophos Anti-Rootkit. Allerdings enttarnen auch diese Programme nicht alle Rootkits. Löschen lassen sich die Rootkit-Dateien in aller Regel mit Killbox.

Viren, Würmer, Bots

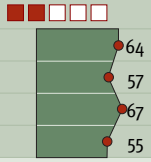
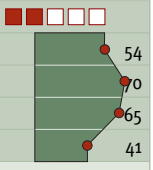
Verdächtige Dateien, die Ihr Scanner nicht erkennt, können Sie auf **http://virusscan.jotti.org** gratis testen lassen. Laden Sie alle Dateien hoch, die Files werden dann von allen gängigen Virenscannern überprüft. Netter Nebeneffekt: Sie erfahren dann auch gleich noch, welcher Virenscanner wirklich weiterhilft.

Übersicht	PLATZ 1	PLATZ 2	PLATZ 3	PLATZ 4	PLATZ 5	PLATZ 6	PLATZ 7	PLATZ 8
	CHIP TESTSIEGER 02/2007	CHIP PREISTIPP 02/2007						
Produkt	Norton Internet Security 2007	Internet Security 2007	InternetSecurity 2007	Internet Security v10	PC-cillin Internet Security 2007	Internet Security 6.0	Internet Security Suite 2007	AVG Internet Security 7.5
Anbieter	Symantec	F-Secure	G Data	BitDefender	Trend Micro	Kaspersky	McAfee	Grisoft
Preis (ca.)	60 Euro	40 Euro	40 Euro	70 Euro	50 Euro	40 Euro	70 Euro	50 Euro
Internet	www.symantec.de	www.f-secure.de	www.gdata.de	www.bitdefender.de	www.avanquest.de	www.kaspersky.de	www.mcafee.de	www.grisoft.de
Gesamtwertung	73	70	69	69	67	66	63	62
Phishing & Spam (30 %)	78	63	74	64	81	63	56	62
Viren, Spyware ... (25 %)	74	76	81	79	69	82	71	65
Firewall (25 %)	72	71	58	71	61	51	78	64
Ergonomie (20 %)	63	69	59	61	50	69	45	56
Preis / Leistung	Befriedigend	Gut	Gut	Befriedigend	Befriedigend	Gut	Ausreichend	Befriedigend
Viren, Würmer, Spyware,Trojaner								
Erkennungsrate bekannter Malware	100 %	100 %	100 %	100 %	100 %	100 %	100 %	100 %
Erkenn. neuer Malware	77 %	82 %	82 %	84 %	77 %	82 %	83 %	64 %
Wartezeit für neue Signaturen	9 bis 10 Stunden	4 bis 5 Stunden	1 bis 2 Stunden	2 bis 3 Stunden	14 bis 15 Stunden	1 bis 2 Stunden	11 bis 12 Stunden	6 bis 7 Stunden
Erkannte aktive Malware	6 von 6	6 von 6	6 von 6	6 von 6	6 von 6	6 von 6	6 von 6	6 von 6
Entfernte aktive Malware (Dateien)	5 von 6	3 von 6	4 von 6	3 von 6	5 von 6	4 von 6	3 von 6	4 von 6
Entfernte aktive Malware (Registry)	3 von 6	0 von 6	1 von 6	0 von 6	4 von 6	0 von 6	3 von 6	0 von 6
Erkenn. Backdoors	99 %	99 %	100 %	97 %	90 %	99 %	94 %	97 %
Erkennungsrate Bots	99 %	97 %	100 %	98 %	92 %	97 %	98 %	97 %
Erkennungsrate Trojaner	99 %	99 %	100 %	96 %	89 %	100 %	92 %	93 %
Scandauer (Standard-Verfahren)	13 min 55 s (alles)	14 min 32 s (alles)	54 min 45 s (alles)	3 min 6 s (nur kritische Bereiche)	8 min 2 s (alles)	29 min 43 s (alles)	8 min 39 s (alles)	11 min 6 s (alles)
CD bootfähig/update-fähig/NTFS-tauglich	● / – / –	● / – / –	● / via Festplatte / ●	• / • via Internet / •	– / – / –	– [5] /via Internet/ ●	– / – / –	– / – / –
Phishing & Spam								
Phishing-Erkennungsrate	83,4 %	98,2 %	89,9 %	99,3 %	92,0 %	93,0 %	99,3 %	92,1 %
Erkennt Phishing-Seiten im Browser	Einige	Keine	Wenige	Keine	Einige	Keine	Keine	Keine
Spam-Erkennungsrate	86,3 %	88,0 %	91,3 %	84,0 %	75,2 %	85,9 %	85,1 %	85,3 %
False-Positives-Rate	1,0 Promille	0,2 Promille	0,2 Promille	0,6 Promille	0,1 Promille	0,9 Promille	1,3 Promille	0,3 Promille
Anbindung an E-Mail-Client	Outlook/Eudora/ Netscape Mail [4]	POP3/IMAP/Out-look-Plugin	POP3/IMAP/ Outlook-Plugin	POP3/Outlook-Plugin	POP3/Outlook-Plugin	POP3/IMAP/ Outlook-Plugin	POP3/Outlook-Plugin	Outlook/Eudora/ The Bat!-Plugins
Download 10 000 Mails [1]	25 min 12 s	95 min 19 s	55 min 53 s	23 min 33 s	29 min 20 s	15 min 40 s	33 min 28 s	34 min 6 s
Firewall								
Verständlichkeit der Meldungen	Nur für erfahrene Nutzer	Nur für erfahrene Nutzer	Nur für erfahrene Nutzer	Nur für erfahrene Nutzer	Nur für erfahrene Nutzer	Nur für erfahrene Nutzer	Nur für erfahrene Nutzer	Nur für erfahrene Nutzer
Systemauslastung bei Analyse von Angriffen	Hohe Auslastung	Hohe Auslastung	Totale Auslastung	Hohe Auslastung	Sehr hohe Auslastung	Hohe Auslastung	Mittlere Auslastung	Hohe Auslastung
Black-/Whitelist	●	●	●	●	●	●	●	●
Reaktion auf Portscan	Kleiner Hinweis	Wird leise geblockt	Kleiner Hinweis	Wird leise geblockt	Nicht geblockt	Kleiner Hinweis	Wird leise geblockt	Wird leise geblockt
Ergonomie								
Belegter RAM	32 MByte	140 MByte	52 MByte	70 MByte	78 MByte	25 MByte	114 MByte	106 MByte
Angelegte Registry-Keys	4302	470	3092	759	1174	2589	4133	709
Boot-Zeit [2]	43 Sekunden	46 Sekunden	38 Sekunden	46 Sekunden	34 Sekunden	43 Sekunden	47 Sekunden	31 Sekunden
Kindersicherung bzw. Webfilter	● [4]	●	●	●	●	–	●	–
Anzahl der Lizenzen	1 für 12 Monate	1 für 12 Monate	1 für 12 Monate	2 für 24 Monate	3 für 12 Monate	1 für 12 Monate	1 für 12 Monate	1 für 12 Monate
Läuft in eingeschränktem XP-Konto	●	●	●	●	●	●	●	●
Vista-Upgrade [3]	Kostenlos	Kostenlos	Kostenlos	Kostenlos	Kostenlos	Kostenlos	Kostenlos	Nicht bekannt
Kosten Technik-Hotline (deutsch)	Ab dritter Minute 1,89 Euro/Min.	0,12 Euro/Minute	0,049 Euro/ Minute	0,12 Euro/Minute	0,69 Euro/Minute	0,12 Euro/Minute	1,00 Euro/Minute	0,12 Euro/Minute
Online-Support (deutsch)	Chat/E-Mail	E-Mail	E-Mail	E-Mail	E-Mail	E-Mail	Chat/E-Mail	E-Mail

Spitzenklasse (100–90)
Oberklasse (89–75)
Mittelklasse (74–45)
Nicht empfehlenswert (44–0)
Alle Wertungen in Punkten (max. 100)

● Ja
– Nein
Wert Bester Wert
Wert Schlechtester Wert

[1] Ohne Suite: 11 Minuten
[2] Ohne Suite: 24 Sekunden
[3] Erscheint kurz nach dem Launch
[4] Nach kostenlosem Upgrade
[5] Muss selbst angelegt werden

	PLATZ 9	PLATZ 10
	Internet Security Suite 2007	Internet Security 2007
	CA	Panda Software
	50 Euro	80 Euro
	www.ca.com/de/	www.panda-software.de
	59	58
		
	Ausreichend	Mangelhaft
	100 %	100 %
	63 %	79 %
	26 bis 27 Stunden	6 bis 7 Stunden
	6 von 6	6 von 6
	4 von 6	4 von 6
	3 von 6	1 von 6
	33 %	87 %
	73 %	97 %
	43 %	89 %
	8 min 3 s (alles)	15 min 30 s (alles)
	– / – / –	● / ● / –
	85,2 %	78,9 %
	Keine	Keine
	82,1 %	69,2 %
	0,4 Promille	0,4 Promille
	POP3/Outlook-Plugin	POP3/Outlook-Plugin
	13 min 42 s	26 min 33 s
	Nur für erfahrene Nutzer	Nur für erfahrene Nutzer
	Totale Auslastung	Sehr hohe Auslastung
	●	●
	Wird leise geblockt	Kleiner Hinweis
	69 MByte	88 MByte
	203	1087
	110 Sekunden	45 Sekunden
	–	●
	1 für 12 Monate	3 für 12 Monate
	–	●
	Kostenlos	Kostenlos
	29,95 Euro/Anruf	Nicht vorhanden
	E-Mail	Nicht vorhanden

KOMPAKT SECURITY-SUITEN

Kauf-Check

Phishing-Filter
E-Mails zu durchsuchen reicht nicht. Der bessere Schutz findet im Browser statt. Achten Sie darauf, dass die Suite Phishing-Attacken nicht nur mit dem Spamfilter bekämpft.

Virenscanner
Aktuelle Antiviren-Programme finden bekannte Malware schnell und zuverlässig. Wichtig ist aber auch, dass sie unbekannte Angreifer finden.

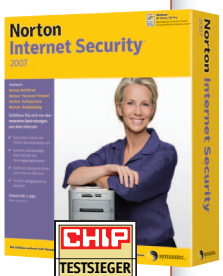
Firewall
In diesem Bereich sind die Unterschiede gering. Programme mit weniger Meldungen stören weniger.

Arbeitsspeicher-Bedarf
Hat Ihr Rechner weniger als 1 GByte RAM, achten Sie unbedingt auf einen geringen Arbeitsspeicher-Verbrauch.

Performance
Security-Suiten bremsen den PC-Start – die in der Tabelle angegebene Bootzeit zeigt, wie sehr.

Support
Für Profis, die selbst Netzwerk-Protokolle auswendig kennen, sind die Programmhilfen ausreichend. Wer sich dagegen nicht täglich mit den Feinheiten seines Systems auseinandersetzt, sollte auf guten und günstigen Support achten.

Sieger



1 Norton Internet Security 2007

Neben dem zuverlässigen Antiviren-Modul besitzt das Programm einen guten Phishing-Schutz für den Webbrowser. Die Performance-Schwächen der Vorgängerversionen sind beseitigt. Nur die Support-Hotline ist recht teuer: 0,20 Euro für die ersten zwei Minuten, 1,89 Euro ab der dritten.
Preis: 60 Euro

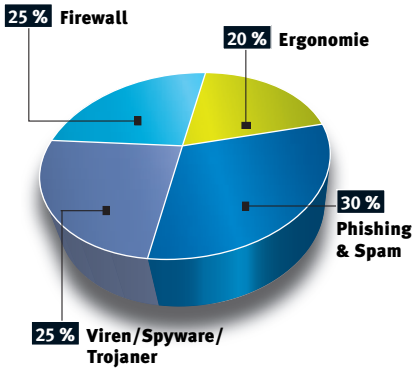
Preistipp

2 F-Secure Internet Security 2007

Mit nur 40 Euro Kaufpreis und einem ausgewogenen Schutz in allen Bereichen ist die Suite von F-Secure ein echter Preistipp. Einen Phishing-Schutz gibt es allerdings lediglich im E-Mail-Client, nicht im Browser. Dafür funktioniert das Ausfiltern der verdächtigen Mails sehr gut. Ein Kritikpunkt: die hohe Systembelastung durch das Programm.
Preis: 40 Euro

SO TESTET CHIP SECURITY-SUITEN

In Kooperation mit dem Virentestlabor AV-Test (**www.av-test.de**) haben wir die Erkennungsraten der Scan-Engines einem harten Test unterzogen. Diesmal sollte die Heuristik auch unbekannte Schädlinge erkennen. Außerdem wollten wir wissen, ob bereits aktive Malware gefunden und komplett entfernt wird. Besonderen Wert legten wir auf einen wirkungsvollen Phishing-Schutz. Im Idealfall hat die Suite einen guten Spam-/Phishing-Filter und einen Phishing-Schutz für den Browser. Die Firewall muss nicht nur sicher sein, sondern auch unkompliziert.



FAZIT

Noch vor einem Jahr hagelte es in puncto Spam- und Phishing-Abwehr rote Karten. Auch dieser CHIP-Test zeigt: Keine Security-Suite schützt hundertprozentig. Selbst der Testsieger Norton Internet Security 2007 erreichte nur 73 Punkte. Immerhin wehrt er Phishing-Attacken am effektivsten ab – sogar im Browser. Vorjahressieger G Data erkennt zwar immer noch die meiste Malware, aber beim Anti-Phishing muss er nachbessern. Fürs gleiche Geld bekommen Sie mit F-Secure einen ausgewogenen Schutz.

BROWSER IM CHIP-TEST

So (un)sicher sind die neuen Webbrowser

Die neuen Browser sind da – und die neuen Bedrohungen ebenfalls. CHIP hat die aktuellen Versionen von Internet Explorer, Firefox und Opera einem Härtetest unterzogen: Welcher Browser schützt wirklich vor Hijackern, Phishern und Hackern?

Foto: S. Grewe; Illustration: S. Schönberger

AUF EINEN BLICK

Wo Geld ist, sind die Betrüger nicht weit. Immer mehr Menschen kaufen im Web ein oder erledigen Bankgeschäfte online – und direkt proportional dazu steigt die Internet-Kriminalität. Kein Programm steht dabei so sehr unter Beschuss wie die Webbrowser. Laut Symantec zielen mehr als 80 Prozent aller Angriffe im Internet entweder auf eine Webseite oder auf den Browser. Vor allem die Nutzer von Microsofts Internet Explorer bekamen das in der Vergangenheit zu spüren.

Mit dem neuen Internet Explorer 7 (IE 7) soll alles besser werden, auch die anderen Hersteller haben aufgerüstet. Wir wollten wissen, mit welchem Browser Sie wirklich sicher surfen können – und ließen Opera 9.02 und Firefox 2.0 gegen den Internet Explorer 7 antreten.

PHISHING

Neuer Schutz vor Online-Betrug

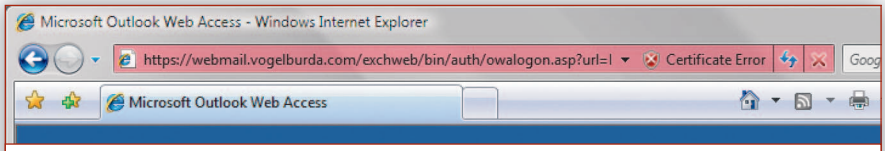
Die Masche der Online-Betrüger ist immer dieselbe: den User auf gefälschte Websites leiten – und dort Passwörter, Kreditkarten-Daten, PINs und TANs abgreifen. Den besten Ansatzpunkt für Schutzmaßnahmen gegen solche Angriffe bietet der Webbrowser. So sollte ein Phishing-Filter vor dem Besuch betrügerischer Webseiten warnen.

Doch nicht alle Browser im Test bieten einen Phishing-Schutz. Opera bleibt diese Sicherheitsfunktion noch schuldig, erst in Version 9.1 soll sie integriert sein. Der Internet Explorer 7 und Firefox 2.0 dagegen sind mit einem Phishing-Filter ausgerüstet, der sich auf Wunsch aktivieren lässt. Im Test arbeitete der Schutz bei beiden Browsern zuverlässig: Alle stichprobenartig angesurften Phishing-Seiten wurden erkannt, die Browser zeigten klare, unübersehbare Warnhinweise. Bei aktiviertem Schutz prüfen die Browser per Heuristik jede aufgerufene Seite auf charakteristische Phishing-Merkmale. Eine Whitelist mit vertrauenswürdigen Websites und eine Blacklist mit bekannten Phishing-Seiten runden den Schutz ab. Diese Listen werden automatisch aktualisiert und auf dem PC gespeichert.

Da aber ständig neue Phishing-Seiten auftauchen, verbinden sich die Browser zu einem Update-Server im Web, wenn die angesurfte Adresse noch nicht lokal verzeichnet ist. Was im Test negativ auffiel: Beim IE lässt sich die Verbindung zum Server nicht separat abschalten. Das heißt: Microsoft könnte über Ihre Surfgewohnheiten ein Nutzerprofil anlegen.

Firefox arbeitet beim Live-Update mit Google zusammen. In diesem Fall werden die aufgerufenen URLs an den Prüfserver des Suchmaschinen-Giganten übermittelt. Wer das nicht möchte, kann diese Funktion abschalten und nur auf die lokale Datenbank zurückgreifen.

Das neue „High Assurance SSL Certificate“ unterstützen alle Browser im Test. Damit wird künftig nicht nur wie bei SSL die Verbindung zwischen Browser und Server verschlüsselt, sondern auch die Gegenstelle von einer unabhängigen Prüfstelle authentifiziert. Ausschließlich so zertifizierte, sichere Seiten zeigen die Browser dann in der Adresszeile grün an. Noch gibt es aber keine Banken oder andere Website-Betreiber, die das Zertifikat einsetzen.



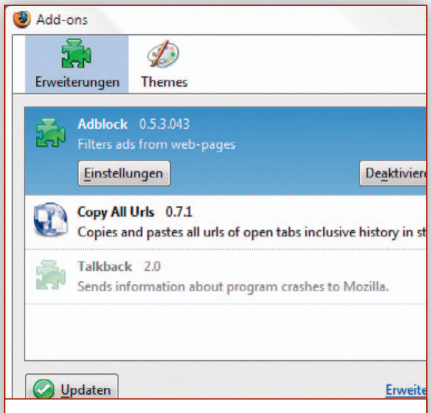
Mehr Sicherheit: Server mit ungültigem „High Assurance SSL Certificate“ werden künftig in der Adressleiste rot angezeigt, außerdem erscheint ein Warnhinweis.

HIJACKING

Angriffe auf den Browser abwehren

Das größte Problem der Browser ist bösartiger Code, den Hacker über Webseiten einschleusen – in erster Linie über Spy- und Adware-Seiten. Meist ist gar nicht der Browser selbst das Angriffsziel, sondern ein Plugin (Addon). Adware versucht vor allem, den Nutzer dazu zu bringen, ein Plugin zu installieren. Spyware dagegen dringt meist über Lücken in bereits installierte Plugins ein. Die Folge: Das Opfer verliert die Kontrolle über den Browser, oft sogar übers Betriebssystem.

Um zu testen, wie gut die Browser solche Angriffe abblocken, ließen wir einen CoolWebSearch-Trojaner auf sie los. Im Internet Explorer nistete sich der Eindringling ein – und lud weitere Schädlinge nach. Diese wurden so schnell und oft aktualisiert, dass unser Antiviren-Pro- →

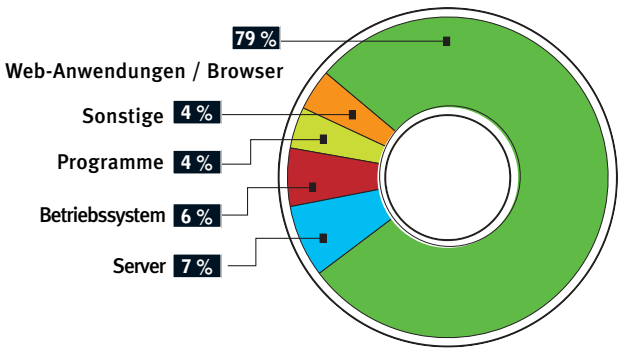


Volle Kontrolle: In allen Browsern können Sie beliebige Addons jederzeit deaktivieren oder löschen.

KNOW-HOW

Das sind die Angriffsziele der Hacker

Direkte Angriffe auf Computer im Internet werden immer seltener. Wesentlich interessanter für Hacker sind dagegen Websites und Browser, über die sie Passwörter auslesen und Bankdaten klauen.



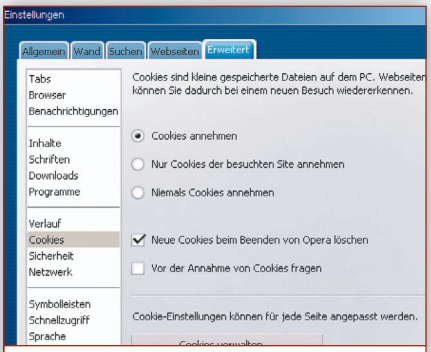
Quelle: www.symantec.de

gramm keine Chance hatte, sie per Signatur zu entdecken. Uns blieb nur die Neuinstallation von Windows. Firefox und Opera blieben – wie erwartet – verschont: Ohne ActiveX sind diese Browser gegen den Angriff immun.

Microsoft hat sich also nicht von den anfälligen ActiveX-Plugins getrennt. Das ist fatal, da ActiveX-Programme – anders als Java-Applets – die gleichen Rechte haben wie der Browser. Sie können also komplett auf das System zugreifen. Erst mit Vista wird das anders. Positiv dagegen: Plugins installiert der IE nur noch mit Zustimmung des Users. Zudem lassen sie sich über eine zentrale Oberfläche deaktivieren und löschen.

Auch bei Firefox und Opera können Sie Plugins deaktivieren und löschen, zudem sind sie meist in JavaScript geschrieben. Damit lässt sich zwar auch Unsinn anstellen, Übergriffe auf das Betriebssystem sind jedoch so gut wie ausgeschlossen. Opera-User mit Programmierkenntnissen können häufig missbrauchte JavaScript-Funktionen sogar abschalten.

Was passiert, wenn der Browser JavaScript ungefiltert ausführt, zeigt unser Test: Wir basteln eine HTML-Seite mit typischen Phishing-Elementen. Mit ein paar Zeilen Code lassen wir die Adresszeile der Browser verschwinden und schreiben dafür „www.citibank.com“ in die Statusleiste – Firefox und Internet Explorer tricksen wir so problemlos aus.



Cookies verwalten: Opera löscht die Cookies auf Wunsch gleich beim Beenden des Browsers.

LOKALE SICHERHEIT

Cookies, Cache und Passwort-Sicherheit

Phishing und direkte Angriffe über das Netz sind nicht die einzigen Gefahren, die im Browser lauern. Ein oft stiefmütterlich behandelter Bereich ist die lokale Sicherheit von Daten. Zwar passiert es nur selten, dass ein Hacker direkt auf den PC und damit auf alle Dateien zugreifen kann. Doch wenn das System von einem Trojaner befallen ist, braucht der Angreifer gar nicht vor Ort zu sein, um lokale Daten auszulesen, beispielsweise den Browser-Cache. Der Inhalt des Caches gibt Aufschluss über das Surfverhalten des Benutzers und enthält oft vertrauliche Informationen – zum Beispiel aus dem Webmail-Account.

Im Test probierten wir aus, was sich im Browser-Cache eines Kollegen Interessantes finden lässt – natürlich mit seiner Erlaubnis. Ergebnis: In allen drei Browsern konnten wir den Cache auslesen – und dem Kollegen eine Mail präsentieren, die ein Foren-Passwort enthält. Ist die Verbindung allerdings per SSL verschlüsselt, werden die Webseiten nicht im Cache gespeichert und geben somit auch keine Daten preis.

Ein sicherer Browser sollte also die Möglichkeit bieten, einzelne Dateien unkompliziert aus dem Cache zu löschen. Der Internet Explorer schneidet an dieser

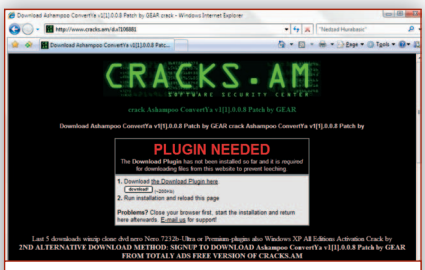
PROFI-TIPPS

So finden Hacker Sicherheitslücken in Webbrowsern

Es vergeht kein Monat, in dem Microsoft nicht ein Update für den Internet Explorer herausbringen muss. Das krasseste Beispiel für löchrige Browser ist „Der Monat der Browser-Bugs“: Einen ganzen Monat lang veröffentlichte der Hacker H. D. Moore auf seinem Blog **http://browserfun.blogspot.com** jeden Tag eine neue Sicherheitslücke – teilweise sogar mit ganz präziser Anleitung zum Hacken. Doch wie finden die Hacker eigentlich so viele Schwachstellen?

Schwachstelle ActiveX: Ein Blick in die Liste der Sicherheitslücken zeigt: So gut wie alle Angriffe konzentrieren sich auf Plugins – nicht auf das Browser-Programm selbst. Das bedeutet aber nicht, dass Microsoft nichts für die Schwachstellen kann. Bereits von Anfang an wurde das System „ActiveX“ von Sicherheitsexperten bemängelt. Wichtigster Punkt: ActiveX-Plugins haben viel zu viele Rechte. Findet ein Hacker eine Lücke, dann stehen die Chancen sehr gut, dass er darüber auch vollen Zugriff auf das Betriebssystem erlangt. Solche Lücken finden Hacker per Zufall – und mit einer guten Spürnase. Eher selten zerlegen sie ein Plugin bis auf die tiefste Ebene, den Maschinencode. Vielmehr geben Abstürze nützliche Hinweise – und die entstehen entweder ganz zufällig oder werden per Brute-Force-Attacken durch ein Tool wie Axman provoziert.

Schwachstelle Windows: Ein weiteres Problem, mit dem in erster Linie der Internet Explorer kämpft, sind die „Shared Libraries“ (DLLs). Damit beispielsweise die Routine zum Anzeigen von GIF-Bildern nicht für jedes Programm neu geschrieben werden muss, wird die Funktion in eine DLL-Datei ausgelagert. Mehrere Programme greifen dann auf ein und dasselbe Stück Code zurück. Findet ein Hacker einen Schwachpunkt in einer DLL, dann ist auch der Internet Explorer davon betroffen, wenn er diese „Shared Library“ benutzt. Der Vorteil für den Hacker: Eine manipulierte GIF-Datei mit Trojaner ist für unterschiedliche Programme geeignet. Am einfachsten ist es jedoch, den Trojaner auf dem Webserver zu präsentieren. Denn sobald die Seite mit dem Browser geöffnet wird, ist der PC infiziert.



Lockvogel Raubkopie: Mit gecrackter Software angelockte Surfer sollen freiwillig ein Plugin installieren – das einen Trojaner enthält.

Schwachstelle User: Die stärkste Waffe der Hacker ist der Anwender selbst. Solange der Benutzer unwissentlich ein bösartiges Programm starten kann, wird es auch Hacker geben, die einen Weg finden, ihn dazu zu bringen. Bestes Beispiel: Plugins können sich im Internet Explorer seit Windows XP Service Pack 2 nicht mehr automatisch installieren. Seitdem versehen Hacker bösartige Plugins auf vielbesuchten Webseiten mit einer passenden Installationsanweisung – und verkaufen damit dem User die Malware als nützliches Programm.

Stelle schlechter ab als Firefox und Opera. Denn IE-Nutzer können nur die Größe des Browser-Caches angeben und den gesamten Cache auf einmal löschen. Um einzelne Dateien zu entfernen, müssten sie sich erst durch die kryptischen Dateinamen kämpfen, unter denen der Browser sie ablegt. Die Konkurrenz dagegen erlaubt nicht nur das Löschen und Kontrollieren des Cache-Verzeichnisses, sondern auch das detaillierte Löschen einzelner Seiten.

Ganz ähnlich sieht es bei Cookies aus. Ein Blick ins Cookie-Verzeichnis verrät uns noch Wochen später, wann und auf welchen Seiten der Browser unterwegs war – abhängig von der Gültigkeitsdauer der Cookies. Zwar kann der Nutzer im Internet Explorer detailliert angeben, welche Cookies er erlaubt und welche nicht. Aber ein automatisches Löschen beim Beenden des Browsers oder sogar beim Verlassen der Seite gibt es bei Microsoft nicht. Opera bietet die umfangreichste Lösung: Dort können Sie die Einstellungen nicht nur für jede Webseite separat speichern, sondern die Cookies sogar lesen und bearbeiten.

Den geringsten Einfluss auf die lokale Sicherheit hat die Passwort-Verwaltung. Denn damit lässt sich der PC zwar gegen einen unerlaubten Zugriff durch den Sprössling absichern – nicht aber gegen ernsthafte Hackerangriffe.

Alle Browser in unserem Test tragen auf Wunsch die Passwörter für die Webseiten automatisch ein. Opera und Firefox bieten – im Gegensatz zum Internet Explorer – außerdem einen guten Kompromiss aus Sicherheit und Komfort. Ein Master-Passwort sichert alle gespeicherten Einträge – eine gute Sache. Allerdings:

Passwort-Manager: Opera erlaubt es, ein Master-Kennwort zu setzen – ein guter Kompromiss aus Sicherheit und Komfort.

FAZIT

Firefox knapp vorn

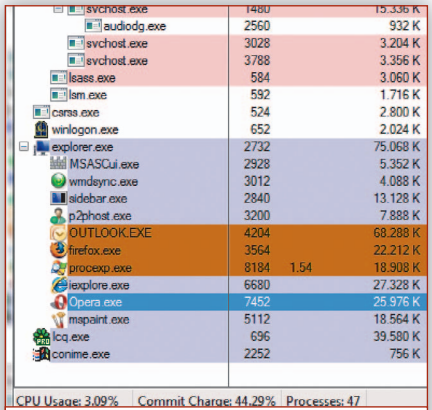
Im direkten Vergleich gewinnt Firefox den Sicherheits-Check. Doch Opera folgt ihm auf dem Fuß. Die kommende Version 9.1 – dann mit Phishing-Filter – dürfte den Fuchs sogar überholen. Den letzten Platz belegt der Internet Explorer. Mit einem Marktanteil von 87 Prozent steht er ganz oben auf der Abschussliste der Hacker – und Microsoft zeigt auch im neuen Internet Explorer 7 wieder Mut zur Lücke.

Das richtige Passwort taucht früher oder später dennoch unverschlüsselt auf – spätestens dann, wenn es auf der Webseite eingetragen wird. In diesem Augenblick kann der Hacker mit Zugriff auf den PC das Passwort abfangen.

UPDATES

Sicherheitslücken und Aktualität beim Patchen

Noch sind kaum Sicherheitslücken der neuen Browser bekannt. Denn Hacker werden meist erst aktiv, wenn die neuen Versionen bereits weiter verbreitet sind. Was uns noch bevorsteht, lässt sich jedoch anhand der Lücken der Vorgänger-Versionen abschätzen. Den einsamen Rekord hält der Internet Explorer: Dort fanden die Hacker bis heute mehr als hundert Löcher, fast zwanzig davon sind noch immer nicht gestopft. Im Vergleich dazu führt die Sicherheitsfirma Secunia (**www.secunia.com**) bei Firefox gerade mal 36 Lücken auf, bei Opera sogar nur 15.



Speicherfresser: Bei vielen geöffneten Seiten braucht der Internet Explorer deutlich mehr RAM als die Konkurrenz.

Wesentlich interessanter für die Hacker ist allerdings das Zeitfenster, in dem sie die Lücken ausnutzen können. Auch an dieser Stelle steht der Internet Explorer am schlechtesten da: Laut Symantec dauerte es im ersten Halbjahr 2006 im Durchschnitt neun Tage, bis Microsoft eine Sicherheitslücke gestopft hatte. Die Open-Source-Gemeinde um Firefox brauchte lediglich einen Tag, die Opera-Entwickler gerade mal zwei.

Die zahlreichen Sicherheitslücken und die Zeit, die verstreicht, bis sie behoben sind, bleiben aller Voraussicht nach das größte Problem – für Microsoft.

PERFORMANCE

Geschwindigkeit und Ressourcen-Verbrauch

Bewertet haben wir in diesem Test nur die sicherheitsrelevanten Features. Trotzdem wollen wir Ihnen die neuen Performance-Werte nicht vorenthalten. Auf der Hersteller-Homepage wird Opera als „der schnellste Browser der Welt“ angepriesen – zu Recht, wie unsere Messungen zeigen. Wir haben die Zeit gestoppt, die die Browser zum Aufbau von HTML-Seiten sowie zum Ausführen von JavaScript brauchen. Ergebnis: Vorsprung für Opera – allerdings nur ganz knapp. Firefox folgt so dicht, dass man im Rahmen der Messtoleranz auch sagen könnte, dass die beiden gleich schnell sind. Für eine HTML-Seite mit 2500 DIV-Elementen brauchten die beiden Browser zwischen 350 und 400 Millisekunden (Test-PC: 2 GHz, 1024 MByte RAM). Der Internet Explorer liegt mit rund 740 Millisekunden weit abgeschlagen dahinter. Bemerkbar machen sich die Geschwindigkeitsvorteile der schnellen Browser vor allem auf neuen, AJAX-betriebenen Webseiten wie Google Maps.

Wichtig ist auch der Arbeitsspeicher-Verbrauch. Wenn keine Webseite geladen ist, braucht der IE noch am wenigsten. Je mehr Webseiten allerdings gleichzeitig geöffnet sind, umso mehr Speicher frisst der Microsoft-Browser. Sowohl Opera als auch Firefox können besser damit umgehen, bei ihnen steigt der Speicherverbrauch nur minimal an. Bei zehn identischen Webseiten braucht Firefox nicht einmal doppelt so viel Speicher, wie wenn keine Seite geladen ist – der Internet Explorer fast die vierfache Menge. →

FEATURES

Mehr Funktionen – und doch kaum Neues

Wirklich Neues bietet allenfalls der Internet Explorer mit RSS-Reader, Tabs oder integrierter Webseiten-Suche. Was noch fehlt, sind Themes und eine Rechtschreibprüfung für Webformulare – Dinge, über die Nutzer von Opera und Firefox nur müde lächeln: Sie nutzen diese Funktionen schon lange. Valentin Pletzer

WEBBROWSER

Sicherheits-Check

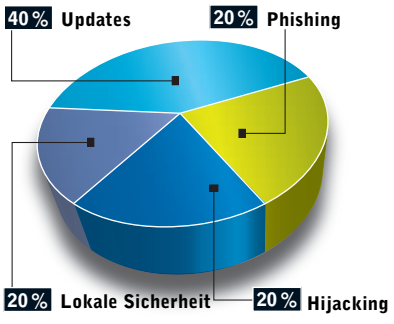
1 Mozilla Firefox 2.0 Der erste Platz geht an den Open-Source-Browser – er ist nicht nur sehr sicher, sondern auch schnell.

2 Opera 9.02 Zweiter Platz für den flotten Browser ohne Phishing-Filter – der wird erst in der Version 9.1 nachgereicht.

3 Microsoft Internet Explorer 7 An letzter Stelle – trotz grandioser Aufholjagd. Viele ungepatchte Lücken erwarten uns auch im IE 7 und kosten Punkte.

So testet CHIP Webbrowser

Alle drei Browser wurden einem gründlichen Sicherheits-Check unterzogen. Als Anhaltspunkt für zukünftige Sicherheitslücken wurde auf die Datenbank der Sicherheitsfirma Secunia zurückgegriffen. Auch lokale Angriffspunkte wie Cache, Cookies und Passwörter fließen in die Bewertung ein. Nicht bewertet wurden die Performance der neuen Browser sowie die Zusatz-Features. Als Testrechner diente ein AMD 64 3000+ mit 2 GHz und 1 GByte Arbeitsspeicher. Die Browser liefen unter Windows XP Pro und Vista.



Übersicht	PLATZ 1	PLATZ 2	PLATZ 3
Produkt	**Firefox 2.0**	**Opera 9.02**	**Internet Explorer 7.0**
Hersteller	Mozilla	Opera Software	Microsoft
Internet	www.mozilla.org	www.opera.com	www.microsoft.com
Sicherheitswertung	93	83	65
Phishing (20 %)	97	39	91
Hijacking (20 %)	97	97	67
Lokale Sicherheit (20 %)	97	97	67
Updates (40 %)	88	94	49
Sicherheit			
Phishing-Filter	Lokale Liste oder Verbindung zu Google-Server	–	Verbindung zu Microsoft-Server
Unterstützung von SSL / High Assurance SSL	● / ●	● / ●	● / ●
Addon-Verwaltung (Hijacking-Schutz)	Deaktivieren und Löschen	Deaktivieren und Löschen	Deaktivieren und Löschen
Cache-Verwaltung	Größe einstellen, alle Seiten und einzelne Seiten löschen	Größe einstellen, alle Seiten und einzelne Seiten löschen	Größe einstellen, nur alle Seiten löschen
Cookie-Verwaltung	Einzelne Cookies und alle Cookies löschen, einzelne Webseiten blocken	Löschen, Blocken und Verändern von Cookies	Einzelne Cookies und alle Cookies löschen, kompliziertes Blocken
Passwort-Verwaltung / Master-Passwort	● / ●	● / ●	● / –
Update-Verfahren	Automatisch	Automatisch (nicht abschaltbar)	Über das Windows-Update
Durchschnittliche Reaktionszeit auf Lücken [1]	1 Tag	2 Tage	9 Tage
Bekannte Lücken der Vorgänger-Version ungepatcht / gesamt [2]	3 / 36	0 / 15	19 / 106
Performance			
HTML-Seite aufbauen	400 ms	376 ms	741 ms
JavaScript ausführen	7,8 Sekunden	7,3 Sekunden	17,7 Sekunden
Arbeitsspeicher (0/5/10 Webseiten)	12,9 / 16,5 / 19,8 MByte	19,8 / 20,2 / 24,6 MByte	7,9 / 21,4 / 29,1 MByte
Features			
Popup-Blocker	Kann für jede Seite separat eingestellt werden	Kann für jede Seite separat eingestellt werden	Kann für jede Seite separat eingestellt werden
Suche nach Webseiten	Weitere Suchmaschinen per JavaScript-Links	Weitere Suchmaschinen manuell eintragen	Weitere Suchmaschinen per OpenSearch-XML
Suche in Webseiten	Instant-Suche (Wörter werden farbig markiert)	Standard-Suchfeld	Standard-Suchfeld
Tabs (mehrere Webseiten in einem Fenster)	Nicht per Mausklick	Per Mausklick	Per Mausklick
RSS-Feeds	Als Bookmarks oder Webseite dargestellt	Angezeigt in einem eigenen Reader	Als Webseite dargestellt
Favoriten-Verwaltung	Umfangreich	Umfangreich	Umfangreich
Themes	●	●	–
Seiten-Skalierung (Betrachten / Drucken)	● / ●	● / ● (inklusive Umformatierung)	● / ●
Rechtschreibprüfung	● (per Update)	●	–
Aktuelle Sitzung speichern	●	● (inklusive Absturz-Recovery)	–
Mehrere Startseiten	●	●	●
Befolgen der W3C-Standards	Gut	Sehr gut	Befriedigend
Mausgesten	Nur per Plugin	●	Nur per Plugin
Mail-Client	Thunderbird	●	Outlook Express

● Ja – Nein Spitzenklasse (100–90) Oberklasse (89–75) Mittelklasse (74–45) Alle Wertungen in Punkten (max. 100)

1) Quelle: Symantec 2) Quelle: www.secunia.com

Ihr PC ist vielen Gefahren ausgesetzt – nicht nur aus dem Internet. CHIP zeigt Ihnen, wie Sie die Risiken richtig einschätzen, um ihnen von vornherein aus dem Weg zu gehen.

Ein PC, der in irgendeiner Form mit der Außenwelt kommuniziert, ist immer der Gefahr von Infektionen ausgesetzt. Die einzige Alternative besteht darin, den Rechner von allen Netzen abzukoppeln und keine Datentransfers zuzulassen – auch nicht über CD, DVD oder USB-Speicherstick. Da dies jedoch keine praktikable Lösung ist, hilft nur umsichtiges Agieren.

CHIP hat für Sie die häufigsten Gefahrenquellen und Sicherheitsrisiken bei der Kommunikation mit der Außenwelt zusammengefasst und zeigt, wie Sie diese Risiken ausschalten können.

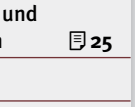
AUF EINEN BLICK

→ Sicherheitsrisiken ausschalten

Alle Tools auf CD

Ad-Aware SE Personal: Spürt die meisten Spyware-Tools auf ◎ Security

AntiVir PE Classic: Schützt effektiv vor Viren und Würmern ◎ Security



Fehlende Updates: PC immer aktuell halten

RISIKO Moderne Software wird zunehmend komplexer – und muss dennoch in immer kürzerer Zeit entwickelt werden. Diese Kombination aus mehr Programmierarbeit und weniger Testaufwand muss zwangsläufig zu mehr Fehlern und damit auch zu einer größeren Zahl von Angriffspunkten führen. Davon ist nicht nur Ihr Betriebssystem betroffen, sondern auch alle Anwendungen, die Sie einsetzen – vom Virenscanner über die Firewall bis zu Ihrem E-Mail- und Messenger-Programm.

LÖSUNG Meist vergeht einige Zeit zwischen der Entdeckung der Schwachstellen durch Hacker und dem Bereitstellen von Sicherheitspatches durch die Hersteller. Sobald diese jedoch da sind, sollten Sie das Update aus dem Internet laden. Damit Sie immer auf dem aktuellsten Stand sind, aktivieren Sie – wo vorhanden – die automatische Aktualisierung übers Inter-

Illustration: S. Schönberger

net. Für alle anderen Anwendungen sollten Sie – etwa über Outlook – eine regelmäßige Erinnerung einplanen, dass Sie selbst im Internet nach Updates suchen und diese installieren.

Nur ein Rechner, bei dem alle bekannten Sicherheitslecks beseitigt sind, ist einigermaßen sicher im Web unterwegs und gegen die dort lauernden Gefahren gewappnet.

2 Achtlosigkeit: Mailen nur mit Virenscanner

RISIKO Die am häufigsten genutzte Internetanwendung heißt nach wie vor E-Mail – und ist damit auch bei Angreifern sehr beliebt. Seit neben der reinen Textmail auch HTML-Mails möglich sind, beschränken sich die Angriffe nicht mehr auf Dateianhänge. Eingebettete Programmzeilen auf Basis von JavaScript oder VB-Script sind zwar eigentlich dafür gedacht, die E-Mail bunter und multimedialer zu machen, sie eignen sich aber auch hervorragend dazu, unerwünschte Programme nachzuladen. Diese Programme infizieren Ihren Rechner und nutzen ihn etwa als Ausgangsbasis für das Versenden von Spammails.

LÖSUNG Setzen Sie Ihren E-Mail-Client grundsätzlich nur im Zusammenspiel mit einem Virenscanner ein. Dafür brauchen Sie nicht unbedingt ein kommerzielles Produkt. Denn auch Freeware-Tools wie etwa AntiVir Personal Edition Classic von Avira (**www.free-av.de/**) können Ihre E-Mails während des Herunterladens überprüfen. Die entsprechende Funktion finden Sie im Experten-Modus unter „Allgemeines | E-Mail“. Geben Sie an dieser Stelle die notwendigen Daten ein, und speichern Sie auch Ihre Anmeldedaten, damit Sie diese nicht jedes Mal manuell eingeben müssen. Achten Sie beim Einsatz des Virenscanners unbedingt darauf, dass er immer auf dem aktuellen Stand der Dinge ist. Genaueres dazu erfahren Sie ab 32.

Viele E-Mail-Provider bieten inzwischen auch einen Online-Virenschutz an – allerdings in der Regel nur gegen Bezahlung. Ein solcher Online-Virenschutz basiert auf den Scan-Engines bekannter Anbieter. So setzt etwa GMX den Virenschutz von Symantec ein.

3 Spam: Schutzmaßnahmen aktivieren

RISIKO Auch Spammer nutzen gerne HTML-Mails – meist mit dem Hintergedanken, mehr über den Empfänger der E-Mail zu erfahren. Durch geschickt eingebaute Bilder, die beim Öffnen der Mail nachgeladen werden, erfährt der Absender zum einen, dass es sich um eine gültige Mailadresse handelt, und zum anderen kann er anhand der IP-Adresse auch Rückschlüsse auf den Standort seines Opfers ziehen. Diese Kombination erhöht den Wert einer E-Mail-Adresse beim Weiterverkauf deutlich.

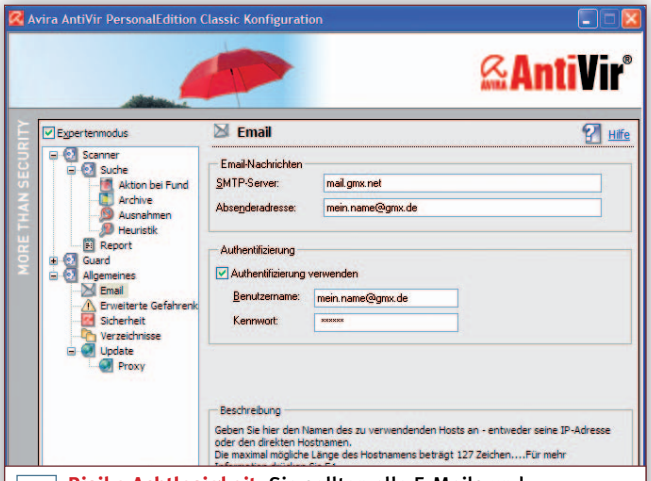
LÖSUNG Damit Bilder nicht automatisch nachgeladen werden, bieten die meisten Mailprogramme einen entsprechenden Schutzmechanismus an. Outlook etwa hat das Laden von Bildern in HTML-Mails von Haus aus unterbunden. Erst nach manueller Freigabe ruft das Mailprogramm die Bilder vom Server des Absenders ab. Sie finden die Einstellungen unter „Extras | Optionen“ auf der Registerkarte „Sicherheit“.

Damit der Spam erst gar nicht auf Ihrem Rechner landet, sollten Sie sich einen Mailprovider suchen, der einen entsprechenden Filter auf seinem Server installiert hat. Alle größeren Anbieter, beispielsweise GMX oder Web.de, stellen eine solche Funktion auch in den kostenlosen Varianten ihres Maildienstes bereit.

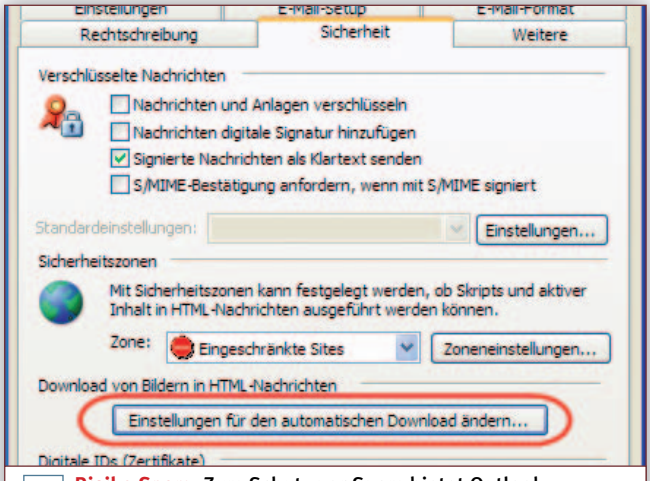
Bei GMX finden Sie alle Antispam-Optionen in der Rubrik „Spamschutz“. An dieser Stelle haben Sie verschiedene Möglichkeiten, Mails zu überprüfen:

- Der „Textmuster-Profiler“ analysiert eingehende Mails und vergleicht sie mit E-Mails in Ihrem „Spamverdacht“-Ordner. Bei hohem Übereinstimmungsgrad verschiebt GMX die Mails automatisch zu den anderen verdächtigen Dokumenten.
- Der „Briefkopf-Analyzer“ untersucht den Inhalt der Betreffzeile. Sind an dieser Stelle einschlägige Begriffe wie etwa „Viagra“ enthalten, verschiebt der Dienst die E-Mail in den „Spamverdacht“-Ordner.
- Der „Spamserver-Blocker“ untersucht die eingehenden Mails auf Fälschung der Absender-Adresse. Diese ist leicht zu manipulieren, nicht jedoch die IP-Adresse des Servers, der als Versender operiert. Bei großen Diensten lässt sich mit diesem Feature Spam zuverlässig identifizieren.

Daneben bietet GMX auch Funktionen zum Anlegen von White- und Blacklists. Darin sind Absender verzeichnet, die ent- →



2 **Risiko Achtlosigkeit:** Sie sollten alle E-Mails und Dateianhänge vor dem Download auf Ihren Rechner von einem Virenscanner wie Aviras AntiVir untersuchen lassen.



3 **Risiko Spam:** Zum Schutz vor Spam bietet Outlook die Option an, dass Bilder in HTML-Mails beim Öffnen nicht automatisch geladen werden.

weder grundsätzlich vertrauenswürdig oder nicht vertrauenswürdig sind. Je nach Einstufung verfährt der Provider mit den E-Mails dieser Absender.

Schließlich gibt es noch zwei Antispam-Listen, mit deren Hilfe GMX E-Mails überprüft: Die globale Antispam-Liste enthält eine Sammlung von Servern, die zum Versand von Spammails genutzt werden. Die Administratoren der GMX-Server verwalten darüber hinaus eine eigene Antispam-Liste, die durch aktive Mitarbeit der GMX-User täglich ergänzt wird.

Die Reaktionsmaßnahmen auf Spammails lassen sich ganz individuell treffen – sowohl direktes Löschen als auch das Speichern im Ordner „Spamverdacht" sind möglich. Letzteres bietet eine nachträgliche Kontrollmöglichkeit für den Fall, dass eine E-Mail aufgrund von allzu restriktiven Regeln fälschlicherweise als Spammail ausgefiltert wurde.

Der Inhalt des Ordners „Spamverdacht" wird vom Provider regelmäßig gelöscht. Die entsprechenden Zeitintervalle lassen sich jedoch – abhängig von dem vorhandenen Paket – ganz individuell festlegen.

Damit Ihr Spamfilter noch effizienter arbeitet, sollten Sie ihn trainieren. Löschen Sie also Spammails nicht nur, sondern markieren Sie sie auch als Spam – entweder mit dem „Durchfahrt verboten"-Schild in der Übersicht oder nach dem Markieren durch Verschieben in den Ordner „Spamverdacht".

Bietet Ihr Mailprovider keinen vergleichbaren Dienst an, sollten Sie auf ein zusätzliches Tool wie die Freeware Spamihilator (auf Heft-CD) zurückgreifen. Es schaltet sich zwischen den E-Mail-Server und den Posteingang und sortiert Ihre Mails vor. Der Spamihilator arbeitet mit einem lernfähigen Filter sowie mit Wortfiltern, die nach bekannten Schlüsselwörtern suchen. Mithilfe von Plugins lässt sich das Tool auch um Funktionen wie Black- und Whitelists erweitern. Der Spamihilator arbeitet mit den bekanntesten Mailprogrammen zusammen (ausführlichere Informationen zum Thema Spamabwehr können Sie ab 56 lesen).

4 Phishing: Bleiben Sie misstrauisch!

RISIKO Während die bis jetzt genannten Gefahren lediglich Bedrohungen für Ihren Rechner und die auf ihm gespeicherten Daten darstellen, geht es Ihnen beim Thema Phishing direkt an den Geldbeutel. Denn die Internetgangster bedienen sich immer dreisterer Methoden, um an Ihr Geld zu kommen.

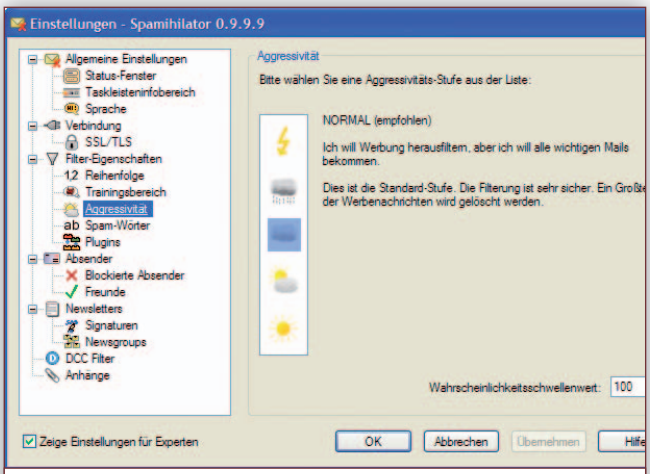
Bei diesem Betrugsversuch erhalten Sie eine offiziell aussehende E-Mail von einer Bank, in der man Sie nach Ihren Zugangsdaten und einer Reihe von Informationen – meist TAN-Nummern – fragt. Die nutzen die Internetgangster anschließend zum Plündern Ihres Kontos.

Es gibt verschiedene Varianten, wie die Angreifer vorgehen: Häufig erscheint etwa innerhalb der Phishing-Mail ein Link, der auf die Webseite Ihrer Bank zeigt. Per Skript wird dieser Link jedoch im Hintergrund umgeleitet, sodass Sie auf der Seite des Phishing-Betrügers landen. Diese Webseite sieht zumeist genauso aus wie die Startseite Ihrer Hausbank. Da dieser Link allerdings auch in Ihrem Browser dargestellt wird, sollten Sie dort genauer hinschauen. Denn meist stimmt der Link nicht hundertprozentig mit der originalen Adresse überein.

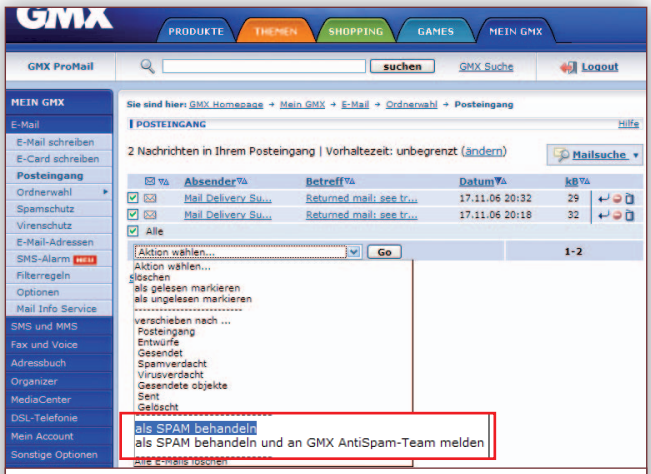
Noch schwieriger zu erkennen sind Veränderungen an der Hosts-Datei unter Windows. Diese Datei hat früher, als es noch keine Proxy-Server gab, dazu gedient, URLs in IP-Adressen zu übersetzen. Wenn Sie in diese Datei eine URL eintragen und dieser eine IP-Adresse zuweisen, akzeptiert der Browser diese IP-Übersetzung, bevor er einen externen Proxy-Server anfragt. Es gibt einige Trojaner, die die Hosts-Datei manipulieren und verschiedene Links auf illegale Server umleiten. Kontrollieren Sie also regelmäßig Ihre Hosts-Datei.

LÖSUNG Die neueste Browser-Generation, also der Internet Explorer 7, Firefox 2 und Opera in der kommenden Version 9.1, sind von Haus aus mit einem Phishing-Schutz ausgestattet, der Sie auf entsprechende Seiten hinweist, bevor Sie irgendwelche Daten eingeben. Aber auch Besitzer älterer Versionen, die noch nicht auf die neueste Browserversion wechseln wollen, können sich mit Zusatzprogrammen schützen. Für Firefox gibt es etwa die Netcraft Toolbar (**https://addons.mozilla.org/firefox/1326/**). Die bekommen Sie auf der Homepage von Netcraft (**http://toolbar.netcraft.com/**) auch für ältere Versionen des Internet Explorer.

Zum Schutz Ihrer Hosts-Datei bietet beispielsweise das Freeware-Tool Spybot



3 Kostenloser Spamschutz: Freeware-Programme wie der Spamihilator schützen Ihren Computer wirkungsvoll vor unerwünschten Werbemails.



3 Spamfilter: GMX bietet – ebenso wie andere Freemail-Provider – lernfähige Scanner zum Erkennen von Spam an. Mit der Zeit landet deutlich weniger Spam in Ihrem Postfach.

– Search & Destroy im erweiterten Modus die Option, die Hosts-Datei als schreibgeschützt zu sperren. Sie erreichen diese Option über „Werkzeuge | IE-Spielereien | Verschiedene Schlösser“.

Seien Sie im Zweifelsfall immer misstrauisch! Folgen Sie nie einem Link aus einer Mail, der vorgibt, von einer Bank zu kommen. Gehen Sie im Zweifelsfall direkt auf die Homepage der Bank, des Versenders oder der Quelle Ihrer Mail. Finden Sie dort keine vergleichbaren Informationen und sind Sie immer noch unsicher, kontaktieren Sie den Kundendienst oder löschen Sie die Mail (mehr zum Thema Onlinebanking lesen Sie ab 86).

5 Trojaner, Keylogger, Rootkits: Den Anfängen wehren

RISIKO Schadprogramme dieser Kategorie zielen darauf ab, die Kontrolle über Ihren PC zu übernehmen und Informationen auszuspähen.

Die längste Historie in diesem Bereich haben Trojaner, benannt nach dem Trojanischen Pferd aus der griechischen Mythologie. Trojaner sind Programme, die sich auf Ihrem PC einnisten, Daten sammeln und in regelmäßigen Abständen an einen Server im Internet schicken. Meist haben Sie diese Programme unbewusst selbst installiert – über eine Anwendung, die Sie auf Ihren PC geladen haben. Downloads aus Tauschbörsen und Filesharing-Bereichen beispielsweise sind besonders riskant.

Trojaner sammeln unterschiedliche Arten von Daten – vom Login für den Internetzugang bis hin zu Kreditkarten-Informationen – und geben sie unbemerkt weiter.

Ähnlich funktionieren Keylogger, die es als Hardware- und als Software-Variante gibt. Sie schalten sich zwischen Tastatur und Betriebssystem und protokollieren die Eingaben. Je nach Intelligenz des Programms zeichnet es entweder den kompletten Datenstrom oder nur bestimmte Informationen auf, beispielsweise Passwörter, Konto- oder Kreditkartendaten.

Der Software-Keylogger speichert die Daten entweder direkt auf der Festplatte oder gibt sie per Internet an den Spion weiter.

Die Hardware-Variante wird zwischen PC und Tastatur gesteckt, sie kann also bei genauem Hinsehen durchaus entdeckt werden. Da die meisten PCs jedoch unter dem Schreibtisch stehen, kann bis zur Enttarnung eines Hardware-Keyloggers einige Zeit vergehen. Die Geräte besitzen entweder einen kleinen Zwischenspeicher oder senden die Daten per Funk weiter. Inzwischen sind auch Tastaturen auf dem Markt, die Keylogger integriert haben – folglich wird es noch schwerer, sie zu erkennen.

Perfekt getarnt sind in der Regel auch Rootkits – die neben den Fähigkeiten von Trojanern und Keyloggern meist auch noch Backdoor-Funktionen auf Ihrem Rechner installieren. Ein Rootkit erlaubt seinen Programmierern, sich unbemerkt Zugang zu Ihrem PC zu verschaffen und ihn als Ausgangsstation für weitere Aktionen zu nutzen, etwa für das Versenden von Spammails. Rootkits ersetzen meist Teile des Betriebssystemkerns durch eigene Versionen und sind daher nur schwer zu identifizieren.

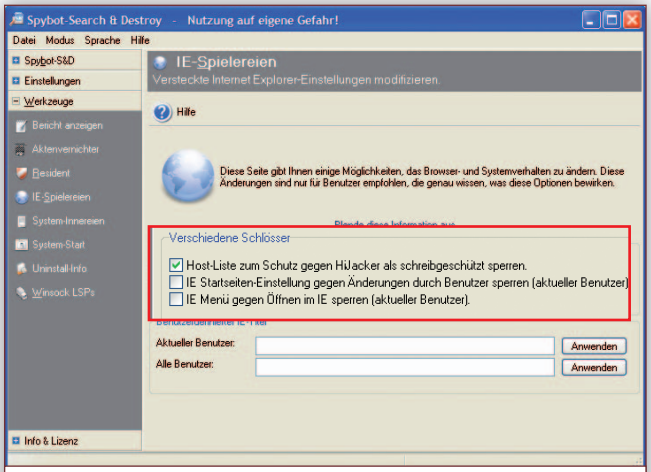
LÖSUNG Alle drei Sicherheitsrisiken haben eines gemeinsam – Sie bemerken meistens nichts von ihrem Auftreten. Deswegen sollten Sie von Anfang an dafür sorgen, dass diese Programme keine Chance haben, sich auf Ihrem Rechner einzunisten. Wie Sie am besten vorgehen und wie Sie die Plagegeister im Ernstfall loswerden, erfahren Sie ab 32.

Die einfache Version der Hardware-Keylogger erkennen Sie daran, dass das Gerät als Stecker zwischen Tastatur und Rechner sitzt. Schwieriger wird es, wenn der Keylogger in die Tastatur integriert ist. Sollten Sie also plötzlich eines Morgens an Ihrem Büro-PC ein neues Keyboard vorfinden, ohne dass Sie danach gefragt haben, könnte sich die Rücksprache mit der Support-Abteilung lohnen.

6 Dialer: Abzock-Vorwahlen sperren lassen

RISIKO Eine weitere Gefahrenquelle sind Dialer. Dabei handelt es sich um Einwahlprogramme ins Internet, die eine Verbindung nicht zum normalen Ortstarif herstellen, sondern über teure Vorwahlnummern – früher über 0190-, heute über 0900-Nummern.

Dabei gibt es eine große Gruppe legaler Dialer, die bei der Nutzung kostenpflichtiger Internetdienste für die Abwicklung des Bezahlvorgangs zuständig sind. Zu Beginn des Jahres 2006 waren →



4 **Risiko Phishing:** Im erweiterten Modus von Spybot – Search & Destroy gibt es eine Funktion zum Schutz der Hosts-Datei. Sie verhindert, dass Sie unwissentlich auf Phishing-Seiten landen.

6 **Risiko Dialer:** Der a-squared Anti-Dialer durchsucht Ihren Rechner nach illegalen Dialern, löscht sie und schützt ihn anschließend mit einem Guard-Programm.

nach Angaben der Website Dialer-Schutz (**www.dialerschutz.de/**) rund 1,77 Millionen Dialer bei der Bundesnetzagentur registriert. Übernimmt ein solcher legaler Dialer die Einwahl, muss der Kunde dennoch explizit auf die Kosten des Dienstes hingewiesen werden.

Illegale Dialer dagegen installieren sich ohne Zustimmung des Users im Hintergrund, kappen die Verbindung zum Internetprovider und bauen stattdessen eine neue, erheblich teurere Verbindung auf. Das böse Erwachen für den Anwender kommt mit der Telefonrechnung am Monatsende.

LÖSUNG Das Risiko, mithilfe von Dialern betrogen zu werden, ist in den letzten Monaten aufgrund der Verbreitung von Breitbandanschlüssen und Volumentarifen oder Flatrates geringer geworden. Eine Bedrohung stellen Dialer nur noch für User dar, die über ein analoges Modem oder ISDN ins Internet gehen. Für DSL-Nutzer besteht keine Gefahr, da bei DSL keine Einwahl stattfindet. Allerdings sollten auch DSL-User darauf achten, dass noch vorhandene Modems oder ISDN-Karten sicherheitshalber vom Telefonnetz getrennt werden.

Beim Erkennen und Beseitigen von Dialern helfen Ihnen etwa die Tools Spybot – Search & Destroy oder a-squared Anti-Dialer. Sie finden beide Programme auf unserer Heft-CD.

Außerdem bieten Telekom und die meisten anderen Telekommunikationsfirmen auch die Sperrung bestimmter kostenpflichtiger Vorwahlen an, sodass Sie hundertprozentig geschützt sind.

7 Adware: Gratis-Tools und Browser können helfen

RISIKO Meist weniger gefährlich, aber dafür unglaublich lästig ist Adware. Dabei handelt es sich um Programme, die sich auf Ihrem Rechner installieren und dort bunte Werbebotschaften, zusätzliche Toolbars im Webbrowser oder dubiose Suchseiten öffnen.

Diese Werbebotschaften haben Sie sich entweder mit einer Testsoftware eingefangen, die sich über Werbung finanziert, oder beim Surfen durchs Internet. Bei Installationen werbefinanzierter Programme sollten Sie auf entsprechende Hinweise der Hersteller achten. Durch die Deinstallation der mit diesen Programmen verbundenen Adware kann es allerdings dazu kommen, dass auch die Software selbst nicht mehr funktioniert. Die Installationsroutinen der Programme sollten einen entsprechenden Hinweis enthalten – dies entschieden auch jüngst amerikanische Gerichte und verurteilten die Firma Zango wegen Einschmuggelns von Adware auf PCs zu einer Geldstrafe von drei Millionen Dollar. Zango hat erst kürzlich negative Schlagzeilen gemacht, als bekannt wurde, dass über irreführende Links innerhalb von MySpace anstelle der erwarteten Videos die Zango-Adware installiert worden war.

Eine andere Adware-Infektionsquelle sind Internetseiten der Kategorie Sex und Warez, die – im Hintergrund oder mit dem Download von Programmen, Filmen oder Bildern – die Werbebanner und -fenster mitinstallieren.

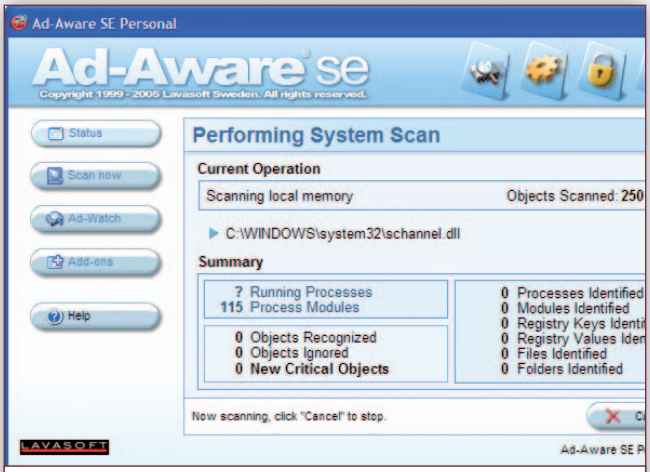
LÖSUNG Programme, die bei der Beseitigung der Werbeeinblendungen helfen, sind etwa das bereits erwähnte Spybot – Search & Destroy, Ad-Aware SE Personal Edition von Lavasoft (**www.lavasoftusa.com/products/ad-aware_se_personal.php**) oder der Spyware Doctor (**www.pctools.com/de/spyware-doctor/**). Die ersten beiden Anwendungen sind Freeware, der Spyware Doctor kostet nach 30-tägiger Testphase rund 35 Euro.

Weitere Werbeeinblendungen, die direkt als Popup über den Browser kommen, stoppen Sie mit Popup-Blockern, die in den neuen Browserversionen von Internet Explorer, Firefox und Opera standardmäßig installiert sind. Mit der Google-Toolbar für den Internet Explorer bekommen Sie zusätzlich einen Popup-Blocker mitgeliefert, für den Firefox gibt es Adblock Plus (auf der Heft-CD), und Opera besitzt bereits in der vorherigen Version einen Adblocker, braucht folglich keine Addons.

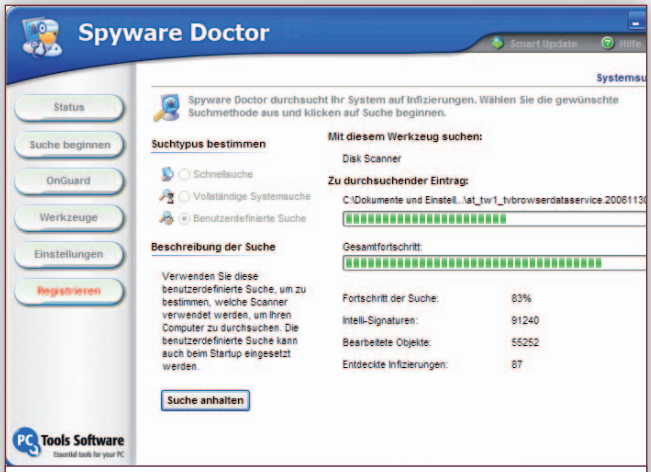
8 Hoaxes: Keine Reaktion ist die richtige Reaktion

RISIKO Während die bisher genannten Bedrohungen einen durchaus realen Hintergrund haben, täuscht ein Hoax eine Gefährdung des Users nur vor. Diese Programme sollen dem Besitzer lediglich Angst einjagen oder ihn desorientieren. Die Falschmeldungen verbreiten sich per E-Mail, in Instant Messengern oder auch via Handy als SMS oder MMS.

Die einzige Gefahr bei derartigen Belästigungen besteht oft genug in der An-



7 Risiko Adware: Die Freeware Ad-Aware Personal Edition SE hilft Ihnen zuverlässig beim Entfernen von Adware und Spyware von Ihrem Rechner.



7 Spyware loswerden: Auch der Spyware Doctor erkennt und entfernt Spy- und Adware. Allerdings kostet das Tool nach der 30-tägigen Testphase rund 35 Euro.

zahl der Warnungen vor einer möglichen Gefahr. Eines der bekanntesten Beispiele dafür ist die Legende vom „Good Time Virus“. Eine E-Mail – 1994 millionenfach verschickt – warnte vor dem Öffnen spezieller E-Mails, die angeblich die Festplatte löschen.

Auch Kettenbriefe fallen unter diese Kategorie. Wer hat sie noch nicht erhalten, die E-Mail vom reichen Onkel aus Nigeria oder der Erbschaft aus Südafrika? Eine interessante Sammlung finden Sie auf den Seiten der Hoaxbusters (**www.hoaxbusters.de**).

Eine sehr ausführliche Hoax-Liste finden Sie auch auf der Website der Technischen Universität Berlin (**www.tu-berlin.de/www/software/hoaxlist.shtml**). Viele der gesammelten Hoax-Beispiele sind mit dem Originaltext der Nachricht dokumentiert.

Manche der Hoax-Mails sind so gut gemacht, dass Sie sich im ersten Moment fragen, ob es sich nicht doch um eine echte Nachricht handelt. Anhand dieser Kriterien können Sie wahre von falschen Nachrichten unterscheiden:

- Sie werden aufgefordert, die Mail an möglichst viele Personen weiterzuleiten.
- Die Themen der Nachricht handeln meist von einem Virus, einer Erbschaft oder einem guten Geschäft.
- Oft wird eine namhafte Firma als Leumund vorgeschoben, die mit der Sache überhaupt nichts zu tun hat.
- In den Mails finden Sie meist keine absoluten Zeitangaben wie etwa „1. Dezember 2006“, sondern nur relative wie „letzten Freitag“ oder „gestern“.

LÖSUNG Letzten Endes gibt es an dieser Stelle nur eine richtige Reaktion. Antworten Sie nicht, leiten Sie die Mail nicht weiter, sondern löschen Sie sie und melden Sie sie Ihrem Spamfilter, damit solche Post beim nächsten Mal gleich im Papierkorb landet.

9 Social Engineering: Schweigen ist Gold

RISIKO Eine nicht zu unterschätzende Gefahrenquelle im IT-Bereich sind die Anwender selbst. Kevin Mitnick, einer der bekanntesten Hacker aller Zeiten, hat die meisten seiner Angriffe auf die unterschiedlichsten Ziele mit „Social Engineering“ vorbereitet.

Social Engineering baut darauf, dass Mitarbeiter am Telefon Informationen preisgeben, wenn man geschickt fragt oder sie unter Druck setzt. Meistens fängt der Datensammler bei der Putzfrau oder der Sekretärin an und versucht, sich ein Bild über Standardvorgänge innerhalb der Firma oder über Abteilungs- und Hierarchiestufen zu machen. Mit diesen Informationen arbeitet er sich in der Organisation Stufe für Stufe nach oben, bis genug Hintergrundwissen vorhanden ist, um bei einem Mitarbeiter mit den notwendigen Netzzugangsrechten anzurufen und ihn mit einer plausibel klingenden Begründung nach Benutzernamen und Passwort zu fragen.

Statistisch gesehen ist diese Methode, an fremde Daten zu kommen, erheblich erfolgreicher als ein Brute-Force-Ansatz, bei dem mithilfe mathematischer Logik automatisiert verschiedene Kombinationen aus Benutzernamen und Passwort abgefragt werden.

LÖSUNG Vor Social Engineering sind Sie nur sicher, wenn Sie per Telefon oder E-Mail grundsätzlich keine sicherheitsrelevanten Daten an Personen weitergeben, die Sie nicht kennen. Bleiben Sie auch unnachgiebig, wenn der Anrufer versucht, Sie mit technischem Fachchinesisch in die Enge zu treiben oder Druck auf Sie auszuüben. Informieren Sie nach einem solchen verdächtigen Anruf umgehend Ihren Vorgesetzten und – falls vorhanden – auch einen Mitarbeiter aus dem Bereich Datensicherheit.

10 Naivität der User: Sicherheit ernst nehmen

RISIKO Im Internet lauern an vielen Ecken unterschiedlichste Bedrohungen – dessen sollten Sie sich immer bewusst sein. Jeder Download ist eine potenzielle Gefahr – laden Sie also Daten nur aus sicheren Quellen herunter. Webseiten mit dubiosen Inhalten, etwa Seriennummern oder Programmen zum Generieren von Registrierungsschlüsseln, stehen immer unter Verdacht, auch Trojaner, Rootkits und Viren zu verteilen. Damit Ihre Ausflüge ins Internet angstfrei stattfinden können, sollten Sie Ihren Rechner also bestmöglich schützen.

LÖSUNG Wenn Ihr Computer von mehreren Personen – auch von Kindern – genutzt wird, achten Sie auf die Einhaltung strenger Sicherheitsrichtlinien. Bewegen Sie sich nie als Administrator des Computers im Internet, und installieren Sie neben Virenscanner und Firewall auch weitere Schutzsoftware, etwa Spybot – Search & Destroy oder den a-squared Anti-Dialer.

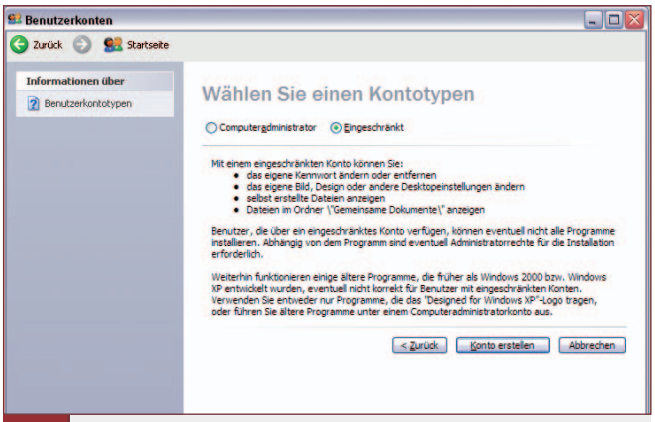
8 Risiko Hoaxes: Auf der Website der Technischen Universität Berlin finden Sie eine ständig aktualisierte Liste von Hoax-Meldungen. Bei vielen Hoaxes haben Sie die Möglichkeit, den Originaltext der Falschmeldung nachzulesen.

Fazit: Misstrauen schützt

Für jede Gefahrenquelle im Internet gibt es auch Software, die Ihren Rechner davor schützen kann. Viele Hersteller bieten diese Tools inzwischen als Sammlung in einer Security-Suite an. Einen Test aktueller Security-Suiten lesen Sie ab 8.

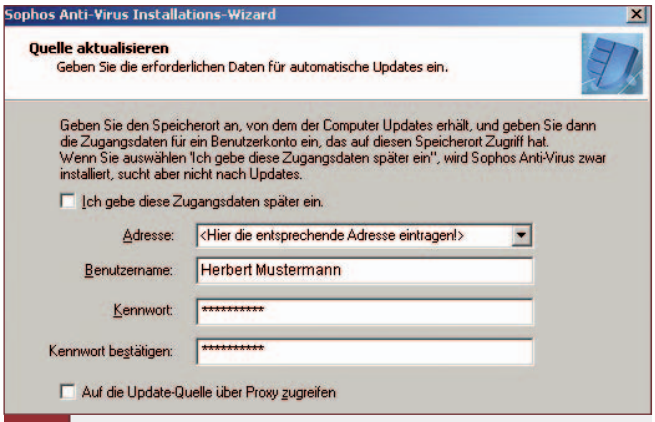
Trotzdem sollten Sie den Schutz Ihres Computers nicht allein der Software überlassen. Wachsamkeit und ein Schuss gesunden Misstrauens sind mindestens ebenso wichtige Faktoren für die Sicherheit Ihres PCs.

Andreas Hitzig



1 Neues Konto anlegen

Verwenden Sie zum Surfen im Internet immer nur ein Benutzerkonto mit eingeschränkten Rechten. Um so etwas anzulegen, schalten Sie die automatische Windows-Anmeldung aus und wählen die Authentifizierung mit Benutzernamen und Passwort. Richten Sie in der Systemsteuerung ein Benutzerkonto ein. Geben Sie ihm einen beliebigen Namen, klicken Sie auf „Weiter“ und wählen Sie „Eingeschränkt“. Verwenden Sie dieses Konto zum Surfen im Web. Schadprogramme haben dann keinen Zugriff auf die Systemeinstellungen.

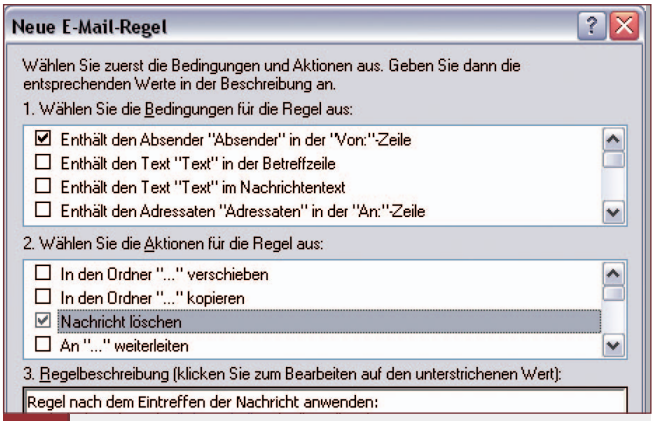


2 Virenschutz installieren

Ohne einen guten Virenschutz sollten Sie keine Verbindung zum Internet aufbauen. Antiviren-Software blockiert Viren und Würmer, die per E-Mail oder auf anderen Wegen auf den Rechner gelangen wollen. Auch Freeware-Tools bieten übrigens oft einen guten Schutz. Installieren Sie das Antiviren-Programm Ihrer Wahl. Achten Sie darauf, den Virenschutz regelmäßig zu aktualisieren (mindestens einmal pro Woche), denn sonst kann die Software neu aufgetauchte Viren und Würmer nicht entdecken.

ALLE TOOLS AUF HEFT-CD

Absichern in 10 Minuten



5 Spammails aussperren

Zwar nicht gefährlich, aber umso lästiger ist Spam: Werbung, die den elektronischen Briefkasten verstopft. Fast jedes Mailprogramm bietet daher Filterregeln an, um den Werbemüll auszusortieren. Benutzer von Outlook Express öffnen dazu das Menü „Extras“ und wählen die Optionen „Nachrichtenregeln“ und „E-Mail“. Erkannte Spammails können in ein besonderes Verzeichnis verschoben oder gleich gelöscht werden. Nach Festlegen der Filterregeln landet spürbar weniger Werbung im E-Mail-Posteingang.

6 Dateien verschlüsseln

Wer vertrauliche Daten auf seinem Rechner hat, sollte sie unbedingt verschlüsseln, um sie vor anderen Personen geheim zu halten. Windows XP bietet dazu die EFS-Verschlüsselung an, die allerdings nur in der Professional-Edition enthalten ist. Für Benutzer der Home-Edition schafft zum Beispiel das Freeware-Programm Easy Crypto Deluxe Abhilfe. Die Software verschlüsselt Ihre Dateien und macht sie für alle unleserlich, die das Passwort nicht kennen. Easy Crypto finden Sie ebenfalls auf unserer Heft-CD.

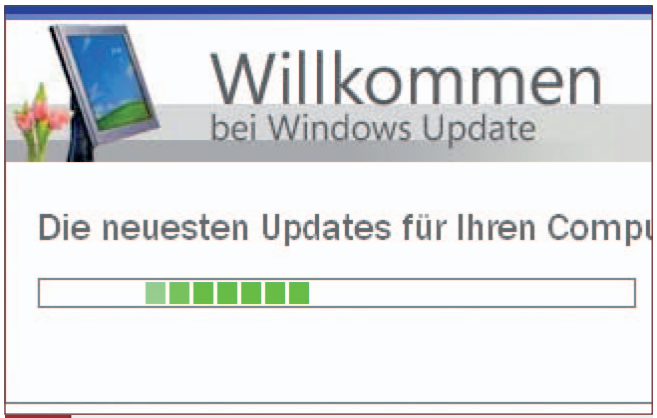
3 Firewall aktivieren

Eine Firewall schützt vor Eindringlingen aus dem Internet und wehrt Hackerangriffe genauso ab wie die meisten Würmer. Windows XP verfügt standardmäßig über einen Port-Blocker, die einfachste Art einer „Brandschutzmauer“. Um ihn zu aktivieren, wechseln Sie in die Systemsteuerung und öffnen dort „Netzwerk- und Internetverbindungen“. Klicken Sie auf „Windows Firewall“ und aktivieren Sie die Funktion. Über das Register „Ausnahmen“ legen Sie die Programme fest, die von außen erreichbar sein sollen, etwa einen Messenger.

4 Spyware abblocken

Besonders perfide sind Programme, die Ihren PC heimlich nach Kreditkarten- oder Kontodaten durchstöbern und ihre Erkenntnisse ins Internet schicken. Man nennt diese Gattung Spyware. Die Schnüffelprogramme sind eine Mischung aus Wurm, Hackerangriff und Surfhilfe. Deshalb sollte jeder PC-Benutzer Antispy-Software zum Entfernen dieser Spione installieren. Programme wie Spybot, Ad-Aware oder XP-Anti-Spy finden Sie auf unserer Heft-CD. Die Anwendungen spüren die lästigen Spione auf und entfernen sie von der Festplatte.

Wenn Sie mit Ihrem PC online gehen, setzen Sie sich vielfältigen Gefahren aus. Den absoluten Schutz kann es zwar nicht geben, aber mit ein paar Handgriffen lässt sich Ihr Windows-Rechner sehr wirkungsvoll gegen Angriffe von Viren, Würmern und Hackern absichern.



7 Betriebssystem aktuell halten

Alle Sicherheitsmaßnahmen nützen wenig, wenn das Betriebssystem nicht auf dem neuesten Stand gehalten wird. Wenn Sie die dafür zuständige Auto-Update-Funktion von Windows XP ausgeschaltet haben, sollten Sie zumindest einmal im Monat nach sicherheitsrelevanten Updates Ausschau halten und sie unverzüglich installieren. Dazu stellen Sie im Internet Explorer unter „Extras“ eine Verbindung zum „Windows Update“ her und klicken auf „Schnellsuche“. Wenn es neue Patches gibt, klicken Sie auf „Installieren“.

TIPP BOSS – Sicherheit vom BSI

Basic Facts: Open-Source-Sicherheitssoftware, die auf dem PC Sicherheitslücken und Schwachstellen aufspürt.

Beschreibung:
BOSS (BSI Open Source Software Security Suite) ist eine Sicherheitssoftware des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Tipp:
BOSS 2.0 ist ein Live-System, mit dem sich der PC direkt von der CD starten lässt. Es basiert auf dem freien Sicherheits-Scanner Nessus (**www.nessus.org**) und überprüft die Sicherheit von Anwendungen, eines lokalen Rechners oder eines Computernetzwerks. Um die Live-CD anzulegen, laden Sie sich von der BSI-Website (**www.bsi.de**) zunächst die ISO-Datei der Anwendung herunter. Anschließend kopieren Sie dieses Image mit einer beliebigen Brennsoftware auf eine CD oder DVD. Die Hardware-Voraussetzungen von BOSS umfassen einen Pentium-Prozessor, 512 MByte Arbeitsspeicher und ein bootfähiges CD-Laufwerk.

GEHEIME SYSTEM-TRICKS

Mehr Sicherheit durch Registry-Tuning

Windows XP bringt einige effiziente Sicherheitseinstellungen mit, die standardmäßig nicht aktiviert sind. CHIP zeigt Ihnen, wie Sie diese Optionen durch gezielte Registry-Eingriffe nutzen.

Mehr Sicherheit für Ihren XP-PC – das erreichen Sie auf zwei Wegen: Entweder ändern Sie direkt die Werte in der Registry, oder Sie greifen auf eines der Tools zurück, die eine Reihe von Registry-Eingriffen über eine grafische Oberfläche zusammenfassen.

AUF EINEN BLICK

Alle Tools auf CD

XP-AntiSpy: Entfernt Spyware und optimiert die Registry ◎ **Windows**

Xpy: Deaktiviert Schnüffelfunktionen in der Registry ◎ **Windows**

→ Registry direkt bearbeiten

Bevor Sie sich mit der Registrierdatenbank von Windows beschäftigen, sollten Sie sich klarmachen, dass Änderungen an der Registry zu Systeminstabilität und Datenverlust führen können. Folgen Sie also den Anweisungen in diesem Beitrag exakt, und sichern Sie zuvor die Registrierdatenbank, sodass Sie sie im Notfall wiederherstellen können.

Rufen Sie dazu den Registrierungseditor auf („Start | Ausführen | Regedit“), und wählen Sie den Menüpunkt „Datei | Exportieren“. Achten Sie beim Speichern der Registry darauf, dass Sie nicht nur die ausgewählte Teilstruktur, sondern alles speichern. Die Auswahl finden Sie am unteren Ende des Fensters.

Auf den nächsten Seiten stellt Ihnen CHIP einige interessante Registry-Einträge vor, mit deren Hilfe Sie Ihren PC absichern und unerwünschte Kommunikation mit der Außenwelt unterbinden.

Registry-Trick 1: Herunterfahren verhindern

Bei PCs, die als Demo-Systeme auf Messen oder Ausstellungen genutzt werden oder permanent als Testrechner laufen sollen, lässt sich die Funktion „Herunterfahren“ deaktivieren. Dieser Eintrag stoppt aber nicht das Herunterfahren eines PCs, das durch Software initiiert wird.

Fügen Sie in der Rubrik „HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer“ ein neues DWord mit dem Wert „No

Illustration: S. Schönberger

Close“ hinzu, und versehen Sie diesen Schlüssel mit dem Wert „1“. Beim nächsten Start Ihres Rechners ist die Schaltfläche „Herunterfahren“ verschwunden, und die Tastenkombination [Alt]+[F4] wird mit einer Fehlermeldung quittiert.

Löschen Sie den Schlüssel „NoClose“, lässt sich der Computer wieder wie gewohnt herunterfahren.

Registry-Trick 2: Windows-Taste sperren

Neben dem Deaktivieren des Herunterfahrens ist auch das Sperren der Windows-Taste möglich. Denn mit ihr lässt sich beispielsweise problemlos der Windows Explorer aufrufen.

Gehen Sie in der Registry zum Schlüssel „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout“ und fügen Sie einen neuen Binärwert mit dem Namen „ScanCode Map“ ein. Versehen Sie diesen mit dem Wert „00 00 00 00 00 00 00 00 03 00 00 00 00 00 5B E0 00 00 5C E0 00 00 00 00“, und starten Sie anschließend den Rechner neu.

Zur Aktivierung der Windows-Taste löschen Sie diesen Schlüssel und booten Ihren PC noch einmal.

Registry-Trick 3: WGA-Prüfung deaktivieren

Microsoft verteilt seit Juni 2006 den Patch 905474, der ein Tool zur Echtheitsprüfung von Windows installiert (WGA, Windows Genuine Advantage). Das Tool untersucht Ihren Registrierungsschlüssel und kontaktiert dabei eine Blacklist im Internet – wird er dort gefunden, erscheint bei jeder Anmeldung ein Warnhinweis. Wer WGA installiert hat, die Kommunikation aber stoppen möchte, muss dazu den Schlüssel „WGALogon“ in der Registry im Pfad „HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify“ löschen.

Registry-Trick 4: Dateien direkt löschen

Der Windows-Papierkorb speichert gelöschte Dateien in einem eigenen Ordner, bis er geleert wird – es sei denn, Sie haben das Entleeren automatisiert. Wenn mehrere Personen an einem PC mit dem gleichen Benutzerkonto arbeiten, sollten Sie aus Sicherheitsgründen den Papierkorb deaktivieren und Windows veranlassen, die Dateien sofort zu löschen.

Ändern Sie dazu im Schlüssel „HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket“ den Wert „NukeOnDelete“ von „0“ auf „1“.

Setzen Sie den Wert auf „0“ zurück, verhält sich der Papierkorb wieder wie gewohnt.

Registry-Trick 5: Programm-Installation schützen

Wenn Sie auf einem Rechner zwar die Installation von Programmen, nicht aber deren Änderung oder gar das Löschen zulassen wollen, gibt es auch dafür einen Weg über die Registry.

In der Systemsteuerung finden Sie unter „Software“ alle installierten Programme – diese weisen zudem den Button „Ändern/Entfernen“ auf oder sogar zwei Schaltflächen – „Ändern“ und „Entfernen“. Wenn Sie einzelne Anwendungen schützen möchten, navigieren Sie in den Bereich „HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall“. Dort finden Sie alle installierten Programme.

Das Löschen und das Ändern werden über die beiden Werte „NoModify“ und „NoRemove“ gesteuert. Diese sind entweder schon vorhanden – ansonsten fügen Sie sie als neue Einträge über DWORD hinzu und versehen sie mit dem Wert „1“. Dieser Wert steht für das Ausblenden eines Eintrags, „0“ dagegen für das Einblenden.

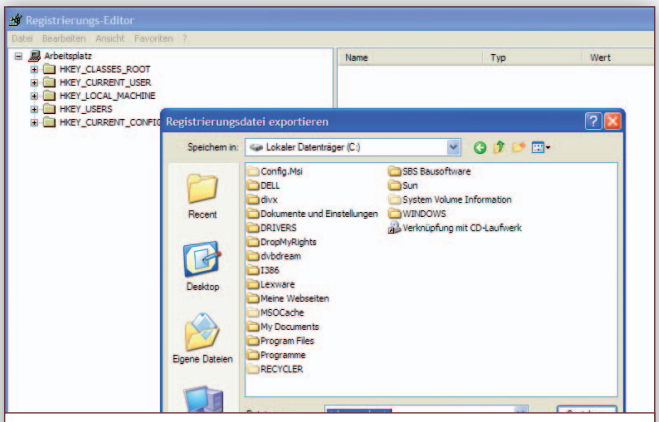
Registry-Trick 6: Systemsteuerung schützen

Computer, die als öffentliches Terminal genutzt werden, sollten besonders vor Veränderungen geschützt werden. Denn gerade in der Systemsteuerung lassen sich viele Parameter verstellen. Mit einem einfachen Registry-Trick verhindern Sie den Zugriff auf bestimmte Funktionen in der Systemsteuerung.

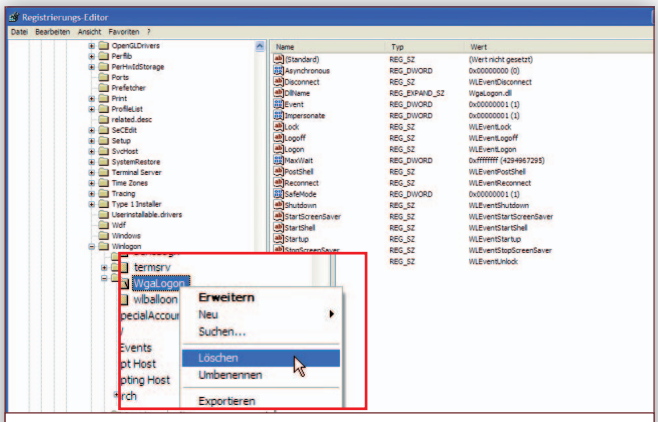
Der Schlüssel „HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ControlPanel\don't load“ definiert, welche Symbole in der Systemsteuerung nicht geladen werden sollen. Legen Sie dazu im rechten Fenster eine neue Zeichenfolge an und geben Sie dieser den Namen des Symbols, das verschwinden soll. Zur Auswahl stehen die folgenden Werte:

desk.cpl: Anzeige

nusrmgr.cpl: Benutzerkonten →



Unbedingt sichern: Vor jeder Änderung der Registrierdatenbank von Windows XP sollten Sie mit dem Befehl „Datei | Exportieren“ eine Sicherungskopie anlegen.



WGA-Prüfung deaktivieren: Die permanente Authentifizierung Ihres Systems bei Microsoft unterbinden Sie durch Löschen des Schlüssels „WgaLogon“ in der Registry.

timedate.cpl: Datum und Uhrzeit
powercfg.cpl: Energieoptionen
joy.cpl: Game-Controller
hdwwiz.cpl: Hardware
inetcpl.cpl: Internetoptionen
main.cpl: Maus und Tastatur
intl.cpl: Regions- und Sprachoptionen
appwiz.cpl: Software
mmsys.cpl: Sounds und Audiogeräte
sapi.cpl: Sprachein- und -ausgabe
sysdm.cpl: System
telephon.cpl: Telefon-/Modemoptionen

Eine Reihe von weiteren Symbolen lassen sich über den Schlüssel ausblenden. Er besitzt eine Reihe von Unterschlüsseln, die unter anderem auch das Aussehen der Systemsteuerung beeinflussen:
{6DFD7C5C-2451-11d3-A299-00C04F8EF6AF}: Ordneroptionen
{7007ACC7-3202-11D1-AAD2-00805FC1270E}: Netzwerkverbindungen
{D20EA4E1-3957-11d2-A40B-0C5020524152}: Schriftarten
{D20EA4E1-3957-11d2-A40B-0C5020524153}: Verwaltung
{D6277990-4C6A-11CF-8D87-00AA0060F5BF}: Geplante Tasks
{E211B736-43FD-11D1-9EFB-0000F8757FCD}: Scanner und Kameras

Wenn Sie eines dieser Symbole entfernen möchten, müssen Sie den entsprechenden Schlüssel löschen. Vor dieser Aktion sollten Sie ihn jedoch exportieren und an einem sicheren Ort speichern, um ihn bei Bedarf wieder in die Registry zu integrieren. Klicken Sie zum Sichern mit rechts auf den Schlüssel, und wählen Sie die Option „Exportieren".

Weitere Werte finden Sie – abhängig von den installierten Programmen –, wenn Sie über den Dateimanager nach *.cpl suchen. Fügen Sie diese wie beschrieben der Rubrik „Don't load" hinzu.

Nach einem Neustart von Windows XP sind die Symbole aus der Systemsteuerung verschwunden.

Registry-Trick 7: Desktop-Eigenschaften schützen

In Desktop-Eigenschaften befinden sich die Einstellmöglichkeiten für die Bildschirmauflösung, den Bildschirmschoner und auch das Passwort des Bildschirmschoners. Zum Schutz des Desktops – das gilt auch für das Symbol „Anzeige" in der Systemsteuerung – weisen Sie dem DWORD-Eintrag „NoDispCPL" unterhalb des Schlüssels „HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies" den Wert „1" zu. Der Eintrag ist allerdings nur für den User gültig, unter dem Sie angemeldet waren, als Sie den Wert angelegt haben. Die Änderung wird beim nächsten Anmeldevorgang wirksam.

Zum Bearbeiten der Anzeige-Eigenschaften löschen Sie entweder den erzeugten Eintrag oder weisen ihm den Wert „0" zu.

Registry-Trick 8: Taskleiste schützen

Die Taskleiste besitzt eine ganze Reihe von Eigenschaften – von der Position über die Anzeige der inaktiven Positionen bis hin zum Aussehen im klassischen oder XP-Stil. Diese Werte lassen sich individuell konfigurieren und schützen. Legen Sie dazu unterhalb des Schlüssels „HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" den DWord-Eintrag „NoSetTaskbar" an, und aktivieren Sie ihn mit dem Wert „1". Damit die Änderung wirksam wird, melden Sie sich neu an.

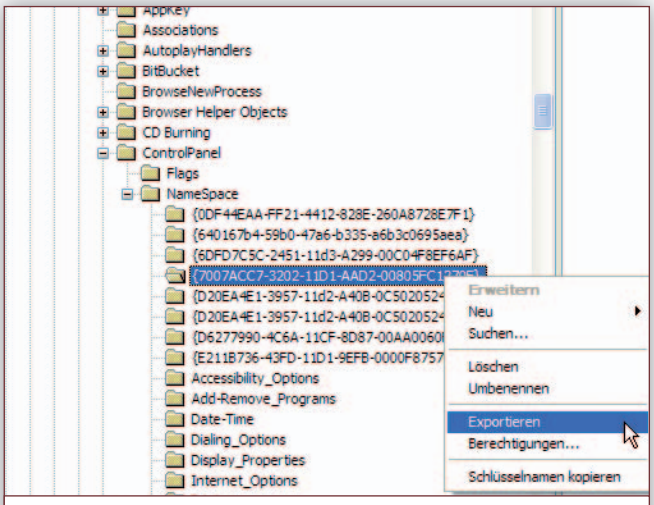
Erneuten Zugriff auf die Eigenschaften der Taskleiste erhalten Sie durch Löschen des angelegten Eintrags oder durch Zuweisen des Werts „0".

→ Tweak-Tools einsetzen

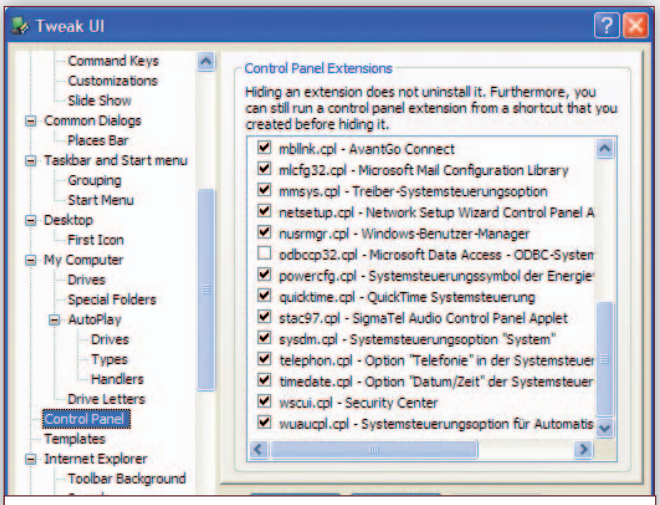
Die Liste interessanter Registry-Parameter lässt sich beliebig erweitern. Noch schneller und komfortabler können Sie die Registry mit Tweak-Programmen modifizieren. Das sind Sammlungen von Registry-Werten, die Sie über eine grafische Oberfläche beeinflussen können. CHIP hat die besten Tools zusammengestellt.

Tweak UI: Tweaken mit Microsoft

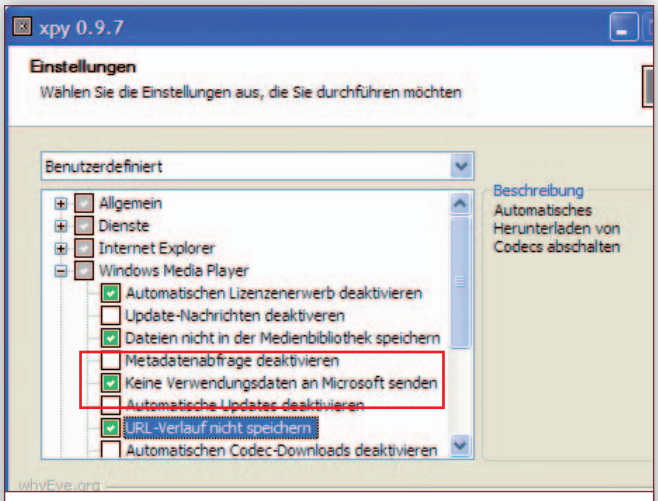
Bereits seit Windows 95 bietet Microsoft Tweak UI an, um Registry-Einträge zu setzen. Das Tool ist inzwischen in die PowerToys integriert (**www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx**).



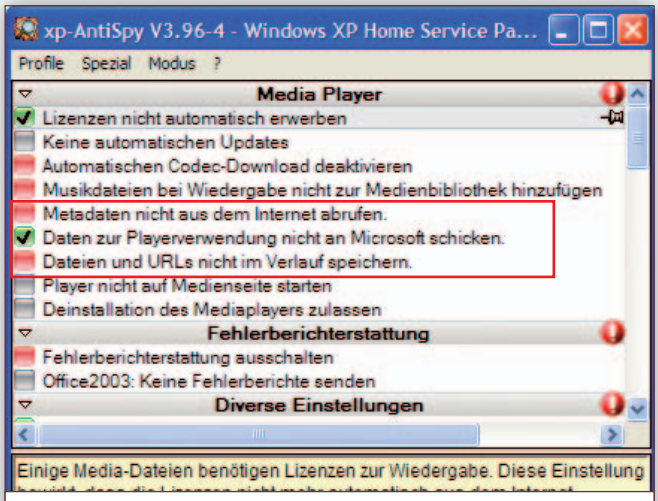
Schlüssel exportieren: Vor dem Löschen von Schlüsseln sollten Sie diese zur Sicherheit exportieren, damit Sie die Werte einfach rekonstruieren können.



Tweak UI: Das Registry-Tool von Microsoft macht diverse versteckte Einstellungen über eine grafische Oberfläche zugänglich, etwa das Ausblenden von Symbolen der Systemsteuerung.



Xpy: Das Open-Source-Tool Xpy ist eine Alternative zu XP-AntiSpy und schützt Ihren Rechner vor allzu neugierigen Herstellern.



XP-AntiSpy: Das Freeware-Tool XP-AntiSpy unterbindet die unerwünschte Kommunikation diverser Programme mit dem Hersteller.

Die Art der Einstellungen ist in verschiedene Rubriken gegliedert. Sie können mit Tweak UI etwa auch innerhalb der Rubrik „Control Panel“ die Systemsteuerungseinträge ein- und ausblenden.

Tweak-XP Pro: Registry professionell bearbeiten

Wesentlich mehr Möglichkeiten bietet das kommerzielle Programm Tweak-XP Pro 4.0.8 (**http://dl1.totalidea.com/files/public/txp4trial.exe**). Beim ersten Start legt es einen Wiederherstellungspunkt und auf Wunsch eine Kopie der Registry an. Damit lässt sich der vorherige Zustand Ihres Windows problemlos rekonstruieren, falls Probleme auftreten.

Tweak-XP Pro bietet drei Rubriken: System, Windows und Internet. Wichtige Änderungsmöglichkeiten aus den Bereichen Sicherheit finden Sie in den Windows-Tricks und den Tweaks für den Internet Explorer.

Darüber hinaus enthält das Programm eine Reihe von Features zur Systemanalyse und Optimierung. Bevor Sie diese einsetzen, sollten Sie allerdings auf jeden Fall einen weiteren Wiederherstellungspunkt anlegen („Einstellungen und Hilfe | Systemwiederherstellungspunkte“).

Xpy & XP-AntiSpy: Mehr Sicherheit via Registry

Die Absicherung des Rechners ist Hauptaufgabe der beiden Tools Xpy (**http://prdownloads.sourceforge.net/xpy/xpy-0.9.7-GERMAN-bin.zip?download**) und XP-AntiSpy (**www.xp-antispy.org/**), die Sie auf der Heft-CD finden.

Xpy ist ein Open-Source-Tool, das unerwünschte Kommunikation zwischen Programmen auf Ihrem PC und Herstellern wie Microsoft unterbindet. Zudem kann Xpy Verknüpfungen und Dateien, die nach der Standardinstallation von Windows XP vorhanden sind, löschen, etwa den Ordner „Beispielmusik“ von XP oder Verknüpfungen zu Microsoft-Programmen. Xpy bietet mittlerweile auch eine Funktion zum Wiederherstellen von Einträgen an. Beim Programmstart geben Sie an, ob Sie die vorherige Konfiguration zurückholen oder neue Einstellungen vornehmen wollen („Standard“).

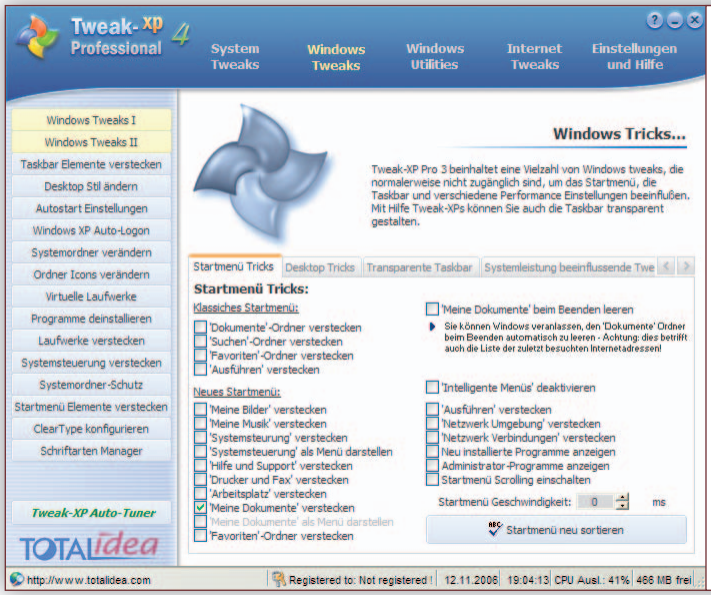
Die Freeware XP-AntiSpy fügt bei der Installation die Taskleiste eines Sponsors auf Ihrem Rechner hinzu. Sind Sie damit nicht einverstanden, deaktivieren Sie den Punkt „Sponsoring“ beim Setup.

Damit Sie bei den Einstellungen und der Auswahl der Optionen schneller vorankommen, gibt es mehrere Standardprofile mit Tweak-Vorschlägen. Die Änderungen in jedem Profil sind rot markiert, und Sie können sie bei Bedarf durch Anklicken aktivieren. Dabei erfahren Sie auch gleichzeitig, welche Funktion Sie damit verändern.

Zum Abschluss bestätigen Sie Ihre Modifikationen über den Button „Einstellungen übernehmen“.

XP-AntiSpy wird laufend erweitert und an neue Programme angepasst, sodass sich ein regelmäßiges Update auf jeden Fall lohnt.

Andreas Hitzig



Tweak-XP Pro: Das kommerzielle Programm Tweak-XP Pro macht zahlreiche Tweaks aus den Bereichen System, Windows und Internet unter einer Oberfläche zugänglich.

MALWARE DAUERHAFT ENTFERNEN

So bleibt Ihr PC virenfrei

Es gibt viele Möglichkeiten, den Rechner mit Viren oder Malware zu infizieren – von der verseuchten E-Mail bis hin zum Surfen im Internet. CHIP zeigt Ihnen, wie Sie die Schadprogramme aufstöbern, entfernen und für alle Zeiten aussperren.

Die Anzeichen für Virenbefall und unerwünschte Eindringlinge in Ihrem Computer sind unterschiedlich – und im schlimmsten Fall gar nicht wahrnehmbar. Deswegen sollten Sie vorausschauend handeln, Ihren Rechner regelmäßig auf Viren und Schädlinge untersuchen und anschließend bestmöglich absichern. CHIP zeigt Ihnen, wie Sie dabei optimal vorgehen.

AUF EINEN BLICK

→ PC säubern & sauber halten

Malware aufspüren & entfernen 32

System optimal abschotten und auf Sicherheit überprüfen 34

Alle Tools auf CD

AntiVir PE Classic: Schützt optimal vor Viren und Würmern ◎ Internet

RootkitRevealer: Spürt gefährliche Rootkits im System auf ◎ Internet

1 PC checken, Scanner einrichten

Als Erstes sollten Sie Ihren Computer auf bereits vorhandene Infektionen untersuchen. Am zuverlässigsten gelingt dies, wenn Sie den Zustand Ihres Rechners mithilfe einer Boot-CD ermitteln. Für diesen Zweck gibt es einige Linux-Boot-CDs mit integriertem Virenscanner. Einfacher funktioniert die Diagnose mit einer Windows-Boot-CD und dem kostenlosen Virenscanner AntiVir. Den Weg zur Windows-Boot-CD zeigt Ihnen der Artikel ab 106. Achten Sie darauf, dass Sie vor dem Scannen Ihres PCs das neueste Viren-Pattern auf Ihre Boot-CD packen.

Nachdem Sie von CD gebootet und Ihren PC untersucht und gesäubert haben, sollten Sie zur Vorsorge einen Virenscanner auf Ihrem Rechner installieren. Sie können dabei auf ein kommerzielles Produkt zurückgreifen – einen Test von Security-Suiten finden Sie ab 8.

Eine sehr gute Alternative ist das für den Privatgebrauch kostenlose Tool AntiVir Personal Edition Classic von Avira (**www.free-av.de/**). Starten Sie gleich nach der Installation das Update von AntiVir – Sie finden es auf der Status-Seite. Nach dem Download zeigt Ihnen AntiVir ein aktuelles Datum für die Virendefinitionen und die Suchmaschine an.

Zwar liefert AntiVir in der Grundkonfiguration gute Ergebnisse, Sie sollten dennoch einige Änderungen an der Standardkonfiguration vornehmen. Rufen Sie

dazu die Konfiguration auf, und wählen Sie den Bereich „Scanner“. AntiVir untersucht entweder Dateien mit definierten Dateierweiterungen, wählt die Dateien individuell aus oder scannt alle Dateien. Letztere Option dauert zwar länger, ist dafür aber auch sicherer.

Im Bereich „Weitere Einstellungen“ sollten alle Optionen aktiviert sein. Im Bereich „Guard“ setzen Sie die Werte für den Echtzeitscanner, der Ihren Rechner zur Laufzeit auf Bedrohungen untersucht. An dieser Stelle sollten Sie ebenfalls alle Dateien einbeziehen und im Suchmodus die Option „Beim Lesen und Schreiben suchen“ aktivieren.

Für die weiteren Einstellungen müssen Sie den „Expertenmodus“ nutzen. Danach haben Sie auch die Option „Allgemein“ zur Verfügung. Binden Sie dort Ihre Mailbox ein, indem Sie den SMTP-Server und Ihre Mailadresse eingeben. Falls Sie für Ihr Postfach eine Authentifizierung vor dem Versenden von Mails aktiviert haben, wählen Sie die Funktion aus und ergänzen die Anmelde-Informationen.

Neben Viren sucht AntiVir auch nach „erweiterten Gefahrenkategorien“ – von Backdoor-Steuersoftware bis hin zu Witzprogrammen. Entscheiden Sie selbst, ob beispielsweise auch Spiele als Gefahrenquelle gelten sollen.

Damit AntiVir diese Gefahren rechtzeitig erkennt, benötigt das Tool aktuelle Updates, an die es Sie auch erinnern kann. Setzen Sie den Wert am besten auf einen Tag. Schützen Sie auch die bestehende Konfiguration und die Dienste selbst vor ungewollten Änderungen, damit sich keine Schadprogramme an AntiVir zu schaffen machen.

AntiVir bietet zwei unterschiedliche Optionen, um Ihren PC zu scannen – durch manuelles Starten oder geplante Jobs. Die manuelle Überprüfung aktivieren Sie über die Registerkarte „Prüfen“. Dort definieren Sie die zu untersuchenden Laufwerke und starten den Vorgang mit einem Klick auf das Lupensymbol.

Arbeiten Sie zu festen Zeiten mit Ihrem Computer, kann auch eine geplante Systemprüfung sinnvoll sein. Nutzen Sie dazu auf der Registerkarte „Planer“ die vorhandenen Jobs, oder legen Sie einen neuen an. Zum Ändern markieren Sie einen Auftrag und starten Sie den Assistenten über das Symbol links neben dem Papierkorb („Ausgewählten Auftrag ändern“). Legen Sie über die Auswahlfenster die Art und den Zeitpunkt des Auftrags fest. Aktivieren Sie auch die Option „Auftrag nachholen, wenn die Zeit bereits abgelaufen ist“, damit die Systemprüfung spätestens nach dem Einschalten des Rechners startet.

Findet AntiVir Schadprogramme auf Ihrem Rechner, fragt das Tool Sie nach dem weiteren Vorgehen: „Löschen“, „In Quarantäne verschieben“, „Umbenennen“ oder „Ignorieren“ sind die Optionen. Alle Objekte, die Sie in Quarantäne genommen haben, sind über die gleichnamige Registerkarte sichtbar.

2 Malware aufspüren & beseitigen

Neben Viren, deren Ziel in der Regel die Zerstörung von Daten ist, gibt es noch eine ganze Reihe weiterer Malware, die es zu beseitigen gilt. Dazu gehören unter anderem Computerwürmer, Trojanische Pferde, Backdoor-Programme und Spyware. CHIP zeigt Ihnen, wie Sie nun die Programme identifizieren und loswerden können, die von Ihrem Virenscanner übersehen wurden.

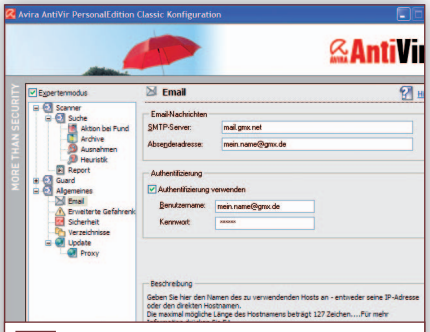
Als Erstes sollten Sie Ihren Rechner auf Rootkits untersuchen. Da es für diesen Zweck kein Spezialtool gibt, lohnt der parallele Einsatz mehrerer Programme.

Einer der Klassiker zum Aufspüren und Entfernen von Rootkits ist Stinger von McAfee (**http://vil.nai.com/vil/stinger/**). Das Tool muss nicht installiert werden und lässt sich sofort nach dem Download einsetzen – etwa auch direkt von einer Windows-Boot-CD.

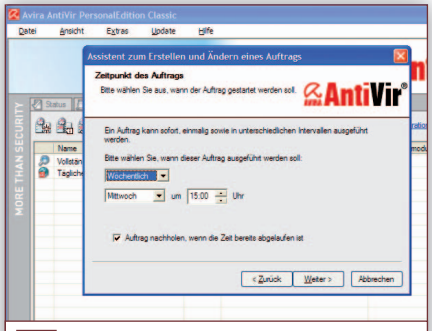
Vor dem Scanvorgang aktivieren Sie unter „Preferences“ zusätzlich die Option „Scan these targets – Boot sectors“. Starten Sie Stinger durch Anklicken von „Scan Now“. In der aktuellen Version 2.6.0 erkennt das Tool insgesamt 55 unterschiedliche Angreifer und beseitigt sie.

Ein wenig weiter geht das Programm IceSword (**www.blogcn.com/user17/pjf/blog/44731756.html**). Es erleichtert die Jagd nach verdächtigen Prozessen und hilft Ihnen, sie von Ihrem Rechner zu entfernen.

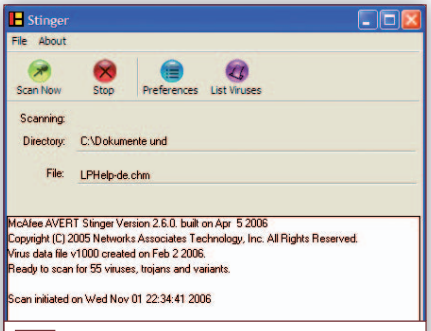
Für das Aufspüren von Rootkits und Remote Access Tools (RATs) gibt es ebenfalls ein kostenloses Programm. Bewährt haben sich an dieser Stelle vor allem der RootkitRevealer (**www.sysinternals.com/**) und Black Light (**www.f-secure.com/blacklight/**). Beide Programme identifizieren verdächtige Anwendungen, indem sie die laufenden Prozesse aus unterschiedlichen Sichten betrachten: einmal aus der Anwenderebene und zum Vergleich dazu auch noch aus der Kernelebene. Verdächtig sind alle Programme, die nur in einer Sicht erscheinen. Die sollten Sie genauer untersuchen und gegebenenfalls löschen. Der RootkitRevealer bietet lediglich eine Suchfunktion, Black Light kombiniert Analyse und das Entfernen unter einer Oberfläche. →



1 AntiVir: Vor dem Download von E-Mails sollten Sie diese von einem Virenscanner überprüfen lassen.



1 AntiVir: Planen Sie die regelmäßige Überprüfung Ihres PCs mithilfe eines zeitgesteuerten Auftrags ein.



2 Stinger: Das McAfee-Tool entfernt die bekanntesten Würmer zuverlässig von Ihrem Rechner.

TIPPS

Die fünf wichtigsten Sicherheitsregeln

Die folgenden fünf Grundregeln sollten Sie zur Absicherung Ihres Rechners unbedingt beachten.

1 Gehen Sie nie ohne den Schutz einer Firewall ins Internet. Setzen Sie am besten eine Software-Firewall wie ZoneAlarm in Kombination mit der Hardware-Firewall Ihres DSL-Routers ein.

2 Schützen Sie Ihren Rechner durch den ständigen Einsatz eines Virenscanners, beispielsweise des kostenlosen Programms AntiVir von Avira.

3 Halten Sie Ihren Computer und Ihre Programme stets auf dem aktuellen Stand der Dinge – am besten über automatische Updates. Nur so sind Sie sicher, dass bekannte Sicherheitslücken schnell geschlossen und neue Bedrohungen abgewehrt werden.

4 Wenn Sie Windows XP einsetzen, achten Sie darauf, dass Sie niemals als Administrator, sondern immer mit eingeschränkten Benutzerrechten im Internet unterwegs sind.

5 Starten Sie in regelmäßigen Abständen einen kompletten Systemscan mit allen beschriebenen Maßnahmen.

Wenn Sie diese Regeln beherzigen und Ihren PC vernünftig absichern, sind Sie im Internet vor Bedrohungen sicher.

Sollte der Löschvorgang mit Black Light nicht klappen, können Sie wieder auf IceSword zurückgreifen. Es listet nach einem Scanvorgang (Button „Prozesse“) alle verdächtigen Dateien auf und bietet auch die Option, sie sofort direkt zu beenden. Klicken Sie dazu einfach mit der rechten Maustaste auf den Prozess und wählen Sie „Terminate Process“.

Der Vorteil von IceSword gegenüber den beiden anderen Tools besteht darin, dass es auch mehrere Dienste gleichzeitig beenden und löschen kann. Dies ist besonders dann vorteilhaft, wenn ein Rootkit neben dem eigentlichen Prozess noch einen Wächterprozess aufweist, der das Schadprogramm nach dem Beenden sofort wieder startet.

Booten Sie nach dem Löschen der Malware Ihren PC neu und kontrollieren Sie noch einmal mit den zuvor eingesetzten Programmen, ob immer noch Schädlinge vorhanden sind. Finden auch die Scanner keine Spuren mehr, scheint die Gefahr gebannt zu sein. Damit sich die Malware nicht wieder durch die Hintertür der Systemwiederherstellung auf Ihren PC schleichen kann, sollten Sie die Systemwiederherstellung vor den Löschaktionen deaktivieren („Start | Systemsteuerung | System | Systemwiederherstellung“).

Nach dem Löschen der Malware aktivieren Sie die Systemwiederherstellung auf dem gleichen Weg wieder.

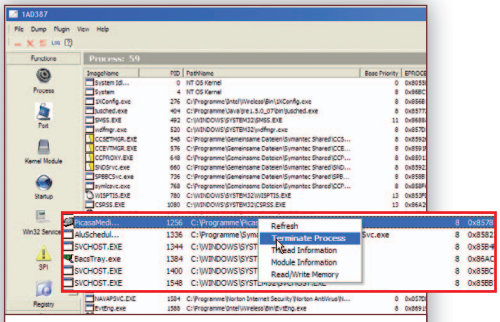
3 Adware eliminieren

Nicht ganz so gefährlich wie Viren und Malware, aber ungemein lästig ist Adware. Diese Schadprogramme sorgen dafür, dass Ihr Rechner mit Werbe-Popups und Produktinformationen zugemüllt wird. Adware können Sie sehr effektiv mit Spybot – Search & Destroy 1.4 (**www.safer-networking.org/de/spybotsd/index.html**) zu Leibe rücken. Die Freeware von Patrick M. Kolla untersucht Ihren PC auf rund 45 000 unterschiedliche Bedrohungen – von verräterischen Cookies bis zu Dialern gibt es eine mittlerweile sehr umfangreiche Bibliothek von Adware und sonstigen Schadprogrammen.

Bei der Installation haben Sie die Möglichkeit, den aktuellen Systemzustand für eine spätere Wiederherstellung zu speichern – falls künftig Probleme auftreten. Diese Option sollten Sie zur Sicherheit nutzen. Denn das Löschen von Informationen kann theoretisch dazu führen, dass bestimmte Programme nicht mehr funktionieren – was allerdings so gut wie nie passiert. Mit dieser Maßnahme haben Sie sich aber trotzdem die Option zum Rollback offengehalten.

Nach der Installation suchen Sie zuerst per Update nach neuen Virendefinitionen. Meist ist der vordefinierte Server überlastet. Wählen Sie am besten vor der Suche einen der Alternativserver aus, starten Sie die Suche nach den Updates und laden Sie sie herunter.

Nachdem Spybot – Search & Destroy auf dem aktuellen Stand der Dinge ist, sollten Sie noch eine Standardoption ändern. Klicken Sie auf die Schaltfläche „Datensätze“, und aktivieren Sie die Option „Alle Datensätze auswählen“ – das erhöht den Suchradius. Starten Sie danach den Scanvorgang im Hauptfenster über die Schaltfläche „Überprüfen“ – je nach Rechner kann der Vorgang bis zu zehn



2 IceSword: Dieses Tool erkennt verdächtige Prozesse nicht nur — es beendet sie auch noch per Mausklick.

Minuten dauern. Als Ergebnis sehen Sie eine Liste mit mehr oder weniger kritischen Bedrohungen für Ihren PC – markieren Sie die Spyware, die Sie entfernen möchten, und bestätigen Sie mit dem Button „Markierte Probleme beheben“.

Nicht alle Schadprogramme sind daraufhin wirklich verschwunden – in manchen Fällen müssen Sie Ihren Rechner nach dem Löschen neu starten.

Als weitere Schutzmaßnahme bietet Spybot – Search & Destroy eine Immunisierung Ihres PCs an. Sie soll verhindern, dass sich Malware über den Internet Explorer auf Ihrem PC festsetzt. Bekannte Installationsprogramme werden somit an ihrem Tun gehindert.

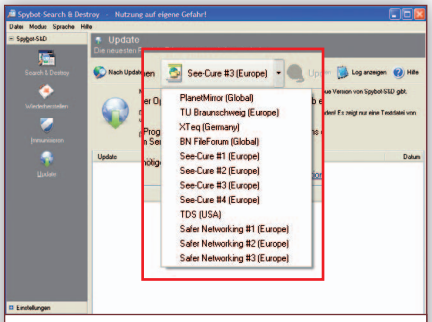
Sollten Sie doch einmal eine Einstellung zu viel gelöscht haben, lässt sich diese – sofern es kein Cookie war – über die Option „Wiederherstellen“ zurückholen. Spybot – Search & Destroy speichert die gelöschten Registry-Schlüssel und erlaubt das nachträgliche Reaktivieren der Werte.

4 System absichern

Nachdem Sie Ihren PC von Malware aller Art befreit haben, sollten Sie auch dafür sorgen, dass er möglichst lange unbehelligt bleibt.

Falls Sie noch keine Firewall auf Ihrem Rechner installiert haben, ist dies nun der erste Schritt, der fällig ist. Damit unterbinden Sie unberechtigte Zugriffe von außen auf Ihren PC und verhindern außerdem die ungewollte Kommunikation eines Eindringlings mit der Außenwelt. Im Blitz-Workshop ab **82** erfahren Sie, wie Sie die Gratis-Firewall ZoneAlarm Free Schritt für Schritt konfigurieren.

Installieren Sie anschließend einen Virenscanner, der permanent auf Ihrem Rechner läuft, ihn regelmäßig durchsucht



3 **Spybot – Search & Destroy:** Sind die Standard-Update-Server ausgelastet, weichen Sie auf Alternativserver aus.

und Downloads sofort nach dem Herunterladen überprüft. Wenn Sie noch keinen kommerziellen Virenscanner besitzen, installieren Sie am besten das kostenlose Programm AntiVir und sehen sich die Einstellmöglichkeiten unter Schritt 1 dieses Workshops noch einmal an.

Sichern Sie auch die Registry ab, etwa mit dem Tool Tea Timer, das in Spybot – Search & Destroy integriert ist. Sie finden es, wenn Sie den Expertenmodus („Modus | Erweiterter Modus“) aktivieren und die „Werkzeuge“ aufrufen. Unter „Resident“ befindet sich eine Checkbox zum Aktivieren von Tea Timer. Künftig informiert Sie das Tool, sobald eine Anwendung die Registry ändern möchte, und holt dazu Ihre Zustimmung ein.

Arbeiten Sie möglichst mit einem Benutzerkonto mit eingeschränkten oder gar keinen Administratorrechten. Das können Sie entweder selbst in der Systemsteuerung anlegen – „Benutzerkonto | Neuer Benutzer | Eingeschränkte Rechte“ –, oder Sie verwenden ein Tool, das Ihnen die Arbeit abnimmt, etwa DropMyRights von Microsoft (**http:// msdn2.microsoft.com/en-us/library/ms972827.aspx**). Legen Sie nach der Installation eine Verknüpfung auf dem Desktop an, und geben Sie als Parameter ein: „C:\DropMyRights\DropMyRights.exe „C:\Programme\Internet Explorer\iexplore.exe““.

In diesem Beispiel ist das Programm DropMyRights im gleichnamigen Verzeichnis installiert und der Internet Explorer unter C:\Programme\Internet Explorer. Passen Sie diese Informationen gegebenenfalls an Ihre Systemumgebung an, falls Sie etwa einen anderen Browser verwenden. Rufen Sie noch einmal die Verknüpfung auf, und ändern Sie den Parameter „Ausführen“ in „Minimiert“. Nutzen Sie zum sicheren Surfen mit dem Internet Explorer von nun an nur noch diese Verknüpfung, falls Sie nicht mit einem Benutzerkonto mit eingeschränkten Rechten arbeiten.

5 System auf Sicherheit testen

Nach dem Absichern des Systems sollten Sie noch einmal überprüfen, ob Ihre Maßnahmen erfolgreich waren. Es gibt Programme, etwa den PC Security Test 2006 (**www.pc-st.com/de/index.htm**), die ein System unter verschiedenen Aspekten automatisiert auf Konformität überprüfen können. Starten Sie das Programm, und wählen Sie die Standardüberprüfungen aus. Sie simulieren verschiedene Angriffe aus den Bereichen Hacking, Virenbefall und Spyware und testen die Absicherung Ihres Rechners.

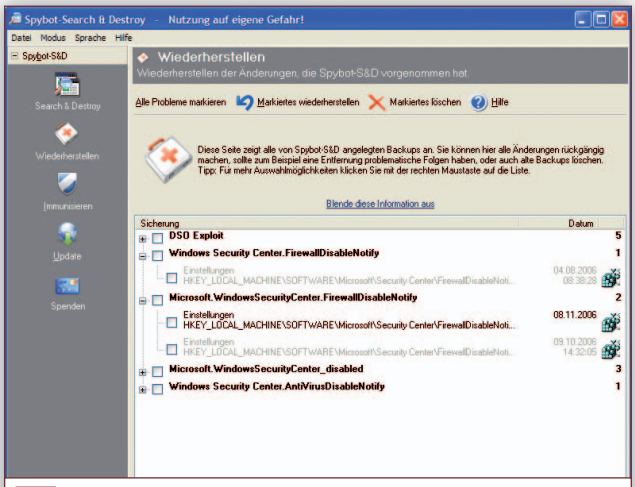
PC Security Test 2006 benötigt während der Arbeit eine Verbindung zum Internet, um die Angriffe zu simulieren. Sie sollten während des Tests eine Reihe von Meldungen von Ihrer Firewall und auch von Tea Timer bekommen. Achtung: Stimmen Sie keiner Installation oder Veränderung von Werten zu!

Als Wunschergebnis sollten Sie im Bereich „Hacking“ den Wert 100 Prozent erzielen und im Bereich „Viren“ mit den eingesetzten Mitteln mindestens 55 Prozent. Erschrecken Sie nicht, falls der Wert für Spyware bei nur 25 Prozent liegt. Die Hauptschuld hat der Internet Explorer – Sie sollten sich also überlegen, ob Sie ihn nicht lieber komplett deinstallieren und auf einen Alternativbrowser, etwa Firefox oder Opera, umsteigen. Damit erreichen Sie auch im Bereich „Spyware“ zumindest einen Wert von mehr als 50 Prozent.

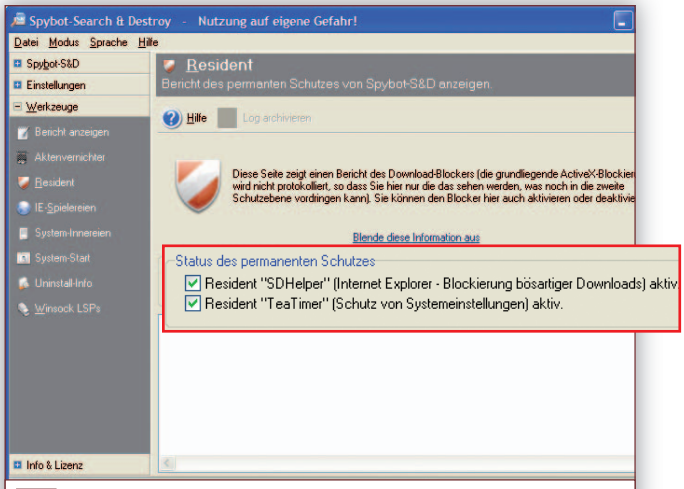
Fazit: Gegen Malware gerüstet

Hundertprozentige Sicherheit gibt es nicht. Denn sobald Ihr PC an ein Netzwerk angeschlossen ist oder Sie externe Datenträger einsetzen, gelangen Daten von außen auf Ihren Rechner, die ihn infizieren können. Damit das gar nicht erst passiert oder die Angreifer es zumindest so schwer wie möglich haben, sollten Sie die fünf wichtigsten Grundregeln zum Thema Sicherheit beachten (siehe Kasten auf **34**).

Kommt trotz aller Vorkehrungen einmal ein Angreifer durch, sind Sie nun gut gerüstet, um die Malware auszuschalten und zu beseitigen. Andreas Hitzig



3 **Spybot – Search & Destroy:** Wenn nach dem Löschen eines Registry-Eintrags ein Programm nicht mehr funktioniert, holt die Funktion „Wiederherstellen“ den Registry-Key zurück.



4 **Spybot – Search & Destroy:** Das Tool Tea Timer wacht darüber, dass Schadprogramme keine Registry-Einträge eigenmächtig setzen oder ändern können.

ADWARE ENTTARNEN

Datendiebe stoppen

AUF EINEN BLICK

Alle Tools auf CD

Ad-Aware: Findet Spyware und säubert den Rechner ◎ **Internet**

Spybot – Search & Destroy: Stoppt schädliche Programme ◎ **Internet**

Adware sammelt ohne Ihr Wissen Informationen über Sie. Im Normalfall dienen sie lediglich Werbezwecken, aber prinzipiell sind alle Daten auf Ihrem Rechner von Ausspähung bedroht. So erkennen und entfernen Sie die lästigen Programme.

Als „Adware“ bezeichnet man Programme, die Informationen über Ihren Rechner und Ihr Surfverhalten an Datenbanken übermitteln. Das geschieht meist zu Werbezwecken und fast immer ohne Ihr Wissen. Geben Sie bei einem Onlinekauf Ihre Kreditkartennummer an, oder ziehen Sie sich gelegentlich aktuelle Songs aus einer Tauschbörse? Adware überwacht Ihre Aktionen und meldet sie unverzüglich.

Eine zweite Sorte von Spionageprogrammen – die Keylogger – zeichnet Ihre Aktivitäten am PC auf. Schnüffeltools wie „FamilyCam“ oder „I am BigBrother“ verraten ihren Einsatzzweck bereits im Namen. Damit lassen sich Mitarbeiter oder Familienangehörige heimlich überwachen. Keylogger leiten E-Mails gleich in Kopie an den Beobachter weiter, zeichnen Chatflirts auf oder machen über zwischengeschaltete Proxy-Server abgerufene Internetinhalte sichtbar.

Spionage-Software kann das System bis hin zu Abstürzen destabilisieren, weil sie bestimmte Funktionen ändert. Von Ihnen unbemerkt wird Popup- und Bannerwerbung auf der Grundlage Ihres Surfverhaltens eingespielt, oder die Suche nach Inhalten wird gezielt auf andere Seiten umgelenkt.

Trübe Quellen: Wo Sie sich Adware einfangen

Adware und Spyware kommt meist per E-Mail, Instant Messaging oder zusammen mit Shareware oder Freeware auf Ihren PC – und zwar massiv. Zwar finden sich in Freeware oder Shareware auch Hinweise auf Spyware, allerdings sind sie in der Regel in langen Datenschutzerklärungen oder Lizenzvereinbarungen versteckt, welche die meisten Anwender ungelesen wegklicken.

Eine Untersuchung des US-Providers Earthlink über einen Zeitraum von drei Monaten ergab bei mehr als einer Million untersuchten Computern fast 30 Millionen Instanzen von Spyware. Den Löwenanteil nahmen dabei mit nahezu 24 Millionen die Cookies ein, mit denen Marketing-Unternehmen umfassende Nutzerprofile anlegen. Mehr als fünf Millionen kamen auf Spyware-Programme. Trojaner und Systemmonitore, die private Daten aufzeichnen und weiterleiten, kamen jeweils auf etwa 200 000 Instanzen.

Mehrere US-Bundesstaaten haben auf dieses massive Problem reagiert und die Installation von Spyware per Gesetz von der Zustimmung des Nutzers abhängig gemacht. So muss auch die US-Regierung eine nationale Lösung finden – die allerdings dank der starken Marketing-Lobby ähnlich harmlos werden könnte wie das 2003 verabschiedete Antispam-Gesetz. Das verbietet nämlich keineswegs den Versand von Werbemails, sondern verlangt lediglich, dass der Empfänger eine Möglichkeit erhält, sich aus der Mailingliste auszutragen.

Die beste Strategie: Adware & Spyware abblocken

Um dem Befall Ihres Rechners mit Adware oder Spyware vorzubeugen, sollten Sie die folgenden Regeln beachten:

- Öffnen Sie niemals Links in Mails mit unbekannten Absendern.
- Installieren Sie nur die Programme, die Sie auch benötigen.
- Lesen Sie vor der Installation die Lizenzvereinbarung oder die Datenschutzrichtlinien. Manche Hersteller weisen dort – möglichst unauffällig – darauf hin, dass zusätzlich zum Programm noch Spyware installiert wird.
- Stellen Sie die Sicherheitseinstellungen in Ihrem Webbrowser richtig ein (ausführliche Informationen dazu finden Sie ab 66).

Bevor Sie ein neues Programm installieren, sollten Sie nachsehen, ob es sich dabei nicht um Spyware handelt. Eine Liste mit mehr als 2200 Programmen finden Sie unter **www.spywareguide.com**. Dort haben Sie auch die Möglichkeit, mithilfe eines ActiveX-Elements online nach Spyware zu fahnden.

Spyware-Produzenten nutzen ebenfalls ActiveX-Elemente, die nur der Internet Explorer ausführen kann. Um so etwas zu verhindern, müssen Sie dem Internet Explorer beibringen, dass er nicht unaufgefordert alles öffnet und ausführt, was aus dem Web kommt – und das sind eben vor allem ActiveX-Elemente. Was der Internet Explorer damit machen soll, legen Sie über den Befehl „Extras | Internetoptionen“ fest. Wechseln Sie zur Registerkarte „Sicherheit“, wählen Sie die Zone „Internet“, und klicken Sie auf „Stufe anpassen“. Im folgenden Fenster stellen Sie unter „ActiveX-Steuerelemente und Plugins“ alle Optionen, die aktiviert sind, auf „Eingabeaufforderung“; die anderen lassen Sie ausgeschaltet. Noch besser ist es, wenn Sie die Sicherheitseinstellungen auf „Hoch“ setzen. Wählen Sie dazu im gleichen Dialog aus der Liste „Zurücksetzen auf“ den Eintrag „Hoch“, und klicken Sie danach auf „Zurücksetzen“.

Zudem können Sie die Browser-Erweiterungen von Drittanbietern abschalten – unter „Extras | Internetoptionen“ auf der Registerkarte „Erweitert“.

Allerdings sollten Sie sich darüber im Klaren sein, dass diese Maßnahmen zu Einschränkungen beim Surfen führen können und bestimmte – durchaus gewollte – Inhalte nicht mehr erscheinen. Darüber hinaus beugen die Sicherheitseinstellungen lediglich der Spyware vor, die sich direkt über das Internet installiert, schützt aber beispielsweise nicht vor Spyware, die mit einer Software installiert wird.

Spione enttarnen: Woran Sie Spyware erkennen

Ob Spyware auf Ihrem PC installiert ist, können Sie mit Spezialtools herausfinden. Wenn Sie noch keine Programme gegen Spyware eingesetzt haben, können Sie bei bestimmten Symptomen davon ausgehen, dass auf Ihrem Computer irgendeine Art von Spyware läuft:

- Sie stellen fest, dass der Rechner langsamer läuft.
- Die Startseite Ihres Internetbrowsers hat sich ohne Ihr Zutun geändert.
- Sie entdecken neue und unbekannte Symbolleisten in Ihrem Webbrowser.
- Das Chat-Programm Windows Messenger blendet ständig Werbung ein.
- Auf bekannten Websites erscheinen auf einmal Popup-Fenster mit Werbung.

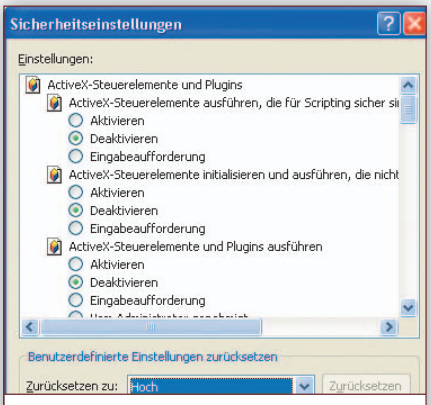
Spione ausweisen: Wie Sie Spyware zuverlässig entfernen

Ein bekanntes Anti-Spyware-Programm ist Ad-Aware von Lavasoft. Das Tool durchsucht den Arbeitsspeicher, die Registrierdatenbank, Festplatten und andere Laufwerke nach schädlichen Dateien sowie nach Werbung und Tracking-Komponenten. Es gibt mehrere Versionen von Ad-Aware – von Freeware bis zu lizenzierten Enterprise-Versionen. Sie können sie unter **www.lavasoft.de** herunterladen beziehungsweise kaufen. Lavasoft verwendet auf seiner Homepage ActiveX-Elemente und JavaScript, hat aber die Homepage inzwischen so programmiert, dass man auch mit hohen Sicherheitseinstellungen zum Ziel kommt.

Klicken Sie auf den Link „Download & Buy“ und im Folgenden auf „Free Download“, um die Freeware-Version von Ad-Aware herunterzuladen; allerdings dürfen dafür die Sicherheitseinstellungen maximal auf „Mittel“ stehen.

Nach der Installation präsentiert sich die Software mit einer einfach zu bedienenden Oberfläche, über die Sie den gesamten Rechner per Mausklick auf Spyware und andere lästige Programme untersuchen können. Klicken Sie auf „Scan now“, um die Festplatte zu überprüfen. Anschließend können Sie aus der Liste der gefundenen Objekte einzelne oder alle Dateien unter Quarantäne stellen. Das →

Spy-Software: Das Programm Spector überwacht Online-Aktivitäten – etwa des Lebensgefährten – und spielt für misstrauische Personen den Detektiv.



Internet Explorer schützen: Mit hohen Sicherheitseinstellungen schalten Sie im Internet Explorer sämtliche ActiveX-Elemente aus.

bedeutet, dass diese keine Informationen mehr sammeln und übertragen können. Allerdings können Sie diese Dateien bei Bedarf wiederherstellen, etwa wenn nach dem Entfernen etwas nicht mehr richtig funktionieren sollte.

Ad-Aware überprüft auch ZIP-Dateien, laufende Prozesse und – je nach Einstellung – die Favoriten im Internet Explorer. In der kostenpflichtigen Version kommt noch die sogenannte „Ad-Watch"-Funktion hinzu, die zum Beispiel Autostart-Sektionen in der Registrierung sperrt oder erkannte Prozesse blockiert. Bevor Sie mit Ad-Aware den Rechner untersuchen, sollten Sie jedoch prüfen, ob bereits eine neue Referenzdatei vorhanden ist, denn in ihr ist bekannte Spyware aufgeführt. Diese Referenzliste, die mit allen Versionen funktioniert, können Sie über das Icon „Webupdate Tool" aus dem Internet herunterladen.

Spybot – Search & Destroy (**www.spybot.info**) ist Freeware. Es untersucht ähnlich wie Ad-Aware das System auf lästige Werbemodule und Spyware. Und ebenso wie Ad-Aware hat Spybot – Search & Destroy eine Update-Funktion, mit der sich aktuelle Erkennungsregeln herunterladen lassen. Ansonsten bietet Spybot – Search & Destroy mehr Such- und Löschmöglichkeiten: Außer nach sogenannten verfolgenden Cookies fahndet das Programm nach Trojanern, Hijackern (Funktionen, die Browser-Startseiten ändern), Dialern oder Keyloggern und sucht nach Sicherheitslücken.

Im Gegensatz zu Ad-Aware erfährt der Benutzer von Spybot – Search & Destroy auch noch etwas mehr über die Firmen, die Cookies oder andere Spuren auf dem Rechner hinterlassen haben. So steht bei manchen Firmen die Privatsphären-Erklärung neben dem gefundenen Cookie. Auf diese Weise erfährt der Anwender, dass etwa das Unternehmen Doubleclick Daten über Browser und Surfverhalten aufzeichnet, um die Anzeigen festzulegen, die im Browser aufgeführt werden. Dazu dienen auch die Cookies anderer Firmen, beispielsweise Advertising.com, Avenue A. oder HitBox.

Spybot – Search & Destroy arbeitet mit zwei Programm-Modi: dem normalen und dem erweiterten Modus. Im normalen Modus ist das System schnell geprüft. Sie scannen den Rechner und löschen die unerwünschten Daten. Der Experten-Modus dagegen erlaubt vielfältige Einstellungen. So können Sie zum Beispiel „Produkt-Ausnahmen" bestimmen, die Search & Destroy während der Prüfung ignorieren soll.

PROFI-TIPP

Windows Messenger komplett abschalten

Wenn Sie nicht mit dem Messenger arbeiten, sollten Sie dessen Aufruf bereits beim Systemstart unterbinden. Dazu öffnen Sie mit „Start | Ausführen" und dem Befehl „msconfig" das Systemkonfigurationsprogramm. Wechseln Sie danach auf die Registerkarte „Systemstart". Dort finden Sie mehrere aktivierte Einträge. Schalten Sie nun das Systemstart-Element „msmsgs" per Klick aus. Zukünftig fährt beim Systemstart der Messenger nicht mehr im Hintergrund hoch.

Ad-Aware vs. Spybot: Wer mehr Spione findet

Eine Prüfung mit Ad-Aware ergab auf einem Testrechner 25 suspekte Objekte – 24 davon Cookies und einen Registrierungsschlüssel des Internet Explorer, der über den Befehl „Extras | Verwandte Links anzeigen" auf den Bot Alexa verweist. Alexa ist bekannt für die Spyware Alexa-Toolbar, die Daten sammelt; ob das für die Suchseite ebenfalls zutrifft, ist nicht sicher.

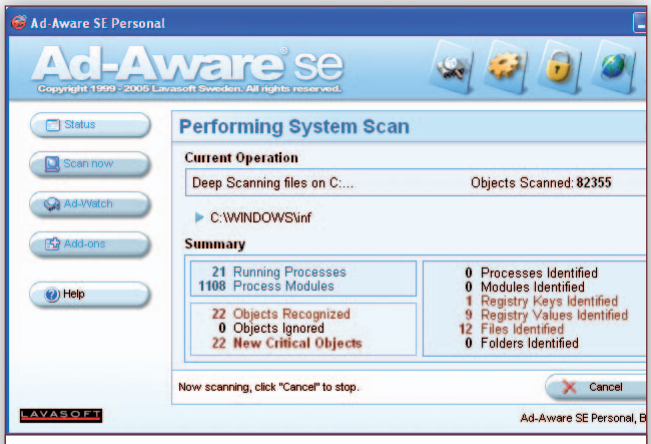
Diesen Befehl des Internet Explorer findet Spybot – Search & Destroy ebenfalls. Allerdings entfernt es nicht den Befehl „Extras | Verwandte Links anzeigen", sondern ersetzt ihn mit dem entsprechenden Google-Befehl.

Ad-Aware findet mehr Cookies als Spybot – Search & Destroy (24 gegenüber 13). Im Gegensatz zu Ad-Aware findet Spybot – Search & Destroy aber noch einige DSO-Exploits, deren Auswirkungen unter der Webadresse **www.greymagic.com/security/advisories/gm001-ie/** beschrieben sind. Ein Klick auf „Markierte Probleme beheben" entfernt die Fundstücke – die DSO-Exploits sind jedoch bei der nächsten Prüfung wieder da.

Fazit: Sie sollten sowohl Ad-Aware als auch Spybot – Search & Destroy regelmäßig einsetzen. Weil Spybot Freeware ist und es auch von Ad-Aware eine Freeware-Version gibt, kostet Sie das nichts weiter als den Download und etwas Platz auf der Festplatte.

Thomas Hümmler

SpywareGuide: Unter www.spywareguide.com finden Sie nicht nur eine Liste bekannter Spyware, sondern haben auch die Möglichkeit, per ActiveX-Element online nach Spyware zu fahnden.



Ad-Aware: Das Anti-Adware-Tool Ad-Aware findet mehr problematische Objekte als Spybot – Search & Destroy, allerdings handelt es sich dabei hauptsächlich um Cookies.

Mitmachen & gewinnen!

Ihre Meinung zählt! Wir möchten gerne wissen, wie Ihnen diese Ausgabe aus der Reihe „Software“ gefallen hat. Helfen Sie uns dabei, das Heft noch besser zu machen. Füllen Sie dazu unter www.chip.de/sicherheit-umfrage den digitalen Fragebogen aus. Mit etwas Glück gewinnen Sie einen der attraktiven Preise.

Preise im Gesamtwert von 1.650 Euro zu gewinnen!

1 x externe Festplatte von TrekStor

Die edle „DataStation maxi z.ul“ im schwarzen Vollaluminium-Gehäuse bietet eine Speicherkapazität von 400 GByte, und durch die verwendete NDAS-Technologie ist eine sehr schnelle Datenübertragung möglich. Ausgestattet mit einem Highspeed-USB 2.0-Anschluss ist sie zudem auch sehr flexibel. Die Festplatte ist vertikal und horizontal einsetzbar und dank praktischer Multifunktionshalterung kann sie sogar platzsparend unter dem Tisch angebracht werden.

Gesamtwert: 350 Euro

10 x Bücher von Microsoft Press

Das Buch „Microsoft Windows Sicherheit — Die technische Referenz“ bietet detaillierte Informationen über die Sicherheitsfunktionen im Windows-Netzwerk. Es wird Sie darin unterstützen, die Sicherheit Ihres Computers zu bewerten, zu verwalten und zu optimieren. Auf der mitgelieferten Buch-CD finden Sie zusätzlich noch mehr als 20 Tools und Hilfsprogramme, die Ihnen dabei helfen, Ihre PCs und Server effektiv zu schützen.

Gesamtwert: 700 Euro

10 x Software von BitDefender

„BitDefender Antivirus Plus V10“ kombiniert die Sicherheitsmodule AntiVirus, Anti-Spyware, Personal Firewall und Anti-Spam zu einem umfassenden Sicherheitspaket für Ihren PC. Neu: die proaktive Heuristik „B-HAVE“ schützt sogar vor unbekannten Viren, für die noch keine Signaturen veröffentlicht wurden. Dieses leistungsfähige Programm bekommen Sie mit zwei Jahren Update-Service für zwei PCs inklusive.

Gesamtwert: 600 Euro

UND SO GEHT'S

1. Online gehen: Rufen Sie unsere Umfrage im Internet unter der folgenden Adresse auf: **www.chip.de/sicherheit-umfrage**

2. Fragebogen ausfüllen: Füllen Sie den Fragebogen aus und geben Sie Ihre Daten und Ihre E-Mail-Adresse an, damit wir Sie im Falle eines Gewinns benachrichtigen können.

3. Gewinnchance: Wer den Fragebogen vollständig ausfüllt, nimmt automatisch an der Verlosung teil.

Teilnahmeschluss: 25. März 2007

Mitarbeiter von Vogel Burda Communications und der beteiligten Sponsoren dürfen nicht teilnehmen. Eine Barauszahlung der Gewinne ist nicht möglich. Der Rechtsweg ist ausgeschlossen.

ALLE PROGRAMME AUF HEFT-CD

Top-Tools für Ihren PC

Geben Sie Hackern, Viren und Trojanern keine Chance: CHIP hat vier Vollversionen und die 50 besten Gratis-Tools auf die Heft-CD gepackt, mit denen Sie Ihr System bombensicher machen.

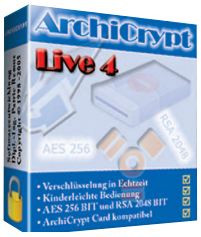
Wer seinen PC nicht abschottet, riskiert Datenverluste, ständige Systemabstürze und gefährliche Spionageangriffe. Mit unseren Tools schalten Sie alle Schnüffelfunktionen ab, schützen sensible Dokumente und spüren Eindringlinge auf.

So stellen Sie etwa mit Security & Privacy Complete den Windows-internen Datenversand ab, überwachen alle Systemänderungen mit Winpooch und vernichten Viren mit AntiVir PE Classic. Nutzen Sie Firefox 2 zum schnellen, sicheren Surfen im Web – und verwischen Sie Ihre Spuren mit JAP oder All-in-one-Secret-maker.

Spielen Sie Windows neu auf Ihr System, fehlen wichtige Programme und Patches: Mit nLite kreieren Sie Ihre eigene Installations-CD.

VOLLVERSION ARCHICRYPT LIVE 4

Daten in versteckten Archiven ablegen



Features
➔Echtzeit-Verschlüsselungssystem
➔Legt virtuelle Laufwerke an
➔Unterstützt Passwörter und Schlüsseldateien

Beschreibung Zum Schutz Ihrer sensiblen Daten richtet das Programm zusätzliche Laufwerke ein, auf denen die Inhalte verschlüsselt gespeichert werden. Dazu legen Sie eine Trägerdatei an, die als virtuelles Laufwerk dient und nur mit einem Passwort funktioniert. Innerhalb der geschützten Ordner können Sie Geheimordner anlegen, die auch beim Öffnen der Standardarchive unentdeckt bleiben. Jedes der acht virtuellen ArchiCrypt-Laufwerke kann bis zu 64 GByte Daten aufnehmen, die in Echtzeit mit der als sicher geltenden 256-Bit-Variante des Advanced Encryption Standards (AES) oder dem Blowfish-Verfahren geschützt werden.

Tipp Sie können alle Laufwerke automatisch schließen lassen. Klicken Sie dazu im Hauptmenü auf „Einstellungen | Verhalten“. Markieren Sie das Kästchen neben „Laufwerke automatisch schließen, wenn Computer nicht benutzt wurde für...“. Einen ausführlichen Workshop finden Sie auf 44.

➔CD-CODE Vollversion

VOLLVERSION DISKRECOVERY 3.0 PERSONAL

Daten retten

Features
➔Stellt zerstörte Daten wieder her
➔Rettet bis zu 50 Dateien pro Suchlauf
➔Liest auch von beschädigten Partitionstabellen

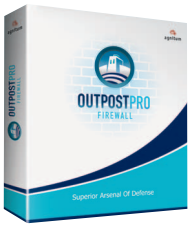
Beschreibung Ob gelöschte Dateien oder beschädigte Festplatten: DiskRecovery ist ein professionelles Tool, mit dem Sie zerstörte Daten problemlos retten können. Die Vollversion lässt sich einfach bedienen und bietet Ihnen zahlreiche Einstellmöglichkeiten. So suchen Sie gezielt nach verloren geglaubten Dokumenten – und reparieren sie (ausführlicher Workshop ab 110).

Tipp Die Seriennummer erhalten Sie nach einer Registrierung unter **www.oo-software.com/de/special/diskrecovery3/**.

➔CD-CODE Vollversion

VOLLVERSION OUTPOST FIREWALL PRO 3.0

Spione abblocken



Features
➔Wehrt Datenspione und Hacker ab
➔Einfache, schnelle Konfiguration
➔Unterstützt lokale Netzwerke, sperrt Werbung und Web-Inhalte

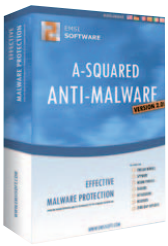
Beschreibung Eine Desktop-Firewall brauchen Sie, sobald Sie Ihren Computer mit dem Internet verbinden. Vorteil der Outpost Firewall Pro 3.0: Sie lässt sich besonders einfach und schnell konfigurieren. So entsteht in kürzester Zeit ein Online-Schutzschild zur Abwehr von Datenspionen, Hackern, Schnüfflern und PC-Schädlingen.

Tipp Zum Freischalten ist eine Registrierung notwendig. Mehr Infos dazu und einen Workshop finden Sie auf 45.

➔CD-CODE Vollversion

VOLLVERSION A-SQUARED ANTI-MALWARE

Spyware enttarnen



Features
➔Findet und entfernt Schädlinge von Ihrem PC
➔Integrierter Hintergrundwächter
➔Schützt zuverlässig Programmprozesse

Beschreibung a-squared Anti-Malware ist ein Spezial-Tool, das Trojanische Pferde und sonstige Schädlinge von Ihrem PC entfernt. Der Hintergrundwächter prüft Programme vor dem Start – und sorgt damit für optimalen Schutz.

Tipp Sie müssen die 6-Monats-Lizenz aktivieren, um die Vollversion nutzen zu können: Legen Sie ein neues Benutzerkonto an, und klicken Sie nach der Anmeldung auf „Gutscheincode einlösen“. Geben Sie „wedira2810“ ein.

➔CD-CODE Vollversion

HINWEISE ZUR CD

So legen Sie los

Die CD startet automatisch. Ist „Autorun“ deaktiviert, öffnen Sie die „AUTOSTART.EXE“ im Hauptverzeichnis der CD. Als Browser benötigen Sie den Internet Explorer ab 4.0, Firefox ab 1.0 oder Opera ab 6.0 mit aktiviertem JavaScript.

Software installieren Zu jedem Tool finden Sie ausführliche Beschreibungen. Unter den im Heft angegebenen CD-Rubriken oder über „Software“ können Sie alle Tools ansteuern. Mit einem Klick auf „Start“ beginnt die Installation. Bei Tools, die nicht direkt installierbar sind, öffnet sich das extrahierende Archiv.

Hinweise zu den Tools Bezeichnungen und Logos sind zugunsten der Hersteller als Warenzeichen und eingetragene Warenzeichen geschützt. Bitte beachten Sie die Lizenzbestimmungen. Hilfe zu den einzelnen Programmen erhalten Sie direkt vom Hersteller.

Bitte schalten Sie die Vollversionen innerhalb der nächsten zwei Monate frei, danach verfallen die Schlüssel.

DIE 50 TOP-TOOLS

→ CD-CODE ◎ AUDIO/VIDEO

→ CD-CODE ◎ INTERNET

→ CD-CODE ◎ OFFICE

→ CD-CODE ◎ SECURITY

→ CD-CODE ◎ WINDOWS

VOLLVERSIONEN AUF DER HEFT-CD

Verstecken und schützen

Ob Viren, Spyware oder gezielte Angriffe: Schad-Software spioniert Sie aus, klaut Passwörter und vernichtet sensible Dateien. Mit diesen Vollversionen verschlüsseln Sie Dokumente in versteckten Laufwerken und schotten Ihr System vor Angriffen aus dem Internet ab.

ARCHICRYPT LIVE 4

Daten in virtuellen Laufwerken verstecken

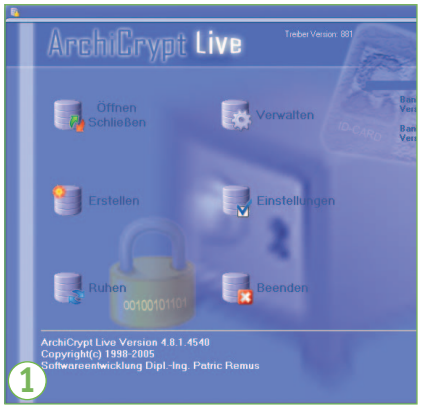
1 Programm installieren: ArchiCrypt Live 4 ist ein Echtzeit-Verschlüsselungssystem, das mit zusätzlichen Laufwerken arbeitet. Sie können bis zu acht solcher Laufwerke einrichten und verschlüsseln. Legen Sie zur Installation die CHIP-Heft-CD ein, und klicken Sie auf „Vollversionen“. Wählen Sie das Programm aus und drücken Sie den Start-Button. Folgen Sie den Installationshinweisen der Software.

2 Crypto-Laufwerk einbinden: Klicken Sie beim Programmstart auf „Ja“, um den Assistenten zum Einrichten eines virtuellen Crypto-Laufwerks zu starten. Legen Sie den Pfad und den Dateinamen der Trägerdatei fest – sie muss auf der lokalen Festplatte liegen. Dann wählen Sie die Größe des Laufwerks aus. Sie können dazu einfach den Schieberegler benutzen. Ihnen stehen pro Laufwerk maximal 64 GByte zur Verfügung. Im nächsten Fenster geben Sie an, ob Sie das Laufwerk mit einem Passwort oder mit einer Schlüsseldatei schützen möchten, die sich auf einer Diskette oder einem USB-Stick befinden kann. Die Schlüsseldatei erspart die manuelle Kennworteingabe. Beide Schutzmethoden lassen sich auch kombinieren, wenn Sie „Schlüsseldatei“ auswählen und „verschlüsselt“ markieren. ArchiCrypt nutzt für die Echtzeit-Verschlüsselung eine als sicher geltende 256-Bit-Variante des Advanced Encryption Standards (AES) oder das Blowfish-Verfahren.

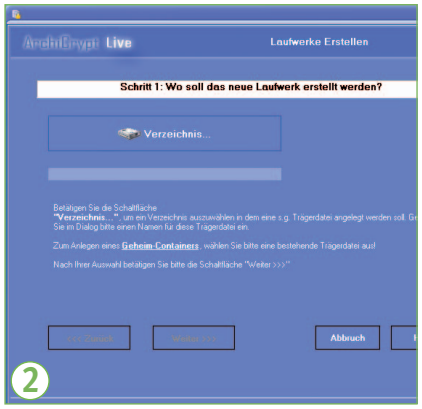
3 Laufwerke aktivieren: Das Hauptfenster zeigt eine Übersicht der virtuellen Laufwerke. Um ein Laufwerk zu aktivieren, markieren Sie oben im Fenster einen Laufwerksbuchstaben. Dann klicken Sie auf die Schaltfläche „Trägerdatei auswählen“ und geben Ihr Passwort ein. Mit „Inhalt ansehen“ öffnen Sie den Windows Explorer und kopieren Ihre Daten in das verschlüsselte Laufwerk. Die Dateien können Sie anschließend wie gewohnt öffnen, bearbeiten und löschen. Über „Schließen“ sperren Sie die Trägerdatei und entfernen das virtuelle Laufwerk. Für besondere Fälle ist die Funktion „Notaus“ bestimmt: Damit schließen Sie ein Laufwerk in Gefahrensituationen ohne Rücksicht auf eventuell geöffnete Daten.

3

4 Versteckte Archive einrichten: Sie können innerhalb eines Laufwerks zusätzliche Archive anlegen, die auch bei einer Aktivierung nicht angezeigt werden. Diese Funktion ist vor allem dann sinnvoll, wenn Sie einem bestimmten Benutzerkreis nur ausgewählte Dateien zur Verfügung stellen möchten. Bevor Sie eine zweite Ebene einrichten, sollten Sie vorhandene Dokumente aus dem virtuellen Laufwerk entfernen – Sie riskieren sonst einen Datenverlust. Klicken Sie im Hauptmenü auf „Erstellen“. Öffnen Sie eine vorhandene Trägerdatei über den Button „Verzeichnis...“ und wählen Sie eine ACL-Datei aus. Bestätigen Sie die Warnung mit „Ja“, und klicken Sie auf „Weiter“. Geben Sie nun das vorhandene Passwort ein, und wählen Sie anschließend die Größe Ihrer zweiten Ebene. Tippen Sie ein neues Passwort für Ihren Geheim-Container ein, und bestätigen Sie Ihre Auswahl. Wenn Sie nun ein Laufwerk öffnen, können Sie wahlweise das Passwort der ersten oder der zweiten Ebene eingeben.



1



2

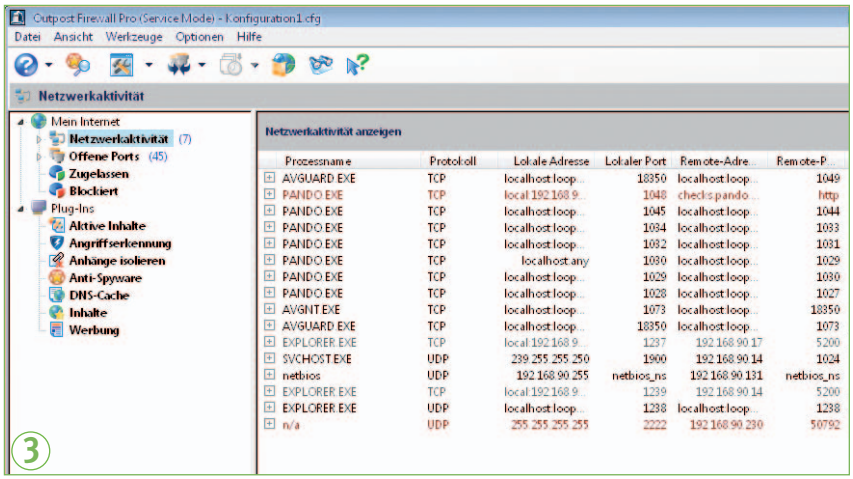
4

→CD-CODE ◎ Vollversion

System vor Internet-Angriffen schützen

1 Firewall installieren: Nur eine gute Firewall bietet ausreichend Schutz vor Angriffen aus dem Internet. Das Problem solcher Tools ist aber oft die richtige Konfiguration. Ist der Schutzschild schlecht eingestellt, lässt er entweder Eindringlinge ins System oder blockiert sämtlichen Datenverkehr. Hier hat die Outpost Firewall Pro 3.0 einen klaren Vorteil: Sie lässt sich besonders einfach und schnell konfigurieren, denn die komplette Einrichtung findet bereits beim Setup statt. Outpost Firewall Pro 3.0 überwacht den ein- und ausgehenden Datenverkehr, hindert Programme am heimlichen Senden von Daten und blockt Internet-Angreifer. Die Software unterstützt lokale Netzwerke, kann Werbung sowie aktive Internet-Inhalte sperren und zeigt in einer Übersicht alle verdächtigen Zugriffsversuche. Während der Installation entscheiden Sie sich am besten für die „Automatische Konfiguration“. Dann ermittelt Outpost die Netzwerkeinstellungen, sucht nach installierten Programmen und legt automatisch Regeln für die installierte Software an. Damit bietet die Firewall ein solides Fundament an Sicherheit. Versierte Anwender starten den „Konfigurationsassistent“, um die Firewall-Einstellungen individuell festzulegen.

2 Programm freischalten: Die Firewall startet beim Hochfahren von Windows automatisch und schützt so Ihren Rechner von Anfang an. In der Systray neben der Uhr finden Sie das Icon von Outpost – einen blauen Kreis mit einem weißen Fragezeichen. Sie müssen das Programm freischalten. Die Option finden Sie unter „Hilfe | Registrierung“. Den passenden Code erhalten Sie unter **www.agnitum.com/promo/chip/**. Als „Promotion Code“ geben Sie „23J64-5K6SL-UFDWW-KG44K-CSCK7“ ein. Anschließend zeigt die Software unten im Programmfenster „Aktualisierungsperiode ist abgelaufen“ an. Das bezieht sich auf Updates zu Outpost Firewall Pro und betrifft vor allem die Aktualisierung des Anti-Spyware-Moduls. Sie können diese Meldung unter „Optionen | Plug-ins einrichten“ abschalten.

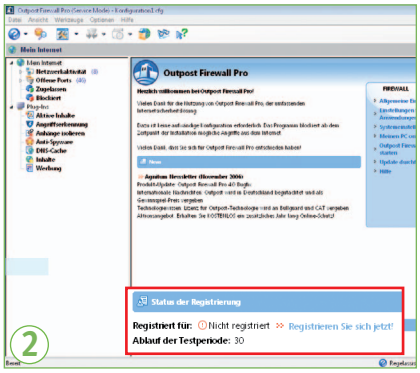


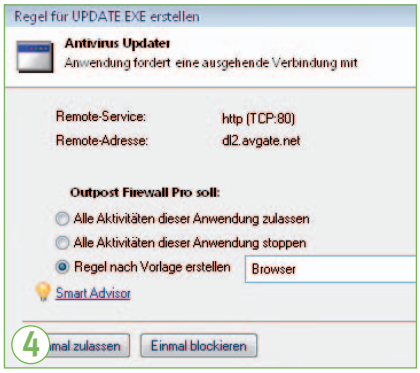
3 Verbindungsübersicht abrufen: Das Hauptfenster der Outpost Firewall ist die Steuerzentrale des Programms. An dieser Stelle überwachen Sie die Verbindungen, definieren Regeln und konfigurieren die Plugins der Firewall. Auf der linken Fensterseite zeigt Outpost unter „Mein Internet“ gefundene Spyware, Anwendungen und offene Ports an, die gerade aktiv sind. Prozesse und Anwendungen, welche die Firewall erlaubt, finden Sie unter „Zugelassen“. Gesperrte Verbindungen stehen unter „Blockiert“.

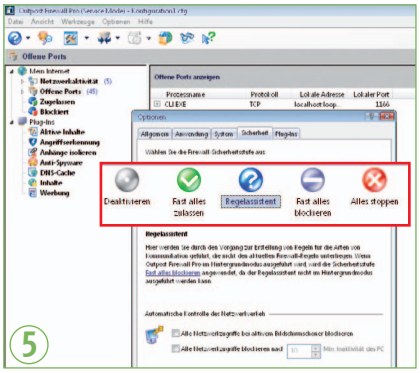
4 Anwendungsregeln einrichten: Ein Assistent hilft beim Anlegen neuer Regeln und schlägt bei unbekannten Anwendungen, die eine Internetverbindung anfordern, Standardregeln vor. Sie können durch Anklicken der entsprechenden Schaltfläche wählen, ob Sie die Verbindung grundsätzlich oder nur dieses Mal erlauben möchten oder ob Outpost sie blockieren soll. Für Programme, die Sie oft benutzen, beispielsweise Ihren Browser, empfiehlt es sich auf jeden Fall, eine eigene Regel anzulegen, damit Sie ohne ständiges Nachfragen der Firewall online gehen können. Regeln, die nicht Ihrem Nutzerverhalten entsprechen, können Sie rückgängig machen. Klicken Sie dazu auf „Optionen | Anwendungen“, und ändern Sie die Regeln der jeweiligen Programme.

5 Einstellungen anpassen: Je nach Anwendung und Surfverhalten können Sie die Sicherheitseinstellungen der Firewall anpassen: Klicken Sie dazu im Menü auf „Optionen | Sicherheit“. Von „Deaktivieren“ bis „Alles stoppen“ lässt sich hier der Schutzschild in Zwischenschritten einstellen. Sinnvoll ist auch die Möglichkeit, bei längerer Inaktivität des Rechners alle Netzwerkzugriffe zu blockieren. Aktivieren Sie dazu die entsprechende Box, und geben Sie die Zeit in Minuten an.

Achtung: Läuft Outpost Firewall Pro im Hintergrundmodus, ist der Regelassistent abgeschaltet. Standardmäßig setzt das Programm die Sicherheit auf „Fast alles blockieren“.





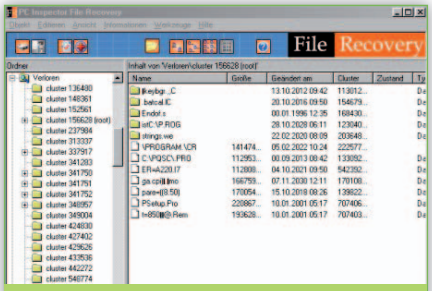


→CD-CODE ⊙ Vollversion

ALLE PROGRAMME AUF HEFT-CD

Die 50 besten Tools

Ungeschützte Rechner sind leichte Beute. Geben Sie Eindringlingen keine Chance, sich in Ihrem System einzunisten: Mit dem CHIP-Sicherheitspaket spüren Sie schädliche Software auf, vernichten Viren und surfen anonym im Web.



PC INSPECTOR FILE RECOV.

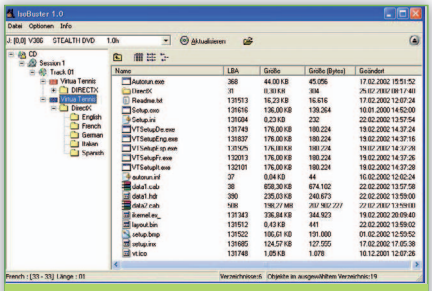
Dateien retten

Features
→ Kann Daten wiederherstellen
→ Unterstützt viele Formate
→ Läuft auf FAT- und NTFS-Systemen

Beschreibung PC Inspector File Recovery rekonstruiert gelöschte Dateien mit Originaldatum und -uhrzeit. Die Freeware kann sogar Dateien retten, bei denen kein Verweis aus einem Verzeichnis mehr vorhanden ist. Das Tool unterstützt Formate wie etwa AVI, EXE, JPG, MP3 und WAV.

Tipp Das Programm darf nicht auf dem zu rettenden Laufwerk installiert werden. Sie müssen das Tool von einem zweiten, unabhängigen Laufwerk starten.

→CD-CODE ◎ Security



ISOBUSTER

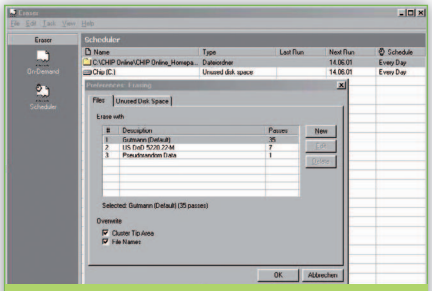
CDs auslesen

Features
→ Liest zerkratzte CDs oder DVDs
→ Speichert noch lesbare Dateien
→ Kann Imagedateien auslesen

Beschreibung Bei zerkratzten CDs oder DVDs bricht Windows den Lesevorgang ab und quittiert den Dienst. Beschädigte Speichermedien lassen sich somit nicht mehr öffnen. Dank IsoBuster können Sie alle noch lesbaren Daten auswerten und auf der Festplatte speichern.

Tipp IsoBuster ist Shareware. Funktionen, die schon vor der Version 1.0 eingebaut waren, sind aber weiterhin unregistriert und unbegrenzt nutzbar.

→CD-CODE ◎ Security



ERASER

Dokumente löschen

Features
→ Vernichtet Daten
→ Zeitverzögertes Löschen
→ Bedienerfreundlich

Beschreibung Mit den herkömmlichen Löschfunktionen unter Windows lassen sich alle Daten problemlos wiederherstellen, da die Festplatten-Cluster hierbei nicht überschrieben werden. Nutzen Sie daher ein Löschprogramm wie den Eraser: Das Open-Source-Programm vernichtet Daten endgültig.

Tipp Um die Zeitsteuerung zu aktivieren, klicken Sie auf den Button „Scheduler“ und anschließend auf „New Task“.

→CD-CODE ◎ Security

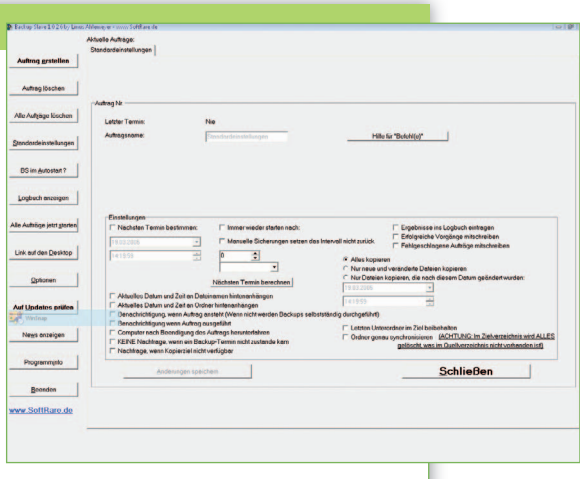
BACKUP SLAVE

Daten vor Verlust schützen

Features
→ Legt ein Backup an
→ Arbeitet automatisch im Hintergrund
→ Flexible Einstellmöglichkeiten

Beschreibung Gibt die Festplatte den Geist auf, sind die Daten in der Regel verloren – wenn Sie nicht vorher ein Backup angelegt haben. Gerade der Verlust sensibler Daten ist nicht nur ärgerlich, sondern kann großen Schaden anrichten. Diese Freeware schützt Sie vor unangenehmen Überraschungen, indem sie eine komplette Sicherung Ihrer Platte anlegt. Neben einer lokalen Speicherung können Sie Ihre Daten auch extern, zum Beispiel auf einem USB-Stick oder einem Netzlaufwerk, ablegen. Um immer die aktuellen Daten zu sichern, können Sie in Backup Slave ein Sicherungsintervall eingeben. Das Programm erledigt seine Aufgabe dann komplett im Hintergrund.

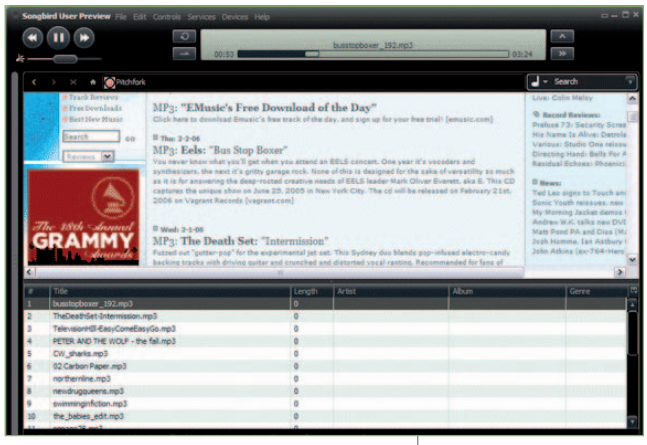
Tipp Für einen optimalen Schutz vor Datenverlust sollten Sie das Programm so einrichten, dass es automatisch Sicherungen Ihrer Festplatte anlegt.



→CD-CODE ◎ Security

SONGBIRD

Musik per Browser hören



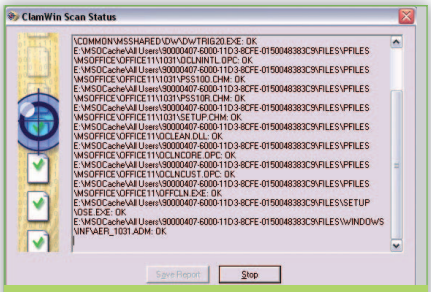
cherte Songs nach Interpret, Album und Titel. Findet Songbird auf einer Homepage abspielbare Dateien, legt es eine dynamische Playlist an und bietet Ihnen die Möglichkeit, alle Lieder herunterzuladen. Eine integrierte Toolbar mit vordefinierten Suchmaschinen vereinfacht die Websuche. Optisch haben sich die Hersteller an Apples iTunes orientiert. Das Tool befindet sich im Entwicklungsstadium. Daher fehlen noch sinnvolle Features, etwa eine Brennfunktion oder die Möglichkeit, Erweiterungen einzubinden.

Features
- ➔ Basiert auf Firefox
- ➔ Integriert Songs von Webseiten
- ➔ Unabhängig vom System

Beschreibung Songbird ist ein übersichtlicher Mediaplayer, der auf dem Firefox-Browser basiert. Sie können mit dem Tool Musik hören, Ihre eigenen Wiedergabelisten anlegen und gleichzeitig im Web surfen. Das Tool verwaltet lokal gespei-

Tipp Unter „Datei | Einstellungen“ können Sie die Sicherheitseinstellungen des Browsers vornehmen, automatische Updates aktivieren und die Startseite festlegen.

➔CD-CODE ◎ Audio/Video



PORTABLE CLAMWIN

Viren aufstöbern

Features
- ➔ Mobiler Virenscanner
- ➔ Durchsucht komprimierte Dateien
- ➔ Integrierte Update-Funktion

Beschreibung ClamWin ist ein schneller Virenscanner, der ursprünglich aus der Linux-Welt stammt. Diese mobile Version können Sie auf einem USB-Stick mitnehmen – und ohne weitere Installation auf jedem Rechner einsetzen. Anders als ClamAV bietet das Programm eine grafische Oberfläche.

Tipp Halten Sie die Virendefinition des Tools auf dem aktuellen Stand. Klicken Sie dazu auf den Button „Starts Internet Update“.

➔CD-CODE ◎ Security

ANTIVIR PE CLASSIC

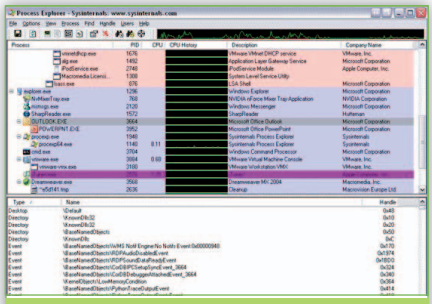
Viren vernichten

Features
- ➔ Erkennt die meisten Viren
- ➔ Zentrales Kontrollcenter
- ➔ Schutzschild inklusive

Beschreibung Das Programm ist eines der besten Antiviren-Tools. Es findet und entfernt mehr als 200.000 Viren, Würmer und Trojaner. Version 7 bietet eine komplett überarbeitete Oberfläche und neue Features, etwa eine zentrale Konfiguration und ein Kontrollcenter.

Tipp Unter „Planer | Neuen Auftrag mit dem Wizard erstellen“ können Sie einstellen, wann und in welchem Umfang das Tool nach Viren suchen soll.

➔CD-CODE ◎ Security



PROCESS EXPLORER

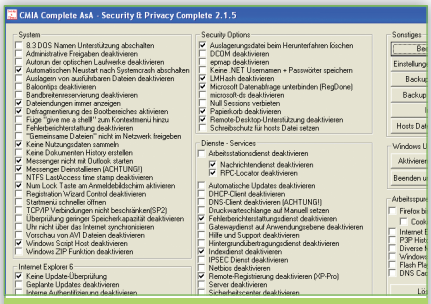
Programme abbrechen

Features
- ➔ Zeigt laufende Prozesse an
- ➔ Bricht DLLs ab
- ➔ Viele Details sichtbar

Beschreibung Process Explorer liefert Ihnen eine genaue Aufstellung darüber, welche Dateien gerade geladen sind, welche Priorität sie besitzen und welche DLLs ausgeführt werden. Darüber hinaus ist das Programm in der Lage, deren Ausführung abzubrechen.

Tipp Möchten Sie eine Anwendung beenden, klicken Sie mit der rechten Maustaste auf die Datei und anschließend auf „Kill Process“.

➔CD-CODE ◎ Windows



SECURITY & PRIVACY COM.

Lücken stopfen

Features
- ➔ Stellt Schnüffelfunktionen ab
- ➔ Unterstützt IE und Firefox
- ➔ Kinderleichte Bedienung

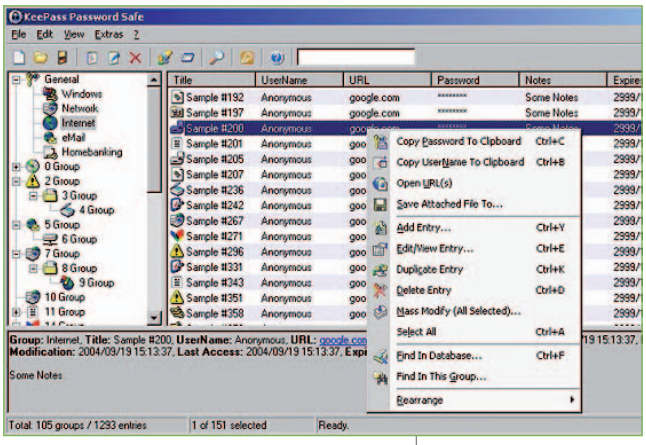
Beschreibung Ähnlich wie XP-AntiSpy oder Xpy stellt auch dieses Open-Source-Tool per Mausklick sämtliche Schnüffelfunktionen in Windows ab. Zusätzlich bietet Security & Privacy Complete auch einfache Einstellmöglichkeiten zum Windows Media Player, Internet Explorer und Mozilla Firefox.

Tipp Um das Programm starten zu können, brauchen Sie ein installiertes .NET Framework.

➔CD-CODE ◎ Security

KEEPASS

Passwörter in einer Datenbank ablegen

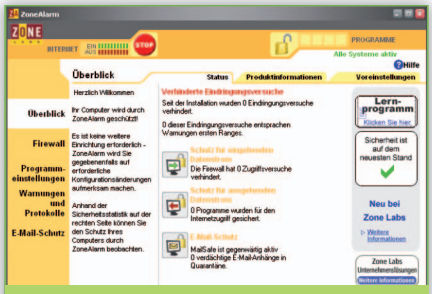


Features
→ Speichert Zugangsdaten
→ Sichere Programm-Verschlüsselung
→ Generiert eigene Passwörter

Beschreibung Für viele Programme und insbesondere Internetdienste brauchen Sie Passwörter, um sich vor Hackern zu schützen. Die Übersicht über die verschiedenen Passwörter kann dabei schnell verloren gehen. KeePass hilft Ihnen, diesen Wirrwarr an Zugangsdaten zu ordnen. Die Passwörter speichert das Tool in einer Datenbank und verschlüsselt sie mit dem Advanced Encryption Standard (AES) und dem Twofish-Algorithmus. Diese Verschlüsselung ist überdurchschnittlich sicher und wird unter anderem auch von Banken eingesetzt. Damit niemand Zugriff auf Ihre Passwort-Datenbank hat, sichern Sie sie mit einem Master-Passwort. Alternativ können Sie eine Key-Disk anlegen. Das Programm generiert auch eigene Passwörter. Dabei steht es Ihnen frei, etwa Länge und Wahl der Zeichen vorzugeben.

Tipp Über „Tools | Options | Advanced“ nehmen Sie weitere Einstellungen vor – etwa das Programmverhalten beim Systemstart.

→CD-CODE ◎ Security



ZONEALARM

Hacker abwehren

Features
→ Verhindert die Verbreitung von Viren
→ Schützt vor Angriffen aus dem Web
→ Leichte Bedienung

Beschreibung ZoneAlarm ist eine Software-Firewall, die verhindert, dass Hacker über das Internet Ihren Computer manipulieren. Zudem kontrolliert sie Programme, die von Ihrem PC aus auf das Web zugreifen. Die Bedienung ist unkompliziert – nach der Installation ist das Programm sofort startklar.

Tipp Unter „Programm Control“ können Sie festlegen, nach welcher Leerlaufzeit der Internetzugriff automatisch gesperrt werden soll.

→CD-CODE ◎ Internet

AIO-SECRETMAKER

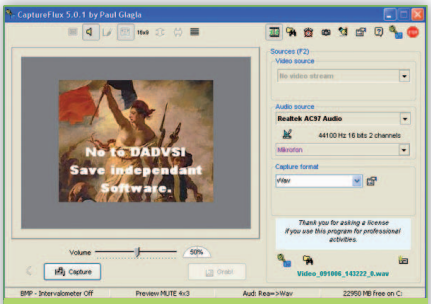
Vor Spionen schützen

Features
→ Blockt Popups, Animationen, Banner
→ Spamschutz
→ Wehrt Viren und Würmer ab

Beschreibung Schützen Sie Ihre Privatsphäre im Internet: Secretmaker bietet nützliche Tools, die Ihnen sicheres Surfen erlauben. Halten Sie Ihre Mailbox von Spam frei, schalten Sie Werbebanner, Popups und Animationen auf Webseiten ab – und schützen Sie sich vor den meisten Viren und Würmern.

Tipp Sie können die Werbeblocker temporär abschalten, indem Sie beim Laden einer Webseite die [Strg]-Taste drücken.

→CD-CODE ◎ Internet



CAPTUREFLUX

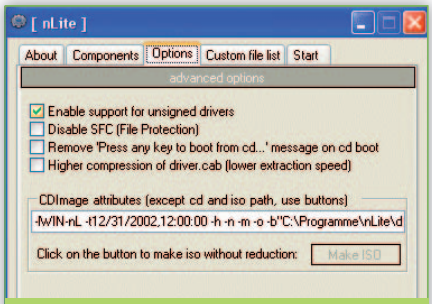
Videos aufnehmen

Features
→ Speichert externe Videos
→ Automatikfunktion
→ Viele Einstellmöglichkeiten

Beschreibung Mit CaptureFlux zeichnen Sie Videos von Webcams, Digitalkameras und TV-Karten als AVI oder WMV auf. Dabei können Sie die Größe und Qualität der Files anpassen. Den Sound speichert das Tool wahlweise als WAV oder MP3. Die „Schedule“-Funktion erlaubt Ihnen auch zeitgesteuerte Aufnahmen.

Tipp Wenn Sie auf den Hilfe-Button drücken, finden Sie unter „System“ die installierten und benötigten Codecs.

→CD-CODE ◎ Audio/Video



NLITE

Win-CD basteln

Features
→ Legt Installations-CD an
→ Grafische Oberfläche
→ Kann neue Tools einfügen

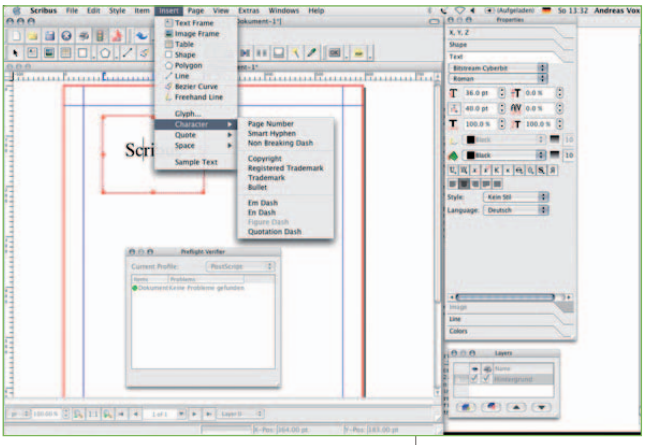
Beschreibung Nach einer Neuinstallation des Systems sieht Windows ziemlich leer aus: Alle Programme müssen Sie von Hand nachinstallieren. Mit nLite legen Sie Ihre eigene Installations-CD an – und können selbst bestimmen, welche Tools die Freeware automatisch hinzufügen soll. Die grafische Oberfläche erleichtert das Anlegen der CD.

Tipp Zum Starten des Tools benötigen Sie das .NET Framework.

→CD-CODE ◎ Windows

PORTABLE SCRIBUS

Professionelle Layouts gestalten



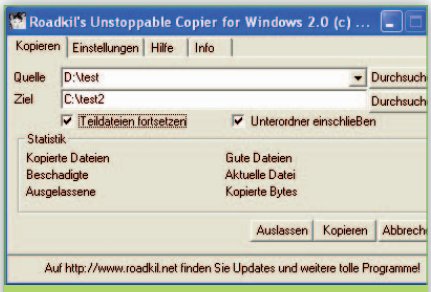
zu normalen Textverarbeitungsprogrammen hat das Tool einen entscheidenden Vorteil: Sie können Bilder und Textabschnitte millimetergenau setzen und ausgeben lassen. Die Ausstattung von Scribus ist großzügig: CMYK-Vorschau, Farbseparation, ICC-Farbmanagement und Vektor-Zeichenfunktionen, Vorlagenverwaltung sowie der Import und Export von SVG- und EPS-Dateien. Die Software kann interaktive PDF-Dateien mit Bookmarks, Notizen, Hyperlinks und Textfeldern anlegen. Mit der Programmiersprache Python schreiben Sie auch eigene Skripte für das Tool.

Features
→ Professionelle DTP-Software
→ Integrierte Vektor-Zeichenfunktion
→ Legt interaktive PDF-Dateien an

Beschreibung Scribus ist eine professionelle Desktop-Publishing-Software (DTP), die durch eine Fülle von Funktionen überzeugt: Kombinieren Sie wirkungsvoll Texte und Grafiken, um etwa Grußkarten, Poster oder CD-Cover zu entwerfen. Im Gegensatz

Tipp Einige Funktionen benötigen ein installiertes Ghostscript. Benutzen Sie etwa das GNU Ghostscript von unserer Heft-CD.

→CD-CODE ◎ Office



UNSTOPPABLE COPIER

CDs retten

Features
→ Daten von defekten CDs kopieren
→ Kombiniert Dateifragmente
→ Komplette Ordnerstrukturen sichern

Beschreibung Unstoppable Copier rettet Daten auf zerkratzten CDs und defekten Festplatten. Auch wenn die Kopierfunktion von Windows versagt, versucht der Copier, alle wiederherstellbaren Daten zu lesen. Selbst Fragmente defekter Daten lassen sich mit dem Programm sichern. Dabei spielt das Tool die noch lesbaren Bytes in einen Ordner.

Tipp Aktivieren Sie im Menü „Kopieren“ das Kästchen „Unterordner einschließen“, um sämtliche Daten zu sichern.

→CD-CODE ◎ Security

WIN-SEO

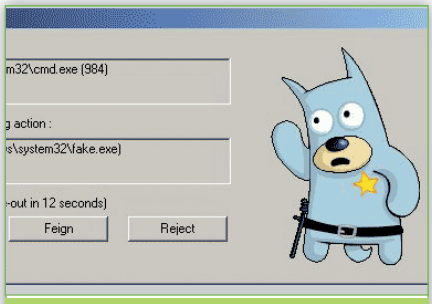
Isoliert arbeiten

Features
→ Errichtet eine sichere Zone
→ Schutz vor schädlichen Dateien
→ Arbeiten in isolierter Umgebung

Beschreibung Win-SeO ist ein kleines Programm, mit dem Sie in einer isolierten Umgebung kritische Anwendungen starten können. So schützt es Ihren PC – und Sie müssen keine Schädlinge fürchten. Ihr System und Ihre Festplatte bleiben sauber.

Tipp Sinnvoll ist der Einsatz dieser Freeware vor allem für Programme, die auf das Internet zugreifen, wie zum Beispiel Browser oder E-Mail-Clients.

→CD-CODE ◎ Windows



WINPOOCH

System überwachen

Features
→ Echtzeit-Überwachung
→ Dokumentiert Änderungen
→ Gibt Ratschläge

Beschreibung Winpooch überwacht die Registry und wichtige Systemverzeichnisse. Beim Eindringen von Spyware oder Trojanern schlägt das Tool sofort Alarm und dokumentiert akribisch jede Veränderung. Zudem gibt es Ratschläge zu jedem gefundenen Schädling. Das Tool befindet sich noch im Beta-Stadium.

Tipp Unter dem Menüpunkt „Konfiguration“ können Sie zum Beispiel neue Filter und Antiviren-Programme integrieren.

→CD-CODE ◎ Security

OPERA 9

Bequem surfen

Features
→ Komfortable Bedienung
→ Integrierter BitTorrent-Client
→ Zahlreiche Widgets

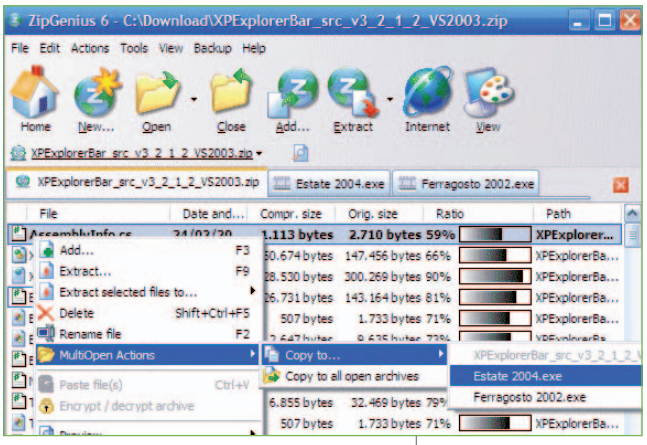
Beschreibung Opera ist ein sicherer Browser, der vor allem durch eines glänzt: Er bietet eine einfache und komfortable Bedienung. Sie können jede Seite spezifisch einstellen und sich Miniaturbilder für Tabs anzeigen lassen. Ein BitTorrent-Client vereinfacht das Herunterladen großer Daten.

Tipp Zahlreiche Widgets für Ihren Desktop finden Sie unter **http://widgets.opera.com**.

→CD-CODE ◎ Internet

ZIPGENIUS SUITE

Daten komprimieren

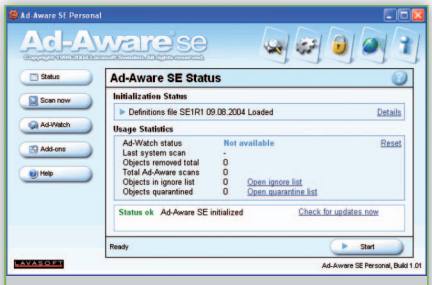


Features
→ Packt und entpackt viele Formate
→ Legt verschlüsselte Archive an
→ Schnelle, einfache Bedienung

Beschreibung Die ZipGenius Suite bindet sich in das Kontextmenü in Windows ein. Damit können Sie mit nur einem Klick die Daten schnell packen oder entpacken. Das Tool liest mehr als zwanzig Dateiformate und komprimiert in neun. Selbst ISO-Dateien können Sie mit dem Programm anlegen. Wenn Sie nicht wissen, ob die von Ihnen versendeten Daten von Freunden oder Kollegen auch wieder entpackt werden können, legen Sie ganz einfach eine selbstextrahierende Datei an. Für optimalen Schutz sorgen Sie mit der Verschlüsselungsfunktion der Archive. Zusätzlich enthält die Freeware die Programme FTPGenius und ZGAlbum. Beide Tools lassen sich bequem über die Oberfläche von ZipGenius steuern.

Tipp Ihre Archive können Sie direkt aus ZipGenius heraus als E-Mail verschicken: Markieren Sie dazu die gewünschte Datei, und klicken Sie auf den Button „Internet“. Das Tool öffnet anschließend Outlook – inklusive Betreff und Anhang.

→CD-CODE ◎ Windows



AD-AWARE SE PERSONAL

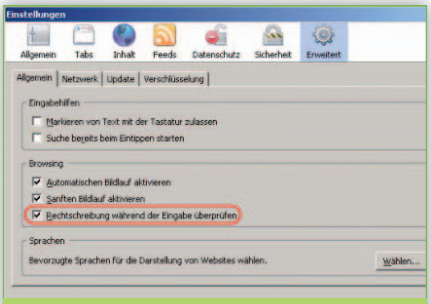
System bewachen

Features
→ Spyware und Malware aufspüren
→ Automatische Säuberung
→ Systemregistrierung bereinigen

Beschreibung Ad-Aware durchsucht den Rechner auf Spyware und andere schädliche Software – und entfernt diese per Mausklick. Wenn Sie häufig im Internet surfen oder Programme aus dem Web installieren, sollten Sie die Freeware regelmäßig starten, um Ihre persönlichen Daten zu schützen.

Tipp Halten Sie Ad-Aware immer auf dem neuesten Stand: Klicken Sie im Hauptmenü auf „Check for Updates now“, um Aktualisierungen herunterzuladen.

→CD-CODE ◎ Security



MOZILLA FIREFOX 2

Sicher surfen

Features
→ Noch schneller und sicherer
→ Anti-Phishing-Filter
→ Restore-Session-Funktion

Beschreibung Firefox hat sich als schlanker, schneller Browser längst etabliert. Die neue Version bietet jetzt noch mehr Funktionen, etwa eine Rechtschreibprüfung und einen integrierten Feed-Reader. Die wichtigste Änderung sind aber neue Schutzmaßnahmen, die Angriffe effektiv abwehren sollen.

Tipp Erweiterungen, mit denen Sie den Browser verändern können, finden Sie unter **https://addons.mozilla.org**.

→CD-CODE ◎ Internet

ADBLOCK PLUS

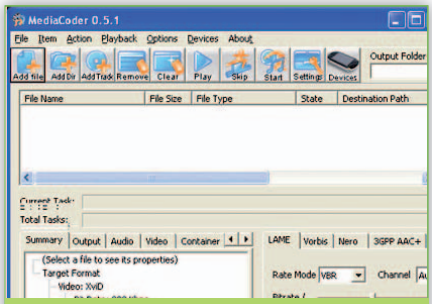
Werbung blocken

Features
→ Verhindert Popups
→ Blockiert Werbung
→ Einfache Bedienung

Beschreibung Adblock Plus ist eine nützliche Firefox-Erweiterung, die nervige Popups und Werbebanner entfernt. Nach der Installation hängt sich ein kleiner Button an jede störende Anzeige. Klicken Sie darauf, um die Werbung von dem Tool ausfiltern zu lassen.

Tipp Unter „Einstellungen | Filter | Filter-Abonnement hinzufügen“ können Sie sich vordefinierte Filter anzeigen lassen und in Adblock integrieren.

→CD-CODE ◎ Internet



MEDIACODER

Filme umwandeln

Features
→ Enthält alle Open-Source-Codecs
→ Konvertiert Audio- und Videofiles
→ Viele Einstellmöglichkeiten

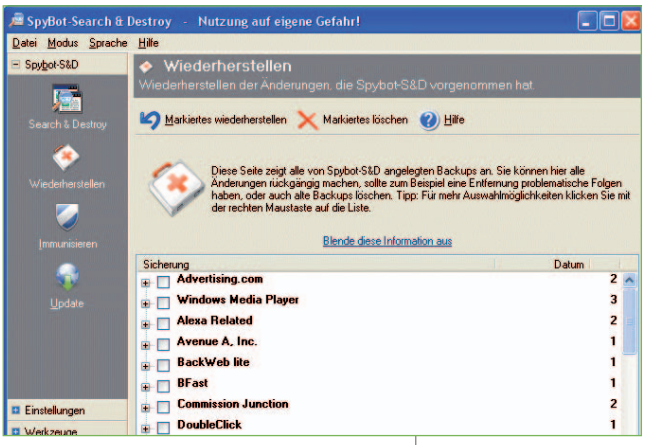
Beschreibung MediaCoder vereint sämtliche Audio- und Videocodecs aus der Open-Source-Welt. Das Tool kann Daten in die verschiedenen Formate konvertieren und für Handys, MP3- oder Videoplayer aufbereiten. Der MediaCoder ist sehr umfangreich und bietet zahlreiche Einstellmöglichkeiten.

Tipp Nach der Installation können Sie die Sprache der Oberfläche über „Options | Language“ ändern.

→CD-CODE ◎ Audio/Video

SPYBOT - SEARCH & DESTROY

Spyware sicher vernichten

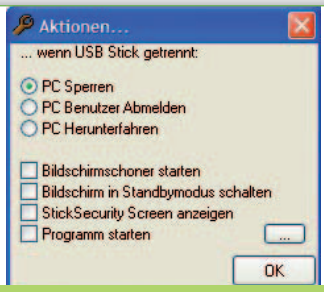


Features
→ Spyware aufspüren und löschen
→ Wirtsprogramme bleiben erhalten
→ Integrierter Registry Cleaner

Beschreibung Schützen Sie Ihren Rechner vor Hackerangriffen und gefährlicher Spyware: Mit Spybot – Search & Destroy durchsuchen Sie Ihren PC nach schädlichen Programmen, die Informationen über Ihr Nutzerverhalten im Internet ausspionieren und an Dritte weiterleiten. Die Freeware erkennt die meisten dieser Spyware-Programme und kann sie automatisch entfernen. Findet das Tool entsprechende Software, löscht es die Werbe- und Spyware-Komponenten, ohne die Funktionalität des „Wirtsprogramms“ zu beeinflussen. Zudem beseitigt es zuverlässig Webspuren wie Verlauf und Cookies – und erhöht somit die Sicherheit beim Surfen. Über die Update-Funktion halten Sie das Programm auf dem neuesten Stand.

Tipp Spybot – Search & Destroy enthält zahlreiche Zusatzfunktionen, zum Beispiel einen Registry Cleaner. Um diese freizuschalten, klicken Sie im Menü „Modus“ auf den Eintrag „Erweiterter Modus“.

→CD-CODE ◎ Security



STICK SECURITY

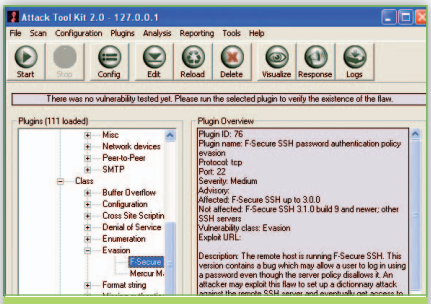
Rechner absperren

Features
→ USB-Stick als Rechnerschlüssel
→ Verschiedene Schutzfunktionen
→ Schnelle Installation

Beschreibung Mit Stick Security müssen Sie sich keine Sorge um die Sicherheit Ihres Rechners machen. Installieren Sie einfach das Tool, stecken Sie einen USB-Stick an und wählen Sie diesen als Schlüssel aus. Nun haben Sie verschiedene Einstellmöglichkeiten. Sie können sich zum Beispiel noch ein Passwort für Ihren Key einrichten.

Tipp Das Programm speichert die Datei „key.go“ auf Ihrem Schlüssel. Diese dürfen Sie bei Aktivierung nicht löschen.

→CD-CODE ◎ Security



ATTACK TOOL KIT

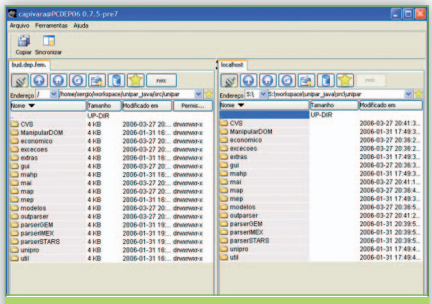
Abwehr testen

Features
→ Testet die Systemsicherheit
→ Simuliert Hackerangriffe
→ Durch Plugins erweiterbar

Beschreibung Ob der Rechner wirklich geschützt ist, erfährt man oft, wenn es bereits zu spät ist. Mit dem Attack Tool Kit testen Sie die Sicherheit Ihres Systems, indem Sie Hackerangriffe aus dem Netz simulieren. Erfahrene Programmierer können die Funktionalität mit eigenen Plugins beliebig erweitern.

Tipp Unter **www.computec.ch/projekte/atk** finden Sie eine Reihe von fertigen Plugins für das Tool.

→CD-CODE ◎ Security



CAPIVARA

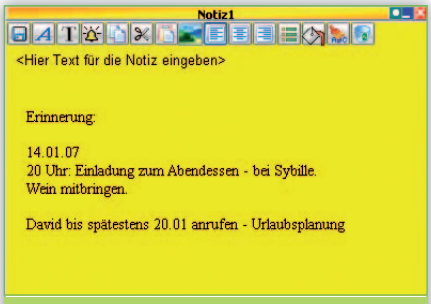
PCs synchronisieren

Features
→ Synchronisiert Datenträger
→ Flexibel einsetzbar
→ Übersichtliche Struktur

Beschreibung Arbeiten Sie oft auf verschiedenen Datenträgern, sollten Sie regelmäßig alle Dokumente abgleichen. Capivara synchronisiert spielend leicht Ihre Daten. Das Tool unterstützt dabei FTP-Server, SSH-Server, lokale Festplatten und Notebooks. Auch der Abgleich zwischen Servern ist möglich.

Tipp Klicken Sie auf „Sync“ und wählen Sie anschließend, welcher Datenträger aktualisiert werden soll.

→CD-CODE ◎ Windows



KLEBEZETTEL NG

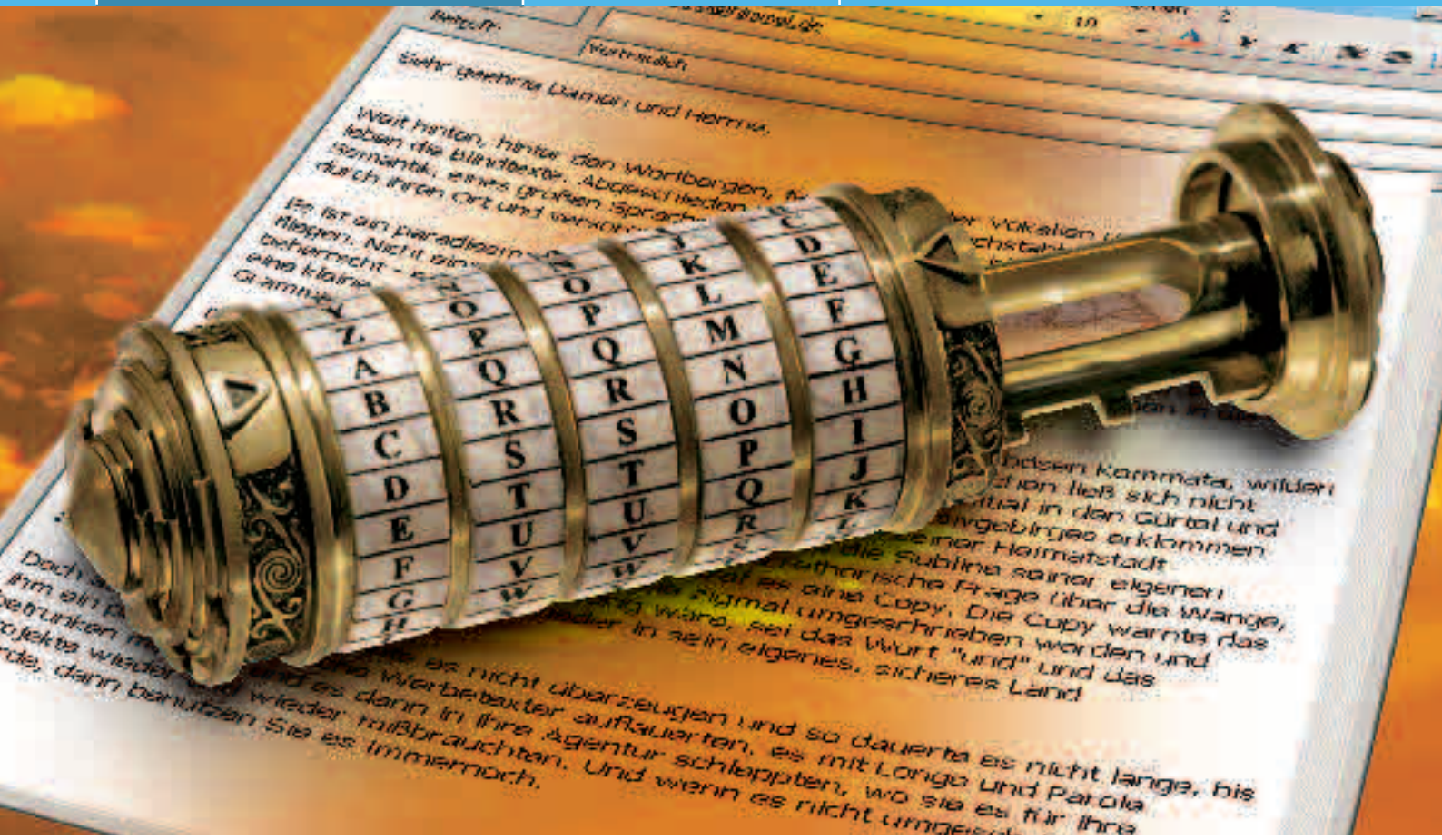
Termine notieren

Features
→ Legt Notizen an
→ Alarmfunktion
→ Verschickt Erinnerungen im Netzwerk

Beschreibung Klebezettel NG hilft Ihnen dabei, die Übersicht über Ihre Termine zu behalten. Das Programm ist mit den wichtigsten Einstellmöglichkeiten und grundlegenden Textverarbeitungsfunktionen ausgestattet. Mit der Alarmfunktion erinnert Sie die Freeware an Jahres- oder Geburtstage.

Tipp Unter „Grundeinstellungen | Visuelle Einstellungen“ können Sie das Tool optisch verändern.

→CD-CODE ◎ Office



CHIFFRIEREN MIT GPG4WIN

E-Mails verschlüsseln

Wenn Sie E-Mails im Klartext verschicken, ist das nichts anderes, als wenn Sie vertrauliche Botschaften per Postkarte übermitteln würden. Damit kein Außenstehender mitlesen kann, sollten Sie die Nachrichten und Anhänge verschlüsseln. So chiffrieren Sie Ihre E-Mails.

Die niedrigen Kosten, die Geschwindigkeit und die Vielseitigkeit machen E-Mail zum perfekten Kommunikationsmittel. Allerdings hat die elektronische Post eine große Schwachstelle: die Sicherheit. Informationen, die Sie per E-Mail versenden, sind letztlich nicht sicherer vor fremden Blicken als eine Nachricht, die Sie auf eine Postkarte schreiben und in den Briefkasten werfen. Denn im Internet kann potenziell jeder Ihre Mails abfangen und mitlesen. Er muss sich dazu „nur“ in einen der vielen Server einhacken, die Ihre Nachricht auf dem Weg zum Empfänger passiert. Wenn Sie sicher sein wollen, dass nur der Empfänger Ihre Nachrichten und die Dateianhänge lesen kann, sollten Sie sie in verschlüsselter Form schicken.

Als bestes Verschlüsselungstool gilt seit Jahren PGP (Pretty Good Privacy). Nachdem die Software lange Zeit für den privaten Gebrauch gratis eingesetzt werden durfte, ist sie mittlerweile nur noch als kommerzielles Tool erhältlich. Eine kostenlose Alternative ist das Open-Source-Tool GnuPG (Gnu Privacy Guard), dessen Verschlüsselungs-Verfahren kompatibel zu dem von PGP ist. Der große Vorteil von GnuPG (**www.gnupg.org**): Es ist für alle gängigen Computer-Plattformen verfügbar, also für Windows, Linux, Mac OS X und sogar für den Pocket PC. Die Nachteile: Zum einen ist GnuPG selbst ein reines Befehlszeilen-Tool. Glücklicherweise sind jedoch grafische Front-ends verfügbar. Zum anderen ist für die Integration von GnuPG in ein E-Mail-Programm ein Plugin erforderlich.

Dieser Artikel zeigt Ihnen, wie Sie mit Gpg4win arbeiten. Dabei handelt es sich um ein Paket, das vom Bundesamt für Sicherheit in der Informationstechnik zusammengestellt wurde und aus mehreren Komponenten besteht. Diese sind:

- GnuPG, die eigentliche Verschlüsselungssoftware
- WinPT, eine grafische Windows-Oberfläche für GnuPG

AUF EINEN BLICK

Chiffrierte Mails verschicken

Alle Tools auf CD

Gpg4win: Tool-Paket, um E-Mails und Dateien zu verschlüsseln ◎ Windows

Foto: Elbenwald.de; Illustration: S. Schönberger

- GPA, ein alternativer Schlüsselmanager, der mit Assistenten arbeitet
- GPCol, ein Plugin für Microsoft Outlook 2003 mit Service Pack 2
- GPGee, ein Plugin für den Windows-Explorer, das die Verschlüsselung von Dateien und Ordnern erlaubt
- Sylpheed-Claws, ein Mailprogramm

Plugins für weitere Mailprogramme finden Sie unter **www.gnupg.org** (unter „MUA Frontends"). Diese Site bietet auch weitere grafische Frontends für Windows und andere Betriebssysteme an. Ein kostenloses Plugin für Outlook und Outlook Express erhalten Sie von G-Data (**www3.gdata.de/gpg/download.html**). Die Software wird allerdings seit 2002 nicht mehr weiterentwickelt. Falls Sie sie dennoch einsetzen wollen, beachten Sie, dass in dem Paket eine veraltete Fassung von GnuPG enthalten ist, die Sicherheitslücken aufweist. Installieren Sie also zuerst GnuPG und GPA, etwa aus dem Gpg4win-Paket auf der CD zu diesem Heft oder von **www.gnupg.org**, und anschließend das Plugin für Outlook.

Im Artikel beschreiben wir die Vorgehensweise anhand von WinPT. Dieses grafische Frontend ist zwar nicht so komfortabel wie ein Plugin, das direkt in die Mailsoftware integriert ist, funktioniert dafür aber mit allen E-Mail-Programmen und sogar mit Webmail-Diensten. Mit WinPT ver- beziehungsweise entschlüsseln Sie die Nachrichten getrennt vom Mailclient. Der Datenaustausch erfolgt dann über die Zwischenablage.

GnuPG arbeitet wie PGP nach dem Public-Key-Verfahren und verwendet zum Ver- und Entschlüsseln ein Schlüsselpaar. Zum Chiffrieren dient der Public Key, zum Dechiffrieren der Private Key. Ihren Public Key geben Sie an alle Personen weiter, die Ihnen verschlüsselte Nachrichten schicken wollen. Den Private Key dagegen besitzen nur Sie: Mit ihm können Sie die empfangenen, verschlüsselten Nachrichten entschlüsseln.

Gpg4win installieren und Komponenten auswählen

Holen Sie sich zunächst von **www.gpg4win.de** die neueste Version des Pakets. In letzter Zeit wurden einige Sicherheitslücken in GnuPG bekannt und kurz darauf behoben, achten Sie also darauf, dass Sie immer die aktuellste Version nutzen. Für die Installation müssen Sie in Windows mit Administratorrechten angemeldet sein. Starten Sie das Installationsprogramm, und wählen Sie die Komponenten aus, die Sie nutzen wollen. Um diesen Workshop mitzumachen, benötigen Sie mindestens GnuPG, WinPT und GPGee. Einsteiger in die Verschlüsselung sollten auch GPA installieren. Folgen Sie dann den weiteren Anweisungen.

PROFI-TIPP

HTML abschalten

Damit es beim Verschlüsseln und Signieren zu keinen Problemen kommt, sollten Sie Mails nicht im HTML-Format versenden. In Outlook Express schalten Sie das HTML-Format für Ihre Mails so ab: Rufen Sie im Menü „Extras" den Befehl „Optionen" auf. Wechseln Sie zum Register „Senden" und wählen Sie als Format für Ihre E-Mails „Nur-Text" aus.

Schlüssel generieren und Passwort erzeugen

Falls Sie noch keine Erfahrung mit Verschlüsselung haben, können Sie mithilfe des Assistenten in GPA das Erzeugen eines Schlüsselpaars und das Verschlüsseln erst einmal üben. Dazu rufen Sie GPA über das Startmenü auf, geben an, dass Sie jetzt die Schlüssel erzeugen wollen, und tragen dann einen Fantasienamen und eine beliebige Mailadresse ein. Folgen Sie den weiteren Anweisungen des Assistenten. Nachdem Sie sich in der Simulation mit den verschiedenen Schritten vertraut gemacht haben, wird es ernst: Erzeugen Sie ein Schlüsselpaar für Ihren realen Namen und Ihre E-Mail-Adresse. Das erledigen Sie entweder in GPA oder, wie im Folgenden beschrieben, in WinPT.

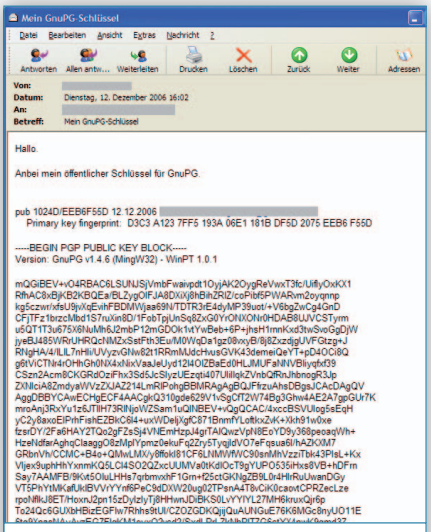
Rufen Sie über das Startmenü WinPT auf und geben Sie an, dass Sie ein GnuPG-Schlüsselpaar erzeugen wollen. Falls Sie bereits über einen Schlüsselbund aus GnuPG oder PGP verfügen, können Sie ihn übernehmen. Tragen Sie Ihren Namen und auch Ihre Mailadresse ein, denn damit werden die Schlüssel verknüpft. Die Option „RSA-Schlüssel bevorzugen" brauchen Sie nur dann zu aktivieren, wenn Sie Schlüssel erzeugen müssen, die zu sehr alten PGP-Versionen kompatibel sind. Geben Sie anschließend das Passwort ein, mit dem Sie Ihren privaten Schlüssel schützen wollen. Falls Sie vorher in GPA geübt haben: Dabei handelt es sich um die „Passphrase". Ein sicheres Passwort besteht aus mindestens zehn Zeichen und enthält eine Mischung aus Ziffern, Buchstaben und Sonderzeichen. Verwenden Sie auf keinen Fall Ihren Namen oder Begriffe, die in einem Wörterbuch zu finden sind. Solche Passwörter lassen sich nämlich sehr leicht knacken. Um sicherzustellen, dass Sie sich nicht vertippt haben, geben Sie das Passwort in der nächsten Zeile des Fensters ein weiteres Mal ein.

GnuPG erzeugt nun den Schlüssel. Danach empfiehlt WinPT, eine Kopie des Schlüsselbunds auf einer Diskette oder einem USB-Stick zu sichern. Diesem Tipp sollten Sie unbedingt Folge leisten, gesichert werden dabei zwei kleine Dateien.

Schlüssel mit anderen Personen austauschen

Klicken Sie im Systemtray der Taskleiste doppelt auf das Schlüsselsymbol, um die Schlüsselverwaltung zu öffnen. Dort erscheint zunächst nur Ihr eigener Schlüssel. Im „Eigenschaften"-Fenster zu Ihrem Schlüssel können Sie übrigens jederzeit das Passwort ändern, mit dem Sie den Schlüssel schützen.

Damit Sie einer anderen Person verschlüsselte Mails schicken können, benötigen Sie deren öffentlichen Schlüssel. Das gilt auch umgekehrt: Wenn jemand Ihnen eine verschlüsselte Nachricht schicken →

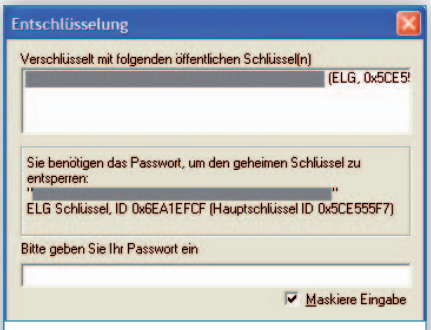


Import: Wenn Sie einen öffentlichen Schlüssel per Mail erhalten haben, importieren Sie ihn in Ihren Schlüsselbund.

möchte, braucht er dazu Ihren öffentlichen Schlüssel. Den verschicken Sie am besten per E-Mail. Alternativ dazu können Sie ihn auch auf einem Schlüsselserver weltweit für jedermann zugänglich machen. Das ist jedoch nicht zu empfehlen: Da Sie auf dem Schlüsselserver auch Ihre Mailadresse hinterlassen müssen, ziehen Sie damit jede Menge Spam an.

Um Ihren Schlüssel an ausgewählte Personen zu übermitteln, wählen Sie ihn in der Schlüsselverwaltung aus und rufen im Menü „Schlüssel“ den Befehl „Exportieren“ auf. Achtung: Auf keinen Fall dürfen Sie dabei auf „Exportiere geheimen Schlüssel“ klicken! Speichern Sie die Datei auf der Festplatte, und schicken Sie sie dann an alle Personen, die Ihren öffentlichen Schlüssel erhalten sollen.

Alternativ dazu können Sie das File auch markieren und mit „Kopiere Schlüssel in Ablage“ in die Zwischenablage übertragen. Dann schreiben Sie eine Mail, kopieren den Schlüssel hinein und versenden sie an alle Adressaten, mit denen



Dechiffrieren: Zum Entschlüsseln geben Sie das Kennwort ein, mit dem Sie Ihren privaten Schlüssel schützen.

Sie verschlüsselte Nachrichten austauschen wollen. Um den Schlüssel einer anderen Person in Ihren Schlüsselbund einzufügen, bitten Sie sie, Ihnen den Schlüssel per Mail zu schicken. Markieren Sie den Inhalt des Schlüssels von der Zeile „Begin PGP Public Key Block“ bis einschließlich „End PGP Public Key Block“, wechseln Sie in die Schlüsselverwaltung und klicken Sie dort auf den Button „Schlüssel aus Ablage einfügen“. Im folgenden Dialogfenster klicken Sie auf die Schaltfläche „Import“, um den Schlüssel Ihrem virtuellen Schlüsselbund hinzuzufügen.

E-Mails und Anhänge chiffrieren und dechiffrieren

Wenn Sie jemandem eine verschlüsselte Nachricht senden wollen, verfassen Sie den Text zunächst wie gewohnt in Ihrem Mailprogramm. Danach kopieren Sie ihn in die Zwischenablage. Rufen Sie WinPT auf, klicken Sie in der Taskleiste mit der rechten Maustaste auf das Schlüssel-Icon und wählen Sie „Zwischenablage“ und danach „Verschlüsseln“.

WinPT zeigt nun Ihren Schlüsselbund an. Setzen Sie ein Häkchen vor den Namen des Empfängers der Nachricht. Sobald Sie auf „OK“ geklickt haben, chiffriert WinPT/GnuPG den Text mit dem öffentlichen Schlüssel des Adressaten. Danach kopiert das Programm sie automatisch in die Zwischenablage.

Wechseln Sie nun wieder in Ihr Mailprogramm, und fügen Sie den verschlüsselten Text in die Nachricht ein. Geben Sie die Mailadresse des Empfängers ein, und achten Sie darauf, dass es sich um die gleiche Adresse handelt, die mit dem öffentlichen Schlüssel verknüpft ist. Nun können Sie die Nachricht verschicken.

Zum Verschlüsseln eines Dateianhangs verwenden Sie den Windows Explorer. In GPGee finden Sie nach einem Klick mit der rechten Maustaste auf eine Datei im Kontextmenü den Eintrag „GPGee“, über den Sie die Datei verschlüsseln können. Dabei müssen Sie ebenfalls den öffentlichen Schlüssel des Adressaten auswählen. Anschließend fügen Sie die Datei als Anhang in Ihre E-Mail ein.

Beim Empfang einer verschlüsselten Mail kopieren Sie den Text inklusive der Zeilen „Begin PGP Message“ und „End PGP Message“ in die Zwischenablage. Klicken Sie mit der rechten Maustaste auf das Schlüsselsymbol in der Taskleiste und rufen Sie „Zwischenablage“ und „Entschlüsseln/Überprüfen“ auf. Anschließend geben Sie das Passwort ein, mit dem Sie Ihren privaten Schlüssel schützen.

Die Nachricht wird nun dechiffriert und in die Zwischenablage kopiert. Von dort aus können Sie sie in ein Textprogramm kopieren oder über die Befehle „Zwischenablage | Bearbeiten“ in WinPT ansehen.

Franz Grieser

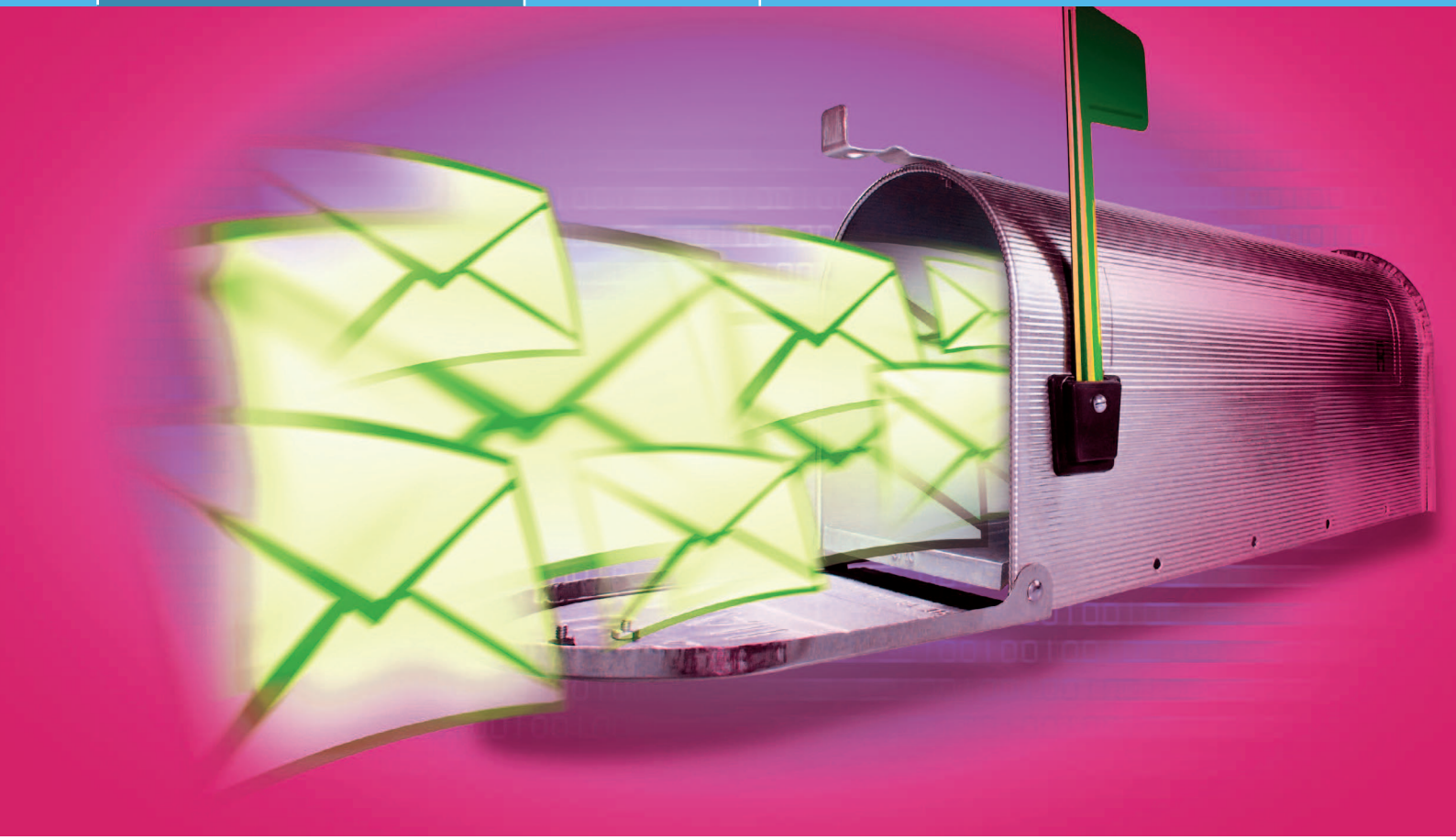
KNOW-HOW

Symmetrisch oder asymmetrisch chiffrieren

Zum Chiffrieren und Dechiffrieren benötigt man einen Schlüssel (Key). Eine symmetrische Verschlüsselung verwendet zum Chiffrieren und Dechiffrieren den gleichen Schlüssel, die asymmetrischen Verfahren (auch als Public-Key-Verfahren bezeichnet) dagegen arbeiten mit zwei Schlüsseln: Zum Verschlüsseln dient der öffentliche Schlüssel (Public Key), zum Entschlüsseln der private Schlüssel (Private Key).

Symmetrische Verschlüsselung: Sie setzt voraus, dass der Absender einer chiffrierten Botschaft dem Empfänger auch den Schlüssel zukommen lässt, damit er die Nachricht wieder dechiffrieren kann. Den Schlüssel zusammen mit der chiffrierten Nachricht zu versenden verbietet sich aus Sicherheitsgründen. Also sollte der Absender dem Empfänger den Schlüssel – am besten persönlich – einmal übergeben, der Adressat kann diesen Schlüssel dann immer wieder verwenden. Doch wenn der Absender diesen Schlüssel aus praktischen Erwägungen heraus auch zum Austausch chiffrierter Nachrichten mit anderen nutzt, läuft er Gefahr, dass sein Schlüssel in falsche Hände gerät und eine andere Person die ganze Korrespondenz, die er mit diesem Schlüssel geschützt hat, entschlüsseln kann. Wer vertrauliche Nachrichten mit einer größeren Anzahl von Adressaten austauscht, steht daher vor der Entscheidung, entweder einen Schlüssel für alle Nachrichten zu verwenden und damit ein hohes Risiko in Kauf zu nehmen oder aber mehrere Schlüssel zu definieren, was das Risiko verringert, dafür jedoch den logistischen Aufwand erhöht.

Asymmetrische Verschlüsselung: Dieses Dilemma löst das asymmetrische Verfahren. Dabei erzeugen alle Personen, die chiffrierte Nachrichten austauschen wollen, zwei zusammengehörige Schlüssel: einen öffentlichen und einen privaten. Den öffentlichen Schlüssel geben sie weiter, den privaten halten sie unter Verschluss (zur Sicherheit wird er durch ein Kennwort geschützt). Jeder, der nun an Empfänger A eine chiffrierte Nachricht senden will, nimmt den öffentlichen Schlüssel von A, chiffriert die Nachricht damit und schickt sie an A. Zum Entschlüsseln ist dann zwingend der private Schlüssel von A erforderlich, die öffentlichen Schlüssel lassen sich lediglich zum Verschlüsseln nutzen. Zusätzlich dient der private Schlüssel auch zum Signieren von Nachrichten. Falls B also an A eine chiffrierte und signierte Nachricht senden will, chiffriert er sie mit dem öffentlichen Schlüssel von A und signiert sie mit seinem eigenen, privaten Schlüssel. Wenn A über den öffentlichen Schlüssel von B verfügt, kann er damit die Echtheit der digitalen Signatur überprüfen.



WERBUNG ABBLOCKEN

Spam-Mails filtern

Benutzer von Outlook Express müssen immer noch auf einen Spamfilter verzichten. Doch mit Spamihilator können Sie Werbung bereits aussondern, bevor sie den Posteingang erreicht. Und Thunderbird bietet sogar eigene Antispam-Funktionen. So richten Sie die Filter ein.

Outlook Express ist gut in Windows integriert und einfach zu bedienen. Zudem ist das Programm kostenlos, denn es ist fester Bestandteil des Betriebssystems und wird automatisch installiert. Für viele Anwender ist es daher der bevorzugte Mailclient.

Doch eine Empfehlung ist die Software nicht: Denn Outlook Express bietet nur wenig Möglichkeiten, Spam- oder Junkmails automatisch auszusortieren. Und das, obwohl derartige Mails seit Jahren den Posteingang füllen und es ausreichend geeignete Abwehrmethoden gibt. Wer viel mit Spam zu kämpfen hat, kann also nicht auf Outlook Express bauen. Im Kampf gegen die unerwünschte Werbung hilft nur ein Spamfilter weiter. Fest integrierte Filter gibt es beispielsweise in Outlook und Thunderbird. Die Alternative ist ein Filterprogramm, das Outlook Express vorgeschaltet wird und die eingehenden Nachrichten bereits im Vorfeld sortiert.

Spamihilator ist so ein Filterprogramm. Es untersucht jede ankommende Mail darauf, ob es sich um eine überflüssige Werbenachricht handelt. Wenn ja, filtert Spamihilator sie heraus, zum E-Mail-Programm weitergeleitet werden nur die „guten“ Nachrichten. Bei der Suche nach Spam wendet die Software gleich mehrere Methoden an: Ein Wortfilter sucht nach bekannten Schlüsselwörtern, lernfähige Bayes-Filterregeln errechnen für jede E-Mail die statistische Wahrscheinlichkeit, dass es sich bei ihr um Spam handelt, und ein DCC-Filter erkennt Massenmails. Durch die Kombination dieser Mittel kann Spamihilator die meisten Spammails herausfiltern. Zudem kann der Benutzer mit einem einfachen Training die Erkennungsrate noch erhöhen. Auf diese Weise werden die Ergebnisse mit der Zeit immer besser.

Spamihilator ist Freeware und damit kostenlos. Es kann mit IMAP- und POP3-Postfächern umgehen, arbeitet mit den

AUF EINEN BLICK

Spamfilter einrichten

Wie Sie mit Spamihilator Ihr Postfach vor Werbemails schützen 57

Thunderbird-Filter konfigurieren 59

Alle Tools auf CD

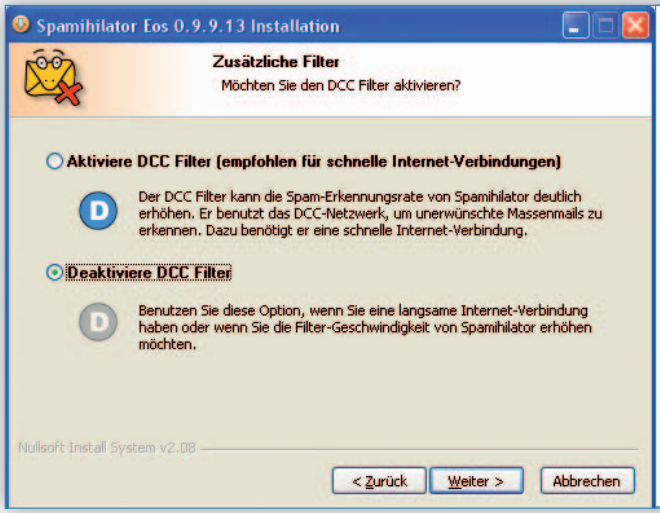
Mozilla Thunderbird: Sicherer und komfortabler Mailclient ◎ Office

Spamihilator: Untersucht E-Mails und filtert nervigen Spam ◎ Security

Foto: CHIPimages

meisten E-Mail-Clients zusammen und läuft auf allen Windows-Versionen seit Windows 95. Auf der Homepage (**www.spamihilator.com**) schweigen sich die Entwickler lediglich noch bezüglich Windows Vista aus.

Mehr als eine Million Mal ist die aktuelle Version 0.9.9 von der Homepage heruntergeladen worden – ein Indiz für die große Popularität des Programms. Verwenden sollten Sie jedoch besser die letzte Betaversion 0.9.9.13. Sie bereinigt nämlich einige ärgerliche Fehler der offiziellen Version, beispielsweise einen Bug im Spamihilator Service Provider, der zu einem Pufferüberlauf führen konnte, und einen anderen Fehler, der teilweise die Zerstörung von E-Mails mit großen Anhängen zur Folge hatte.



Massenmails: Den DCC-Filter für Massenmail-Sendungen sollten Sie nur bei einer schnellen Internetverbindung einschalten.

Spamihilator: Installation und erste Schritte

Das Setup-Programm von Spamihilator verspricht, dass es mit seinem Assistenten das E-Mail-Programm automatisch für die Zusammenarbeit mit der Filtersoftware einrichtet. Erfolgreich getestet wurde das bisher mit den neueren Versionen von Outlook und Outlook Express sowie mit Opera, Eudora, Pegasus Mail, Phoenix Mail, Netscape/Mozilla, Thunderbird und Incredimail.

Die aktuelle Version von Spamihilator steht unter **www.spamihilator.com/download** bereit, die Betaversion gibt es auf der Seite **www.spamihilator.com/eos**. Das Programm ist kleiner als anderthalb Megabyte und daher schnell übertragen.

Starten Sie das Setup mit einem Doppelklick auf die EXE-Datei des Downloads. Während der Installation können Sie auswählen, welche Komponenten eingerichtet werden sollen. Alle zusammen benötigen jedoch weniger als fünf Megabyte Platz auf der Festplatte, Sie können also getrost alle Bestandteile von Spamihilator einrichten – zumal die abwählbaren Module (Hilfe und wichtige Plugins) gerade mal ein Megabyte beanspruchen. Nur bei einer langsamen Internetverbindung sollten Sie eventuell den DCC-Filter abschalten. Er erkennt Massenmails mithilfe der Distributed-Checksum-Clearinghouse-Methode. Dabei wird für jede Nachricht eine Prüfsumme gebildet, die der Filter mit den Spameinträgen auf öffentlichen Servern vergleicht. Im Fall einer Übereinstimmung wird die Mail aussortiert. Das Verfahren ist aber nur mit einer schnellen Datenleitung sinnvoll.

Nach der Installation startet der Setup-Assistent von Spamihilator. Mit ihm konfigurieren Sie Ihr Mailprogramm für die Zusammenarbeit mit den Filtern. Dazu sollte der Mailclient geschlossen werden, das gilt auch für eventuelle Programmstarter im Systemtray der Taskleiste. Die Dialoge des Assistenten sind schnell durchlaufen; nach wenigen Klicks hat Spamihilator die Daten Ihres E-Mail-Kontos übernommen. Danach startet die Software und platziert ihr Symbol im Systemtray. Mit einem Doppelklick darauf erreichen Sie in der Voreinstellung den Spamihilator-Papierkorb, ein Klick mit der rechten Maustaste auf das Symbol öffnet das Menü des Programms. Von dort aus haben Sie Zugriff auf alle wichtigen Programmteile:

- Der „Papierkorb“ enthält die ausgefilterten Mails. Sie können sie an dieser Stelle mit einem Klick komplett löschen, sie ansehen oder einzelne wiederherstellen.
- Die „Spam-Statistik“ zeigt Ihnen, wie viele Mails Spamihilator in den letzten 30 Tagen herausgefiltert hat und wie viele Sie im Durchschnitt täglich erhalten.
- Im „Trainingsbereich“ verbessern Sie die Erkennungsquote des Programms.
- Der Dialog „Einstellungen“ dient zur Feinjustierung des Spamfilters.

KNOW-HOW

Voraussetzungen für die Spam-Abwehr

Spamihilator 0.9.9
- Windows 95, 98, Me, NT 4.0, 2000, XP, 2003 Server
- Pentium 100 MHz, 32 MByte RAM, 5 MByte freier Festplattenspeicher
- Empfohlene Mindestkonfiguration: Windows XP, Pentium 400 MHz, 128 MByte RAM, 20 MByte freier Festplattenspeicher

Thunderbird für Windows
- Windows 98, Me, NT 4.0, 2000, XP
- Pentium 233 MHz, 64 MByte RAM, 52 MByte freier Festplattenspeicher
- Empfohlene Mindestkonfiguration: Windows XP, Pentium 500 MHz, 128 MByte Arbeitsspeicher

Spamihilator: Freunde akzeptieren, Feinde ignorieren

Freund und Feind, also wichtige Nachrichten und Werbung, kann Spamihilator nicht immer auseinanderhalten. Ab und zu müssen Sie dem Programm daher auf die Sprünge helfen. Sollte versehentlich einmal eine wichtige Mail im Papierkorb des Spamfilters gelandet sein, fischen Sie sie einfach wieder heraus: Klicken Sie dazu mit der rechten Maustaste auf die Mitteilung und gehen Sie auf „Absender zu meinen Freunden hinzufügen“. Künftig werden Mails von diesem Absender nicht mehr auf Spam-Inhalte geprüft und stattdessen ohne Umwege direkt an das E-Mail-Programm weitergeleitet.

Möchten Sie dagegen Nachrichten von bestimmten Personen nicht mehr empfangen, dann wählen Sie den Kontextmenü-Eintrag „Absender permanent blockieren“. Die Adresse landet dann im Killfile, einer Liste mit Absendern, mit denen →

Sie nichts zu tun haben wollen. Sämtliche E-Mails von diesem Absender werden künftig einfach gelöscht.

Sie können deren Nachrichten aber auch gleich auf dem Posteingangs-Server löschen und damit bereits die Übertragung auf Ihren Rechner unterbinden. Dazu wechseln Sie in Spamihilator zu den „Einstellungen“ und rufen „Absender | Blockierte Absender“ auf. Schalten Sie dort die Option „Mails von blockierten Absendern nicht herunterladen“ ein.

Sollte aus Versehen die Adresse eines Freundes im Killfile gelandet sein, holen Sie sie über dasselbe Menü wieder heraus. Markieren Sie den Eintrag der E-Mail-Adresse, und klicken Sie auf „Löschen“.

Besteht in Ihrem E-Mail-Programm bereits eine Liste blockierter Adressen, so kann Spamihilator sie importieren und nutzen. Klicken Sie dazu auf die Schaltfläche „Importieren“. Das gilt selbstredend auch für Freunde: Spamihilator übernimmt auf Wunsch die Einträge im Windows-Adressbuch oder lädt mit Kommas getrennte Adressen aus einer Textdatei.

Spamihilator: Trainingslager für den Spamfilter

Den „Trainingsbereich“ erreichen Sie über das Hauptmenü. Er zeigt Ihnen die zuletzt empfangenen Nachrichten an, die Sie nun mithilfe der Schaltflächen als „Spam“ oder „Non-Spam“ markieren können. Danach klicken Sie auf „Lernen“. Spamihilator untersucht daraufhin die markierten Nachrichten und errechnet auf Basis der Inhalte für jede E-Mail die Wahrscheinlichkeit, dass es sich um Spam oder Ham (Bezeichnung für erwünschte Mails) handelt. Durch das Training entsteht eine Liste mit Wörtern, die in Ihren Spam- und Ham-Nachrichten besonders häufig vorkommen. Jedes weitere Training erweitert die Liste. Je öfter Sie den Filter trainieren, desto besser wird folglich auch die Erkennungsrate.

Schnell erledigt: Der Assistent passt den Spamihilator automatisch an das verwendete E-Mail-Programm an.

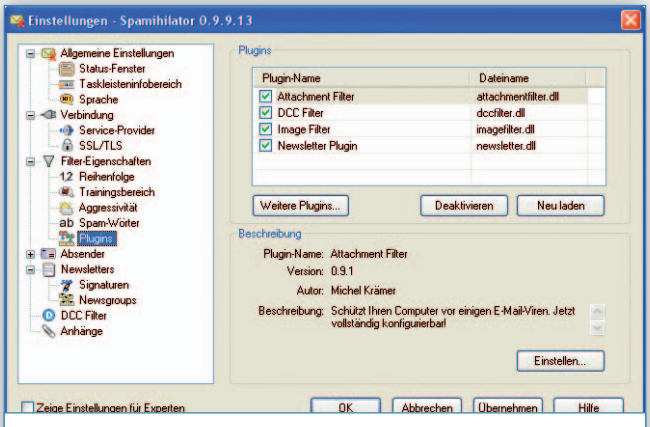
Spamihilator: Wichtige Einstellungen vornehmen

Im Fenster „Einstellungen“ finden Sie noch eine Reihe weiterer nützlicher Optionen. Unter dem Menüeintrag „Allgemeine Einstellungen“ legen Sie im Bereich „Papierkorb“ fest, wie lange Spammails gelagert werden sollen, bevor das Programm sie selbstständig löscht. Im Untermenü „Allgemeine Einstellungen | Taskleisteninfobereich“ können Sie eine Kindersicherung mit Passwort aktivieren. Eine sinnvolle Einstellung, denn anschließend ist Ihrem Nachwuchs der Zugriff auf den Papierkorb, den Trainingsbereich und die anderen Einträge im Spamihilator-Menü verwehrt – eine wirksame Maßnahme, um Kinder beispielsweise vor den Inhalten und Links pornografischer Werbemails zu schützen.

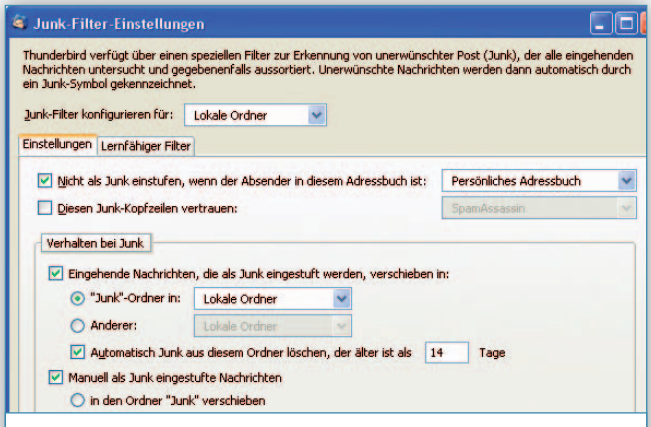
Im Menü „Filtereinstellungen“ legen Sie unter anderem fest, in welcher „Reihenfolge“ die Plugins und Filter angewendet werden sollen. Durch Verändern der Reihenfolge können Sie die Bearbeitung der Mails unter bestimmten Voraussetzungen etwas beschleunigen. Wenn Sie beispielsweise viele E-Mail-Viren erhalten, setzen Sie den „Attachment Filter“ an die erste Stelle. Dann werden die Nachrichten, die Schadprogramme enthalten, bereits im ersten Durchlauf erkannt und gelöscht, und die Arbeit für die restlichen Filter wird verringert.

In der Voreinstellung überwacht Spamihilator neu eingehende Nachrichten mit normaler „Aggressivität“. Dabei sortiert die Software bereits viele Werbemails heraus. Sie können diese Einstellung um jeweils zwei Stufen verschärfen oder lockern. Wenn Sie sich nicht mehr ärgern lassen wollen, schalten Sie beispielsweise auf „Sehr hoch“. Dann werden nur noch die E-Mails von Freunden zugestellt, also von Personen, die auf Ihrer Adressliste stehen. Der Nachteil: Sie verpassen so unter Umständen wichtige Mails bislang unbekannter Personen.

Es gibt eine ganze Reihe zusätzlicher Plugins, mit denen Sie den Funktionsumfang von Spamihilator erweitern können. Ein Klick auf die Schaltfläche „Weitere Plugins“ lädt eine Liste, in der Sie die gewünschten Addons oder Plugins einfach markieren und damit installieren können. Die besten Erweiterungen stellen wir Ihnen im Kasten „Plugins und Addons für Spamihilator“ vor.



Abwehr verstärken: Spamihilator bringt bereits vier Plugins mit. Zusätzliche Filter zur Spamabwehr installieren Sie einfach über die Schaltfläche „Weitere Plugins“.



Endlich Ruhe: Wenn Thunderbird nach etwas Training Spam weitgehend zuverlässig erkennt, sollten Sie die Junk-Einstellungen so ändern, dass der Müll automatisch entsorgt wird.

Thunderbird: Junkmail-Filter einrichten

Wenn Sie keinen Spamfilter vor das Mailprogramm schalten, sich aber wirkungsvoll vor Werbung schützen wollen, ist ein Mailprogramm mit integriertem Spamfilter wie beispielsweise Thunderbird erste Wahl. Die kostenlose Software gibt es für Windows, Linux und den Macintosh. Die aktuelle deutschsprachige Version finden Sie unter der Adresse **www.thunderbird-mail.de/thunderbird**. Die Installation ist schnell erledigt, auch der Wechsel von Outlook Express wird Ihnen leicht gemacht – denn Thunderbird importiert die vorhandenen Konten und andere Einstellungen selbsttätig, sodass Sie gleich loslegen können.

Das Programm untersucht alle eintreffenden E-Mails auf Spam. Wird es fündig, markiert es die Nachrichten mit dem Symbol eines Papierkorbs. Das Training des Spamfilters erfolgt direkt im Mailprogramm. Eine unerwünschte Nachricht, die Thunderbird nicht automatisch erkannt hat, kennzeichnen Sie mit einem Klick auf das Symbol „Junk“ als Spam. Falsche Positive – also erwünschte Mails, die der Filter irrtümlich als Spam erkannt und markiert hat – können Sie mit einem Klick auf die Schaltfläche „Kein Junk“ vor dem Löschen bewahren.

Über „Extras | Junk-Filter-Einstellungen“ legen Sie das Verhalten der Spamabwehr von Thunderbird fest. Nach ein paar Trainingseinheiten sollten Sie in diesem Fenster die Option „Eingehende Nachrichten, die als Junk eingestuft werden, verschieben in“ einschalten, um den Spam automatisch in einen gesonderten Ordner zu verschieben. Durch Aktivieren der Option „Automatisch Junk aus diesem Ordner löschen, der älter als 14 Tage ist“ können Sie den Ordner regelmäßig löschen. Wie lange Thunderbird die Nachrichten aufbewahrt, ist dabei einstellbar, sodass Ihnen genügend Zeit für gelegentliche Kontrollen bleibt.

Die Option „Manuell als Junk eingestufte Nachrichten“ sollten Sie ebenfalls einschalten. In der Voreinstellung verschiebt Thunderbird Nachrichten nach einem Klick auf das „Junk“-Symbol zunächst in den Junkordner. Da Sie die Nachricht aber bereits als Spam identifiziert haben, können Sie sie auch sofort löschen lassen.

Thomas Hümmler

KNOW-HOW

Plugins und Addons für Spamihilator

Derzeit gibt es 35 Plugins und Addons für Spamihilator, die unterschiedliche Aufgaben erfüllen. Die Tabelle zeigt eine Übersicht der Komponenten, die von Nutzern auf der Homepage des Programms mindestens mit der Note „Befriedigend“ bewertet wurden.

0190-Filter	Filtert E-Mails heraus, die eine 0190-Nummer enthalten.
A Blacklist Filter v0.9.0	Erkennt Junkmails mithilfe der öffentlichen Schwarzen Listen.
Addressee Filter	Filtert Nachrichten heraus, bei denen Ihre E-Mail-Adresse nicht im Empfänger- oder Cc-Feld steht.
Air Filter 0.1.5	Blockiert Nachrichten, die an „Almost Identical Recipients“ (fast identische Empfänger) gesendet werden.
Alphabet Soup Filter 1.0	Filtert Mails mit sinnlosen Zeichenketten heraus.
Attachment Extensions Filter v0.9.5	Blockiert Mails mit bestimmten Erweiterungen. Der Filter ist eine erweiterte Version des bereits vorinstallierten Attachment-Filters.
Bad Tag Filter 0.2.3	Filtert Mails heraus, die viele ungültige HTML-Tags oder zahlreiche Kommentare enthalten. Die Spammer nutzen diese Kommentare, um Spamfilter zu verwirren.
Charset Plugin	Filtert Mails mit bestimmten Zeichensätzen heraus.
DNSBL 0.8.0	Prüft, ob ein Absender-Server auf einer DNS-Blacklist steht.
Domain Filter	Untersucht in Mails enthaltene URLs mit heuristischen Methoden, um Domain-Namen zu ermitteln, die nur in Spammails vorkommen.
Empty Mail Filter v1.1.2	Blockiert leere E-Mails und Nachrichten mit sehr wenigen Wörtern.
Export Senders Plugin v1.0.3	Exportiert die Listen der Freunde und der blockierten Absender in eine Textdatei.
Filter Statistics v1.0.4	Erzeugt aus den Dateien spamihilator.ini und filter.log Filterstatistiken.
Hercule Filter	Prüft auf ungültigen oder schlechten HTML-Code oder Mail-Header.
HTML Links Filter v1.0.2	Blockiert HTML-Mails mit zu vielen http- oder mailto-Links.
Mystic-Signs-Filter 1.1.1	Filtert Mails heraus, die im Betreff zufällige Sonderzeichen sowie chinesische und andere Zeichen einstreuen.
No Comment! Filter v1.0.2	Sortiert Mails mit HTML-Kommentaren aus.
POP3 Notifier 0.2.0	Durchsucht das Postfach regelmäßig nach neuen Nachrichten und weist mit einer kleinen Meldung am unteren Bildschirmrand auf neue Mails hin.
RFC-Validator 1.2.0	Filtert nicht-RFC-konforme Mails aus, also Nachrichten ohne Absender oder mit einem zu langen Betreff.
Scripts Filter v1.0.4	Filtert Mails mit eingebetteten Skripten heraus.
Server-Tester 0.5.1	Sortiert Mails mit gefälschten Absenderangaben aus.
Signature Filter 0.5.2	Umgeht alle anderen Filter, sobald ein Teil der Signatur des Empfängers im Text der Mail enthalten ist.
Spami2Service	Richtet Spamihilator als Windows-Dienst ein.
Spamihilator E-Mail Report 0.8.1 BETA (Dec, 2004)	Verfasst täglich eine E-Mail mit einem Bericht über den erhaltenen Spam, sodass man fälschlich als Spam identifizierte Nachrichten schnell erkennen und den Absender direkt aus dem Mailcient zur Freund- oder Feindliste hinzufügen kann.
Spamihilator-Forum-Reader-Plug-In 1.5.0	Wenn das Spamihilator-Forum die Benutzer über ein neues Posting informiert, öffnet dieser Filter den Beitrag automatisch im Browser. Das Plugin sollte möglichst an erster Stelle der Filterliste stehen.
SpamiOL – Add-In für Microsoft Outlook	Fügt zwei Schaltflächen in die Outlook-Symbolleiste ein, über die man Freunde und unerwünschte Personen zu den Spamihilator-Listen hinzufügen kann.
Strange-Country-Filter v 1.1.0	Filtert Mails aus Spam-verdächtigen Ländern anhand des Mail-Headers und der entsprechenden Einträge heraus.
Substring-Filter v 1.5.0	Sortiert E-Mails aus, die bestimmte Zeichenfolgen enthalten.
URL-Filter v 1.8.0	Filtert Mails mit URLs, die auf Spam-beworbene Webseiten verweisen.
Virtual POP3-Server 1.0 Beta 2	Ein virtueller POP3-Server für Plugin-Autoren, das den aufwändigen Testmail-Verkehr über den echten POP3-Server ersetzt.
Whitestring-Filter v 1.5.0	Identifiziert Ham-Mails anhand bestimmter Zeichenfolgen. Sinnvolle Zeichenfolgen sind beispielsweise Teile der Signatur. Indem er die Signaturen von abonnierten Newslettern und Mailing-Listen eingibt, kann der Benutzer diese Massenmails automatisch durch die Filter passieren lassen.
Wordlist-Extractor v 1.0.0	Speichert die Liste des Wortfilters in einer Textdatei. Auf diese Weise lassen sich die Einträge einfacher überprüfen.
X-Header-Filter 1.5.5	Filtert Mails mit bestimmten X-Headern heraus.

WEBBROWSER ABSICHERN

Schotten dicht bei Internet Explorer, Firefox & Opera

Die drei am weitesten verbreiteten Internetbrowser bieten in ihren aktuellen Versionen eine Vielzahl von Sicherheitsfeatures und Plugins. CHIP zeigt Ihnen, wo Sie Hand anlegen sollten, um im Internet möglichst sicher unterwegs zu sein.

Die Webbrowser sind das Hauptangriffsziel der Hacker. Um sie abzusichern, sollten Sie zuerst einige allgemeine Regeln befolgen.

Prüfen Sie als Erstes, ob Ihr Browser noch auf dem aktuellen Stand der Dinge ist. Den Internet Explorer etwa aktualisieren Sie über das Windows Update. Die Einstellungen dazu finden Sie in der Systemsteuerung unter „Automatische Updates“. Außerdem gibt es unter „Extras | Einstellungen“ auf der Registerkarte „Erweitert“ den Punkt „Automatische Überprüfung auf Aktualisierungen von Internet Explorer“.

Bei Firefox ist die Update-Funktion ein wenig versteckt in der zweiten Ebene der Einstellungen unterhalb des Menüpunkts „Erweitert“ zu finden. Auf der Registerkarte „Update“ legen Sie fest, ob Firefox nur für den Browser oder auch für die installierten Erweiterungen, Themes und Suchmaschinen nach neueren Versionen suchen soll.

Sind die Updates identifiziert, haben Sie die Wahl, ob Firefox sie sofort installieren oder lieber erst nachfragen soll, welche Aktion Sie bevorzugen.

Bei Opera ist es nicht ganz so komfortabel. Dort kommen Sie unter dem Menüpunkt „Hilfe | Auf Updates überpüfen“ zu den gewünschten Aktualisierungen. Eine Funktion zur automatisierten Suche und Installation ist nicht vorgesehen.

Alle Browser bieten das Speichern von Passwörtern und Benutzernamen auf der lokalen Festplatte an. Das ist zwar hilfreich, aber gleichzeitig ein Sicherheitsrisiko. Falls Sie bereits den Überblick über Ihre Passwörter verloren haben, sollten Sie lieber einen Passwort-Manager einsetzen. Diese Tools bieten meist eine bessere Verschlüsselung und integrieren Benutzer und Passwort häufig auch automatisch in die Webseiten. Interessante Vertreter aus dieser Kategorie sind beispielsweise Password Safe (**http://passwordsafe.sourceforge.net/**) oder KeePass (**http://keepass.sourceforge.net/**).

AUF EINEN BLICK

Webbrowser sicher machen

Internet Explorer 6 & 7 abschotten 61

Sicher surfen mit Firefox 1.5 & 2.0 und Opera 9 61

Alle Tools auf CD

Password Safe: Speichert Passwörter sicher in einer Datenbank ◎ Security

NoScript: Stoppt gefährliche JavaScripts im Firefox-Browser ◎ Internet

Illustration: S. Schönberger

Internet Explorer 6 und 7

Einfluss auf die Sicherheit des Internet Explorer nehmen Sie im Menü „Extras | Einstellungen“ auf den beiden Registerkarten „Sicherheit“ und „Datenschutz“. Darüber hinaus gibt es noch einige Werte, die Sie auf der Karte „Erweitert“ in der Rubrik „Sicherheit“ setzen können.

Das Sicherheitskonzept des Internet Explorer basiert auf den Sicherheitszonen „Internet“ und „Intranet“, für die Sie unterschiedliche Rechte vergeben können. Außerdem haben Sie die Möglichkeit, einzelne Websites explizit als „vertrauenswürdig“ oder „eingeschränkt vertrauenswürdig“ zu klassifizieren.

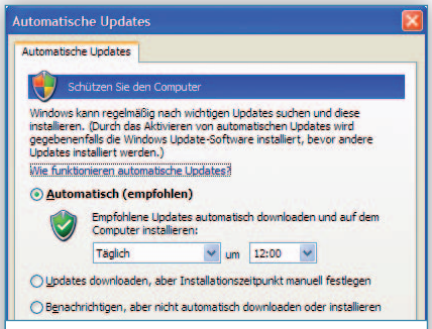
Jeder dieser Bereiche hat seine eigene Sicherheitsstufe, die sich per Schieberegler zwischen „sehr niedrig“ und „hoch“ klassifizieren oder individuell konfigurieren lässt. Für das „Internet“ sollten Sie mindestens die Stufe „mittel“ wählen, die vor den wesentlichen Gefahren warnt. In der Sicherheitsstufe „hoch“ sind alle kritischen Aktionen entweder gesperrt, oder Sie werden vor der Ausführung noch einmal explizit gefragt.

Können Sie mit den vordefinierten Sicherheitsstufen nichts anfangen, müssen Sie sie manuell anpassen. Wählen Sie dazu am besten die Stufe als Ausgangspunkt, die Ihren Anforderungen am nächsten kommt, und wählen Sie anschließend „Stufe anpassen“. Im folgenden Fenster ändern Sie die Werte nach Ihren Vorstellungen.

Sollten die Sicherheitseinstellungen für spezielle Webseiten immer noch nicht ideal sein, nutzen Sie ergänzend die beiden Zonen für vertrauenswürdige und vertrauensunwürdige Sites. An dieser Stelle geben Sie ganz bestimmte Websites an. Das ist etwa dann sinnvoll, wenn Sie Ihre Einstellungen sehr restriktiv gesetzt haben, Ihre favorisierte Website aber ActiveX-Elemente erfordert, die von der hohen Sicherheitsstufe blockiert würden.

Den „Datenschutz“ regeln

Die Registerkarte „Datenschutz“ umfasst hauptsächlich Einstellungen zu Cookies und Popup-Fenstern. Bei den Cookies reicht die Bandbreite von „Alle Cookies annehmen“ bis „Alle Cookies sperren“. Einige Zwischenstufen lassen Cookies –



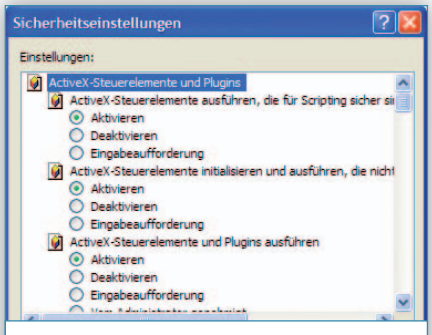
Internet Explorer: Auch für den Internet Explorer sollten Sie das automatische Windows Update mitnutzen.

mehr oder weniger großzügig – zu. Daneben bietet der Internet Explorer eine Cookie-Definition auf Website-Ebene an, über die Sie für bestimmte Websites die Speicherung von Cookies generell zulassen oder ablehnen.

Auch in den erweiterten Einstellungen beeinflussen Sie die verschiedenen Sicherheitsstufen. An dieser Stelle schalten Sie zwischen manueller und automatischer Verarbeitung von Cookies um.

Beim Internet Explorer 6 kam erstmals der automatische Popup Blocker hinzu – er lässt sich nicht nur an- und ausschalten, sondern auch detailliert konfigurieren. In den erweiterten Einstellungen geben Sie die Filterungsstufe an sowie die Art der Benachrichtigung beim Blocken eines Popups. Auch an dieser Stelle gibt es eine Ausnahmeregelung für Seiten, deren Popups Sie immer sehen möchten.

Eine Reihe weiterer Einstellungen, die besonders auf den Aspekt „Datensicherheit“ ausgerichtet sind, setzen Sie am besten mit dem Tool XP-AntiSpy. Damit deaktivieren Sie nicht nur JavaScript, sondern veranlassen auch das Löschen des Cache nach dem Beenden des Internet Explorer. So hinterlassen Sie keine Surfspuren auf Ihrem PC.



Internet Explorer: Passen die definierten Sicherheitsstufen nicht zu Ihren Bedürfnissen, können Sie manuell anpassen.

Außerdem sollten Sie auf der Registerkarte „Allgemein“ die Anzahl der Speichertage für den Verlauf auf „0“ setzen, damit die von Ihnen besuchten Websites nicht dokumentiert werden.

Was der IE 7 Neues bringt

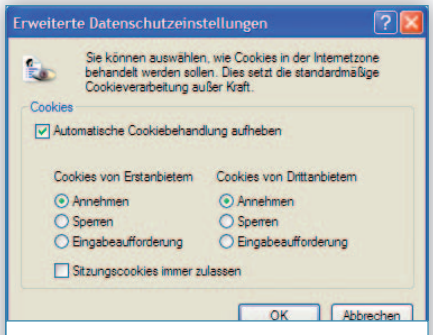
Die wichtigste neue Sicherheitsfunktion beim Internet Explorer 7 ist der Phishing-Filter. Er untersucht die angesteuerte Website, ob es sich dabei um das Original oder eine umgeleitete Fälschung handelt. Der Phishing-Filter hat drei Einstellmöglichkeiten: „Keine Überprüfung“, „Automatische Überprüfung aktivieren“ und „Überprüfung deaktivieren“. Wenn Sie den Phishing-Filter einsetzen, wird jede URL an Microsoft gesendet und dort mithilfe einer Datenbank überprüft. Ist die Seite dort registriert, erhalten Sie eine entsprechende Warnung. Es gibt aber auch die Option, einzelne Seiten manuell zu überprüfen und gegebenenfalls an Microsoft zu melden.

Besitzern des Internet Explorer 6 bietet Microsoft den Phishing-Filter über die MSN Toolbar an. Er arbeitet genauso wie der des Internet Explorer 7 (**http://addins.msn.com/phishingfilter/**).

Gegenüber der Vorgängerversion hat sich auch die Handhabung der Sicherheitsstufen geändert. Die Regler für die Einstellungen sind verschwunden, das Prinzip ist allerdings gleich geblieben.

Firefox 1.5 und 2.0

Beim Open-Source-Konkurrenten Firefox ist inzwischen die Version 2.0 am Start. An den wesentlichen Sicherheitseinstellungen hat sich nicht viel geändert. Wie beim Internet Explorer 7 gibt es nun einen Phishing-Filter im Browser. →



Internet Explorer: Für die Annahme von Cookies lassen sich bei manueller Bearbeitung individuelle Regeln definieren.

Die grundlegenden Sicherheitseinstellungen finden Sie unter „Extras | Einstellungen“ im Bereich „Sicherheit“ auf sechs Registerkarten. In der Registerkarte „Chronik“ etwa legen Sie fest, wie lange die Links der besuchten Seiten gespeichert werden sollen. Die Standardeinstellung ist neun Tage.

Firefox unterscheidet zwischen gespeicherten Formulardaten im Allgemeinen und Passwörtern im Speziellen. Auf der Registerkarte „Gespeicherte Formulardaten“ legen Sie die generelle Speicherung fest – an dieser Stelle können Sie diese auch per Knopfdruck löschen.

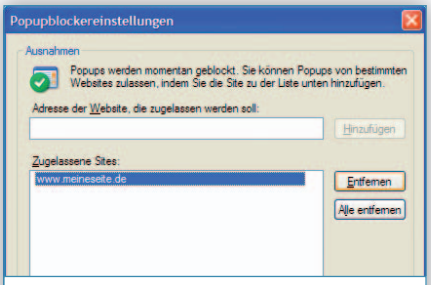
Zum Schutz Ihrer Passwörter bietet Firefox die Kennwortsicherung durch ein Master-Passwort an. Das sollten Sie auf jeden Fall aktivieren, da die Passwörter ansonsten im Klartext sichtbar sind. Wählen Sie das Master-Passwort mit Bedacht – denn wenn Sie es vergessen, verlieren Sie auch den Zugriff auf Ihre sonstigen gespeicherten Passwörter.

Firefox verfügt über einen Download-Manager, in dem auch der Verlauf der Downloads gespeichert ist. Auf der entsprechenden Registerkarte haben Sie die Auswahl, ob und wann diese Dokumentation gelöscht wird.

Mit Cookies & Cache umgehen

Dem Umgang mit Cookies ist eine eigene Registerkarte gewidmet. Neben dem prinzipiellen Aktivieren der Speicherung bietet Firefox eine erweiterte Konfiguration an. Parallel zum generellen Freifahrtschein definieren Sie über die Schaltfläche „Ausnahmen“ die Websites, die keine Cookies auf Ihrem PC ablegen dürfen.

Haben Sie ein Cookie schon einmal von Ihrem Rechner gelöscht und die Funktion „…falls von der Website gesetzte Cookies nicht schon einmal entfernt wurden“ ist aktiviert, wird eine erneute Speicherung unterbunden.



Internet Explorer: Beim Popup-Filter lassen sich für Websites, bei denen die Fenster zugelassen sind, Ausnahmen definieren.

Gerade Webseiten mit integrierten Werbebannern legen in der Regel mehrere Cookies ab – seitenspezifische und auch die Cookies der Werbekunden. Die Webseite funktioniert in den allermeisten Fällen auch ohne die Werbe-Cookies – Sie können die zusätzlichen Cookies folglich ohne Weiteres mit der Option „Nur von der ursprünglichen Website“ deaktivieren.

Viele Websites speichern Ihre Anmeldedaten oder den letzten Warenkorb als Cookie. Je nach Lebenszeit des Cookies sind diese Informationen auch beim nächsten Besuch der Seite noch vorhanden – es sei denn, Sie verkürzen die Lebenszeit dieser Informationen unter „Cookies behalten“ individuell.

Firefox bietet mit dem Befehl „Cookies anzeigen“ eine integrierte Verwaltungsfunktion an. An dieser Stelle sehen Sie sämtliche gespeicherten Cookies, erfahren, woher sie kommen und was genau abgelegt ist. Innerhalb des Fensters können Sie zwischen dem Löschen einzelner und dem Löschen aller Cookies wählen.

Auf der letzten Registerkarte in diesem Bereich – „Cache“ – legen Sie die Größe des Cachespeichers fest und können ihn auch manuell löschen.

Privatsphäre schützen

Eine hilfreiche Funktion zum generellen Löschen ist „Private Daten löschen“. Über die Schaltfläche „Einstellungen“ gelangen Sie zu einer Übersicht, in der Sie festlegen, welche Daten Firefox beim Schließen löschen soll. Dies geschieht dann entweder automatisch oder nach einer Nachfrage durch den Browser.

Zusätzliche Einstellungen

Weitere Sicherheitseinstellungen finden Sie im Menüpunkt „Inhalt“. Auch Firefox bietet von Haus aus einen Popup-Blocker, den Sie nach dem Aktivieren mit einer Whitelist für zugelassene Websites ergänzen können.

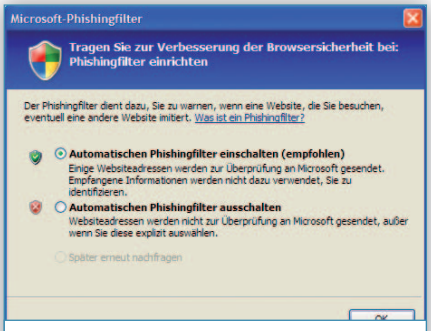
Auch Einstellungen zu Java und JavaScript sind dort zu finden. Bei JavaScript haben Sie über die „Erweiterten Einstellungen“ noch zusätzliche Konfigurationsoptionen zur Auswahl.

Wichtig in Sachen Sicherheit ist die Option „Nur freigegebenen Websites das Installieren von Ergänzungen ermöglichen“, da Firefox einen großen Teil seiner Beliebtheit der Vielzahl verfügbarer Plugins verdankt. Mit dieser Option stellen Sie sicher, dass autorisierte Websites Erweiterungen installieren dürfen und sich somit kein Programm durch die Hintertür auf Ihren Rechner einschleichen kann.

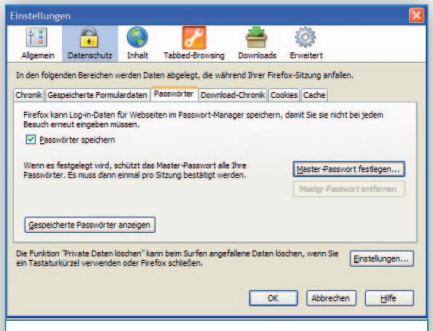
Was Firefox 2.0 Neues bringt

Sämtliche neuen Features von Firefox 2.0 sind unter der Adresse **http://en-us.www.mozilla.com/en-US/firefox/2.0/releasenotes/** aufgeführt.

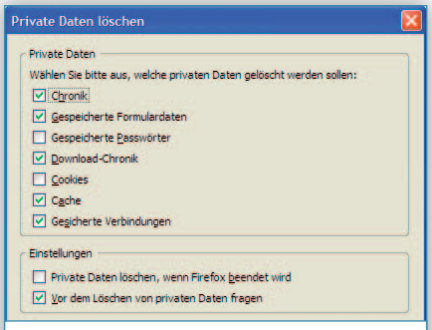
Im Bereich Sicherheit ist jedoch lediglich der Schutz vor Phishing besonders hervorzuheben. Diese Funktion ist standardmäßig aktiviert und überprüft einen Link entweder anhand einer lokal gespeicherten oder globalen Liste. Beide Listen bietet derzeit nur Google an – die globale Liste überprüft Ihre angesteuerten Seiten sofort. Die lokale Liste wird alle 30 bis 60 Minuten auf der Basis von Googles Datenbeständen aktualisiert, bei der Überprüfung müssen Sie jedoch keine direkte Anfrage stellen. Die Optionen zum Phi-



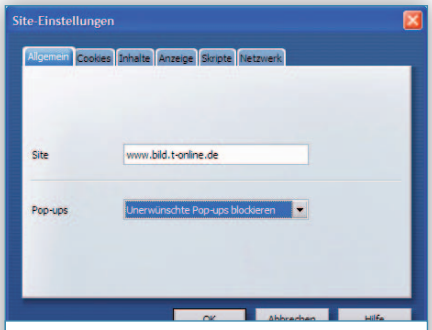
Internet Explorer: Ist der Phishing-Filter des Internet Explorer 7 aktiviert, untersucht Microsoft automatisch jede Website, bevor sie geladen wird.



Firefox: Wenn Sie Benutzernamen und Passwort über Firefox speichern, sollten Sie sie mit einem Master-Passwort vor dem Ausspähen schützen.



Firefox: Beim Beenden des Open-Source-Browsers können Sie alle hinterlassenen Surfspuren löschen.



Opera: Für jede Website lassen sich bei Opera Werte und Eigenschaften festlegen, etwa das Blockieren von Popups.

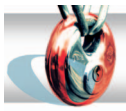
shing-Filter finden Sie unter „Extras | Einstellungen | Sicherheit".

Sicherheits-Addons einrichten

Neben den Funktionen im Standardumfang gibt es einige Erweiterungen, die den Browser noch sicherer machen:

- NoScript (**https://addons.mozilla.org/firefox/722/**) verhindert das Ausführen von JavaScript.
- Adblock (**https://addons.mozilla.org/firefox/1865/**) lässt Sie Werbung individuell ausblenden – die rechte Maustaste genügt.
- CookieSafe (**https://addons.mozilla.org/firefox/2497/**) hilft Ihnen bei der Kontrolle der Cookies auf Ihrem PC.
- Flashblock (**https://addons.mozilla.org/firefox/433/**) sperrt das automatische Anzeigen von Flash-Elementen.

Alle Plugins gibt es sowohl für Firefox 1.5 als auch für die aktuelle Version 2.0. Noch mehr Erweiterungen finden Sie auf der Mozilla-Webseite in der Rubrik „Privacy and Security" (**http://addons.mozilla.org/search.php?cat=12&app=firefox&appfilter=firefox&type=E**).



Opera 9

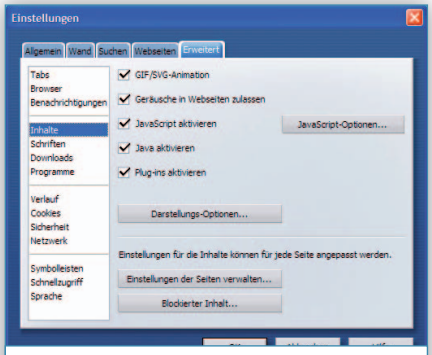
Auch von Opera gibt es inzwischen eine neue Ausgabe – die deutschsprachige Version 9. Damit können Sie etwa selbst bestimmen, welche Werbeinhalte Sie noch sehen möchten. Die Entwickler von Opera haben die Funktion bereits ins Kontextmenü der rechten Maustaste integriert. Damit lassen sich unerwünschte Werbebotschaften einfach per Mausklick entfernen. Opera merkt sich die von Ihnen vorgenommenen Einstellungen und wendet sie beim nächsten Besuch der Webseite an.

Die Möglichkeiten des Content-Blockers beschränken sich momentan noch darauf, Bilder und Flash-Animationen verschwinden zu lassen. Integrierte Google-Anzeigen kommen bei Opera derzeit noch ungeschoren davon.

Ein weiterer Schwerpunkt bei der Entwicklung der neuen Version war das Blockieren von Werbebotschaften über Pop-up-Fenster. Die Einstellungen lassen sich – ebenso wie das Blocken von Content – individuell für jede Website setzen. Klicken Sie dazu nach dem Aufruf einer URL mit der rechten Maustaste in die Seite und wählen Sie den Menüpunkt „Seitenspezifische Einstellungen". An dieser Stelle finden Sie auf der ersten Registerkarte „Allgemein" die unterschiedlichen Optionen für Popups. Sie reichen von „Alle Pop-Ups öffnen" bis zu „Alle Pop-Ups blocken".

Opera sicher machen

Das Auswahlmenü erlaubt über sechs Registerkarten das Aktivieren weiterer seitenspezifischer Sicherheitseinstellungen. Im Menü „Cookies" legen Sie fest, wie sich Opera beim Empfang von Cookies verhalten soll. Sie können veranlassen,



Opera: Die meisten Sicherheitseinstellungen sind noch einmal auf der Registerkarte „Erweitert" zusammengefasst.

dass der Browser Cookies generell ablehnt, immer akzeptiert oder nur von besuchten Webseiten speichert. Wenn Sie es den Cookie-Absendern schwerer machen wollen, können Sie die Cookies beim Beenden von Opera löschen lassen. Im unteren Fenster sehen Sie, welche Cookies gerade auf Ihrem PC gespeichert sind.

Im Bereich „Inhalte" finden Sie ebenfalls einige Sicherheitsoptionen. Dort bestimmen Sie, ob Java aktiviert wird und ob sich Plugins wie Flash-Anwendungen starten lassen.

Für die Regeln zum Ausführen von Skripten gibt es eine eigene Registerkarte. An dieser Stelle lässt sich JavaScript generell deaktivieren oder in der Funktionalität für bestimmte Fälle einschränken.

Zwei weitere wichtige Sicherheitsoptionen können Sie auf der Registerkarte „Netzwerk" aktivieren. An dieser Stelle ist es möglich, die Übertragung Ihrer IP-Adresse sowie die automatische Weiterleitung auf eine andere Website zu unterbinden.

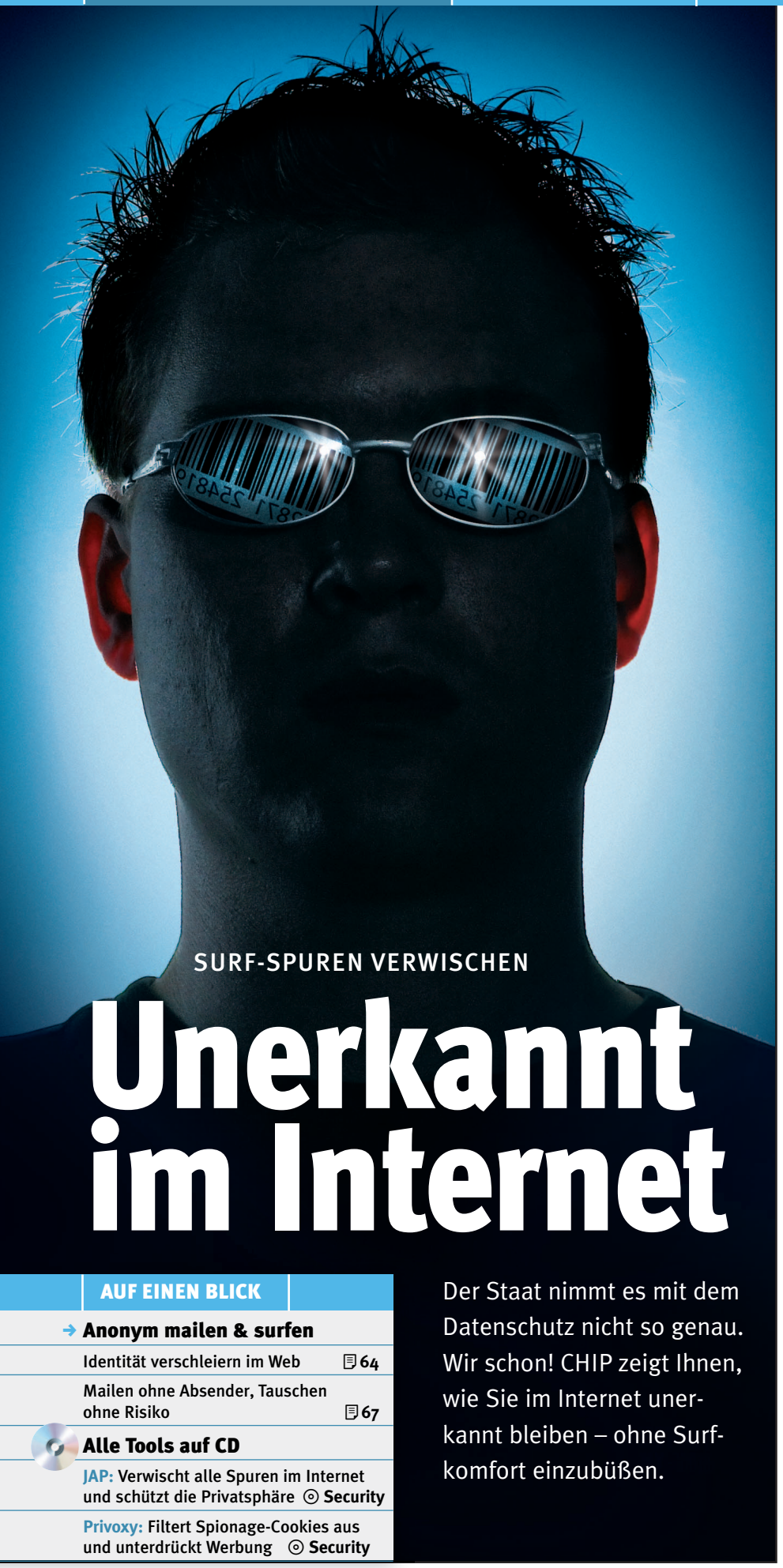
Globale Einstellungen, die für alle Webseiten gültig sind, lassen sich über das Menü „Extras | Einstellungen" definieren. Die allgemeinen Werte bestimmen das Verhalten von Opera 9 etwa bei Popups über die Startseite bis hin zur Sprachsteuerung des Browsers. Die für die Datensicherheit und den Datenschutz wichtigen Werte sind in den Menüpunkten „Verlauf", „Cookies", „Sicherheit", „Inhalte" und „Netzwerk" angeordnet und auf der Registerkarte „Erweitert" zu finden.

Diese Einstellungen entsprechen im Wesentlichen den Werten, die Sie bereits aus den eben erwähnten seitenabhängigen Menüs kennen. Die dort getroffenen Festlegungen gelten für alle Webseiten außer für die mit speziellen Einstellungen.

Einige seitenübergreifende Funktionen sind nur an dieser Stelle zu finden. Auf der Registerkarte „Wand" haben Sie die Wahl, ob Opera Passwörter speichern soll oder nicht, auf der Karte „Erweitert" können Sie unter „Inhalte" alle seitenspezifischen Einstellungen direkt aufrufen, sie verändern oder auch löschen.

Die Registerkarte „Verlauf" verwaltet den Cache und die besuchten Seiten. Wenn Sie alle Surfspuren nach dem Schließen des Browsers beseitigen möchten, setzen Sie die Zahl der zu speichernden Adressen auf „0" und lassen Opera den Cache leeren.

Andreas Hitzig



SURF-SPUREN VERWISCHEN

Unerkannt im Internet

AUF EINEN BLICK

Der Staat nimmt es mit dem Datenschutz nicht so genau. Wir schon! CHIP zeigt Ihnen, wie Sie im Internet unerkannt bleiben – ohne Surfkomfort einzubüßen.

Bundeskanzlerin Angela Merkel ist eine moderne Frau. Sie wendet sich sogar regelmäßig per Video-Podcast (**www.bundeskanzlerin.de**) an ihr Volk. Zuletzt regte Frau Bundeskanzlerin darin noch mehr Überwachung der Internetnutzung an. Über Vorratsdatenspeicherung, Anonymisierungs-Verbot und Identifizierungspflicht für Mailkonten denkt Frau Merkel derzeit nach – alles im Dienste der Sicherheit.

Doch der einzelne Internetnutzer büßt dabei sogar Sicherheit ein. Werden die Pläne umgesetzt, rollen noch mehr Werbung und Spam auf uns zu – und damit mehr Gefahr durch Betrügereien. Dabei räumt uns das Teledienstedatenschutzgesetz das Recht ein, anonym oder unter Pseudonym zu surfen. Wenn es also Provider und Behörden mit dem Datenschutz nicht so genau nehmen, müssen Sie Ihre Identität im Web eben selbst schützen. CHIP zeigt Ihnen, wie das geht.

INTERNET

Cookie & Co: Identität wirksam verschleiern

Beim Surfen bekommen Sie laufend Etiketten mit Ihrer Identität aufgeklebt. Das kann technisch notwendig sein – wie bei der IP-Adresse. Cookies oder Referrer-Einträge dagegen zeugen von blanker Neugier der Website-Betreiber. Sehen Sie also zu, dass Sie diese verräterischen Etiketten loswerden.

COOKIES: Abschalten und trotzdem bequem surfen – auch mit dem Internet Explorer 7

Dank Cookies wissen Webseiten-Betreiber, wer Sie sind und wofür Sie sich bei Ihren letzten Besuchen interessiert haben. Ärgerlich: Die großzügigen Grundeinstellungen aller großen Webbrowser erlauben das ungefragte Ablegen der Datenpäckchen. Unterbinden Sie diese unaufgeforderte Paketzustellung.

Internet Explorer: Fortschrittlich zeigt sich das Cookie-Management ausgerechnet beim viel gescholtenen Internet Explorer. Microsofts Browser hat auch in der neuen Version 7 die Plattform P3P integriert, die im Hintergrund das Einhalten von Datenschutzregeln überwacht – und Cookies zulässt oder abweist.

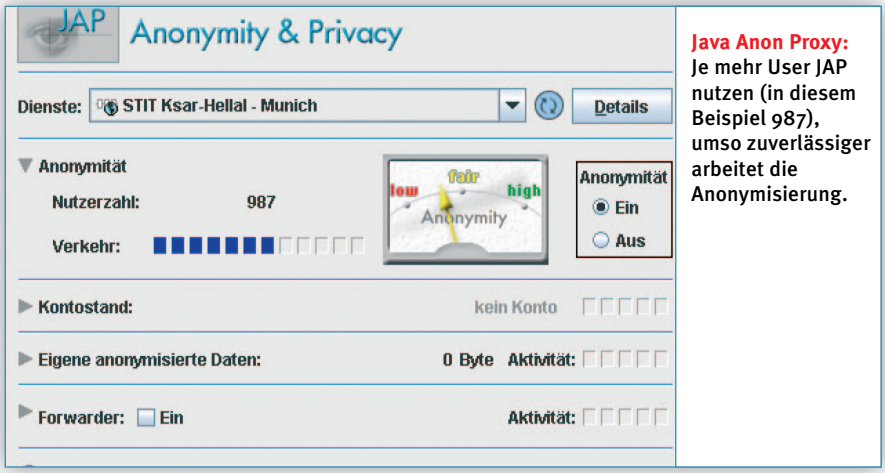
Das funktioniert so: Die Platform for Privacy Preferences ist eine durch das WWW-Consortium standardisierte Platt-

Foto: S. Butschek; Illustration: H. Fuchsloch

form zum Austausch von Datenschutzinformationen. Jeder Webseiten-Betreiber, der sich an P3P beteiligt, hat auf seinem Server eine Datenschutzvereinbarung liegen, die der in den Internet Explorer integrierte P3P-Client ausliest und mit den von Ihnen gesetzten Sicherheitsansprüchen vergleicht. Über „Extras | Internetoptionen | Datenschutz“ legen Sie Ihren individuellen Schutzlevel fest. Unsere Empfehlung: Stellen Sie den standardmäßig auf „Mittel“ gesetzten Regler auf „Hoch“. Die P3P-Datenschutz-Ansprüche können Sie übrigens unter **www.w3.org/p3p** nachlesen.

Wollen Sie sich nicht auf die Microsoft-Regeln verlassen, passen Sie sie an. Das Schreiben einer persönlichen Datenschutzregel ist aber nicht gerade einfach. Microsoft hat auf seinem Entwicklerportal MSDN (**www.msdn.microsoft.com**) eine ausführliche englischsprachige Anleitung veröffentlicht. Suchen Sie auf dem Portal nach „How to create a customized privacy import file“ (Suchoption „alle Sprachen“ aktivieren!).

Opera: Rufen Sie „Extras | Einstellungen“ auf, und klicken Sie in der Registerkarte „Erweitert“ auf „Cookies“. Mit der Option „Nur Cookies der besuchten Seite annehmen“ sperren Sie alle Cookies von Werbe-servern aus. Haben Sie grundsätzlich etwas gegen die Datenablagerungen, wählen Sie „Niemals Cookies annehmen“.



Java Anon Proxy: Je mehr User JAP nutzen (in diesem Beispiel 987), umso zuverlässiger arbeitet die Anonymisierung.

Der Nachteil dieses Generalausschlusses: In Foren müssen Sie sich ständig neu einloggen. Und auf bestimmte Seiten kommen Sie überhaupt nicht – das Einloggen auf Ebay etwa funktioniert nicht mehr. Um das zu verhindern, geben Sie über „Cookies verwalten“ einzelnen Seiten die Erlaubnis, Cookies abzulegen. Die Freigabe funktionierte in unseren Tests allerdings nicht zuverlässig – das Ebay-Login gelang trotz Erlaubnis nicht. Schalten Sie besser die Cookie-Verweigerung bei Bedarf temporär ab. Dazu drücken Sie die Taste [F12] und setzen ein Häkchen bei „Cookies zulassen“. Aber Vorsicht: Nicht vergessen, beim Weitersurfen die Sperre wieder einzuschalten!

Firefox: Werbe-Cookies lassen sich beim beliebten Open-Source-Browser nicht separat aussperren. Sie haben nur die Wahl zwischen ganz oder gar nicht: Klicken Sie unter „Extras | Einstellungen“ auf „Datenschutz“ und entfernen Sie das Häkchen bei „Cookies akzeptieren“, um alle abzulehnen. Die Adressen der Seiten, von denen Sie Cookies akzeptieren, geben Sie über „Ausnahmen“ ein. Alternative: das Cookie-Management mit der Erweiterung „Remove Cookie(s) for Site“. Installieren Sie das Addon, klicken Sie mit der rechten Maustaste in die Webseite und wählen Sie „Remove Cookie(s) for Site“. Der Klick löscht alle Cookies, die die aufgerufene Webseite abgelegt hat.

REFERRER: Geschwätzig, aber unnötig – so bringen Sie ihn zum Verstummen

In den Referrer schreibt Ihr Webbrowser Informationen über das verwendete Be- →

BLITZ-WORKSHOP

Anonym surfen mit ArchiCrypt Stealth

Die Software von der Heft-CD verschleiert Ihre Identität mit anonymisierenden Proxies, verwaltet Cookies und führt Webserver in die Irre.

1 Über „Aktionen“ stellen Sie unter „Anonymität“ das Intervall zum Wechseln der Proxy-Server ein. Je häufiger, desto perfekter funktioniert die Anonymisierung – allerdings auf Kosten der Surfgeschwindigkeit. Ein Kompromiss ist ein Wert zwischen 20 und 30 Sekunden.

2 Klicken Sie auf „Identität“, um den Inhalt des Referrers zu manipulieren. Aktivieren Sie „Herkunft verschleiern“, gaukelt ArchiCrypt Stealth jedem Zielserver vor, eine Seitenanfrage komme beispielsweise von Google – obwohl sie von Ihnen stammt.

3 ArchiCrypt blockt bekannte Spyware-Komponenten. Sie können diesen Schutz ausweiten: Klicken Sie unter „Spyware“ die Option „Alle ActiveX-Komponenten filtern“ an. Damit SIe die Funktion nutzen können, muss auf der Hauptseite der Datenfilter aktiviert sein.

KNOW-HOW

Anonym zu bleiben ist Ihr gutes Recht

Die Politik betrachtet Datenschutz eher als Deckmantel für Kriminelle. CHIP sagt Ihnen, welche Rechte Sie haben – und wann Ihr Recht auf Datenschutz verwirkt ist.

Provider muss Nutzerdaten löschen: Das Speichern von Nutzerdaten ist in Deutschland nur zu Abrechnungszwecken erlaubt. Surfen Sie mit einem Pauschaltarif (Flatrate), ist eine Datenerhebung also nicht nötig. Ein Nutzer von T-Online bekam diesbezüglich vor dem Landgericht Darmstadt recht. Der Provider muss nun die Nutzerdaten des Klägers löschen. Allerdings ist das kein Grundsatzurteil – es gilt nur für den verhandelten Fall. Wer die Datenspeicher-Praxis nicht hinnehmen will, kann sich wehren: Was Sie unternehmen sollten, ist auf der Webseite **www.daten-speicherung.de** detailliert beschrieben – inklusive vorformulierter Anschreiben. Eine Musterklage finden Sie außerdem auf der Heft-CD.

Wo das Recht auf Anonymität aufhört: Immer wieder geraten Internetnutzer, die Anonymisierungsdienste missbrauchen, in die Schlagzeilen. So wurden im vergangenen Jahr in Deutschland aufgestellte TOR-Server von der Staatsanwaltschaft konfisziert, weil über sie Webseiten mit Kinderpornographie angesurft wurden. Wikipedia sperrte TOR-Nutzer aus, weil sie Artikel manipuliert hatten. Als Anwender von JAP oder TOR sollte man sich also nicht in Sicherheit wiegen: Auch diese Dienste verfügen über Logfiles, die den Traffic protokollieren. Und die händigen sie dem Staatsanwalt völlig zu Recht aus, wenn die User den Anonymisierungsservice für illegale Zwecke missbrauchen.

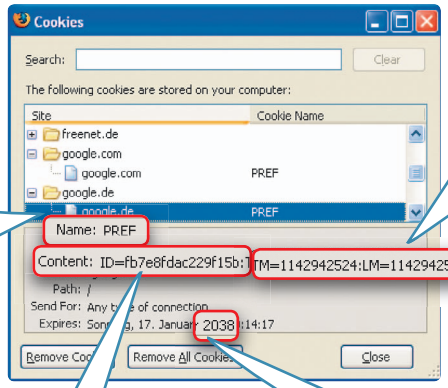
Juristen-Rat: Das für Ihren Provider zuständige Amtsgericht finden Sie auf **www.daten-speicherung.de.**

triebssystem, unterstützte Anwendungen (ActiveX, Java etc.) und verrät darüber hinaus, welche Webseite Sie vorher besucht haben. Bordmittel zum Ausschalten des Referrers bringt lediglich Opera mit: Öffnen Sie dazu mit der Taste [F12] die Schnelleinstellungen, und entfernen Sie das Häkchen bei „Herkunft (Referrer) übertragen". Um dem Referrer beim Surfen mit anderen Browsern das Plappern auszutreiben, brauchen Sie eines der zusätzlichen Tools, die wir im nächsten Abschnitt vorstellen – die erledigen das automatisch.

KNOW-HOW

Was Cookies über Sie verraten

Entdeckt: Browser wie Firefox zeigen an, welche Cookies eine Website auf Ihrem PC gespeichert hat. Pro Domain können das bis zu zwanzig sein.



Nutzerprofil: Der Cookie-Inhalt – bis zu 4 KByte groß und zumeist verschlüsselt – bleibt dem Website-Betreiber überlassen. Oft sind das ID-Nummern, die zu den Nutzerprofilen auf den Firmenservern verlinken.

User-ID: Diese Kenn-Nummer macht Sie bei jedem Besuch der Website identifizierbar.

Gültigkeitsdatum: An dieser Stelle steht, wie lange Ihr Profil gespeichert bleibt – bei Google bis zum 17. Januar 2038!

IP-ADRESSE: Technisch nötig, aber per Verschleierungstaktik manipulierbar

Nur anhand der IP-Adresse kann Ihr PC mit anderen Rechnern im Web kommunizieren – also Mails verschicken oder Webseiten aufrufen. Weil Internetservice-Provider in Logfiles protokollieren, welche IP-Adresse welchem Nutzer zu welcher Zeit zugewiesen wurde, lässt sich über drei Monate hinweg genau nachvollziehen, auf welchen Webseiten Sie sich bewegt haben. In vielen Fällen handeln die Provider mit dieser Praxis nicht legal (siehe Kasten auf 67). Also können Sie sich guten Gewissens selbst um Ihren Datenschutz kümmern.

Proxy-Server: Klar, die IP-Adresse lässt sich verschleiern, indem man in den Browsereinstellungen einen anonymisierenden Proxy-Server einträgt. Listen solcher Server spuckt Google in rauen Mengen aus, doch empfehlen können wir diese simple Methode nicht. Denn der Datentransfer nimmt dabei eine Umleitung – und was der Betreiber des Proxys mit Ihren Verbindungsdaten anstellt, können Sie nicht überblicken.

Tools: Setzen Sie lieber auf Anonymisierungstools. Die nutzen zwar auch Proxy-Server, aber vertrauenswürdige. Zuverlässig sind etwa die Open-Source-Projekte Java Anon Proxy (JAP) und The Onion Router (TOR), die Sie beide auf der Heft-CD finden. JAP ist übrigens der Client des AN.ON-Projektes der Universität Regensburg und der Technischen Universität Dresden, welches vom Bundeswirtschaftsministerium gefördert wird – so widersprüchlich ist die Politik.

AN.ON verwendet zur Anonymisierung eine mindestens aus drei Servern bestehende Kaskade von Mix-Proxys. Das sind Rechner von Organisationen, die die JAP-Betreiber als vertrauenswürdig einstufen. Jeder Mixvorgang wirbelt die Daten in einem komplizierten Verfahren durcheinander. Da die einzelnen Proxy-Betreiber nicht in Verbindung stehen, lässt sich am Ende auch nicht nachvollziehen, welcher Teilnehmer welche Daten angefordert hat.

TOR funktioniert ein wenig anders, arbeitet jedoch ähnlich effektiv. Bei TOR werden die Routen für die Kommunikation aus zufällig aus einem Netzwerk ausgewählten Clients generiert.

Voraussetzung für eine starke Anonymisierung sind bei beiden Verfahren

möglichst viele Teilnehmer. Welches Tool Sie einsetzen, bleibt dagegen Ihrem Geschmack überlassen. Beide arbeiten auf vergleichbarem Sicherheitsniveau. In unseren Tests waren die Verbindungen über JAP etwas schneller, das Tempo schwankt allerdings je nach Tageszeit. JAP und TOR installieren sich auf dem PC als lokale Proxy-Server. Um anonym zu surfen, müssen Sie die Verbindungseinstellungen Ihres Webbrowsers anpassen.

Internet Explorer: Unter „Extras | Internetoptionen | Verbindungen | LAN-Einstellungen“ setzen Sie ein Häkchen bei „Proxyserver für LAN verwenden“. Tragen Sie als Adresse „localhost“ ein sowie für JAP den Port 4001 oder für TOR 8118. Gehen Sie danach auf „Erweitert“, und setzen Sie ein Häkchen bei „Für alle Protokolle denselben Server verwenden“.

Opera: In „Extras | Einstellungen | Erweitert | Netzwerk | Proxyserver“ tragen Sie als Adresse „localhost“ ein. JAP verwendet den Port 4001, TOR 8118. Wichtig: Diese Angaben müssen auch Sie bei SSL- und FTP-Verbindungen eintragen.

Firefox: Aktivieren Sie unter „Extras | Einstellungen | Erweitert | Netzwerk | Proxyserver | Verbindungs-Einstellungen“ die Option „Manuelle Proxy-Konfiguration“. Tragen Sie für alle Protokolle als Adresse „localhost“ sowie die Ports 4001 für JAP und 8118 für TOR ein.

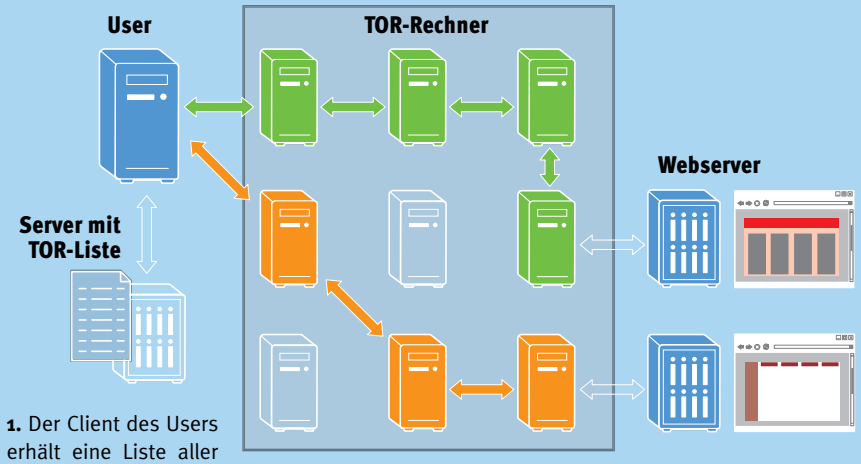
BROWSER: ActiveX immer abschalten – sonst bleiben Hintertüren offen

Ein wichtiger Tipp noch: Im Auslieferungszustand sind die meisten Browser anfällig für Datenspionage. Schalten Sie bei Opera und beim Internet Explorer ActiveX aus (über „Extras | Einstellungen“). Firefox hat diese Technik gar nicht erst integriert. Denn mit den richtigen Skripten lassen sich darüber alle erdenklichen Routinen im Browser ausführen – auch solche, die Daten ausspionieren. Und gehen Sie einem solchen Skript auf den Leim, helfen die besten Tipps nicht.

KNOW-HOW

So funktioniert der Anonymisierer TOR

Der Trick dieses Gratis-Anonymisierungs-Dienstes: Der Weg zum Ziel ist zufällig und jedes Mal anders. Die Anzahl der Proxies ist nur von der Teilnehmerzahl begrenzt.



1. Der Client des Users erhält eine Liste aller am TOR-Netzwerk teilnehmenden Knoten vom Verzeichnisserver.

2. Der Client wählt per Zufallsauswahl einen Pfad über mehrere TOR-Knoten bis zum Zielserver.

3. Für jede neue Anfrage nutzt der TOR-Client andere, zufällig ausgewählte TOR-Rechner als Knoten.

Verschlüsselte Verbindungen

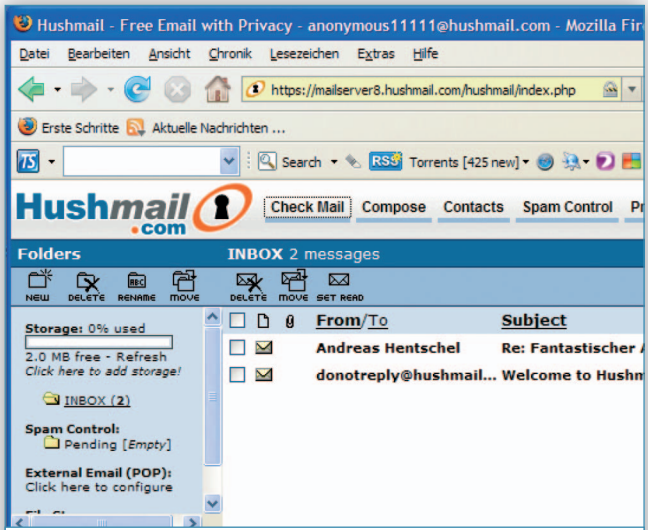
Unverschlüsselte Verbindung

MAIL

Header-Infos: Spuren verwischen

Eine anonyme E-Mail ist kein Problem – Absender weglassen, fertig. Wer anonym Usenet-Postings verfassen oder einen Beratungsservice anmailen will, muss dagegen tricksen. →

Cookie-Problem: Wer Cookies grundsätzlich aussperrt, kann manche Webseiten nicht betreten – etwa das Ebay-Login.



Anonyme Briefe: Der Webservice Hushmail ist leicht zu bedienen, die von ihm gewährte Anonymität nur schwer zu lüften.

KEIN ABSENDER: Die einfache Lösung für gelegentliche anonyme Mails

E-Mail-Clients oder Webmailer schreiben in den Header jeder Nachricht Ihre Mail- oder IP-Adresse. Die Idee, sich für anonyme Mails mit falschen Personenangaben bei einem Freemailer wie etwa Web.de anzumelden, sollten Sie verwerfen: Das verstößt gegen die AGBs und kann Ärger geben. Legal können Sie bei Webservices wie **www.gilc.org/speech/anonymous/remailer.html** anonyme Mails verschicken – allerdings ohne die Möglichkeit, Antworten zu bekommen.

Dauerhaft anonym mailen: Auf der sicheren Seite sind Sie mit Remailersystemen. Das sind Mailclients mit den gewohnten Funktionen, die den Absender und alle weiteren Informationen, welche Rückschlüsse auf Ihre Person zulassen, aus dem Header löschen. Solche Remailersysteme sind eine Lösung für Freaks – weil kompliziert zu handhaben.

Vereinzelt anonym mailen: Ein Mail-Anonymisierer für jedermann ist Hushmail.com, ein webbasierter Freemailer, bei dem Sie sich ohne Angabe persönlicher Daten anmelden. Trotz Anonymisierung arbeitet er sehr simpel und verschlüsselt die Mails auf Wunsch sogar mit dem Open-PGP-Standard. Der kostenlose Account enthält 2 MByte Speicher – nicht üppig, aber genug für gelegentliche anonyme Mails. Auf das kostenpflichtige Upgrade, bei dem es mehr Speicher gibt, sollten Sie lieber verzichten: Die Abrechnung erfolgt über Kreditkarte – und dies würde Ihre Anonymität gegenüber dem Anbieter aufheben.

WEBSITE-LOGINS: Verraten Sie nicht Ihre Mailadresse – teilen Sie Identitäten

Viele (vor allem amerikanische) Webseiten verlangen eine kostenfreie Registrierung via Mailadresse. Wollen Sie die nicht herausgeben, aber trotzdem einen Artikel der „New York Times“ lesen oder ein geschütztes Video bei YouTube ansehen, geht das mit diesem Trick: Auf der Seite **www.bugmenot.com** werden Login-Daten getauscht – sowohl Nutzernamen wie auch Passwörter für registrierungspflichtige Angebote. Um an die Login-Daten zu kommen, tippen Sie einfach in der Suchzeile die URL der jeweiligen Webseite ein – und betreten sie mit den Daten.

TAUSCHEN

Filesharing im anonymen Netzwerk

Seit sich Musik- und Filmwirtschaft für Tauschbörsen-Nutzer interessieren, stehen alle User von BitTorrent & Co. unter Generalverdacht – auch wenn Tauschbörsen an sich legal sind. Ein Ausweg: die Filesharing-Protokolle der nächsten Generation – sie sind anonym und sicher.

VERSCHLÜSSELTER TAUSCH: So sorgt ANts P2P für anonymen Filetransfer

Die neuen Tauschbörsen kombinieren die dezentrale Netzstruktur von BitTorrent mit den gängigen Anonymisierungstechniken wie Proxies oder Mixe. Sie übertragen die Daten schnell, sind leicht zu bedienen – und erfüllen dennoch ein hohes Maß an Sicherheit.

Als besonders sicher gilt in der Filesharer-Szene ANts P2P. Der Client anonymisiert sämtliche Datenströme über ein ausgeklügeltes Routingsystem. Anders als bei BitTorrent wird der Traffic nicht direkt zwischen den Teilnehmern getauscht, sondern über Knoten umgeleitet. Jeder Teilnehmer kennt nur die IP-Adresse des unmittelbaren Nachbarn. So weiß also der Sender einer Datei nicht, wohin das File geschickt wird – und ebenso wenig weiß der Empfänger, wo sich die Quelle befindet. Ein weiteres Sicherheitsplus: Zwischen den Sendern und Empfängern werden die Daten mit dem symmetri-schen Advanced Encryption Standard verschlüsselt, sodass kein Proxy oder Internetprovider die Daten mitlesen kann. Das ANts-P2P-Angebot ist noch nicht so reichhaltig wie bei BitTorrent – wächst aber ständig.

Andreas Hentschel

KNOW-HOW

Wo der Geheimdienst schnüffelt

Das ausgefeilteste System zum Ausspähen von Datenspuren haben die US-Geheimdienste entwickelt: Echelon. Das Netz aus weltweit verteilten Abhöranlagen belauscht alle modernen Kommunikationswege: Fax und Telefongespräche, aber auch Internet und E-Mails. Zwar gibt es zu diesem System keine offiziellen Informationen. Doch immer wieder tauchen Indizien auf, die zeigen, dass E-Mails automatisch nach Schlüsselwörtern überprüft werden. 2004 musste die im oberbayerischen Bad Aibling angesiedelte Echelon-Basis auf Anordnung der Europäischen Union schließen: Es galt als erwiesen, dass sie in erster Linie zur Wirtschaftsspionage gegen die EU eingesetzt wurde.

KNOW-HOW

Wo die Anonymisierer versagen

Lücken in der Tarnkappe

Für Webseiten gibt es mittlerweile so viele Features und Plugins, dass es gewiefte Hacker schaffen, den Schleier eines Anonymisierers zu lüften und an die echte IP-Adresse des Surfers zu kommen.

Ein Beispiel: Mit dem im HTML-Standard verankerten Meta-Tag „refresh“ lässt sich mancher Browser ungewollt auf eine Anonymisierungsfalle umleiten. Eigentlich dient dieser Tag dazu, den Besucher der Webseite nach einem Timeout auf eine andere Seite umzuleiten. Wird allerdings als Zieladresse des Refresh-Tags nicht eine HTTP-, sondern eine Telnet-Adresse angegeben, kann es passieren, dass Windows XP und der Internet Explorer 6 eine Telnet-Verbindung aufbauen. Da es dafür keinen Proxy gibt, wird eine direkte Verbindung aufgebaut, die der Gegenstelle die IP-Adresse des Opfers verrät. Ähnliche Tricks gibt es für andere Browser und andere Betriebssysteme – etwa mit dem neuen Flash-9-Plugin.

Kein Zutritt ohne IP-Adresse

Nicht immer ist es sinnvoll, anonym zu surfen. Die Nutzung einiger Webdienste ist nämlich anonym gar nicht möglich. Auch in manche Internetforen, wie etwa das Journalistennetz Jonet, kommt man anonym oder mit einer Fake-Adresse gar nicht erst rein.

Zu langsam für Power-Downloader

Auch User, die viel Geld für einen schnellen DSL-Anschluss ausgeben, werden eher mal auf die Anonymisierung verzichten, um in den vollen Genuss ihres Highspeed-Zugangs zu kommen. Denn bei großen Downloads kann eine vorgeschaltete Proxy-Kaskade die Ladezeiten stark in die Höhe treiben.

Vorsicht mit Anonymisierungs-Tools am Arbeitsplatz: Mitarbeitern, die keinerlei Spuren in ihren Logdateien hinterlassen, begegnet man oft mit Argwohn. Wenn Sie also auf Nummer sicher gehen wollen, sprechen Sie sich vor dem Einsatz eines Anonymisierungs-Tools mit Ihrem Systembetreuer und Ihrem Vorgesetzten ab.

STAATLICHE LAUSCHANGRIFFE

Neue Attacke auf Ihre Privatsphäre

Die Vorratsdatenspeicherung ist beschlossen. Jetzt wird die staatliche Überwachung ganz neue Dimensionen erreichen.

Der gläserne Bürger ist keine Zukunftsvision mehr, sondern demnächst bedrückende Realität: Nach der EU-Richtlinie zur Vorratsdatenspeicherung vom Mai 2006, die alle EU-Staaten bis Mitte 2007 in nationales Recht umzusetzen haben, müssen Telefon- und Internetprovider die persönlichen und die Kommunikationsdaten ihrer Kunden bis zu zwei Jahre lang speichern.

Zu diesen Daten zählen der Name, die Anschrift, der Anschlussinhaber, angerufene Nummern und Anrufzeiten sowie IP-Adressen, Voice-over-IP- und E-Mail-Verkehrsdaten. Nicht gespeichert werden dürfen die Inhalte der Kommunikation. Das Bundesjustizministerium erarbeitet bereits einen Gesetzentwurf zur Vorratsdatenspeicherung in Deutschland.

Derzeit dürfen die Provider nur die für die Abrechnung kostenpflichtiger Dienste erforderlichen Verbindungsdaten speichern, also beispielsweise keine Standort- und E-Mail-Verbindungsdaten. Bei der Nutzung von Flatrates entfällt die Rechtsgrundlage einer Speicherung von Verbindungsdaten ohnehin.

Doch schon heute sind die Datensammler aktiv wie nie (siehe rechte Spalte und Info-Grafik). Erkundigen Sie sich daher bei den zuständigen Datenschutzbeauftragten (siehe Web-Tipps unten) danach, was über Sie gespeichert ist. Sie haben grundsätzlich Anspruch auf Auskunft über die gespeicherten Daten. Auf der Webseite **www.datenschutzzentrum.de/selbstdatenschutz** finden Sie zahlreiche Formulare für Auskunftsanfragen.

Darüber hinaus haben Sie das Recht, sich aktiv vor dem Ausspähen zu schützen – also etwa Ihre E-Mails und sonstigen Daten mit Tools wie Pretty Good Privacy effektiv zu verschlüsseln (siehe Kasten unten). Einen „Generalschlüssel" für kryptografische Programme, den staatliche Stellen zum Entschlüsseln nutzen könnten, gibt es trotz gegenteiliger Vermutungen nicht.

Andreas Vogelsang

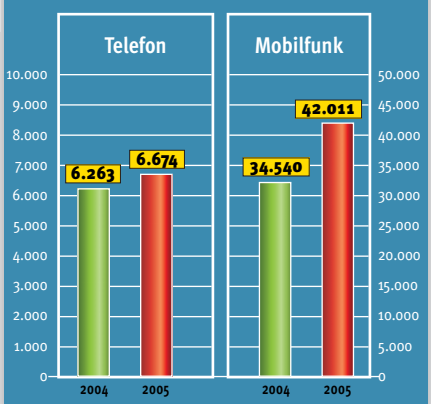
KNOW-HOW

Michael Schweizer, Rechtsanwalt und Partner ADVEO Rechtsanwälte. Weitere Informationen finden Sie unter www.chip.de/recht.

Das darf der Staat

- **Telekommunikation überwachen** aufgrund richterlicher Anordnung beim Verdacht auf schwerwiegende Straftaten z. B. gegen die öffentliche Ordnung
- **Kriminalakte anlegen** im Rahmen strafrechtlicher Ermittlungsverfahren der Polizei
- **Personenbezogene Daten speichern** Die Meldebehörde darf Daten wie etwa die Adresshistorie speichern.
- **Fingerabdrücke nehmen** Strafverfolgungsbehörden dürfen biometrische Kennzeichen beschlagnahmen.
- **Personen per Video überwachen** insbesondere an Kriminalitätsschwerpunkten durch die Polizei
- **Daten an Sozialversicherung melden** Die gesetzlichen Krankenkassen fungieren dabei als Einzugsstellen.
- **Lichtbilder übermitteln** Behörden, die Ordnungswidrigkeiten verfolgen, können Lichtbilder von den Passbehörden anfordern.

LAUSCHANGRIFFE: DER STAAT HÖRT IMMER HÄUFIGER MIT



Auf dem Weg zum Schnüffelstaat: Die Zahl der angeordneten Lauschangriffe bewegt sich steil nach oben – Handy-Nutzer sind besonders betroffen.

Quelle: Bundesnetzagentur

TIPPS

So schützen Sie Ihre Privatsphäre

Mit diesen Maßnahmen erschweren Sie den Lauschern ihre Arbeit:

Mails verschlüsseln: Verschicken Sie ausschließlich verschlüsselte E-Mails (etwa mit Pretty Good Privacy).

Gesetze ausschöpfen: Widersprechen Sie staatlichen Datenübermittlungen und Auskunftserteilungen.

Anonym surfen: Akzeptieren Sie nicht unüberlegt Cookies, löschen Sie Cookies und den Verlauf (History) im Browser mit der Freeware Cleanit 2.0, und verschicken Sie Mails über anonyme Remailer. Schotten Sie Ihr Funknetzwerk mit der WPA-Verschlüsselungstechnik ab.

Persönliche Daten abschirmen: Geben Sie Ihre persönlichen Daten nur heraus, wenn es sich nicht vermeiden lässt. Schützen Sie Accounts oder sensible Daten mit sicheren, mindestens siebenstelligen Passwörtern.

WEB-TIPPS

www.bundesdatenschutzbeauftragter.de: Rechtliche Argumente gegen die EU-Richtlinie

www.datenschutz.de: Wertvolle Infos

www.datenschutzzentrum.de/selbstdatenschutz: Tipps und Know-how zum Schutz Ihrer persönlichen Daten

CROSS-SITE SCRIPTING

Gefährliche Lücken auf jeder Webseite

Mit einfachen Tricks knacken Hacker unbemerkt Onlinebanken, Webshops und Newsseiten. Selbst die Big Player wie Apple, Stern und der TÜV Süd sind davon betroffen. CHIP zeigt Ihnen, mit welchen Methoden Hacker arbeiten und wie Sie sich und Ihre Webseite schützen.

Das Problem Cross-Site Scripting (XSS) wird unterschätzt – sehr zu Unrecht. Denn die eher simpel gestrickten Fälle, die bisher über die Medien bekannt wurden, vermitteln ein zu harmloses Bild. Zu diesen Beispielen gehört der MySpace-Hack „Samy is my hero". Ein einfaches Stück JavaScript, versteckt im Benutzerprofil von Samy, brachte dem Hobby-Hacker innerhalb von zwanzig Stunden mehr als eine Million „Freunde" in dem Community-Portal. Denn jeder Besucher, der seine oder die Webseite eines seiner Opfer aufrief, führte ungewollt einen XSS-JavaScript-Wurm aus, der zwei Dinge bewirkte: In das MySpace-Profil des Besuchers wurde der Satz „But most of all, Samy is my hero" hinzugefügt, und der Wurm wurde hineinkopiert. Für den Giganten MySpace war dieser Hack kein großes Problem: Das Portal war kurz offline, der Fehler wurde bereinigt – schon war die Sache vergessen.

Dass ein XSS-Angriff nicht immer so harmlos abläuft, zeigt der Fall PayPal. An dieser Stelle beließen es die Hacker nicht beim Verändern der Webseite, sondern klauten Kreditkartennummern und persönliche Daten. Doch der Trick, mit denen es ihnen gelang, ähnelt dem von Samy: Ein XSS-JavaScript konnte die Daten aus den Profilen jedes Besuchers auslesen und an den Hacker verschicken.

AUF EINEN BLICK

Cross-Site Scripting

Illustration: S. Schönberger

Aber auch das ist längst noch nicht alles: Das neueste Spielzeug der XSS-Hacker ist die sogenannte JavaScript-Shell. Ruft das Opfer die JavaScript-Shell auf, kann der Hacker wie mit einem Trojaner alles mitlesen, Webseiten verändern und private Daten klauen. Ist das Opfer beispielsweise bei Google Mail ständig angemeldet, kann der Hacker alle E-Mails lesen, E-Mails verschicken und den Google-Account verändern.

Wie wenig bekannt das Problem selbst bei Experten ist, konnte man auch an der Webseite des TÜV Süd erkennen. Obwohl der TÜV eine eigene Abteilung unterhält, die sichere Webseiten zertifiziert, war die eigene Seite selbst anfällig. Sehr dankbar für diesen Hinweis, hat man die TÜV-Webseite umgehend gepatcht.

So erkennen Sie Cross-Site Scripting auf Webseiten

Derzeit unterscheiden Sicherheitsexperten bei Cross-Site Scripting drei verschiedene Angriffstypen:

Typ 0: Der Hacker baut eine Webseite, in die er ein bösartiges JavaScript einbaut. Der Vorteil für den Angreifer: Da es seine eigene Seite ist, unterliegt er keinen Beschränkungen. Aber er muss sein Opfer auf seine – möglicherweise verdächtige – Webseite locken.

Typ 1: Der Hacker findet eine XSS-Lücke auf einer bekannten Webseite. Über eine spezielle URL der Webseite schafft er es, sein bösartiges JavaScript in die sonst harmlose Webseite einzubauen. Diesen Link schickt er dann seinem Opfer, das die Seite nichtsahnend öffnet und das JavaScript des Hackers ausführt. Nachteil für den Hacker: Öffnet das Opfer nicht genau diesen Link, scheitert der Angriff.

Typ 2: Die Benutzer einer Webseite haben die Möglichkeit, Nachrichten für andere Benutzer auf einer bekannten Webseite zu speichern. Der Hacker speichert nicht harmlosen Text, sondern sein bösartiges JavaScript. Vorteil für den Angreifer: Er muss das Opfer nicht dazu bringen, einen präparierten Link zu öffnen – ein Besuch auf der Nachrichten-Seite reicht.

So funktioniert der Webseiten-Angriff im Detail

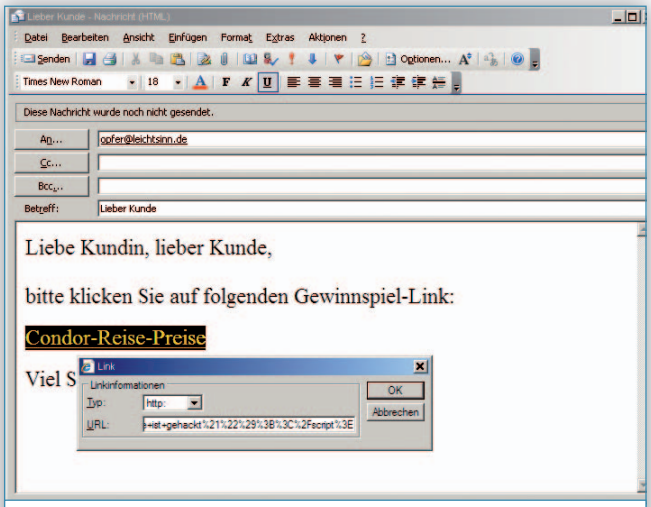
Warum fast jede Webseite von Cross-Site Scripting betroffen ist, liegt an Features wie der Suche oder dem Forum. Immer dann, wenn der Benutzer etwas in eine Webseite eingeben kann, was später wieder ausgegeben wird, besteht die Gefahr eines Cross-Site-Scripting-Angriffs.

Ein Beispiel ist die Suchfunktion eines großen Flugreiseunternehmens: Meist gibt der Benutzer Begriffe wie „Paris“, „Amerika“ oder „Hotel“ in die Eingabemaske der Suchfunktion ein. Sobald er auf „Suchen“ drückt, wird der Begriff an den Webserver geschickt und eine neue Webseite mit den Suchergebnissen geladen. Dort findet der User neben den Ergebnissen auch einen Satz wie: „Ihr Suchbegriff ‚Paris‘ ergab folgende Suchergebnisse:“. Der Link zu dieser Ergebnisseite lässt sich speichern und später wieder aufrufen.

Gibt der Hacker in die Eingabemaske nicht „Paris“ ein, sondern ein Stück HTML und JavaScript, sieht die Ergebnisseite der Suche ganz anders aus. Für unser Beispiel wählen wir den Begriff: „<script >alert(‚Hallo‘);</script>“. Im Webbrowser steht dann nur noch „Ihr Suchbegriff „ “ ergab folgende Suchergebnisse:“. Jetzt erscheint weder ein Suchbegriff, noch werden irgendwelche sinnvollen Ergebnisse angezeigt. Dafür erscheint ein Popup „Hallo“, das beweist, dass der XSS-Angriff erfolgreich war.

Ein Blick in den Quellcode der Webseite offenbart, dass der eingegebene Suchbegriff in die Webseite eingebaut wurde und dann vom Webbrowser als HTML-Code interpretiert wurde. An der entsprechenden Stelle im Quellcode erscheint: „Ihr Suchbegriff ‚<script>alert (‚Hallo‘);</script>‘ ergab folgende Suchergebnisse:“. Da es sich bei „<script>“ um ein ganz legales HTML-Tag handelt, interpretiert der Browser es und stellt es nicht einfach nur als ein Stück Text dar. Hätten wir nicht nur ein einfaches „alert(‚Hallo‘);“, sondern eine JavaScript-Shell angegeben, könnten wir jetzt den Browser kontrollieren.

Der Link in der Adresszeile, den wir verschicken könnten, enthält übrigens Folgendes: „query=%3Cscript%3Ealert%28%27Hallo%27%29%3B%3C%2Fscript%3E“. Der Begriff „query“ ist die Variable, in der der Webserver den Suchbegriff ablegt. Die etwas merkwürdig anmutenden Zeichenkolonnen, die von einem Prozentzeichen angeführt werden, enthalten Sonderzeichen wie „<“ und „“. Der Webbrowser wandelt die Zeichen automatisch um, da viele Sonderzeichen →



Lockvogel-E-Mail: Hacker müssen ihre Opfer dazu bringen, einen präparierten Link zu öffnen, hinter dem sich ein Skript verbirgt.

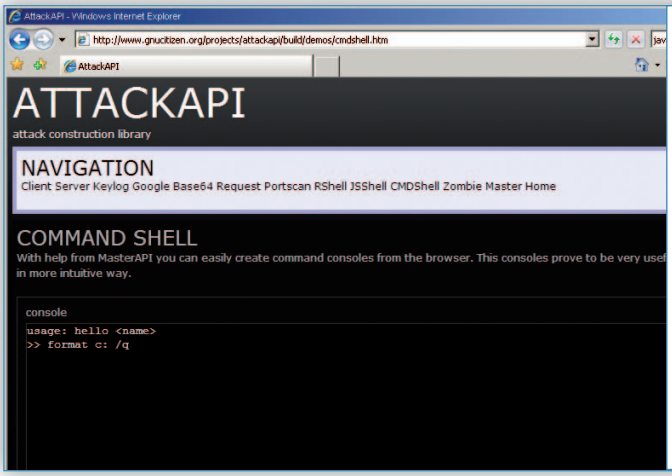
Kalt erwischt: Viele kommerzielle Webseiten, etwa die einer großen Fluggesellschaft, weisen Cross-Site-Scripting-Lücken auf.

nicht in einer URL verwendet werden dürfen. In der Webseite selbst werden die Zeichen aber wie gewohnt dargestellt.

Wie Browser beim Cross-Site Scripting helfen

Wer glaubt, dass simples Suchen & Ersetzen von dem HTML-Tag „<script>“ in den Benutzereingaben genügt, irrt. Es gibt mehr als nur einen Weg, JavaScript-Code in eine Webseite einzuschleusen. Der einfachste Hacker-Trick: Groß- und Kleinschreibung. Denn dem Browser ist es egal, ob der HTML-Tag nun „script“, „Script“ oder gar „sCrIpT“ lautet – ausgeführt wird der Befehl immer. Und selbst wenn der Betreiber der Webseite auch das berücksichtigt: Der Tag „script“ ist längst nicht der einzige Befehl, der ein JavaScript enthalten kann. Die zweithäufigste Variante sind die Action-Tags „onload“ und „onerror“. Ein simples „<img onload=“javascript:alert (‚Hallo‘);“>“ bewirkt im Wesentlichen dasselbe wie das „script“-Tag unseres Beispiels.

Aber das ist immer noch nicht das Schlimmste für den Betreiber der Webseite. Denn auch ein kaputter HTML-Tag wie etwa „<IMG SRC=“jav
ascript: alert(‚Hallo‘);“>“ wird von manchen Browsern noch ausgeführt. Und dabei handelt es sich keineswegs um Exoten. Dieser obskure Befehl funktioniert im Internet Explorer 6, Netscape und Opera.



Extrem kreativ: Um ein Leck perfekt auszunutzen, programmieren Hacker Tools, für die JavaScript eigentlich nicht vorgesehen ist, etwa die Kommandozeile.

Auf einschlägigen Webseiten sammeln Hacker alle Varianten, die in Frage kommen. Wer sich davor schützen möchte, muss also sehr genau hinschauen.

XSS: Es muss nicht immer ein Script-Tag sein

Die Annahme, dass Cross-Site Scripting auf HTML-Tags angewiesen ist, trifft nicht zu. Viele moderne Webseiten übergeben die Benutzereingaben auch an JavaScripts. Die Zeile „var text = „hier kommt der text vom Anwender“;“ kann für den Hacker ein echter Glücksfall sein. Denn filtert der Betreiber nur die Sonderzeichen „<>“ aus, kann immer noch eine XSS-Attacke stattfinden. Schließlich befindet sich der Text des Hackers bereits in einem Stück JavaScript. Jetzt gilt es nur noch, den Anführungszeichen zu entkommen.

Die Zeile „‘; alert(‚Hallo‘);“ bewerkstelligt genau dies. Mit „‘;“ wird die Übergabe des Textes an die JavaScript-Variable „var text=“ abgebrochen und somit Platz geschaffen für das obligatorische „Hallo“.

So schützen Sie Ihre Webseite vor unerwünschten JavaScripts

Damit Sie Ihre Webseite effektiv schützen können, sollten Sie zuerst eine Liste aller möglichen Angriffspunkte anlegen. Die Suchfunktion ist nur der offensichtlichste Punkt. In Frage kommen so ziemlich alle Formulare, in die der Besucher etwas eintragen darf. Dazu gehören auch Mailformulare, Foren und Chaträume. Aber auch Upload-Möglichkeiten sind ein Sicherheitsrisiko. Die entscheidende Frage lautet: Kann der Besucher die Ausgabe auf der folgenden Seite beeinflussen? Wenn ja, sollten Sie einen Filter einbauen.

Ein Trick, die gefährdeten Stellen zu finden, stammt von den Hackern selbst. Die Zeichenfolge „‘;!--“<XSS>=&{()}“ verrät sofort, ob Cross-Site Scripting möglich ist. Tippen Sie diese Zeichenfolge in ein Formularfeld ein, und öffnen Sie von der Ergebnisseite aus den Quellcode. Suchen Sie dort nach der Zeichenkette „<XSS“. Können Sie dieses Suchwort finden, wissen Sie, dass dieses Formular mit ziemlicher Sicherheit ein Ansatzpunkt für Hacker ist, da die Tags ungefiltert im HTML-Code landen.

Filtern Sie deshalb am besten mit der radikalsten Methode: Lassen Sie nur Buchstaben und Zahlen zu, und filtern Sie alle anderen Zeichen aus. Damit machen Sie XSS-Attacken unmöglich. Allerdings:

KNOW-HOW

Hacker-Tools beim Cross-Site Scripting

Wer glaubt, Cross-Site Scripting sei ungefährlich, liegt daneben. Javascript läuft zwar im Webbrowser in einer Sandbox, die keine lokalen Zugriffe erlaubt, aber trotzdem kann ein Hacker mit XSS jede Menge Unsinn anrichten, wie diese Beispiele zeigen:

Portscans starten: Zwar kann JavaScript nicht direkt Ports öffnen, aber mit einem Trick bekommt man fast dieselbe Funktionalität. Dabei hilft das HTTP-Protokoll, das es erlaubt, Inhalte nicht nur von Port 80 zu laden. Das JavaScript muss also nur versuchen, Elemente, zum Beispiel Bilder, von unterschiedlichen Ports anzufordern.

Zwischenablage auslesen: Über einen einfachen JavaScript-Befehl lässt sich der Inhalt der gesamten Zwischenablage auslesen. Dieser Trick funktioniert allerdings nur im Internet Explorer und auch dort nur bis einschließlich Version 6.

Cookies lesen und schreiben: Dieser Trick ist quasi eine Grundfunktionalität. Für den Hacker bedeutet das den Zugriff auf Logins, Passwörter und Session-IDs – alles perfekt geeignet, um Accounts zu übernehmen.

HTML-Inhalte verändern: Manipulierte Börsenkurse, gefälschte Nachrichten und andere Arten von Desinformation – mit Cross-Site Scripting kein Problem. JavaScript verändert den Inhalt jeder Webseite nach Belieben. So platzieren Hacker das neue iPhone genauso leicht auf der Apple-Seite, wie sie PIN und TANs von der Bank-Website auf ihre Hackerseite umleiten.

Firefox-Plugins manipulieren: Der wohl spektakulärste JavaScript-Hack ist die Manipulation des Kennwort-Safes von Firefox. Mit einem simplen Script kann der Hacker sämtliche Logins und Passwörter auslesen. Einziger Schutz: Den Safe nicht benutzen!

Dieser Weg funktioniert nicht immer. Ein Forum etwa, in dem man weder Punkt noch Komma eingeben dürfte, würde einen merkwürdigen Eindruck machen.

Eleganter und fast ebenso effektiv ist die Escape-Methode: Jedes Sonderzeichen, das der Benutzer eingibt, wird nicht unverändert übernommen, sondern speziell codiert. Im HTML-Code werden die Zeichen dann nicht als Befehls-Tags interpretiert, in der Ausgabe aber trotzdem richtig dargestellt. Auch diese Methode klappt jedoch nicht immer: Wollen Sie dem Benutzer beispielsweise erlauben, URLs anzugeben, etwa um ein JPEG zu verlinken, dürfen diese nicht codiert werden, da sonst die URL ungültig wird. Wenn aber die Zeichen nicht codiert werden, kann der Hacker in der URL JavaScript verstecken. So wird zum Beispiel der Eintrag „<img src=javascript: alert(‚Hallo‘);>“ vom Internet Explorer 6, von Netscape 8 sowie von Opera 9.02 unmittelbar beim Laden der Webseite ausgeführt.

Finger weg: So fallen Sie nicht auf XSS-Links herein

Noch versagen sämtliche Phishing-Filter beim Schutz vor Cross-Site Scripting. Denn es gibt einfach zu viele Möglichkeiten, eine XSS-Attacke zu tarnen. Außerdem finden die meisten XSS-Angriffe nicht auf irgendeiner Seite statt, sondern auf einer ganz seriösen Webseite. Im Extremfall kann das sogar die HTTPS-verschlüsselte Webseite einer Bank sein.

Der wichtigste Tipp lautet deshalb: Vertrauen Sie keinem Link – und damit sind nicht nur Links in E-Mails gemeint. Weitere typische Quellen für XSS-verseuchte Links können Blogs, Chat-Nachrichten und RSS-Feeds sein.

Surfen Sie die Webseite lieber selbst an, und klicken Sie sich bis zur gesuchten Seite durch. Erreichen Sie sie nur über einen speziellen Link, ist die Wahrscheinlichkeit, dass es sich um einen Hackerangriff handelt, sehr hoch.

Cross-Site Request Forgery: Web 2.0 für Hacker

„Cross-Site Request Forgery“ (abgekürzt XSRF) ist das Cross-Site Scripting 2.0 der Hacker. Der Unterschied ist sehr gering, aber wichtig: Während Cross-Site Scripting das Vertrauen des Benutzers in die Webseite ausnutzt, nutzt XSRF das Vertrauen aus, das eine Webseite in den Benutzer hat.

XSRF funktioniert zum Beispiel so: Hacker und Opfer sind Teilnehmer eines Chats, der auf einer Webseite läuft. Der Hacker schleust ein Stück JavaScript ein, das den Browser des Opfers dazu veranlasst, auf einer anderen Webseite Einstellungen zu manipulieren. Das klappt allerdings nur dann, wenn das Opfer bereits auf dieser Webseite eingeloggt ist und die Webseite aus diesem Grund auf seine Anfragen reagiert.

Google Mail ist das typische Beispiel für so ein Angriffsziel, denn fast jeder, der dort einen Account besitzt, ist dort immer angemeldet – Cookie sei Dank.

Mailaccounts sind noch das harmloseste Beispiel von XSRF-Angriffen. Viel interessanter sind Angriffe auf Netzwerkgeräte mit Web-Interface. So kann der Hacker, der im Internet sitzt, das JavaScript dazu benutzen, den Router von der LAN-Seite aus umzukonfigurieren.

Vor solchen Angriffen können Sie sich so gut wie gar nicht schützen. Aber Sie können das Risiko minimieren. Dazu müssen Sie Ihr Surfverhalten umstellen und komplexer machen: Löschen Sie die Cookies einer Webseite sofort nach dem Besuch, und melden Sie sich jedes Mal ab. Dann kann der Hacker nicht auf die Daten einer bereits authentifizierten Session zurückgreifen – und der Angriff läuft ins Leere.

Valentin Pletzer

PROFI-TIPP

Webseiten testen

Je größer eine Webseite wird, umso komplexer wird es auch, alle Angriffspunkte der Hacker zu überwachen. Damit Sie Ihre Seite nicht in mühevoller Handarbeit Schritt für Schritt überprüfen müssen, hat die Firma Mayflower den automatisierten Scanner Chorizo! entwickelt. Das kostenlose Webtool können Sie für das Scannen einer Webseite nutzen, was für die meisten privaten Homepages ausreicht. Chorizo! ist ein Proxy, den Sie in Ihrem Browser einrichten und der auf einen Webserver bei Mayflower verweist.
Sie surfen nun mit Ihrem Browser wie gewohnt im Web. Auf jeder Webseite erscheint ein Check-Fenster, mit dem Sie die Seite nach Sicherheitslücken durchsuchen können. Entdeckt das Tool eine Lücke, bekommen Sie eine Meldung, um welche Art von Leck es sich handelt und wo es gefunden wurde.

Hacker-Nachricht: Seiten wie das CHIP-Forum gehören zu den beliebtesten Opfern. XSS-Angriffe lassen sich sogar speichern.

Hacker-Web 2.0: Webseiten wie Live.com von Microsoft nutzen viel JavaScript und sind deshalb in Zukunft das Ziel der Hacker.

ANGRIFFSPUNKTE ANALYSIEREN

Der große W-LAN-Check

Noch immer ist eine Vielzahl privater Funknetze nur unzureichend abgesichert, was Angreifern Tür und Tor öffnet. CHIP zeigt Ihnen, wie Sie die Schwachstellen Ihres drahtlosen Netzwerks mithilfe von Profi-Werkzeugen schnell identifizieren können.

Der große Vorteil drahtloser Netzwerke ist gleichzeitig auch ihre Achillesferse. Der Verzicht auf nervigen Kabelsalat wird mit erhöhter Verwundbarkeit gegenüber Angreifern erkauft. CHIP zeigt Ihnen in diesem Artikel, wie Sie mithilfe des W-LAN-Scanners NetStumbler und des Analysetools Nessus Sicherheitsrisiken Ihres Funknetzes erkennen.

Häufig sind sich die Betreiber von W-LANs der Probleme und Risiken, die beim Aufbau eines drahtlosen Netzwerks lauern, gar nicht bewusst. Der NetStumbler (**www.stumbler.net/**) kann für das nötige Problembewusstsein sorgen. Das Tool demonstriert Ihnen, welche Informationen die Außenwelt über Ihr W-LAN bekommt. Vor der Installation sollten Sie jedoch prüfen, ob Ihre W-LAN-Karte mit dem NetStumbler zusammenarbeitet. Eine Liste bekannter kompatibler Karten und Chipsätze finden Sie auf der Homepage des Programms unter **www.stumbler.net/compat**.

1 NetStumbler konfigurieren

Nach der erfolgreichen Installation von NetStumbler aktivieren Sie die Funktion „Auto Reconfigure“. Die stellt sicher, dass NetStumbler mit dem Windows-Dienst „Wireless Zero Configuration“ zusammenarbeitet und der Empfang einwandfrei funktioniert.

Als Nächstes wählen Sie die passende W-LAN-Karte aus dem Menü „Device“ aus. An dieser Stelle stehen Ihnen normalerweise eine NDIS-Karte sowie ein Eintrag mit dem Namen eines Chipsatzes zur Verfügung. Versuchen Sie als Erstes eine Verbindung über den Chipsatz-Eintrag aufzubauen. Sollte dies nicht funktionie-

AUF EINEN BLICK

Alle Tools auf CD

NetStumbler: Spürt alle Access Points in Ihrer Umgebung auf ⓒ Internet

Illustration: S. Schönberger

ren, wählen Sie den NDIS-Eintrag aus. Damit ist Ihre NetStumbler-Installation einsatzbereit.

2 Umgebung analysieren

Der NetStumbler sucht nun die Umgebung Ihres Rechners ab und zeigt Ihnen alle zur Verfügung stehenden Access Points. Mithilfe der Farben Rot, Gelb und Grün meldet das Tool die Signalstärke eines Funknetzes; ein Schlüssel im farbigen Kreis verrät, dass dieses Netzwerk eine Verschlüsselung aktiviert hat. Neben diesen Informationen bekommen Sie auch die MAC-Adresse des jeweiligen Access Point zu sehen.

Diese Informationen sehen Sie auch mit dem W-LAN-Tool von Windows XP. Der entscheidende Vorteil von NetStumbler besteht im permanenten Absuchen der Umgebung nach Access Points. Damit gelingt es Ihnen, sich ein genaues Bild über die Reichweite Ihres W-LAN zu verschaffen. Installieren Sie den NetStumbler einfach auf einem Notebook und starten Sie Ihre Erkundungstour. Klicken Sie zuvor auf die SSID im linken Fenster, und die Ansicht im Hauptfenster zeigt auch eine grafische Übersicht zur Visualisierung der Signalstärke an.

Sie werden erstaunt sein, wie weit außerhalb Ihrer Wohnung oder Ihres Hauses Ihr Funknetz noch sichtbar ist. Gerade leistungsfähige W-LAN-Router, die mit größerer Reichweite werben, funken ohne Weiteres auch über die Grundstücksgrenze hinaus. Falls Sie in einem Mehrfamilienhaus wohnen, gehen Sie doch einfach mal in das nächste und übernächste Stockwerk. Je nach Bauweise des Hauses und Typ des Routers bekommen Sie auch an diesem Standort noch ein gutes bis ausreichendes Signal. Genau dieser Umstand sollte Sie dazu veranlassen, Ihr W-LAN bestmöglich abzusichern. Worauf Sie achten sollten, lesen Sie im Kasten auf **76**. Detaillierte Anleitungen zum Absichern Ihres drahtlosen Netzwerks finden Sie im Beitrag ab **77**.

3 W-LAN-Check mit Nessus

Nachdem Sie Ihr W-LAN vor dem Abhören abgesichert haben (siehe Beitrag ab **77**), dürfen Sie sich noch nicht in Sicherheit wiegen. Sie haben jetzt zwar eine Sicherheitslücke gestopft, in Ihrem Netzwerk können jedoch – abhängig von der Konfiguration – noch eine Reihe anderer Schwachstellen existieren. Denn weil Sie über einen Router mit dem Internet verbunden sind, gibt es an dieser Stelle eine weitere Tür für ungebetene Gäste. Wie weit diese Tür offensteht, können Sie recht einfach mithilfe einer Toolsammlung namens Nessus (**www.nessus.org/**) herausfinden. Dabei handelt es sich um einen Netzwerk- und Schwachstellen-Scanner, der ursprünglich für Linux und Unix entwickelt wurde, inzwischen aber auch für Windows verfügbar ist.

Nessus besteht aus zwei Komponenten – einem Client und einem Server. Der Server ist für die Angriffssimulationen zuständig. Nach seinem Start lädt der Server automatisch die installierten Plugins, wie sie in der Abbildung unten rechts zu sehen sind. Der Client, der entweder auf dem gleichen oder einem anderen Rechner im Netzwerk installiert wird, verbindet sich anschließend über eine SSL-gesicherte Verbindung mit dem Server. Anschließend können Sie das Angriffsziel und die Parameter für die Sicherheitsüberprüfung festlegen. Nach dem Testlauf bekommen Sie eine detaillierte Analyse der offenen Ports und anderer Schwachpunkte Ihres Netzwerks geliefert.

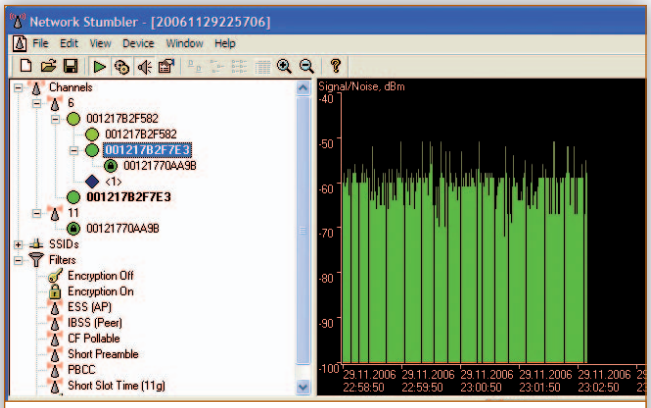
4 Testlauf vorbereiten

Vor dem Download der Windows-Version von Nessus müssen Sie einige persönliche Angaben machen und auch Ihre E-Mail-Adresse verraten. An diese Adresse wird anschließend ein Registrierungscode geschickt, den Sie bei der Installation benötigen. Sollte er auf sich warten lassen, schauen Sie am besten im Spamordner Ihres E-Mail-Accounts nach. War die Installation erfolgreich, sollte nun ein Dienst mit dem Namen Tenable Nessus auf Ihrem Rechner laufen. Das können Sie über die Systemsteuerung unter „Verwaltung | Dienste“ nachprüfen.

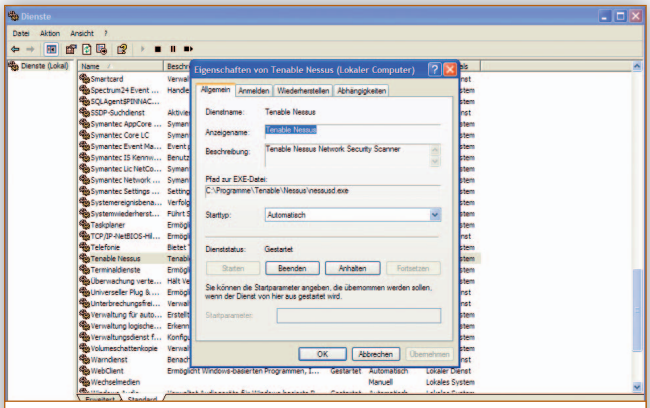
Stellen Sie anschließend mit dem Nessus-Client eine Verbindung zu Ihrem Nessus-Server her – den finden Sie unter „Start | Tenable Network Security | Nessus | Tenable Nessus“.

Auf der Einstiegsseite stehen im Hauptfenster zwei Funktionen zur Auswahl: das Starten des Scanvorgangs oder die Anzeige der in letzter Zeit generierten Reports. Nach Aktivierung der Analyse fragt Nessus Sie nach der IP-Adresse des Nessus-Servers. Befinden sich sowohl der Client als auch der Server auf dem gleichen Rechner, geben Sie an dieser Stelle 127.0.0.1 ein. Andernfalls tragen Sie die passende IP-Adresse Ihres Servers im Netzwerk ein.

Im nächsten Schritt legen Sie die Art der Überprüfungen fest. Nessus ist modular aufgebaut und bietet mit mehr als →



2 Abgehört: Gerade bei der Analyse der Signalstärke ist der NetStumbler mit seiner grafischen Darstellung sehr hilfreich.



3 Dienstbereit: Nach der Installation des Analysetools finden Sie Nessus unter den Windows-Diensten wieder.

10 000 Plugins und Skripten eine große Auswahl an Möglichkeiten zur Schwachstellenanalyse Ihres Rechners. Damit Sie sich mit der Zusammenstellung Ihres Testlaufs nicht allzu lange aufhalten müssen, sind die Tests in verschiedene Risikogruppen eingeteilt.

Wenn Sie bereits etwas Erfahrung in der Analyse von Netzwerken haben, steht jedoch einer ganz individuellen Zusammenstellung der Tests nichts im Wege. Da einige Testfamilien allerdings auch die Stabilität Ihres Systems bewusst in Mitleidenschaft ziehen, sollten Sie sich als Einsteiger erst vorsichtig herantasten. Dazu bietet Nessus die Option „Enable all but dangerous plugins with default settings“, die solche „Denial of Service (DoS)“-Tests ausschließt und die Checks mit den Standardparametern vornimmt.

Sind Client und Server nicht auf demselben Rechner installiert, geben Sie im nächsten Schritt die Anmeldedaten für den Remote-Server ein.

5 Eigene Policies anlegen

Während des Scannens hält Nessus Sie über den prozentualen Fortschritt seiner Arbeit ständig auf dem Laufenden. Am Ende des Testlaufs bekommen Sie eine Auswertung auf HTML-Basis angezeigt. Sie können einen Scanvorgang auch jederzeit unterbrechen. Nessus speichert dann die ermittelten Ergebnisse zwischen, sodass Sie auf diesem Stand problemlos wieder aufsetzen können.

5 Flexibel: Mithilfe eigener Policies erlaubt Nessus auch das individuelle Zusammenstellen von Testläufen.

Neben der Überprüfung mit Standardwerten erlaubt Nessus auch eine individuelle Konfiguration des Plugins und der Testszenarien. Dazu müssen Sie im ersten Schritt eine neue „Policy“ anlegen und können danach die allgemeinen Testeinstellungen pflegen und über „Edit Plugins“ Testfamilien sowie die korrespondierenden Tests an- und ausschalten.

Zu den bereits vorhandenen Plugins kommen regelmäßig neue Plugins hinzu, und die bestehenden werden an neue Sicherheitslücken angepasst. Sie sollten deswegen vor einem neuen Scan-Durchlauf immer nach neuen Tests Ausschau halten. Dazu steht Ihnen ein eigener Assistent zur Verfügung, den Sie über „Update Plugins“ aufrufen.

6 Ergebnisse auswerten

Nessus gruppiert die Ergebnisse in vier Risikokategorien: „Offene Ports“, „Bemerkungen“, „Warnungen“ und „Sicherheitslöcher“. In der Ergebnisliste finden Sie jeweils eine Erklärung zu dem Scan-Vorgang, der das Problem aufgedeckt hat. Häufig bekommen Sie auch gleich eine Problemlösung angeboten. Diese sollten Sie – besonders für die Rubriken „Warnungen“ und „Sicherheitslöcher“ – möglichst schnell umsetzen. Schauen Sie sich also die Auswertungen genau an. Sie finden sie auch unter „View Reports“ und können dort die Ergebnisse von zwei Testläufen vergleichen.

7 Missbrauch unterlassen

Nessus sollten Sie ausschließlich zur Sicherheitsanalyse Ihres eigenen Netzwerks einsetzen. Versuchen Sie nicht, damit die Schwachpunkte anderer Netze herauszufinden und auszunutzen, denn damit machen Sie sich unter Umständen strafbar.

Sie sollten Nessus auch nicht im Firmennetzwerk einsetzen – es sei denn, Sie sind der Administrator und wissen, was Sie tun. Gerade das Experimentieren mit DoS-Tests kann schnell dazu führen, dass ein komplettes Netzwerk durch die Last der Anfragen in die Knie gezwungen wird. Führt dies in einer Produktionsumgebung zu einem Netzwerkausfall, sodass Ihre Kollegen nicht mehr weiterarbeiten können, kann dies auch strafrechtliche Konsequenzen haben.

Wer für einen solchen Crash verantwortlich ist, lässt sich gerade in einem lokalen Firmennetz einfach herausfinden, da der Datenverkehr zumindest am Proxy, teilweise aber auch an Netzwerkknoten analysiert wird.

Andreas Hitzig

PROFI-TIPPS

Die wichtigsten Schutzmaßnahmen

Nahezu jeder W-LAN-Router bietet die gleichen Sicherheitseinstellungen – lediglich die Menüstrukturen sind unterschiedlich aufgebaut. Auf die folgenden Punkte sollten Sie besonders achten.

Administrator-Passwort: Beim ersten Anmelden sollten Sie das Administrator-Passwort und – falls möglich – auch den Administrator-Namen ändern. Ansonsten können Angreifer, nachdem sie eine IP-Adresse bekommen haben, Ihre W-LAN-Einstellungen ungehindert ausspähen.

SSID (W-LAN-Name): Jedes W-LAN sendet seinen Namen nach außen, bis Sie dies unterbinden. Damit ist das W-LAN zwar noch sichtbar, nicht aber sein Name – und der ist zum Anmelden notwendig.

Verschlüsselung: Noch immer funken viele W-LANs – absichtlich oder unabsichtlich – ohne aktivierte Zugangsprüfung. Wählen Sie die höchstmögliche Verschlüsselung – in der Regel ist das WPA 2. Bei WEP lässt sich, selbst mit 128-KBit-Schlüssel, mit einer geringen Anzahl abgefangener Pakete der Schlüssel errechnen.

MAC-Filter: Beschränken Sie den Zugang zu Ihrem Funknetz auf bestimmte Netzwerkkarten. Das ist über die MAC-Adresse möglich. Sie finden diese Angabe entweder auf der Unterseite Ihres Notebooks oder unter Windows XP über die Eingabeaufforderung und den Befehl „ipconfig /all“.

Firewall: Aktivieren Sie zusätzlich – falls Ihr Router als DSL-Modem fungiert – die Firewall Ihres Rechners. Diese unterbindet, bereits bevor die Pakete auf dem PC landen, einen Teil der Angriffe aus dem Internet.

Detaillierte Informationen über den Komplettschutz eines drahtlosen Netzwerks finden Sie im Artikel ab 77.

Foto: CHIPimages; Illustration: S. Schönberger

SICHERHEITSPAKET FÜR FUNKNETZE

Komplettschutz für Ihr W-LAN

Der Datenverkehr in einem Funknetz lässt sich von jedem abhören, der sich mit einem Notebook und einem W-LAN-Adapter gerade in Reichweite befindet. CHIP zeigt Ihnen, wie Sie potenzielle Eindringlinge von Ihrem Funknetzwerk fernhalten.

Funknetzwerke sind konstruktionsbedingt weniger sicher als verkabelte Netzwerke: Die Daten werden schließlich nicht über abgeschirmte Kabel transportiert, sondern vom Access Point und den W-LAN-Clients per „Rundfunk" verschickt. Auf diese Weise sind sie nicht nur im Büro, sondern auch in der Nachbarschaft zu empfangen. Jeder, der sich im Sendebereich befindet, kann sie mit einem Notebook mit W-LAN-Adapter abhören.

Mithilfe einer zusätzlichen Antenne kann ein Angreifer Signale sogar über eine Entfernung von bis zu 150 Metern abfangen, beispielsweise im Auto am Straßenrand oder in einem Nachbarbüro. Die Hausmauern dämpfen die Funksignale zwar, schirmen sie jedoch in der Regel nicht vollständig ab.

In diesem Beitrag erfahren Sie am Beispiel des W-LAN-Routers Fritz!Box und eines Gigaset-Access-Points, wie Sie Ihr Funknetz komplett absichern. →

AUF EINEN BLICK

→ Sicherheitspaket für W-LANs

Alle Tools auf CD

Airsnort: Zeichnet Daten auf und rekonstruiert WEP-Schlüssel ◎ Internet

Kismet: Spürt alle erreichbaren W-LAN-Netze auf ◎ Internet

Wer ein W-LAN angreift, hat es viel einfacher als ein Hacker, der in ein Kabelnetzwerk eindringen will: Er muss nur nahe genug an das W-LAN herankommen – dann kann er bequem alle Datenpakete aufzeichnen. Er braucht sich keinen Zugriff auf die Router oder Server zu verschaffen, über die die Daten transportiert werden – es reicht, sich mit dem notwendigen Werkzeug in der Nähe des fraglichen Büros aufzuhalten.

Dabei kann der Lauscher nicht nur die übertragenen Daten abhören und gefälschte Datenpakete einschleusen: Er hat auch die Möglichkeit, in das Netzwerk einzubrechen und die dort verfügbaren Ressourcen zu nutzen – beispielsweise über Ihren DSL-Anschluss kostenlos zu surfen oder vielleicht sogar in Filesharing-Diensten Raubkopien von Songs oder Filmen zu tauschen. Ebenso können Spammer Ihren Computer kapern und darüber Spammails verbreiten; es ist auch möglich, dass Kriminelle Ihren Internetanschluss für Denial-of-Service-Attacken auf Webserver missbrauchen.

Vor allen diesen Bedrohungen können Sie sich schützen. Ein solcher Komplettschutz erfordert allerdings einiges an Eigeninitiative durch die für das W-LAN verantwortliche Person. Schließlich liefern die meisten Hersteller ihre W-LAN-Produkte aus, ohne Sicherheitsfeatures zu aktivieren.

2 SSID modifizieren: Ändern Sie den vorgegebenen Netzwerknamen (SSID), und schalten Sie das SSID-Broadcasting ab („SSID bekannt geben").

Die meisten Sicherheitsvorkehrungen treffen Sie direkt am Access Point, mit dem Sie das Funknetz aufbauen. Einige Einstellungen – insbesondere die Verschlüsselung – müssen Sie allerdings zusätzlich auf jedem einzelnen Rechner vornehmen, der Zugang zu Ihrem W-LAN erhalten soll.

1 Access Point konfigurieren

Verbinden Sie den Access Point per USB- oder Ethernet-Kabel mit Ihrem Computer. Starten Sie danach die Konfigurationssoftware Ihres Access Point – entweder als eigenständiges Programm wie das AVM Fritz!Box Startcenter oder durch Eingabe der IP-Adresse des Access Point im Webbrowser (etwa 192.168.2.1).

Damit niemand die Einstellungen im Access Point manipulieren kann, schützen Sie das Gerät durch Eingabe eines Kennworts – die meisten Modelle erlauben die Eingabe eines Systemkennworts. Bei der Fritz!Box-Software klicken Sie auf dem Button „FritzBox" im Startcenter und danach auf „Einstellungen | System | FritzBox-Kennwort". Aktivieren Sie den Passwortschutz und geben Sie ein Kennwort ein, das nicht leicht zu erraten ist. Übernehmen Sie unter keinen Umständen das vorgegebene Kennwort (etwa „administrator"), da Angreifer meist die Voreinstellungen der Geräte kennen.

2 SSID ändern und geheim halten

Damit ein Client Zugang zum W-LAN erhält, muss er den Netzwerknamen (auch als SSID oder ESSID bezeichnet) kennen. Bei vielen Access Points ist eine SSID voreingestellt – manchmal lautet sie einfach „SSID", oft wird auch der Name des Herstellers oder des Geräts verwendet. Solche Namen sind sehr leicht zu erraten – zudem weiß der Angreifer dann sofort, mit welchem Gerät er es zu tun hat. Wählen Sie daher einen Netzwerknamen, der nicht leicht zu erraten ist – also weder Ihren Familien- oder den Firmennamen noch Wörter, die man in einem Wörterbuch finden kann.

Die SSID zu ändern reicht aber nicht: Denn fast alle Access Points sind so eingestellt, dass sie die SSID in den Äther funken. Das ist zwar praktisch, wenn Sie einen neuen Client ins W-LAN einbinden wollen, da die Software auf dem Client eine

KNOW-HOW

Wofür W-LAN-Betreiber haften müssen

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) warnt davor, dass Betreiber eines nicht geschützten Funknetzes nach der herrschenden Rechtsprechung in Deutschland für Straftaten verantwortlich gemacht werden, die über ihr W-LAN begangen wurden. Der BITKOM empfiehlt daher dringend das Verschlüsseln des W-LAN sowie die Beschränkung der Nutzer. Insbesondere bei Funknetzen, auf die ein größerer Kreis von Nutzern zugreift, sollte der Verantwortliche den Schlüssel (WEP, WPA oder WPA2) regelmäßig wechseln. Außerdem sollte man sich von den Nutzern des W-LAN eine schriftliche Erklärung geben lassen, dass diese den Webzugang nur für legale Zwecke nutzen.

Hintergrund der Empfehlungen des BITKOM ist eine Entscheidung des Hamburger Landgerichts: Die Richter hatten eine Familie dafür haftbar gemacht, dass sie keine angemessenen Maßnahmen ergriffen hatte, um den Zugang zu ihrem W-LAN zu schützen. Über das W-LAN hatten Unbekannte 244 Musikdateien auf ein Peer-to-Peer-Netzwerk geladen und damit das Urheberrecht einer Plattenfirma verletzt.

Die Betreiber des W-LAN versicherten, dass sie die Musikdateien nicht öffentlich zugänglich gemacht hatten. Da sie ihr W-LAN nicht geschützt hätten, müsse jemand anderes den Internetzugang der Familie missbraucht haben. Das Gericht urteilte, die Familie hätte für die Sicherung des W-LAN zu sorgen gehabt und habe gegen zumutbare Prüfungspflichten verstoßen. Damit habe sie für die Rechtsverletzungen einzustehen. Schließlich sei es allgemein bekannt, dass ungeschützte W-LAN-Verbindungen von Dritten missbraucht werden.

Liste aller W-LANs im Umkreis anzeigen kann. Auf diese Weise verraten Sie aber auch Unbefugten Ihre SSID.

Schalten Sie deshalb das SSID-Broadcasting sofort ab; bei der Fritz!Box heißt diese Option „Name des Funknetzes (SSID) bekannt geben“.

3 Verschlüsselung aktivieren

Ein Angreifer mit den passenden Werkzeugen und genügend Zeit wird keine Probleme haben, die meisten der an dieser Stelle beschriebenen Maßnahmen zu überwinden. Der einzige wirklich sichere Schutz ist das Verschlüsseln des gesamten Datenverkehrs im W-LAN. Ein Angreifer kann die übertragenen Daten dann zwar vielleicht noch empfangen, aber nicht mehr entziffern.

Derzeit stehen drei Verschlüsselungsverfahren zur Auswahl: WEP, WPA und WPA2. WEP ist das am wenigsten vertrauenswürdige Verfahren, WPA2 das sicherste. Wenn alle Clients im W-LAN WPA2 beherrschen, sollten Sie dieses Verschlüsselungsverfahren einsetzen. Falls sich in Ihrem Funknetz aber ältere Notebooks oder W-LAN-Adapter befinden, die lediglich WEP unterstützen, bleibt Ihnen nichts anderes übrig, als WEP zu verwenden oder neue, WPA2-fähige Adapter anzuschaffen. Es lässt sich nämlich immer nur ein Verschlüsselungsverfahren im W-LAN einsetzen – das gleichzeitige Nutzen etwa von WEP und WPA2 ist unmöglich.

Bei einigen Geräten haben Sie die Wahl zwischen WEP mit 40 und 128 Bit langen Schlüsseln (falls es nur eine Option gibt, ist es in der Regel WEP 128). Nehmen Sie dann WEP 128, da es schwieriger zu knacken ist als WEP 40.

Geben Sie den Schlüssel ein, mit dem die Daten chiffriert und beim Empfänger dechiffriert werden. Wählen Sie einen Schlüssel, der sich nicht erraten lässt und auch einer Wörterbuchattacke standhält. Er sollte aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen. WEP-Schlüssel müssen genau 13 Stellen umfassen (WEP 40 fünf Stellen). WPA- und WPA2-Schlüssel dürfen zwischen acht und 63 Stellen lang sein. WEP-Schlüssel geben Sie im ASCII- oder im Hex-Format ein (im Hex-Format sind es zehn beziehungsweise 26 Stellen).

Der Schlüssel muss an jedem Clientrechner eingetragen werden, der Zugriff auf das W-LAN erhalten soll. Halten Sie den Schlüssel geheim: Schicken Sie ihn also nicht per E-Mail herum.

4 MAC-Filterung einschalten

Eine weitere Maßnahme, Unbefugten Zugang zu Ihrem Funknetz zu verwehren, ist die MAC-Filterung. Denn jedes Netzwerkgerät verfügt über eine individuelle MAC-Adresse (MAC: Media Access Control), über die es sich identifizieren lässt. Jedes Datenpaket, das von einem bestimmten W-LAN-Gerät gesendet wird, enthält auch dessen MAC-Adresse. Sie können Ihren Access Point so einstellen, dass er nur Datenpakete von Geräten akzeptiert, deren MAC-Adresse Sie als „autorisiert“ bezeichnen. Dazu schalten Sie im Access Point die MAC-Filterung ein.

Ermitteln Sie nun die MAC-Adressen aller Computer und sonstiger Netzwerkgeräte, die Zugang zum W-LAN erhalten sollen. Diese Adressen finden Sie meist auf einem Aufkleber am Gerät, oder sie lassen sich auf Windows-Rechnern über den Befehl „ipconfig /all“ in einem MS-DOS-Fenster anzeigen.

Geben Sie alle in Ihrem W-LAN zulässigen MAC-Adressen in die Filtertabelle →

PROFI-TIPP

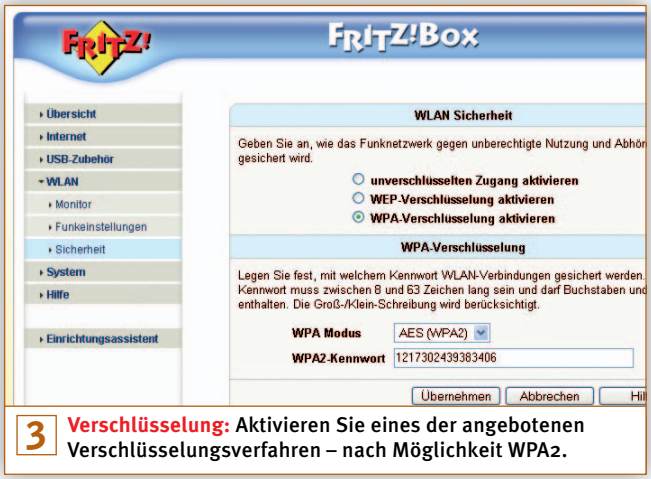
Sichere Schlüssel für WPA finden

Wer versucht, sich im Internet über W-LAN-Verschlüsselung zu informieren, wird gelegentlich auf die Behauptung stoßen, auch WPA könne geknackt werden. Das stimmt, hat aber nichts mit WPA zu tun. Denn jede Verschlüsselung – selbst ein starkes Verfahren wie WPA, WPA2 oder AES – ist nur so sicher wie der verwendete Schlüssel.

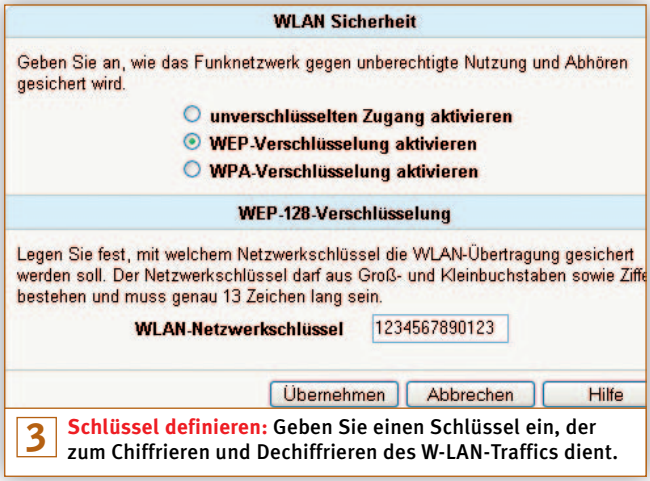
Ein Angreifer wird es meist zuerst mit einer Wörterbuchattacke versuchen. Wenn Sie einen leicht zu erratenden Schlüssel verwenden, etwa Ihren Namen oder etwas Vergleichbares, wird ein Angreifer nicht viel Mühe haben.

Sicherheitsexperten haben eine Schwachstelle in der Behandlung der Schlüssel in WPA entdeckt: Ein Angreifer kann WPA-Schlüssel, die weniger als zwanzig Stellen umfassen und für Wörterbuchattacken anfällig sind, vergleichsweise leicht knacken. Dazu muss er den ersten Schlüsselaustausch zwischen einem W-LAN-Client und dem Access Point abhören. Falls die Verbindung bereits besteht, kann er sie unterbrechen und einen erneuten Schlüsselabgleich erzwingen – und so die Informationen herausfinden. WPA2 weist diese Schwachstelle nicht auf.

Deshalb: Wählen Sie einen WPA-Schlüssel, der länger als zwanzig Stellen ist und Ziffern, Buchstaben und Sonderzeichen enthält – und keine Wörter, die man in einem Wörterbuch findet. Das Letztere gilt auch für WPA2.



3 Verschlüsselung: Aktivieren Sie eines der angebotenen Verschlüsselungsverfahren – nach Möglichkeit WPA2.

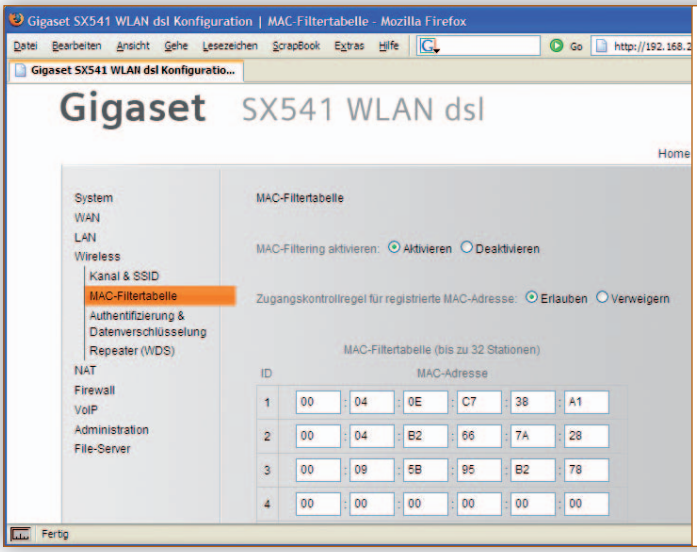


3 Schlüssel definieren: Geben Sie einen Schlüssel ein, der zum Chiffrieren und Dechiffrieren des W-LAN-Traffics dient.

auf dem Access Point ein. Falls Sie die MAC-Adresse eines Geräts kennen, das auf keinen Fall Zugang erhalten soll, können Sie es auch explizit ausschließen.

Während es bei vielen Access Points möglich ist, die MAC-Filtertabelle nach und nach mit Adressen zu füllen, müssen Sie bei der Fritz!Box einen anderen Weg gehen: Schalten Sie alle W-LAN-Geräte ein, die der MAC-Adressfilter akzeptieren soll, und aktivieren Sie unter „WLAN | Monitor“ die Option „Keine neuen WLAN-Netzwerkgeräte zulassen“.

Die MAC-Filterung allein bietet allerdings keinen ausreichenden Schutz: Denn wenn Sie den Datenverkehr nicht verschlüsseln, wird die MAC-Adresse in den Datenpaketen im Klartext übertragen – und lässt sich von einem Angreifer abhören. Mithilfe sogenannter Spoofing-Software kann der dann Ihrem Access Point vorspiegeln, er habe einen PC mit einer der zulässigen MAC-Adressen.



4 MAC-Filterung: Aktivieren Sie die MAC-Filterung. Dann haben nur Geräte Zugang zu Ihrem Funknetz, deren MAC-Adresse Sie in die Liste eingetragen haben.

5 UPnP-Zugriffe blockieren

Einige Access Points, etwa die Fritz!Box, erlauben Fernzugriffe per Universal Plug & Play (UPnP). Über diese Schnittstelle kann UPnP-fähige Software Einstellungen verändern. Das ist durchaus nützlich, wenn Sie über eine Internetverbindung, etwa aus dem Ausland, Einstellungen am Access Point ändern müssen. Allerdings ist UPnP damit auch eine potenzielle Sicherheitslücke. Schalten Sie im normalen Betrieb diese Schnittstelle aus.

6 Firewall aktivieren

Viele Access Points sind Bestandteil eines Kombigeräts, das oft auch eine Firewall mitbringt. Auch wenn auf allen Clientcomputern im W-LAN eine Desktop-Firewall installiert ist, sollten Sie unbedingt auch die Firewall im Access Point aktivieren. Die meisten dieser Firewalls vermitteln Ihnen eine exakte Kontrolle des Datenverkehrs ins und aus dem Internet. Beim Siemens Gigaset etwa finden Sie die Einstellungen unter „Firewall | Hackerabwehr“. Lassen Sie nur den Traffic zu, der tatsächlich gebraucht wird. „UDP“ brauchen Sie für das Domain Name System (DNS), für Streaming-Anwendungen, Voice over IP, BitTorrent und Online-Spiele. „H.323“ wird ebenfalls für VoIP und für Videokonferenzen benötigt.

7 Signalstärke reduzieren

Noch zwei Hinweise zum Access Point: Platzieren Sie ihn nicht an einer Außenwand oder an einem Fenster zur Straße, sondern in der Mitte Ihres Büros oder Ihrer Wohnung. Lauscher vor dem Haus profitieren sonst von der hohen Signalstärke. Stellen Sie die Signalstärke niemals auf maximale Leistung: Regeln Sie sie vielmehr so, dass der W-LAN-Client, der am weitesten vom Access Point entfernt ist, noch ein ausreichend gutes Signal bekommt – nicht mehr.

8 Clients konfigurieren

Gerade bei älteren W-LAN-Adaptern empfiehlt es sich, auf der Website des Herstellers nachzusehen, ob es ein Treiber- oder Firmware-Upgrade gibt, das eine stärkere Verschlüsselung unterstützt. Falls ein solches Upgrade verfügbar ist, laden Sie es herunter und installieren es.

Zum Konfigurieren des W-LAN-Adapters rufen Sie die zugehörige Software auf. Darin aktivieren Sie das gleiche Verschlüsselungsverfahren wie auf dem Access Point, geben den gleichen Schlüssel ein und klicken auf den Button „Anwenden“. Sobald die Verbindung steht, leuchtet ein

KNOW-HOW

Für kleine W-LANs ist auch WEP gut genug

WEP (Wired Equivalent Privacy) ist das älteste der W-LAN-Verschlüsselungsverfahren. Es gilt heute nicht mehr als sicher: 2003 hat das FBI vorgeführt, wie man mit im Internet erhältlichen Tools in wenigen Minuten die WEP-Verschlüsselung knacken kann. Denn das WEP-Verfahren weist eine Reihe von Schwachstellen auf, an denen Angreifer ansetzen können, wenn sie über die passenden Werkzeuge und die notwendige Rechenpower verfügen. Setzen Sie deshalb – wenn möglich – auf WPA oder WPA2.

Allerdings gibt es immer wieder Fälle, in denen eine Verschlüsselung mit WPA oder WPA2 nicht möglich ist – etwa wenn Sie ein älteres Notebook oder einen betagten W-LAN-Adapter besitzen, die nur WEP unterstützen und die Sie aus Kostengründen nicht ersetzen können oder wollen. Auch bei Linux-Rechnern kann es vorkommen, dass die Treiber für den W-LAN-Adapter nur mit WEP korrekt arbeiten. Dann bleibt Ihnen nur WEP als Alternative zum offenen W-LAN.

Trotz seiner Schwachstellen kann WEP durchaus einen ausreichenden Schutz für kleine W-LANs bieten: Denn um die Verschlüsselung mit einem Tool wie etwa Aircrack zu knacken, muss ein Angreifer zwischen 200 000 und 500 000 verschlüsselte Datenpakete protokollieren. In einem W-LAN mit wenig Traffic kann es mehrere Tage oder sogar Wochen dauern, bis der Schnüffler die notwendige Datenmenge gesammelt hat. So viel Geduld haben die wenigsten Script-Kiddies und Möchtegern-Hacker.

Um aber auch geduldigen Angreifern das Spiel zu verderben, sollten Sie den WEP-Schlüssel regelmäßig ändern: Denn nach jedem Schlüsselwechsel darf der Angreifer mit der Paketsammlung von vorne anfangen.

6 **Firewall:** Schalten Sie unbedingt die Firewall in Ihrem Access Point ein, um den Datenverkehr zu kontrollieren.

grünes Lämpchen am Adapter auf; oft zeigt auch ein grünes Feld im Softwaredialog, dass Sie erfolgreich waren.

Speichern Sie die Einstellungen nun in einem Profil, sodass Sie sie nicht immer wieder neu eingeben müssen, wenn Sie häufig das W-LAN wechseln – etwa mit einem Notebook, das Sie im Büro und zu Hause nutzen.

9 Funknetz abschalten

Falls Sie Ihr W-LAN für eine bestimmte Zeit nicht nutzen, etwa am Wochenende oder im Urlaub, schalten Sie den Access Point am besten ganz aus – so kann niemand in Ihrer Abwesenheit in Ihr Funknetz einbrechen. Praktisch sind Access Points, bei denen sich die W-LAN-Funktion separat abschalten lässt. Dann stehen die übrigen Funktionen des Gerätes, etwa Telefonanlage und Anrufbeantworter, weiter zur Verfügung.

Fazit: Was das lückenlose Absichern eines Funknetzes erschwert, ist die Tatsache, dass Angreifer die meisten der einzelnen Sicherheitsvorkehrungen überwinden können: Auch ohne Broadcasting der SSID kann spezielle Software sie durch Analysieren des W-LAN-Traffics ermitteln. Um unbekannte Computer aus dem W-LAN auszuschließen, kann der Administrator die MAC-Filterung aktivieren. Obwohl jedes Netzwerkgerät eine eindeutige und einmalige MAC-Adresse aufweist, ist es jedoch nicht schwer, per MAC-Spoofing dem Access Point eine andere Adresse vorzuspiegeln – der Angreifer muss lediglich herausfinden, welche Adressen im W-LAN verwendet werden.

PROFI-TIPP

Sicherheitstest: Das eigene W-LAN hacken

Um herauszufinden, ob Ihr Funknetz nun noch Sicherheitslücken hat, schlüpfen Sie am besten in die Rolle eines Hackers, der in Ihr W-LAN einbrechen will (wie Sie dabei im Detail vorgehen, lesen Sie ab 74).

Es gibt zwar auch eine Reihe von Tools für Windows (etwa NetStumbler und Nessus, mehr dazu ab 74), die besten Angriffsprogramme laufen allerdings unter Linux. Falls Sie kein Linux installiert haben: Mit Troppix und Whax stehen zwei von CD ausführbare Linux-Distributionen zur Verfügung, die alle Hackertools sowie die Treiber für die gängigen W-LAN-Adapter mitbringen. Die ISO-Images dieser Distributionen erhalten Sie unter **http://files.tuto-fr.com**.

Wenn Sie selbst mit einem Notebook als „Wardriver" versuchen wollen, von außen in Ihr Funknetzwerk einzubrechen, empfiehlt es sich, auch eine ähnliche Hardwareausstattung zu verwenden: Die Antenne der meisten W-LAN-Adapter, insbesondere der auf der Notebook-Platine integrierten, ist vergleichsweise schwach. Deshalb nutzen Hacker gern Adapter, an die sie eine externe Antenne anschließen können. Typische Werkzeuge von Wardrivern sind die drei W-LAN-PC-Cards Orinoco/Proxim 802.11b/g Gold, Buffalo AirStation WLI-CB-G54S und Buffalo MaxxGain AirStation 53CS. Alle diese Adapter verfügen über einen Anschluss für externe 2,4-GHz-Antennen und lassen sich gut unter Linux einsetzen. Bei Ebay finden Sie die Buffalo-Karten häufig im Set mit einer Antenne als „Wardriving Kit" für rund 90 Euro. Nun brauchen Sie nur noch eine Reihe von Softwaretools.

Digitaler Schlüsseldienst: Kismet ist ein Packet Sniffer, der den Traffic in einem Funknetz protokolliert. Die abgehörten Pakete lassen sich in einem Dateiformat speichern, die das Entschlüsselungsprogramm Airsnort (siehe unten) lesen kann. Zudem lassen sich damit die im Funknetzwerk verwendeten MAC-Adressen ausspionieren. Die aktuelle Version finden Sie unter **www.kismetwireless.net**.

Falls Sie die WEP-Verschlüsselung einsetzen, probieren Sie mit Airsnort oder Aircrack aus, wie lange es dauert, bis der Traffic dechiffriert ist: So wissen Sie, wie häufig Sie den Schlüssel wechseln müssen, um Angriffe mit Airsnort oder Aircrack ins Leere laufen zu lassen. Airsnort überwacht heimlich den W-LAN-Traffic und ermittelt den verwendeten Schlüssel, sobald es genügend Datenpakete gesammelt hat. Allerdings sind bei Traffic, der mit WEP 128 verschlüsselt wurde, bis zu 500 000 Datenpakete notwendig, die mit dem gleichen Schlüssel chiffriert wurden.

Airsnort erhalten Sie unter **http://sourceforge.net/projects/airsnort**. Damit Sie das Tool unter Windows nutzen können, benötigen Sie eine Reihe zusätzlicher Programmpakete: Falls Sie das Bildbearbeitungsprogramm GIMP installiert haben, sollten Sie über alle Pakete verfügen. Falls nicht, laden Sie sich von **www.gimp.org/~tml/gimp/win32/downloads.html** die aktuellen Pakete GTK, Glib, Pango und ATK herunter. Die Installation von Airsnort und der Pakete ist nicht ganz einfach. Am besten halten Sie sich an die Anleitung unter **http://airsnort.shmoo.com/win_setup.html**.

Mit Aircrack (**www.aircrack-ng.org**) können Sie nicht nur die WEP-Verschlüsselung, sondern auch WPA angreifen. Es besteht aus verschiedenen Modulen, die die bekannten Schwachstellen von WEP ausnutzen. Für Angriffe auf WPA setzt Aircrack auf Brute-Force-Attacken.

Aber denken Sie daran: Setzen Sie diese Tools nur in Ihrem eigenen W-LAN ein!

Der wirksamste Schutz eines drahtlosen Netzwerks besteht in seiner Verschlüsselung. Allerdings ist WEP – das schwächste Verschlüsselungsverfahren – nicht besonders sicher. Ein Angreifer mit dem entsprechenden Know-how und den richtigen Werkzeugen kann die WEP-Verschlüsselung knacken – sofern es ihm gelingt, genügend Netzwerktraffic zu protokollieren.

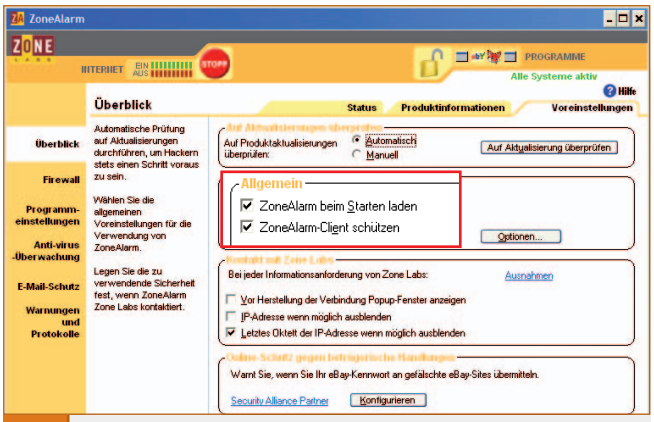
Die stärkeren Verfahren – WPA und WPA2 – dagegen gelten als sicher. Es ist derzeit keine Angriffsmethode bekannt, die WPA oder WPA2 knacken könnte. Unmöglich ist aber auch das nicht: Falls der verwendete Schlüssel schwach und leicht zu erraten ist, lässt sich auch WPA2 knacken.

Den bestmöglichen Schutz für ein Funknetz erreichen Sie, indem Sie alle möglichen Sicherheitsmaßnahmen kombinieren. Denn je mehr Hürden ein Angreifer überwinden muss, desto schwieriger wird es für ihn.

Franz Grieser

1 Status quo abfragen

Einen guten Überblick über die aktuelle Konfiguration Ihrer Firewall bietet die Registerkarte „Status“. Achten Sie an dieser Stelle darauf, dass die Firewall auf dem neuesten Stand der Dinge ist, und gehen Sie gegebenenfalls den abgewehrten Zugriffsversuchen nach. Auf dieser Registerkarte finden Sie außerdem eine Übersicht über die Anzahl der zugelassenen Programme und eine Information, ob bereits verdächtige Anhänge durch MailSafe geblockt wurden.

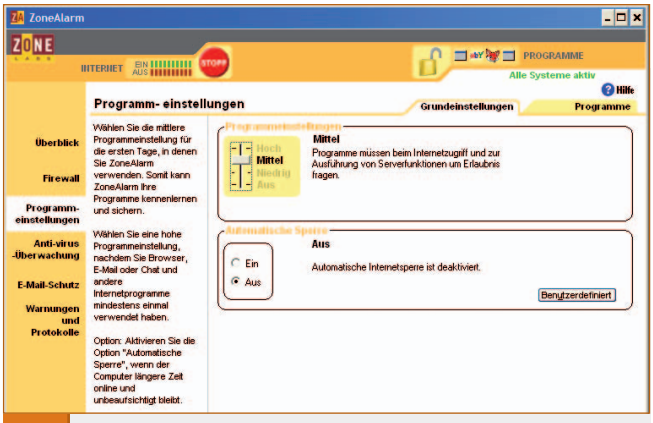


2 Voreinstellungen treffen

Damit Sie jederzeit mit der aktuellsten Version von ZoneAlarm arbeiten, sollten Sie die automatische Produktaktualisierung aktivieren. Laden Sie ZoneAlarm direkt beim Windows-Start, und schützen Sie den Client, damit er nicht von einem Angreifer ohne Ihr Wissen deaktiviert wird. Sind Sie häufig bei Ebay aktiv und verzichten auf den Einsatz der Ebay-Toolbar, kann auch ZoneAlarm Sie vor dem Diebstahl Ihres Auktions-Passworts schützen.

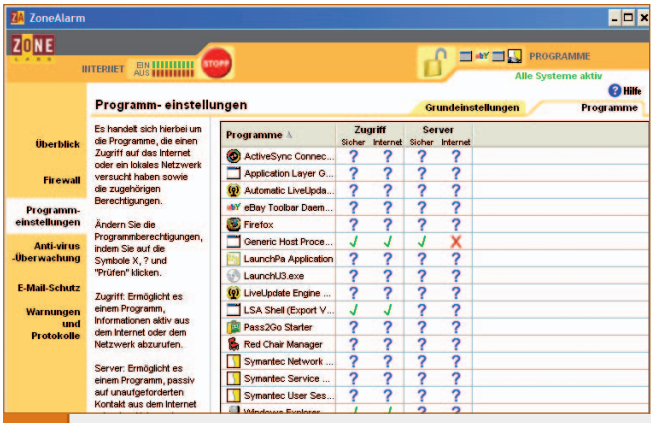
AUF DER HEFT-CD: ZONEALARM

Firewall richtig einstellen



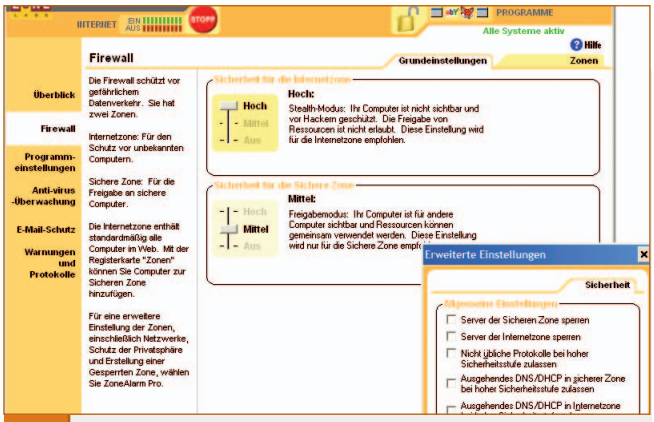
5 Zugriffsregeln für Programme

Damit keine Anwendung ohne Ihre Erlaubnis aufs Internet zugreift, bietet ZoneAlarm die Definition von Regeln an. Vordefinierte Verhaltensweisen geben Sie über die Programmeinstellungen ein. In dieser Version von ZoneAlarm ist maximal die Einstellung „Mittel“ möglich. Eine automatische Sperre der Kommunikation mit dem Internet sollten Sie aktivieren, wenn Ihr PC längere Zeit ohne Aufsicht läuft. Noch mehr Einstellungen können Sie unter „Benutzerdefiniert“ aktivieren.



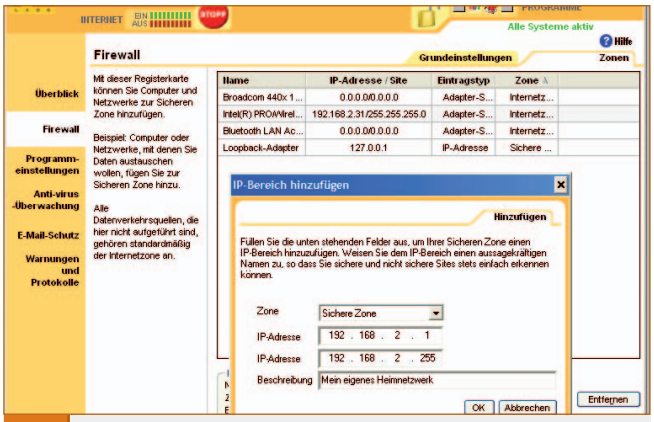
6 Programm-Freigaben ändern

ZoneAlarm analysiert zunächst alle laufenden Anwendungen, vergibt bei bekannten Diensten Standardwerte und fragt bei neu hinzugekommenen nach den zulässigen Aktionen. Auf der Registerkarte „Programme“ lässt sich die Freigabe eines Programms jederzeit ändern, indem Sie es aus der Liste löschen. Sie können aber auch andersherum entscheiden und Anwendungen manuell hinzufügen, indem Sie sie auf der Festplatte suchen und auswählen.



3 Sicherheitslevel festlegen

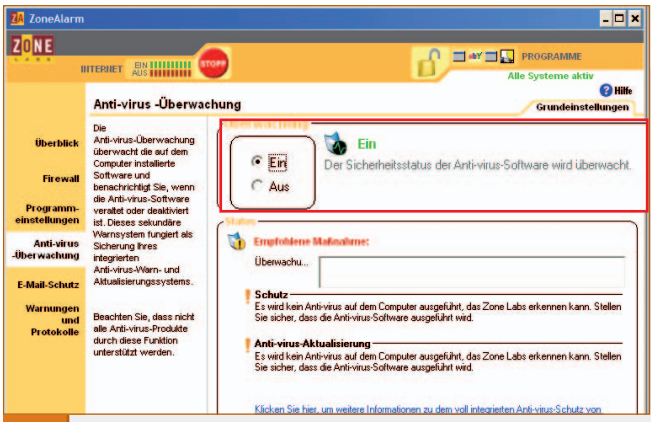
Sie konfigurieren ZoneAlarm zunächst über zwei Schieberegler. Die Sicherheit der „Internet Zone“ sollten Sie auf „Hoch“ setzen, um nach außen unsichtbar zu bleiben. Innerhalb der „Sicheren Zone“ haben Sie die Option, Ressourcen, etwa Drucker oder Laufwerke, freizugeben. In den erweiterten Einstellungen sollten Sie auf jeden Fall den Datenverkehr filtern, der über einen höheren Port als 1394 kommuniziert. Zum Schutz vor Phishing sollten Sie die Hosts-Datei sperren, sodass Angreifer keine Fälschungen eintragen können.



4 Sicherheitszonen definieren

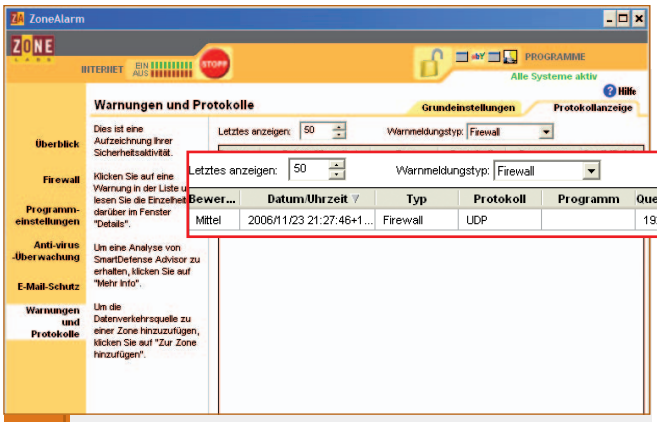
Wenn sich mehrere PCs in Ihrem Netzwerk Laufwerke teilen, sollten Sie an dieser Stelle sichere Zonen festlegen – entweder direkt für eine IP-Adresse oder für einen kompletten Bereich. Klicken Sie auf „Hinzufügen“ und wählen Sie:
Host / Site gibt einen Server über einen logischen Namen oder eine URL frei.
IP-Adresse erlaubt die Freigabe über eine IP-Adresse.
IP-Bereich ermöglicht das Einrichten einer sicheren Zone für mehrere PCs mit zusammenhängenden IP-Adressen.

Ihre Ausflüge ins Internet sollten Sie am besten mit einer Desktop-Firewall absichern. CHIP zeigt Ihnen in diesem Blitz-Workshop, wie Sie die kostenlose Firewall ZoneAlarm optimal konfigurieren und Sicherheitszonen für Netz-PCs einrichten.



7 Virenscanner integrieren

Manche Viren oder Trojaner schützen sich, indem sie unbemerkt den Virenscanner deaktivieren. Um dies zu unterbinden, lassen Sie Ihren Virenscanner von ZoneAlarm überwachen. Die Firewall meldet Ihnen, welcher Virenscanner auf Ihrem Rechner installiert und aktiv ist. Erscheint an dieser Stelle kein Eintrag, sollten Sie zunächst Ihren Virenscanner überprüfen und anschließend eine Komplettuntersuchung Ihres Rechners auf Malware starten.



8 Protokolle auswerten

Prüfen Sie die Einträge unter „Warnungen und Protokolle“ regelmäßig. Zwei Fälle sind besonders kritisch:
Ein unbekannter Rechner versucht wiederholt, via Internet eine Verbindung zu Ihrem PC aufzubauen. Achten Sie darauf, dass Ihre Firewall auf dem neuesten Stand ist.
Ein Programm auf Ihrem Rechner versucht, auf einen unbekannten Rechner im Internet zuzugreifen. Ist Ihnen das Programm nicht bekannt, sollten Sie Ihre Festplatte sofort von einem aktuellen Virenscanner überprüfen lassen.

DSL-ROUTER KONFIGURIEREN

Fritz!Box einrichten

Die Fritz!Box Fon ist DSL-Modem, DSL-Router, DHCP-Server, Firewall und Telefonanlage in einem und bietet schon beim Anschließen viel Sicherheit. Wie Sie das Gerät in einem Netzwerk einsetzen und per Web-Oberfläche mit jedem Betriebssystem einrichten, erfahren Sie in diesem Beitrag.

Dem Hersteller AVM ist mit der Fritz!Box Fon ein feiner Coup gelungen. Das Gerät arbeitet in jedem Netzwerk ohne Ansehen des Betriebssystems. Zum Konfigurieren brauchen Sie lediglich einen JavaScript-fähigen Internetbrowser wie beispielsweise Firefox oder den Internet Explorer. Sogar die Firmware-Updates können Sie direkt über das Gerät auf einen Computer laden und von dort installieren.

Über jeden PC, der mit der Fritz!Box verbunden ist, können Sie per DSL im Internet surfen. Mit angeschlossenen Telefonen (bis zu drei analoge und acht ISDN-Geräte) telefonieren Sie über das Internet – aber auch auf herkömmlichem Weg über Euro-ISDN oder das analoge Festnetz. Die Bandbreite fürs Telefonieren übers Web kann die Fritz!Box Fon automatisch verwalten, sodass eine konstante Sprachqualität gewährleistet ist.

Sie können die Fritz!Box per Netzwerkkarte, USB-Schnittstelle oder W-LAN mit einem oder mehreren Rechnern verbinden. Um das Gerät einrichten und nutzen zu können, müssen Sie die Netzwerkkarte so konfigurieren, dass sie ihre IP-Adresse automatisch vom Fritz!Box-DHCP-Server erhält.

Die Fritz!Box Fon 7050 hat auf der Rückseite außer den DSL-, USB- und Netzwerkbuchsen fünf Anschlussmöglichkeiten für analoge und ISDN-Endgeräte. In der W-LAN-Variante kommt außerdem eine Stummelantennne hinzu, und das Kästchen dient zusätzlich als Access Point.

AUF EINEN BLICK

DSL einrichten per Assistent: Wählen Sie den Internetprovider und geben Sie das Kennwort und den Benutzernamen für Ihre DSL-Verbindung ein.

1 Fritz!Box anschließen

Zuerst schließen Sie die Fritz!Box an das Stromnetz an, danach verbinden Sie sie mit dem DSL-Splitter. Falls Sie noch ein DSL-Modem besitzen, können Sie es abklemmen, da die Fritz!Box dessen Funktion übernimmt. Nun folgt der Anschluss ans ISDN- oder analoge Telefonnetz. Dazu stecken Sie das mitgelieferte ISDN/Analog-Kabel in die gleichnamige Buchse der Fritz!Box. Das andere Ende des Kabels kommt bei einem ISDN-Anschluss in den NTBA, bei analoger Telefonverbindung mit dem entsprechenden Adapter auf die F-Buchse des DSL-Splitters.

Damit Sie die Benutzeroberfläche der Fritz!Box Fon nutzen können, brauchen Sie eine Netzwerkverbindung per W-LAN, LAN oder USB von Ihrem PC zur Fritz!Box. Eine LAN-Verbindung kann auch über einen Switch oder Hub erfolgen; dazu stecken Sie das Netzwerkkabel in die Uplink-Buchse des Switchs oder Hubs.

2 DSL einrichten

Ist alles richtig angeschlossen, geben Sie „fritz.box“ in die Adresszeile eines Webbrowsers ein. Daraufhin erscheint die Oberfläche der Fritz!Box. Wählen Sie den „Einrichtungsassistent“, um den DSL-Zugang zu konfigurieren. Nach einem Klick auf „Weiter“ wählen Sie im folgenden Fenster aus der Liste Ihren Provider aus und tragen darunter die Internet-Zugangskennung und das Internet-Zugangspasswort ein. Danach legen Sie die Art der Verbindung fest – für einen Flatrate-Tarif können Sie an dieser Stelle etwa „Flatrate“ wählen. Ein Klick auf „Weiter“ zeigt die Verbindungsdaten noch einmal an; ein abermaliges „Weiter“ speichert die Daten und prüft die Internetverbindung. Nach dem nächsten „Weiter“ können Sie mit „Assistent jetzt beenden“ zur Eingangsmaske zurückkehren.

3 Firewall nutzen

Die Fritz!Box ist mit einer Firewall vor dem Zugriff von außen geschützt. Eine eigene Firewall auf den Client-Rechnern ist somit überflüssig – allerdings gilt das nur, wenn die Fritz!Box als DSL-Router und nicht als DSL-Modem genutzt wird.

Wie jede Firewall erlaubt auch die Fritz!Box die Freigabe für bestimmte Dienste. Wenn Sie beispielsweise einen Mail- oder Webserver betreiben, muss dieser von außen zugänglich sein. Das gilt auch für andere Programme wie etwa Filesharing-Anwendungen oder Software, die für das Netzwerk die Systemzeit mit einem Zeitserver synchronisiert. In solchen Fällen müssen Sie bestimmte Ports für eingehende Verbindungen freigeben. Ports dienen dazu, Serverdienste bei nur einer IP-Adresse unterscheidbar zu machen.

Ports geben Sie frei über „Internet | Portfreigabe“. An dieser Stelle sind bereits einige Anwendungen aufgeführt. Wollen Sie eine dieser Anwendungen freigeben, klicken Sie in der Liste der Portfreigaben links neben der gewünschten Anwendung

auf das Kästchen „Aktiv“ und danach auf „Übernehmen“.

Sind mehrere PCs mit der Fritz!Box verbunden, klicken Sie neben der Anwendung auf die Schaltfläche „Ändern“. Im folgenden Fenster tragen Sie die IP-Adresse des Computers ein, auf dem ein Port freigegeben werden soll. Aktivieren Sie die Option „Freigabe aktiv“, und klicken Sie auf „Übernehmen“.

Fehlt für eine bestimmte Anwendung ein Eintrag, legen Sie über den Button „Neue Portfreigabe“ eine weitere Portfreigabe an. Geben Sie ihr einen aussagekräftigen Namen, wählen Sie das nötige Protokoll und tragen Sie den Port ein, den Sie für Besucher aus dem Internet freigeben möchten. Anschließend tragen Sie die IP-Adresse des Rechners und den Port ein, den Sie im lokalen Netzwerk freigeben wollen. Aktivieren Sie wiederum die Option „Freigabe aktiv“, und klicken Sie auf „Übernehmen“.

4 Push-Service nutzen

Eine interessante Funktion für Administratoren ist der „Push-Service“, den Sie mit „System | Push Service“ aktivieren. Nun bekommen Sie von der Fritz!Box regelmäßig Mails mit Verbindungs- und Nutzungsdaten. Tragen Sie Ihre E-Mail-Adresse ein und darunter eine „E-Mail-Absenderadresse“. In der Liste „SMTP-Server“ wählen Sie Ihren E-Mail-Anbieter und tragen darunter die Anmeldedaten ein. Mit „Übernehmen“ speichern Sie die Einstellungen, mit „Test-E-Mail versenden“ können Sie überprüfen, ob Ihre Einstellungen korrekt sind.

5 Firmware updaten

AVM aktualisiert die Systemsoftware der Fritz!Box, sobald Fehler korrigiert wurden oder neue Funktionen hinzugekommen sind. Diese Updates besorgen Sie sich ganz einfach über „System | Firmware-Update“. Klicken Sie in der Registerkarte „Automatisches Update“ auf „Neue Firmware suchen“, um die Homepage des Herstellers AVM auf eine neue Version zu prüfen, die automatisch heruntergeladen wird. Eine Imagedatei auf der Festplatte können Sie über die Registerkarte „Firmware-Datei“ auswählen und anschließend über „Update starten“ aktualisieren. Da dieser Vorgang einigermaßen systemkritisch ist, sind sämtliche Telefon- und Internetverbindungen für die Dauer der Aktualisierung unterbrochen.

6 Strom sparen im W-LAN

Mit der Funktion „System | Nachtschaltung“ befördern Sie die Fritz!Box zu festgelegten Zeiten in den Ruhezustand. Über die Option „Nachtschaltung aktivieren“ tragen Sie eine Zeitspanne ein, in der die Nachtschaltung laufen soll. Schalten Sie auch die Option „Funknetz (WLAN) abschalten“ ein, wird auch das W-LAN während dieser Zeit ausgeschaltet – allerdings erst dann, wenn keine Funkverbindungen mehr zwischen den W-LAN-Netzwerkgeräten und der Fritz!Box bestehen. Diese Optionen reduzieren den Stromverbrauch der Fritz!Box. Möchten Sie nach Aktivieren der Nachtschaltung eine W-LAN-Verbindung nutzen, wählen Sie den Tastencode „#96*1*“ an einem Telefon, das an der Fritz!Box angeschlossen ist – zum Ausschalten des W-LAN dient der Tastencode „#96*0*“.

7 Netzwerk konfigurieren

Wenn Sie im Menü „System | Ansicht“ die „Expertenansicht“ eingeschaltet haben, erreichen Sie unter „System | Netzwerkeinstellungen“ auch die Funktion „IP-Adressen“. An dieser Stelle sollten Sie wegen der Datei- und Druckerfreigabe die Option „Alle Computer befinden sich im selben IP-Netzwerk“ eingeschaltet lassen. Schalten Sie die Funktion aus, können Sie bei den Verbindungen „LAN A“, „LAN B“, „USB“ und „WLAN“ eigene IP-Adressen für die Fritz!Box definieren.

Im Feld „IP-Adresse“ legen Sie für die Fritz!Box eine beliebige IP-Adresse fest; die Vorgabe ist „192.168.178.1“. Legen Sie eine neue fest, müssen die verbundenen PCs neu gestartet werden, sofern die Option „DHCP aktivieren“ eingeschaltet ist.

Tipp: Sie erreichen die Fritz!Box immer über die fest einprogrammierte IP-Adresse 192.168.178.254. Dafür müssen aber der PC und die Fritz!Box über dasselbe Netzwerk verbunden sein. Ändern Sie die IP-Einstellungen des Computers, indem Sie ihm die feste IP-Adresse 192.168.178.250 geben. Diese Adresse geben Sie dann in der Adresszeile Ihres Webbrowsers ein. Jetzt können Sie unter „System | Netzwerkeinstellungen“ die IP-Adresse prüfen, sofern Sie die „Expertenansicht“ eingeschaltet haben. Nach dem Prüfen und eventuellen Korrigieren der IP-Adresse stellen Sie auf Ihrem Rechner die ursprünglichen Werte wieder her.

Thomas Hümmler

PROFI-TIPP

DHCP: Client-PCs auf Empfang schalten

„DHCP“ steht für „Dynamic Host Configuration Protocol“. Mit DHCP ist es möglich, in einem Netzwerk IP-Adressen und weitere Parameter wie Netzmaske, Gateway und andere dynamisch und vor allem automatisch zuzuweisen. Das hat den Vorteil, dass Client-Rechner ohne zusätzlichen Konfigurationsaufwand in ein Netzwerk eingebunden werden können. Am Client selbst muss lediglich der automatische Bezug der IP-Adresse eingestellt werden.

Windows: Starten Sie die Systemsteuerung, und öffnen Sie darin die „Netzwerk- und Internetverbindungen“. Im folgenden Fenster klicken Sie auf das Applet „Netzwerkverbindungen“. Daraufhin öffnet sich ein weiteres Fenster mit dem Symbol „LAN-Verbindung“. Markieren Sie es, und wählen Sie links aus der Liste „Netzwerkaufgaben“ den Eintrag „Einstellungen dieser Verbindung ändern“. Nun öffnet sich der „Eigenschaften“-Dialog. Markieren Sie darin in der Liste „Diese Verbindung verwendet folgende Elemente“ den Eintrag „Internetprotokoll (TCP/IP)“, und klicken Sie darunter auf die Schaltfläche „Eigenschaften“. Im folgenden Dialogfenster wählen Sie auf der Registerkarte „Allgemein“ die Option „IP-Adresse automatisch beziehen“ und bestätigen mit „OK“. Danach schließen Sie alle geöffneten Dialoge und die Systemsteuerung.

SUSE Linux: In SUSE Linux starten Sie das Konfigurationstool YaST. Dort klicken Sie zunächst links im Menü auf „Netzwerkgeräte“ und danach rechts auf „Netzwerkkarte“. Die Netzwerkkonfiguration startet. Wurde die Netzwerkkarte nicht automatisch erkannt, müssen Sie sie an dieser Stelle noch „Konfigurieren“; danach können Sie das Modell angeben. Ist die Netzwerkkarte bereits erkannt und konfiguriert, klicken Sie auf die Schaltfläche „Ändern“, wählen die Karte aus und klicken auf „Bearbeiten“. Im Folgedialog wählen Sie „Automatische Adressvergabe (mit DHCP)“, danach „Weiter“ und anschließend „Beenden“.

INTERNET-BANKING

Sicherer Geldverkehr im Internet

Mal eben den Kontostand abfragen oder eine Überweisung tätigen – noch nie waren Geldgeschäfte so einfach. Damit dabei die Sicherheit nicht auf der Strecke bleibt, nennt CHIP die Fallen beim elektronischen Zahlungsverkehr und sagt Ihnen, worauf Sie beim Onlinebanking achten sollten.

AUF EINEN BLICK

Die Bankgeschäfte online zu erledigen ist für die meisten Menschen eine Selbstverständlichkeit geworden. Schließlich bieten die Finanzgeschäfte über das Internet eine Menge Vorteile: einfache Bedienung, keine Parkplatzsuche, keine Warteschlangen, ständige Verfügbarkeit – nur noch selten ist ein persönlicher Besuch in der Filiale nötig. Kein Wunder, dass mittlerweile fast drei Viertel aller Internetnutzer ihre Bankkonten online führen.

Allerdings ist mit der Verbreitung von Onlinebanking und Onlineshopping auch das Thema Sicherheit immer wichtiger geworden. Denn fast täglich werden in der Tagespresse Fälle publik, in denen raffinierte Betrüger versuchen, gutgläubige Onlinekunden bis aufs Hemd auszunehmen. Dabei ist Internet-Banking im Grunde genommen sicher – wäre da nicht der Risikofaktor Mensch. Doch wenn Sie sich an einige Grundsätze halten, bleibt Ihr Risiko überschaubar.

Was Sie selbst für sicheres Onlinebanking tun können

Fast alle Geldinstitute haben in den letzten Jahren viel unternommen, um Internet-Banking immer sicherer zu machen. Ob verschlüsselte Verbindungen, Kartenlesegeräte oder Streichlisten, die Sicherheitssysteme verhindern unbefugte Zugriffe auf die Konten – zumindest theoretisch. Denn für Bankgeschäfte über das Internet gilt dasselbe wie für den Einsatz der EC-Karte: Das ausgeklügeltste Sicherheitssystem bringt nichts, wenn die Anwender unvorsichtig sind.

Es ist schon merkwürdig: Die PCs vieler Bankkunden sind zwar technisch auf dem neuesten Stand – aber dem Thema Sicherheit schenken die User immer noch zu wenig Aufmerksamkeit: Ein regelmäßiges Update der Antiviren-Software etwa ist unerlässlich, um sich vor Malware-Angriffen zu schützen. Die Online-Adresse des Geldinstituts hat in der Favoritensammlung nichts zu suchen; Sie sollten sie immer manuell eingeben. Achten Sie vor jeder Transaktion darauf, dass die Webadresse mit „https“ beginnt.

Nach dem erstmaligen Login ins Internet-Bankingsystem sollten Sie unbedingt das zugewiesene Passwort ändern – und auf nahe liegende Begriffe wie den Namen Ihres Kindes oder das eigene Geburtsdatum verzichten. Schließen Sie vor dem Einloggen alle Programme und offenen Browserfenster.

Große Sicherheitsrisiken tun sich auf, wenn Sie Ihre Bankgeschäfte an öffentlich zugänglichen PCs, etwa in Bibliotheken oder Internetcafés, erledigen. Denn jede Onlinesitzung hinterlässt digitale Spuren, die sachkundige Benutzer nachträglich sichtbar machen können. Achten Sie penibel darauf, sich korrekt aus dem System auszuloggen und die während der Sitzung entstandenen temporären Dateien zu eliminieren.

Gefahrenquellen aus dem Internet ausschalten

Der weitaus größte Teil der Onlinebanker verwendet den Internet Explorer als Standardbrowser. Allerdings weist diese Software einige gravierende Sicherheitsmängel auf. Die Achillesferse des Microsoft-Browsers ist ActiveX – eine Technik, die ungefragt Software auf dem lokalen Rech-

KNOW-HOW

Phishing erkennen und abwehren

Vor gut einem Jahr war es noch recht einfach, Phishing-Mails zu erkennen. Die meisten waren in schlechtem Deutsch geschrieben, und die angebotenen Links sahen auch nicht gerade vertrauenswürdig aus. Doch die Tricks der Phisher nehmen an Raffinesse zu – und deshalb wird es immer schwerer, die Spreu vom Weizen zu trennen.

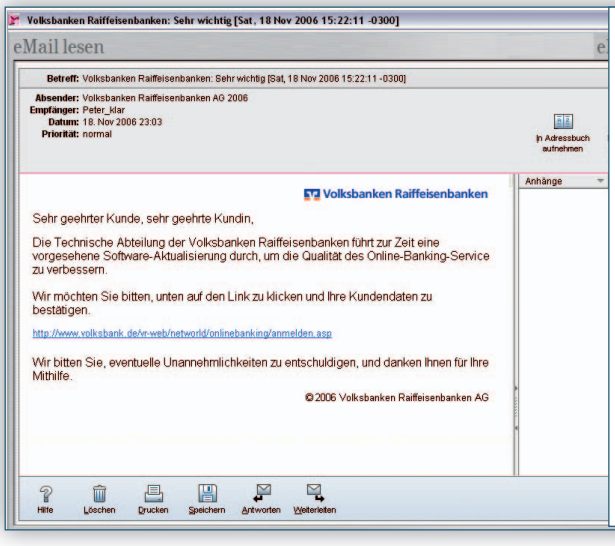
Phishing-Attacken erkennen

- In einer Phishing-Mail werden Sie unter einem Vorwand aufgefordert, einen Link anzuklicken und anschließend vertrauliche Angaben zu machen (etwa Kontonummer, Vertragsnummer, Passwort, PIN-Code oder Sicherheitsnummern).
- Achten Sie darauf, ob Sie in der E-Mail mit Vor- und Zunamen angesprochen werden. Ihr Geldinstitut kennt Ihren Namen, die Phisher meist nicht. Trotzdem ist eine korrekte Anrede noch kein Beweis für die Echtheit der Mail, denn die Namen lassen sich oft aus der E-Mail-Adresse ableiten.
- In der Betreffzeile oder im Mailtext tauchen meist Begriffe wie „Sicherheit“, „Datenpflege“ oder „Untersuchung von Unregelmäßigkeiten“ auf.
- Im Text stehen oft Sätze wie: „Ihr Konto wurde gesperrt“, „Ihre Kontoangaben müssen erneut bestätigt werden“, „Ihre Kreditkarte/Konto wurde gesperrt“ oder „Sie haben einen hohen Geldbetrag auf Ihrem Konto, bitte überprüfen Sie die Transaktionen“.
- In vielen Fällen wird auf die Dringlichkeit der Angelegenheit hingewiesen. Oft wird auch damit gedroht, dass Ihre Kontodaten „verloren gehen“ oder aber Ihr Konto ganz gesperrt wird, wenn Sie nicht unverzüglich handeln.
- Manchmal erkennen Sie an der schlechten Rechtschreibung oder fehlenden Umlauten, dass die Nachricht mit hoher Wahrscheinlichkeit nicht aus Deutschland stammen kann. (Beispiel: „Wir schaetzen hoch Ihr Business ein. Es ist uns ein Vergnuegen, Sie zu bedienen. Kundenunservice deutsche bank.“)

Phishing-Attacken abwehren

- Löschen Sie alle E-Mails, die Sie zur Eingabe persönlicher Daten auffordern.
- Öffnen Sie nie den Anhang einer E-Mail ohne vorherige Prüfung auf Viren, Würmer oder Trojanische Pferde – und schon gar nicht, wenn Sie den Absender nicht kennen. Ein guter Antiviren-Schutz ist heute ebenso unverzichtbar wie eine Firewall. Ganz wichtig: Aktualisieren Sie den Virenschutz regelmäßig.
- Alle Phishing-Mails enthalten Links oder Formulare. Diese Links führen auf gefälschte Websites (sogenannte Spoof-Sites), über die Ihre Daten an Betrüger gesendet werden. Am besten klicken Sie erst gar nicht auf den Link. Tun Sie es trotzdem, geben Sie auf keinen Fall persönliche Daten ein.
- Wenn Sie mit dem Mauszeiger über den Link fahren, können Sie die Zieladresse ablesen. Überprüfen Sie diese Adresse. Eine Abfrage bei einem Whois-Server (etwa **www.iks-jena.de/cgi-bin/whois**) bringt Ihnen Gewissheit. Steht der Rechner des Absenders zum Beispiel in Osteuropa, handelt es sich mit Sicherheit nicht um eine Nachricht Ihres Geldinstituts.
- Leiten Sie alle Phishing-Mails an Ihr Geldinstitut weiter, und melden Sie alle Ihnen verdächtig erscheinenden Vorkommnisse.

Tipp: Testen Sie, ob Sie gegen Phishing-Angriffe gefeit sind, und machen Sie den Mail-Frontier-Phishing-IQ-Test (**http://german.mailfrontier.com/survey/phishing_de.jsp**). Dabei sollen Sie unter zehn E-Mails die echten Phishing-Mails identifizieren.



Phishing-Mail: Offiziell und echt wirkende E-Mails sollen die Onlinebanking-Kunden dazu verleiten, vertrauliche Informationen von Internetbanking-Zugängen preiszugeben – vor allem Benutzernamen und Passwörter oder PIN und TAN.

→

ner installieren und ausführen kann. ActiveX-Steuerelemente können in Webseiten integriert sein, um etwa Multimedia-Stücke abzuspielen. Allerdings bietet diese Technik auch ein Schlupfloch für Viren oder Hacker, die dadurch Zugriff auf fremde Daten erhalten – einschließlich der Kontodaten.

Wer das ActiveX-Risiko ausschalten möchte, sollte deshalb auf die alternativen Webbrowser Firefox oder Opera umsteigen. Diese Gratisprogramme haben dem Internet Explorer in Sachen Sicherheit einiges voraus. So findet bei ihnen ActiveX keine Unterstützung. Zudem bieten sie standardmäßig einen Popup-Blocker, der das Öffnen nicht angeforderter Seiten unterbindet. Bei der alten Version des Internet Explorer lässt sich ein Popup-Blocker nur mit dem Service Pack 2 installieren. Beim Internet Explorer 7 ist der Popup-Blocker ebenfalls Standard.

Firefox: Die Schutzfunktion von Firefox 2 erkennt Phishing-Versuche anhand einer Datenbank.

Doch damit noch nicht genug. Bei nahezu allen Browsern bildet das sogenannte Cross-Site Scripting ein großes Sicherheitsrisiko – eine auf JavaScript basierende Technik (einen ausführlichen Beitrag dazu lesen Sie ab 70). Cross-Site Scripting gibt Betrügern die Möglichkeit, Ihren Browser zu manipulieren, um etwa Passwörter zu fischen (daher der Name „Phishing“, siehe Kasten auf 87). Um sich vor Cross-Site Scripting zu schützen, können Sie das Ausführen von JavaScript deaktivieren. Beim Internet Explorer geht das im Menü „Extras“ unter „Internetoptionen“. Bei Firefox lässt sich JavaScript unter „Extras | Einstellungen | Web-Features“ ausschalten. Dort entfernen Sie das Häkchen bei „Javascript aktivieren“. Es kann allerdings passieren, dass Sie bei deaktiviertem JavaScript nicht mehr auf Ihr Onlinebanking-Konto zugreifen können. Außerdem verzichten Sie mit der Deaktivierung von JavaScript auf Surfkomfort: Schöne Menüs oder Galerien sind dann eventuell nicht mehr nutzbar.

Misstrauisch bleiben: Die Attacken der Passwort-Fischer

Moderne Betrüger beschränken sich allerdings nicht auf das Internet. So kann es durchaus auch ein persönlicher Kontakt etwa via Telefon sein, bei dem sich der Betrüger als Mitarbeiter Ihres Geldinstituts ausgibt, um so an Ihre persönlichen Daten zu gelangen.

Am häufigsten starten Phishing-Attacken – „Phishing“ ist ein Kunstwort aus „Password fishing“ – jedoch über eine fingierte E-Mail mit einem Link zu der angeblichen Website des Finanzdienstleisters. Mit Aufforderungen wie „Bitte prüfen Sie umgehend Ihren Onlinebanking-Zugang!“ werden die Kunden auf eine Webseite der Betrüger gelockt. Die E-Mails sind so formuliert, dass ein seriöser Eindruck entstehen kann, der Absender ist jedoch gefälscht.

Die Phishing-Betrüger gehen immer raffinierter vor, um an persönliche Daten zu gelangen. So werden zum Beispiel ähnlich klingende URLs („www.sparkassemeinort.net“) oder gefälschte Absenderangaben in E-Mails verwendet. Sehr häufig führen die Links in den Phishing-Mails zu Servern im Ausland, wo eine Strafverfolgung nur schwer oder überhaupt nicht möglich ist.

Doch damit ist die Phisher-Mafia mit ihrem Latein noch lange nicht am Ende.

PROFI-TIPPS

Onlinebanking: So gehen Sie kein Risiko ein

Das Internet ist immer so sicher, wie Sie es für sich einrichten. Beim Onlinebanking bleiben Sie auf der sicheren Seite, wenn Sie die folgenden Regeln beachten:

Allgemein

- Aktualisieren Sie das Betriebssystem regelmäßig. Sie verhindern so das Entstehen von Sicherheitslöchern.
- Benutzen Sie immer die aktuellste Browserversion.
- Verwenden Sie einen Virenschutz, und aktualisieren Sie ihn regelmäßig (automatische Aktualisierung empfehlenswert).
- Installieren und aktivieren Sie eine Firewall.
- Speichern Sie Ihre PIN und Ihre TANs niemals auf Ihrem Computer.
- Verwenden Sie nur Software aus vertrauenswürdiger Quelle.
- Schließen Sie bei Banking-Transaktionen alle anderen Anwendungen. Während dieser Zeit sollten Sie auch nicht chatten, Dateien downloaden oder im Web surfen.
- Sichern Sie Ihre Daten regelmäßig auf einem Wechseldatenträger.
- Wählen Sie ein sicheres Passwort: Es muss mindestens sechs Stellen aufweisen – bestehend aus zufällig aneinandergereihten Buchstaben, Zahlen und Sonderzeichen.
- Notieren Sie sich die Notfall-Telefonnummer Ihres Geldinstituts, damit Sie im Ernstfall auch außerhalb der Öffnungszeiten jemanden erreichen können.
- Überprüfen Sie regelmäßig (mindestens einmal im Monat) die Umsätze anhand der Kontoauszüge, und melden Sie verdächtige Buchungen sofort Ihrem Geldinstitut.

Beim Einloggen

- Schließen Sie alle Browserfenster, und öffnen Sie erst danach ein neues Fenster.
- Geben Sie die URL in der Adresszeile des Browsers manuell ein; klicken Sie nicht auf Links.
- Überzeugen Sie sich in der Adresszeile davon, dass die Adresse mit „https“ beginnt.
- Das Sicherheitsschloss in der Browserzeile muss sichtbar und geschlossen sein.
- Überprüfen Sie gegebenenfalls das Sicherheitszertifikat.

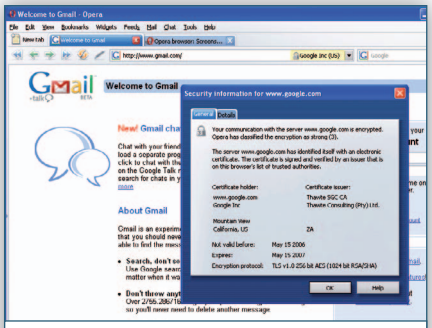
Nach dem Einloggen

- Öffnen Sie während der Transaktion kein zusätzliches Browserfenster.
- Erscheinen auffällige Fehlermeldungen, brechen Sie die Operation ab.

Nach dem Ausloggen

- Beenden Sie Ihre Onlinebanking-Sitzung grundsätzlich mit „Logout“.
- Löschen Sie anschließend den Cache und den Verlaufsspeicher Ihres Browsers.
- Schließen Sie das Browserfenster.

Extra-Tipp: Eine Möglichkeit, Onlinebanking ohne Angst vor Phishing-Angriffen zu betreiben, besteht in der Verwendung des signaturgestützten HBCI-Verfahrens mit einer Chipkarte. Diese Variante des Internet-Bankings ist darüber hinaus sehr komfortabel, da das Eingeben von TANs entfällt. Ein weiterer Sicherheitsgewinn ist die abgeschirmte PIN-Eingabe, bei der ein Belauschen der PIN-Eingabe mit einem Keylogger oder Trojaner nicht möglich ist. Voraussetzung dafür ist ein entsprechender Chipkartenleser mit eigenem PIN-Pad.



Opera: Eingeblendete Site-Informationen machen das Surfen mit dem Browser Opera deutlich sicherer.

Inzwischen haben die Betrüger einen Weg gefunden, Webseiten, die in einem neuen Browserfenster geöffnet werden, zu manipulieren – das sogenannte „Phishing mit Fenstern". Das ist möglich, wenn Sie vorher etwa auf einen präparierten Link aus einer Phishing-Mail geklickt haben. Dabei wird die gefälschte Seite des Angreifers versteckt im Hintergrund geladen. Wenn Sie nun auf einen Link klicken, der ein neues Browserfenster öffnet, dann öffnen Sie die manipulierten Inhalte im neuen Fenster.

Wichtiger Tipp: Bevor Sie sich mit Onlinebanking-Transaktionen beschäftigen, schließen Sie Ihren Webbrowser, und starten Sie ihn neu.

Mit dem sogenannten „Pharming" haben sich die Internetbetrüger einen neuen Phishing-Trick einfallen lassen, um an Ihre persönlichen Onlinebanking-Daten zu gelangen. Dazu versenden sie E-Mails mit Scripting-Code, der die Hosts-Datei von Windows-Rechnern manipuliert. Die Hosts-Datei ist eine lokale Textdatei für die Zuordnung von Hostnamen und IP-Adressen. Sie wird beim Aufruf einer Internetseite im Webbrowser zuerst abgefragt. Nur wenn der angefragte Hostname in der Hosts-Datei fehlt, bemüht Windows einen DNS-Server, um die IP-Adresse zu ermitteln.

Ein Beispiel: Wenn Sie in der Eingabezeile des Browsers „www.sparkasse-irgendwo.de" eingeben, wird die URL-Adresse in eine numerische IP-Adresse wie etwa 180.12.92.155 umgewandelt. Mit dem Scripting-Code aus der Pharming-Mail wird in der Hosts-Datei eine IP-Adresse eingetragen, die auf einen präparierten Server des Betrügers verzweigt. Selbst wenn Sie dem Link nicht folgen und statt dessen die URL per Hand eingeben oder aus der Favoritensammlung aufrufen, landen Sie durch diesen Trick der Angreifer auf der falschen Seite. Der Einsatz von aktuellen Virensignaturen oder das Deaktivieren des Windows Scripting Host können vor Pharming schützen.

Tipp: Über wichtige Neuigkeiten zum Thema „Datensicherheit im Internet" informiert Sie ein Newsletter des Bundesamts für Sicherheit in der Informationstechnik (BSI) unter **www.bsi.bund.de** oder **www.buerger-cert.de**.

Von Phishern ausgetrickst? Was Sie jetzt tun müssen

Wenn Sie glauben, dass Sie Ihre Kontodaten auf einer gefälschten Website (Spoof-Site) eingegeben haben, müssen Sie schnell handeln. Setzen Sie sich sofort mit der Hotline Ihrer Bank oder Ihres Kreditkartenunternehmens in Verbindung. Sie sollten außerdem unverzüglich Ihre PIN-Nummer ändern und die Liste Ihrer TANs, der Transaktionsnummern, sperren lassen. Werden trotzdem Beträge von Ihrem Konto oder Ihrer Kreditkarte abgebucht, fordern Sie Ihr Geldinstitut oder Ihr Kreditkartenunternehmen auf, die Buchungen schnellstens rückgängig zu machen. Speichern Sie die Phishing-Mail, und erstatten Sie danach Strafanzeige bei der nächsten Polizeidienststelle.

Wer haftet, wenn die Phisher zugeschlagen haben?

Auch wenn Phishing-Attacken im Internet schon seit geraumer Zeit stattfinden, ist die Frage der rechtlichen Haftung noch keineswegs entschieden. Einschlägige Gerichtsurteile stehen noch aus. Die Allgemeinen Geschäftsbedingungen (AGB) der Kreditinstitute enthalten in Sachen Onlinebanking nur die Bestimmung, dass die Weitergabe der PINs und TANs an Dritte nicht fahrlässig ermöglicht werden darf.

Doch wie ist die Rechtslage, wenn es einem Angreifer gelingt, auf dem Rechner des Bankkunden ein Schadprogramm zu installieren, das die Konvertierung der IP-Adresse so manipulieren kann, dass der Kunde zwar sorgfältig seine Bankadresse eingibt, aber trotzdem unbemerkt auf einem feindlichen Server landet, wo er Betrügern seine Daten preisgibt? Die Frage, ob in solchen Fällen auch von Fahrlässigkeit auszugehen ist, dürfte zu ausgedehnten juristischen Diskussionen führen.

PROFI-TIPPS

Was Sie nie tun sollten

Ein Angreifer ist nur erfolgreich, wenn er in irgendeiner Weise Zugang zu Ihrem Computer erhält – sei es beim Surfen im Internet, beim Herunterladen von Dateien, über E-Mail oder externe Datenträger. Damit Sie nicht zum Opfer von Datenfischern werden, sollten Sie den folgenden Risiken grundsätzlich aus dem Weg gehen.

- Geben Sie niemals – weder persönlich noch telefonisch oder per E-Mail – Ihre Zugangsdaten beziehungsweise PIN- und/oder TAN-Nummern preis. Keine seriöse Bank wird Sie danach fragen.
- Im Internet finden Sie viele verlockende Angebote. Nicht alle halten, was sie versprechen – im Gegenteil: Schadprogramme (Viren, Würmer, Trojanische Pferde) verbergen sich mit Vorliebe hinter einer attraktiven Verpackung.
- Wer eine E-Mail von seiner Bank erhält, sollte grundsätzlich misstrauisch sein. Allerdings setzen immer mehr Banken auf moderne Kommunikationsmedien; daher ist nicht jede E-Mail einer Bank notwendigerweise eine Fälschung.
- Starten Sie Online-Transaktionen niemals auf einem fremden Rechner – und schon gar nicht, wenn er in einem Internetcafé steht.
- Führen Sie niemals ein sogenanntes Sicherheits-Update für das Internet-Banking aus, wenn man Sie per E-Mail dazu auffordert. Banken und Sparkassen verschicken solche Updates nie per E-Mail. Schauen Sie auf der Homepage Ihres Geldinstituts nach, ob dort auf ein solches Update hingewiesen wird.
- Brechen Sie die Online-Transaktionen sofort ab, wenn das Schloss-Symbol in der Statuszeile des Browsers nicht geschlossen ist. Dies weist darauf hin, dass die Verbindung nicht verschlüsselt ist.
- Unerwartete Gutschriften auf dem eigenen Konto sollten Sie extrem misstrauisch machen. Lassen Sie sich nicht vorschnell auf Rücküberweisungen ein – schon gar nicht an andere Konten als an das, von dem die Überweisung kam.

Foto: ampelmann.de

Für den Onlinebanking-Kunden ist vor allem eines wichtig: dass sein Rechner vor Angriffen von außen geschützt ist – durch aktuelle Virenscanner, eine Firewall und regelmäßige Updates des Betriebssystems.

Peter Klau

AKTENVERNICHTUNG AM PC

Vertrauliche Daten sicher löschen

Das Löschen aller Dateien und das Leeren des Windows-Papierkorbs reichen nicht aus, wenn Sie Ihre Hardware verkaufen wollen: Denn Ihre Dokumente lassen sich schnell wiederherstellen – und das kann peinlich oder teuer werden. So stellen Sie sicher, dass Ihre Daten wirklich weg sind.

AUF EINEN BLICK

→ Daten rückstandslos löschen

Alle Tools auf CD

DBAN: Löscht rückstandslos komplette Festplatten ◎ Security

TrueCrypt: Verschlüsselt zuverlässig Ihre persönlichen Daten ◎ Security

Weder das Löschen von Dateien noch das Formatieren einer Festplatte entfernt die Daten restlos vom Datenträger: Zwar wird das Inhaltsverzeichnis bereinigt, sodass die Dateien für den Nutzer nicht mehr sichtbar sind. Die Daten selbst aber bleiben auf der Platte und lassen sich mit Spezialwerkzeugen wiederherstellen. Das gilt nicht nur für Festplatten, sondern auch für USB-Sticks, Speicherkarten und Handys (lesen Sie dazu den Beitrag ab 94).

Eine Software, die Daten wirklich sicher von einem Datenträger entfernen soll, muss zwei Anforderungen erfüllen:

- Sie muss die Daten oft genug mit Zufallsdaten überschreiben.
- Sie muss die freien Bereiche auf dem Datenträger ebenfalls bereinigen können.

Gerade am zweiten Punkt scheitern viele Gratis-Tools, die sicheres Löschen versprechen – aber auch eine Reihe von kommerziellen Produkten. Die in diesem Beitrag vorgestellten Tools beherrschen jedoch das Löschen der freien Bereiche.

Darüber, wie oft die Cluster überschrieben werden müssen und mit welcher Art von Daten, gehen die Meinungen auseinander. So gibt es eine ganze Reihe von Standards, die von amerikanischen,

Foto: CHIPimages; Illustration: S. Schönberger

deutschen oder auch russischen Behörden empfohlen werden. Der bekannteste und von fast allen Löschtools unterstützte ist der Standard 5220.22-M des US-Verteidigungsministeriums, der allerdings nicht als ausreichend für als „Secret“ oder „Top Secret“ eingestufte Dokumente gilt. Er arbeitet mit drei Überschreibungen: im ersten Durchlauf mit einem fest vorgegebenen Wert, im zweiten mit einem Zufallswert und im dritten mit dem Komplementärwert des ersten. Als absolutes Minimum gilt heute die Weiterentwicklung 5220.22-M ECE, die sieben Überschreibungen vorsieht.

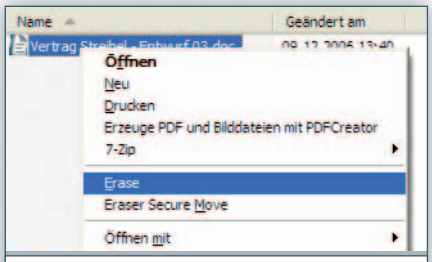
Wer noch gründlicher vorgehen will, sollte auf das von Peter Gutmann vorgeschlagene Verfahren setzen (**www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/**). Dabei werden sämtliche bekannten Bitmuster, die zur Speicherung auf der Festplatte verwendet werden können, hintereinander geschrieben und somit das Signal derart verrauscht, dass eine Rekonstruktion der Daten fast unmöglich ist. Das Gutmann-Verfahren sieht allerdings 35 Durchläufe vor, was bei großen Dateimengen ziemlich lange dauern kann.

Zum sicheren Löschen von geheimen Daten bei Militär oder Regierung ist übrigens keines der genannten Verfahren zugelassen. Behörden und Geheimdienste vertrauen ausschließlich auf einen Degausser – also ein Gerät, das die Daten mittels Magnetfeld löscht, oder auf die Zerstörung der Platte.

Gratis: Die besten Tools zum Platteputzen

Aus der Flut an kommerziellen und kostenlosen Löschtools für Windows stellen wir Ihnen auf den nächsten Seiten zwei Gratisprogramme vor, deren Quelltext frei zugänglich ist. Denn bei sicherheitskritischen Aufgaben sind Tools vertrauenswürdiger, deren Quelltext man ansehen und die man – wenn man besonders sicherheitsbewusst (um nicht zu sagen paranoid) ist – auch selbst kompilieren kann. Beide Tools sind seit einigen Jahren auf dem Markt und weit verbreitet – bisher ist bei keinem eine Schwachstelle oder Hintertür bekannt.

Das Löschtool mit dem besten Ruf in der Sicherheitsszene heißt Eraser und stammt von der irischen Firma Heidi Computers (**www.heidi.ie/eraser/**, auf Heft-CD). Damit löschen Sie Dateien und Ordner, die unter Windows 9x/ME/NT/2000 und XP oder unter DOS gespeichert wurden, sowie die „freien“ Bereiche auf dem Datenträger. Es unterstützt die gängigen Löschverfahren (Gutmann, 5220.22-M) und lässt sich außerdem zum Bereinigen der gesamten Festplatte nutzen. Der Eraser arbeitet mit dem gleichen Verfahren wie Darik's Boot and Nuke (siehe 93).



Unwiederbringlich löschen: Eraser lässt sich bequem aus dem Kontextmenü des Explorers für Dateien und Ordner aufrufen.

Rufen Sie das Tool über den Explorer auf, und klicken Sie die zu löschende Datei oder einen überflüssigen Ordner mit der rechten Maustaste an. Danach markieren Sie im Kontextmenü den Befehl „Erase“, stellen das Löschverfahren ein (Eraser merkt sich die Einstellungen für die nächsten Löschaktionen) und bestätigen, dass gelöscht werden soll. Im Kontextmenü finden Sie auch noch einen Befehl zum rückstandslosen Verschieben von Dateien und Ordnern.

Sie können den Eraser aber auch über das Startmenü aufrufen. In diesem Fall haben Sie zusätzliche Möglichkeiten: So können Sie etwa über den Scheduler festlegen, dass ausgewählte Dateien oder Ord- →

KNOW-HOW

Warum einfaches Löschen nicht ausreicht

Ein kurzer Exkurs in die physikalische Beschaffenheit der Speichermedien soll deutlich machen, was beim Speichern und Löschen im Einzelnen passiert: Die Daten werden auf einer Festplatte in binären Sequenzen von 1 und 0 gespeichert; die Sequenzen wiederum werden von unterschiedlich magnetisierten Teilen einer Festplatte repräsentiert. Dabei wird eine 1, die auf die Festplatte geschrieben wurde, vom Controller auch als 1 gelesen; für eine 0 gilt das Gleiche. Wird jedoch eine 0 mit einer 1 überschrieben, dann ist das Ergebnis nicht eine volle 1, sondern nur 0,95. Ebenso ist das Ergebnis beim Überschreiben einer 1 mit einer weiteren 1 nicht eine ganze 1, sondern durch die Verstärkung des Magnetismus etwas größer, etwa 1,05. Im Alltag ist dieser minimale Unterschied irrelevant – die Werte werden korrekt interpretiert.

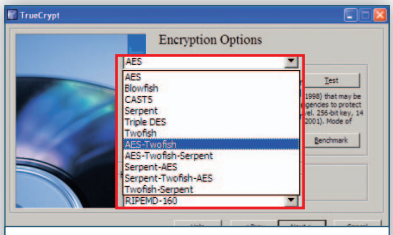
Gelöschte Daten auslesen: Wenn jedoch jemand mit dem richtigen Equipment und Know-how eine gelöschte Festplatte in die Hände bekommt, kann er die „unter“ den aktuellen Daten liegenden Schichten auslesen. So lässt sich beispielsweise aus dem Wert 0,95 die vorher dort gespeicherte 0 rekonstruieren. Und nicht nur das: Auch die noch tiefer liegenden Datenschichten lassen sich mit entsprechendem Aufwand wiederherstellen, wenn man die Magnetisierung der Festplatten-Sektoren und der übrigen Spuren analysiert. Allerdings wird die Rekonstruktion umso schwieriger, je häufiger die Daten überschrieben wurden. Nach wie vielen Überschreibungen eine Wiederherstellung nicht mehr möglich ist, darüber gehen die Meinungen auseinander. Verschärft wird die Sicherheitslage durch ein weiteres Problem: Daten verbergen sich auch an Stellen, auf die der Benutzer keinen direkten Zugriff hat – und zwar an den sogenannten Cluster-Tips oder in als defekt markierten Clustern.

Gefahr durch große Cluster: Eine Festplatte wird beim Formatieren in Cluster, die kleinste Speichereinheit, unterteilt. Bei einer Clustergröße von beispielsweise 64 KByte belegt selbst eine nur 2 KByte große Datei im Inhaltsverzeichnis die vollen 64 KByte – die restlichen 62 KByte bleiben ungenutzt. Das ist zwar Platzverschwendung, fällt aber bei den heutigen Festplattengrößen nicht ins Gewicht. Problematisch wird es, wenn zum Beispiel eine 60 KByte große Datei gelöscht und in diesen Cluster eine kleinere Datei geschrieben wird, die vielleicht nur 1 KByte belegt. Dann bleiben die über das neu geschriebene KByte hinausgehenden 59 KByte der gelöschten Datei weiter auf dem Datenträger und lassen sich mit einem Disk-Editor rekonstruieren. Das gilt nicht nur für Dateien, die kleiner als die Clustergröße sind, sondern auch für die Daten im jeweils letzten Datenblock von Dateien. Auch in als defekt markierten Clustern überleben Datenreste, ohne dass man darauf mit den Bordmitteln des Betriebssystems Zugriff hätte – in einem Speziallabor dagegen lässt sich ein Zugriff noch ermöglichen.

PROFI-TIPP

Ordner und USB-Sticks verschlüsseln

TrueCrypt verschlüsselt Dateien, Ordner, ganze Partitionen (außer der Boot-Partition) und Speichermedien wie etwa USB-Sticks. Dazu stehen die derzeit als nicht knackbar geltenden Algorithmen AES, Blowfish und weitere zur Verfügung. TrueCrypt legt eine Containerdatei an, in der es die chiffrierten Dateien speichert. Dieser Container steht im Betriebssystem als eigenes „Laufwerk“ zur Verfügung, ist aber nur für den zugänglich, der das TrueCrypt-Kennwort kennt.



Daten-Tresor: TrueCrypt kann Ihre Dateien mit Algorithmen wie Blowfish oder AES-Twofish verschlüsseln.

ner regelmäßig, beispielsweise an einem bestimmten Wochentag, bereinigt werden sollen. Ebenso können Sie vor dem Herunterfahren des Rechners automatisch die Windows-Auslagerungsdatei löschen lassen – denn aus dieser Datei kann man unter Umständen die zuletzt bearbeiteten Daten rekonstruieren (das Bereinigen der Swap-Datei empfiehlt sich, wenn Sie Ihre Dokumente durch Verschlüsselung vor neugierigen Augen schützen).

Wenn Sie sich live davon überzeugen wollen, dass eine vertrauliche Datei wirklich nicht mehr zu lesen ist, können Sie über „Start | Eraser“ den Befehl „Eraser Verify“ aufrufen. Dazu wählen Sie die Datei und die Bereinigungsoptionen aus und lassen die Sektoren, die die Datei belegt, von den Zufallsdaten überschreiben – nach jedem Durchlauf zeigt Eraser dann den aktuellen Inhalt der Sektoren an.

Nummer sicher: Auch nicht belegte Sektoren bereinigen

Falls Sie häufig mit Ihrem Notebook unterwegs sind und verhindern wollen, dass nach einem eventuellen Diebstahl Ihre vertraulichen Daten auf der Festplatte rekonstruiert werden können, sollten Sie den Befehl „Erase“ nicht nur auf nicht mehr benötigte Dateien anwenden, sondern regelmäßig auch die nicht belegten Sektoren auf der Platte bereinigen. Aus diesen lassen sich nämlich auch längst gelöschte Daten wiederherstellen. Außerdem sollten Sie die ganze Festplatte – oder doch zumindest die wichtigsten Dokumente – mit einem Tool wie TrueCrypt verschlüsseln.

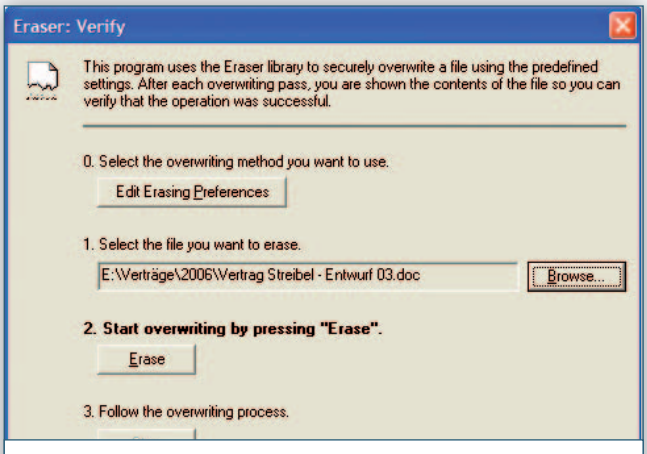
Zum Löschen der nicht belegten Sektoren rufen Sie den Eraser über das Startmenü auf. Stellen Sie über den Befehl „Edit | Preferences | Erasing“ auf der Registerkarte „Unused Disk Space“ die Bereinigungsoptionen ein: Wenn Sie die nicht belegten Sektoren regelmäßig bereinigen, reicht es, sie jeweils einmal mit „Pseudorandom Data“ überschreiben zu lassen. Aktivieren Sie aber in jedem Fall noch die drei Optionen „Free Disk Space and Master File Table Records“, „Cluster Tip Area“ und „Directory Entries“. Danach rufen Sie den Befehl „File | New Task“ auf, aktivieren „Unused space on drive“ und wählen das Laufwerk aus. Anschließend geben Sie auf der Registerkarte „Schedule“ an, in welchem Rhythmus und zu welcher Uhrzeit der Vorgang starten soll. Sorgen Sie schließlich über „Edit | Preferences | Scheduler“ dafür, dass der Scheduler beim Windows-Start automatisch aufgerufen wird.

SDelete: Rückstandslos löschen per Befehlszeile

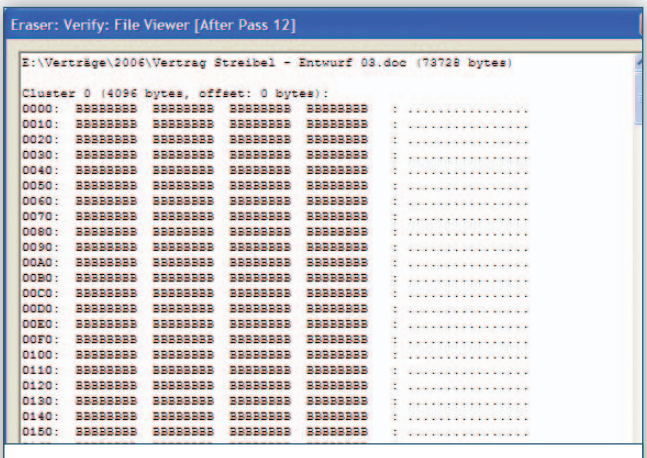
Ein zweites Windows-Programm, das Dateien unwiederbringlich löscht, bietet der inzwischen von Microsoft übernommene Tools-Spezialist Sysinternals an: SDelete (**www.microsoft.com/technet/sysinternals/utilities/SDelete.mspx**). Das Programm wird über die Befehlszeile aufgerufen und eignet sich somit gut für die Batch-Verarbeitung. Laut Sysinternals funktioniert SDelete unter Windows 9x/NT und 2000, im Test hat es aber auch unter Windows XP problemlos seinen Dienst verrichtet.

Eine ausführliche Dokumentation zu SDelete finden Sie unter der genannten Webadresse. Die beiden wichtigsten Schalter sind „-p“, wonach Sie die Anzahl der Durchläufe angeben (etwa „sdelete –p 35 vertrag.doc“), und „-s“, womit sich Unterverzeichnisse rekursiv löschen lassen.

SDelete ist praktisch, wenn Sie den Befehl in einer Batch-Datei nutzen wollen, um das Bereinigen zu automatisieren. Da sich das Löschen mit SDelete nicht



Datenvernichtung live: Wer sich davon überzeugen will, dass seine Daten wirklich nicht mehr wiederhergestellt werden können, kann Eraser Verify beim Überschreiben zusehen.



Restlos verschwunden: Nach jedem Durchlauf zeigt Eraser Verify an, mit welchem Wert die Sektoren überschrieben wurden. Diesen Vertrag kann niemand rekonstruieren.

mehr rückgängig machen lässt, sollten Sie dabei überlegt vorgehen.

Komplettlösung: Die ganze Festplatte säubern

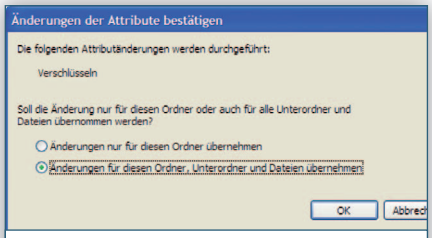
Wenn Sie den Inhalt einer ganzen Festplatte oder Partition sicher löschen wollen, greifen Sie am besten auf Darik's Boot and Nuke (DBAN) zurück, das Sie unter **http://dban.sourceforge.net** und auf der Heft-CD finden. Damit legen Sie eine Boot-Diskette oder -CD mit Linux-Kernel an, mit deren Hilfe Sie betriebssystemunabhängig einzelne Festplatten (IDE und SCSI) löschen können; auch die Installation auf Disketten oder USB-Sticks ist möglich.

Falls Sie eine Boot-Diskette mit DBAN anlegen wollen, ist es ausreichend, Eraser 5.8 zu installieren: Anschließend finden Sie im Startmenü von Windows im Eraser-Ordner den Befehl „Create Nuke Boot Disk", mit dem Sie eine Boot-Diskette erhalten.

DBAN stellt die wichtigsten Bereinigungsverfahren zur Auswahl, darunter 5220.22-M und Gutmann. Sämtliche Einstellungen und Aufgaben definieren Sie über eine übersichtliche Bedienoberfläche. Sie haben sogar die Möglichkeit, die Festplatten im Computer direkt nach dem Booten automatisiert zu löschen.

Als Alternative können Sie auch ein von CD oder DVD bootfähiges Linux nutzen, etwa Knoppix oder Ubuntu. An dieser Stelle geben Sie über die Befehlszeile das folgende Kommando ein:

```
dd if=/dev/zero of=/dev/hda
bs=64k
```



Bordmittel: Windows 2000 und XP Professional bringen mit EFS ein Verschlüsselungswerkzeug für Ordner und Dateien mit.

Der Befehl „dd" („Disk Dump") überschreibt die gesamte Festplatte mit Nullen („/dev/zero"). Dabei löschen Sie mit „hda" das Master-Laufwerk am primären IDE-Kanal. Falls Sie jedoch die Slave-Platte löschen wollen, geben Sie „hdb" statt „hda" ein.

Wenn Sie Ubuntu oder Kubuntu verwenden, setzen Sie die Anweisung „sudo" direkt vor den „dd"-Befehl (in der gleichen Zeile).

Daten verschlüsseln: Schutz vor neugierigen Blicken

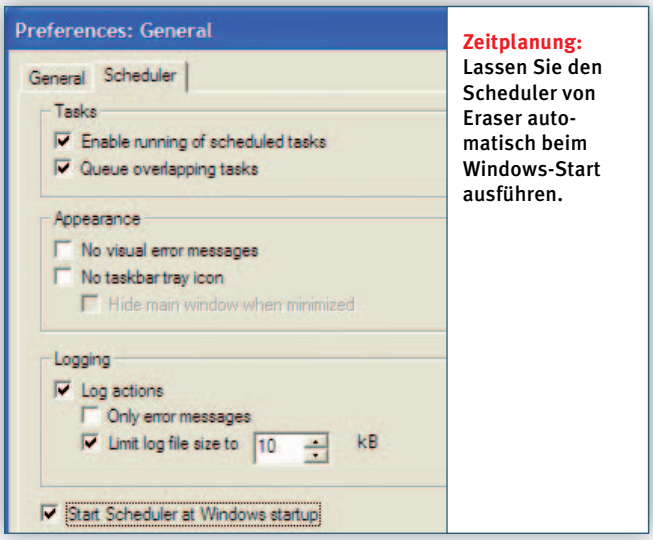
Insbesondere wenn sich andere Personen Zugang zu Ihrem PC verschaffen können, empfiehlt es sich, wichtige Dateien verschlüsselt auf der Festplatte abzulegen. Dann können nur Sie selbst als autorisierter Nutzer die Dateien dechiffrieren. Unter Windows 2000 oder XP Professional können Sie das im Betriebssystem integrierte Encrypting File System (EFS) nutzen und damit Dateien oder Ordner auf einer mit NTFS formatierten Festplatte verschlüsseln. Die Verschlüsselung ist transparent. Solange Sie also ordnungsgemäß in Windows 2000 oder XP Professional mit Ihrem Benutzerkonto angemeldet sind, entschlüsselt Windows chiffrierte Dateien, die Sie etwa mit einem Textprogramm öffnen, automatisch und verschlüsselt sie, sobald Sie sie speichern und schließen. Sie müssen also kein Kennwort eingeben – das haben Sie ja beim Windows-Start bereits getan.

Ein Unbefugter aber, der sich etwa mit einer Boot-Disk Zugang zur Festplatte verschafft hat, kann die chiffrierten Dateien nicht lesen. Er sieht zwar, welche Dateien vorhanden sind, doch ihr Inhalt ist für ihn nicht zu entziffern. Allerdings kann er die verschlüsselten Dateien auf eine CD oder einen USB-Stick kopieren und mitnehmen – etwa um in aller Ruhe an anderer Stelle zu versuchen, die Verschlüsselung zu knacken.

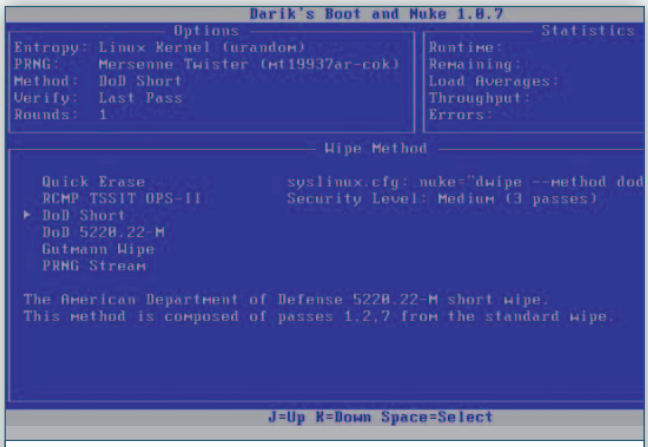
Das EFS nutzt den Verschlüsselungsalgorithmus DESX (Windows 2000 und XP) oder Triple-DES (XP) – allerdings gibt es bereits einige Tools, mit denen sich die Verschlüsselung von EFS-Containern knacken lässt. Das gilt nicht für die EFS-Verschlüsselung in Windows Server 2003, die den AES-Algorithmus nutzt – er gilt derzeit als nicht knackbar.

Eine Alternative zu EFS ist das kostenlose Verschlüsselungsprogramm TrueCrypt (**www.truecrypt.org**, auf Heft-CD), das sich auch unter Windows XP Home einsetzen lässt. TrueCrypt arbeitet nicht nur mit NTFS-Partitionen, sondern auch mit FAT 32 und bietet darüber hinaus eine breite Auswahl an starken Verschlüsselungsalgorithmen – darunter auch AES, sodass es, verglichen mit EFS, die bessere Wahl ist.

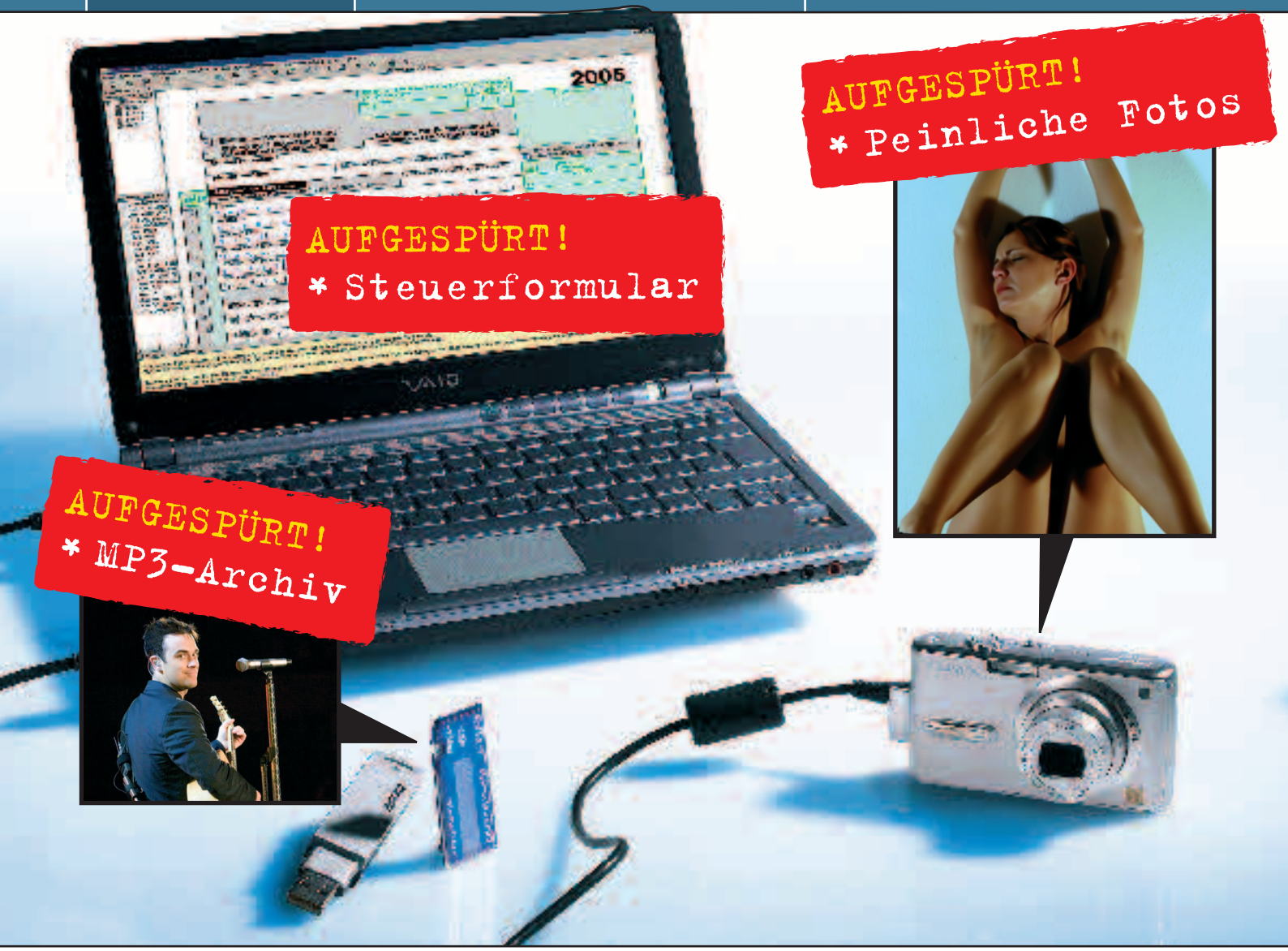
Franz Grieser



Zeitplanung: Lassen Sie den Scheduler von Eraser automatisch beim Windows-Start ausführen.



Platte richtig plattmachen: Darik's Boot and Nuke bietet die gleichen Bereinigungsoptionen wie Eraser – allerdings für die gesamte Festplatten-Partition.



WAS ALTE HARDWARE VERRATEN KANN

Datenreste finden

Alte Festplatten verkaufen und damit Geld machen – eine gute Idee. Doch viele versteigern mit ihrer Hardware ungewollt auch persönliche Daten. So vermeiden Sie peinliche Enthüllungen.

AUF EINEN BLICK

Alle Tools auf CD

Eraser: Löschen Sie alle Daten rückstandslos von Ihrem System ◎ Security

Restoration: Mit diesem Tool retten Sie gelöschte Dateien ◎ Security

Das Jahreseinkommen, Unterhaltszahlungen, Steuerklasse – das sind keine Informationen, die man gern an die große Glocke hängt. Und doch kommen so persönliche Daten wie die Steuererklärung recht häufig bei Ebay unter den Hammer. Denn mehr als 10 000 USB-Sticks, Festplatten, Speicherkarten und Mobiltelefone wechseln dort täglich den Besitzer. Besonderer Verkaufsschlager sind Festplatten: Etwa 1250 werden jeden Tag verscherbelt – und mit ihnen auch alle persönlichen Informationen, die sich noch darauf befinden: Steuererklärungen, Passwörter, intime Fotos und Videos oder auch vertrauliche Firmendokumente.

Die Vorbesitzer sind zwar fest davon überzeugt, sie hätten ihre Speicher vor dem Verkauf gelöscht. Haben sie ja auch. Doch „einfach“ gelöschte Daten lassen sich kinderleicht wiederherstellen. Dazu braucht man nur die passende Software, und die meisten Recovery-Tools gibt's sogar gratis im Web.

Foto: M. Miller; EMI Music; J. Willmann, Photocase.com

CHIP hat die Probe aufs Exempel gemacht und bei Ebay eingekauft – neben Festplatten und USB-Sticks auch Digicams, Speicherkarten und Handys. Die Neuerwerbungen haben wir dann intensiv unter die Lupe genommen – und waren überrascht, wie viele vertrauliche und leicht rekonstruierbare Daten sich darauf fanden. Urlaubsbilder, Raubkopien, ein kompletter SMS-Verkehr samt Telefonnummern, die eingangs erwähnte Steuererklärung – die Vorbesitzer gewährten einen tiefen Einblick in ihr Privatleben.

Bevor Sie also Ihre ausrangierte Hardware zu Geld machen oder entsorgen, sollten Sie sicherstellen, dass sich wirklich keine Daten mehr im Speicher befinden. Anstatt einfach die Festplatte zu formatieren, sollten Sie den kompletten Speicher überschreiben. Das dauert bei einer 200-GByte-Festplatte zwar mehrere Stunden, doch der Aufwand lohnt sich auf jeden Fall. Die passende Software dafür finden Sie auf der Heft-CD.

Lesen Sie nun, was wir auf der ersteigerten Hardware alles gefunden haben – und wie Sie den jeweiligen Speichertyp sicher löschen.

AUF FESTPLATTE & USB-STICK

Raubkopien, MP3-Archiv, Steuererklärung

Gelöschte Daten wiederherstellen – das ist für Recovery-Tools kein Problem. Ob von Festplatte oder USB-Stick, das macht für sie keinen Unterschied. Denn Platte und Stick haben die gleichen Dateisysteme (FAT oder NTFS), und Windows besitzt alle nötigen Schreibrechte für einen umfassenden Zugriff.

USB-Stick: Gebrauchte USB-Sticks sind preiswert – und als Datenquelle ganz schön ergiebig. Von vielen Sticks holten unsere Tools die gelöschten Files zurück, etwa MP3-Songs und raubkopierte Software. Problemlos klappte das etwa bei einem Q-Max-Stick mit 128 MByte: Zwar war alles gelöscht, aber schon ein kurzer Check mit dem Tool Restoration (auf Heft-CD) brachte 115 Files zum Vorschein. Von denen waren 41 noch intakt, bei den anderen handelte es sich um Einträge von teilweise überschriebenen Dateien. Unter den Fundstücken war auch eine lauffähige Raubkopie von WinDVD 7. Die konnten wir komplett extrahieren – ein lauffähiges neues Programm zum Nulltarif. Mit der mitgelieferten Datei „keygen.exe“ konnten wir auch noch die passende Seriennummer generieren.

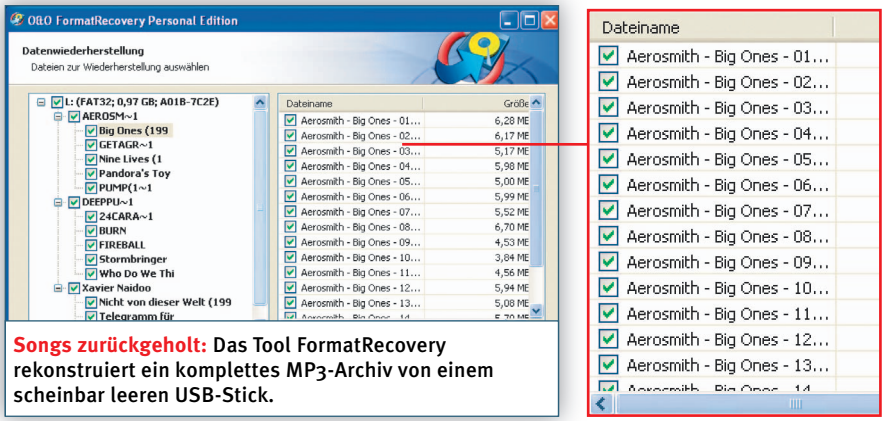
Etwas schwieriger auszulesen war ein 1-GByte-Stick der Marke Sharkoon. Ihn hatte der Vorbesitzer neu formatiert. Das Tool Restoration scheitert: Es macht keinen RAW-Scan und kann deshalb gelöschte Dateien nicht anhand eines Bitmusters oder einer Dateisignatur erkennen. Es ist vielmehr auf die als gelöscht markierten Einträge in der File Table angewiesen – und die ist nach einer Neuformatierung leer.

Wir haben deshalb auf das Spezialtool FormatRecovery (Demo-Version auf Heft-CD) zurückgegriffen, das sogar alle Dateinamen wiederherstellt. Einmal kurz drüberlaufen lassen, und schon waren alle Daten wieder präsent. Resultat: ein MP3-Archiv mit fast 170 Songs von Aerosmith bis Xavier Naidoo.

Festplatte: Beim Verkauf gebrauchter Harddrives scheint das Sicherheitsbewusstsein etwas ausgeprägter zu sein. Auf einer alten 80-GByte-Maxtor-Platte wurden wir trotzdem fündig. Wir schlossen sie ans IDE-Kabel an und sahen zunächst nichts: keine Daten drauf, alle Partitionen gelöscht. Doch ein Durchlauf mit „TestDisk“ ergab ein anderes Bild: Das Tool fand eine primäre Boot-Partition und drei logische Laufwerke in einer erweiterten Partition. Diese Platte wurde wohl einfach mit einem Partitionierungs-Programm oder dem entsprechenden Windows-Werkzeug „geleert“.

Gelöschte Laufwerke markiert TestDisk als „D“ wie „deleted“. Diese lassen sich aber mit dem Attribut „L“ für „logical“ ändern und über „Write“ wiederherstellen. Nach dem Neustart waren die Partitionen der Maxtor-Platte wieder sichtbar, die Daten aber noch nicht. Die hatte der Vorbesitzer zusätzlich gelöscht – schlau, aber nicht schlau genug. Denn nun läuft die Wiederherstellung wie gehabt: Recovery-Tool nehmen, analysieren und Daten wiederherstellen. Am besten ist der Zugriff von außen, ohne dass XP neu startet und Daten auf die Platte schreibt.

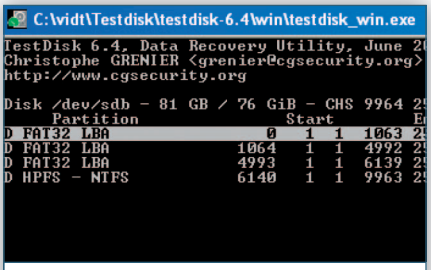
Also mit Linux booten – etwa mit Knoppix – und Freeware-Tools einsetzen →



Songs zurückgeholt: Das Tool FormatRecovery rekonstruiert ein komplettes MP3-Archiv von einem scheinbar leeren USB-Stick.

wie „fatback“ und „ntfsundelete“. Der Nachteil: Das geht nur per Kommandozeile – und gerade wenn viele Dateien zu rekonstruieren sind, kostet das Zeit. Deshalb haben wir uns für eine kommerzielle Linux-Software entschieden: Data Rescue von Prosoft (**www.prosofteng.com**). Die ist einfach zu bedienen – nach dem Motto „einlegen, booten, scannen“ – und hat den Vorteil, dass sie vor Hardware-Fehlern warnt: Dann einfach weiterzumachen kann nämlich zu Datenverlust führen. In einem solchen Fall kann Data Rescue die komplette Platte als Image klonen. Von dort aus werden die Daten wiederhergestellt. Das ist übrigens auch der Weg, den Rettungsprofis in der Regel gehen.

Nach dem Scan präsentierte Data Rescue Tausende alter Dateien: auf einer Partition etwa eine Raubkopie des Blockbusters „The Sixth Sense“, auf einer anderen die Imagedatei einer kompletten Windows-Installation – beides gab's beim Festplattenkauf also gratis dazu.



Partitionen entdeckt: Das Tool TestDisk spürt sogar gelöschte Laufwerke auf und macht sie sichtbar.

Noch wesentlich interessanter sind Dokumente, die persönliche Informationen über den Vorbesitzer preisgeben. Highlight unserer Recovery-Tour: Auf der Partition mit der Bezeichnung „Backup“ stießen wir auf mehrere PDF-Dokumente, darunter die komplette Steuererklärung für 2005. Der Ex-Besitzer der Maxtor-Platte hat sich extrem leichtsinnig verhalten!

So löschen Sie richtig: Nehmen Sie einen Datenvernichter wie den Eraser (siehe Kasten auf 97). Damit überschreiben Sie zuerst den sogenannten Freispeicher sowie sämtliche Datenverstecke. Im zweiten Schritt vernichten Sie dann die existierenden Ordner und Dateien. Noch mehr Informationen zum sicheren Löschen von Festplatten-Daten finden Sie im Beitrag ab 90.

AUF DIGICAM & SMARTCARD

Peinliche Selbstporträts, jede Menge Urlaubsfotos

Hobbyfotografen haben es mit zwei Speichern zu tun – dem internen in ihrer Digicam und einer Smart Card, etwa einer SD-Card oder einem Memory-Stick.

Digicam-Speicher: An dieser Stelle gibt es ein Problem. Denn der interne Speicher lässt sich in der Regel gar nicht überschreiben. Datenvernichter wie der Eraser funktionieren selten – als Windows-Programm fehlen ihm schlicht die Schreibrechte. Auf der Kamera selbst gibt es zwar eine Funktion zum Löschen der Bilder, aber die geht genauso vor wie Windows. Alle Daten sind also noch drauf, sie werden nur nicht mehr angezeigt. Daher wurden wir bei der frisch gekauften Nikon Coolpix L6 mit 16 MByte internem Speicher auch auf Anhieb fündig.

Den Zugriff vom PC aus erhielten wir ganz einfach über das USB-Kabel. Ein schneller Suchlauf mit dem aufs Wiederherstellen von Fotos spezialisierten Open-Source-Tool Photorec (im TestDisk-File auf der Heft-CD) förderte sechs hochauflösende JPEGs zutage – darunter ein wenig schmeichelhaftes Porträt des Vorbesitzers. Sein Glück: Anscheinend war die Kamera nicht oft in Gebrauch, sondern wurde gleich weiterverkauft, denn der interne Speicher war nur zur Hälfte gefüllt.

Smart Card: Ältere Kameramodelle haben keinen internen Speicher, sie legen die Fotos gleich auf einer Smart Card ab. Die von dort gelöschten Fotos wiederherzustellen ist ein Kinderspiel und funktioniert im Prinzip so wie bei einem USB-Stick. Auch das Dateisystem ist in der Regel dasselbe, nämlich FAT.

Wir konnten anhand einer gebrauchten Smart Card einen turbulenten Familien-

KNOW-HOW

Wie Daten sogar das Formatieren überleben

Löschen Sie eine Datei unter Windows, landet sie im Papierkorb. Wenn Sie den leeren, ist sie zwar unsichtbar, aber noch lange nicht vernichtet.

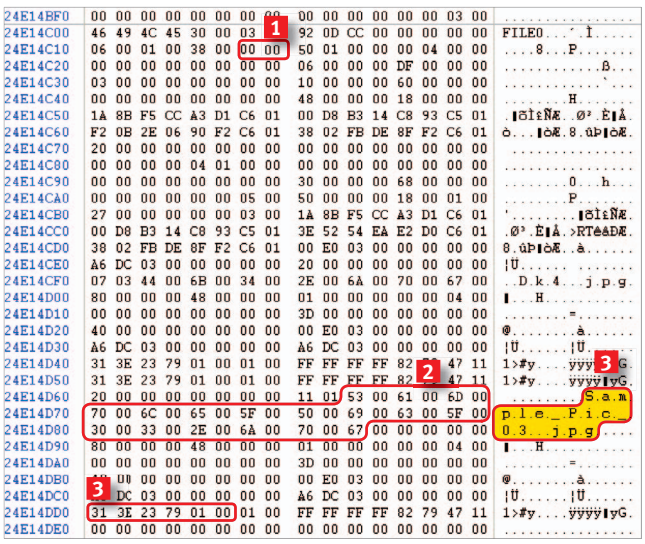
Einfacher Fall: Wirft Windows eine Datei aus dem Papierkorb, passiert Folgendes:

1 XP ändert in der Partitionstabelle zwei Bytes. Sie sagen: Dieses File ist gelöscht.

2 Alle anderen Werte bleiben erhalten, beispielsweise der Dateiname.

3 Deshalb kann ein Recovery-Tool in der Partitionstabelle einfach auslesen, in welchen Clustern sich die Daten befinden. Dieser Bereich nennt sich „Dataruns“ und enthält Informationen darüber, auf wie viele Cluster sich die Daten erstrecken, in wie viele Fragmente sie aufgeteilt sind und auf welchem Cluster die Datei beginnt. Damit kann ein Recovery-Tool jede Datei wiederherstellen.

Schwieriger Fall: Komplizierter wird es, wenn Windows den Eintrag in der Partitionstabelle wieder überschrieben hat oder das Laufwerk neu formatiert wurde. In solchen Fällen muss das Recovery-Tool den eigentlichen Datenbereich scannen und anhand eines Dateimusters ermitteln, um was für einen Typ es sich handelt und über wie viele Cluster sich die Daten erstrecken. Aber auch das ist in vielen Fällen machbar. Bei einer JPEG-Datei funktioniert das Ganze beispielsweise so: Deren Header enthält am Anfang die Kennung „JFIF“, und die eigentlichen Bilddaten enden schlicht mit der Markierung „EOI“, also „End of image“. Nur bei Dateiformaten, die das Tool nicht kennt, muss es passen.



urlaub in Las Vegas rekonstruieren: Auf einer 1-GByte-SD-Card fanden wir 104 Fotos, teils im TIF-, teils im JPEG-Format – alles hochauflösend, beste Qualität. Nur ein wenig Geduld mussten wir mitbringen: Photorec brauchte etwa eine Stunde, um alle Fotos wiederherzustellen. Und was mit einer SD-Card funktioniert, geht auch mit allen anderen Speicherkarten.

So löschen Sie richtig: Bei Smart Cards gehen Sie genauso vor wie bei USB-Sticks – Eraser nehmen und überschreiben. Den internen Digicam-Speicher überschreiben Sie, indem Sie ihn einfach mit sinnlosen Fotos füllen.

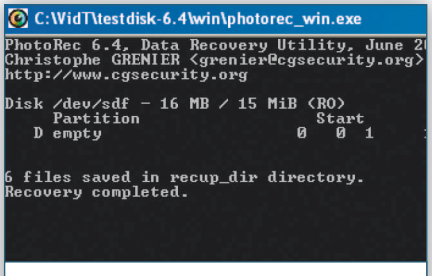
AUF SMARTPHONE & HANDY

Gelöschte SMS, viele Telefonnummern

Mobiltelefone lassen sich in zwei Klassen einteilen: Bei der einen, den Smartphones, ist das Aufspüren gelöschter Daten einfach. Das normale Durchschnittshandy dagegen bereitet deutlich mehr Schwierigkeiten, aber auch an dieser Stelle gibt es einen Weg zum Erfolg.

Smartphone: Wie leicht diese Geräteklasse zu knacken ist, konnten wir an einem frisch erworbenen Nokia E61 durchexerzieren. Einmal im Datentransfer-Modus angeschlossen, erkennt Windows das Nokia automatisch als Laufwerk und gewährt jeder beliebigen Recovery-Software Zugriff auf das Gerät. Aber warum auch nicht? Schließlich läuft auf dem Smartphone das Betriebssystem Symbian OS. Das erlaubt FAT als Dateisystem, und mehr braucht die Recovery-Software nicht, um den internen Speicher eines Smartphones komplett auszulesen.

Dankbare Opfer sind auch Mobiltelefone von Sony Ericsson: Wir haben ein K610i über die mitgelieferte PC-Suite angeschlossen. Solange die läuft, kann auch eine Windows-Anwendung auf das Handy zugreifen. Die Convar-Freeware PC Inspector File Recovery zum Beispiel fand einige gelöschte Bilder und Videos von einem Badeurlaub am Mittelmeer. Sie lagen im Verzeichnis „100MSDCF“, in dem die Handykamera das selbst geschossene Material gewöhnlich ablegt.



Blick in die Kamera: Das Tool Photorec rekonstruiert gelöschte Fotos aus dem internen Speicher einer Digicam.

Handys: Bei Mobiltelefonen, die sich nicht als Laufwerk in Windows einbinden, wird es schwierig. Jeder Hersteller hat ein eigenes Betriebssystem, oft sogar mehrere, nämlich für jede Baureihe eines – und das wird mit jedem neuen Modell nochmals modifiziert. Eine Recovery-Software zum Wiederherstellen gelöschter Handydaten gibt es daher nicht.

Was es aber gibt: Programme, die bei der Computer-Forensik zur Beweismittelsicherung dienen. Sie sind in der Regel teuer und werden von Ermittlungsbehörden und Rettungslabors eingesetzt. Marktführer Kroll Ontrack (**www.krollontrack.de**) etwa verwendet ein Produkt der Firma Paraben (**www.paraben-forensics.com**). Deren Parade-Programm Device Seizure kostet 800 Dollar und bietet Plugins für viele Modelle der großen Hersteller. Gelöschte Daten spürt die Software je nach Handy über ein „Physical Plugin“ auf. Sie legt also ein bitgenaues Image des Handyspeichers an. Das lässt sich danach im Hex-Editor auswerten.

Wir mussten dazu den USB-Treiber des entsprechenden Telefons installieren, da Device Seizure lediglich mit Kabelverbindungen arbeitet, nicht mit Bluetooth oder Infrarot. Zunächst legten wir einen „Case“ an, um danach die Scan-Funktion des Programms aufzurufen. Als die Forensik-Software mit dem „Physical Plugin“ auf das Handy zugriff, gab es alle Daten preis. So haben wir in einem gebrauchten Motorola E1000 etwa den gelöschten SMS-Verkehr entdeckt – samt den passenden Telefonnummern.

So löschen Sie richtig: Vor dieser Art von Datenspionage kann sich ein Normaltelefonierer nur schwer schützen. Mit welcher Software soll er auch den internen Speicher im Handy überschreiben? Einen Eraser dafür gibt es schließlich nicht. Allerdings sind die forensischen Tools, die man zum Rekonstruieren von Handydaten braucht, teuer und kompliziert zu bedienen. Außerdem arbeiten sie immer nur mit bestimmten Geräten einer Baureihe zusammen. Wirklich hartnäckige Datenklauer hält das jedoch nicht davon ab, persönliche Kontakte oder intime SMS auszulesen.

Wer sein Handy bei eBay verkaufen möchte, dem bleibt deshalb nur: Alle Daten im internen Handyspeicher physisch überschreiben, ihn also mit sinnlosen Informationen auffüllen. Mandau

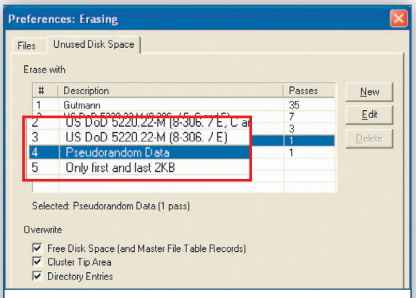
PROFI-TIPP

Alle Daten restlos vernichten

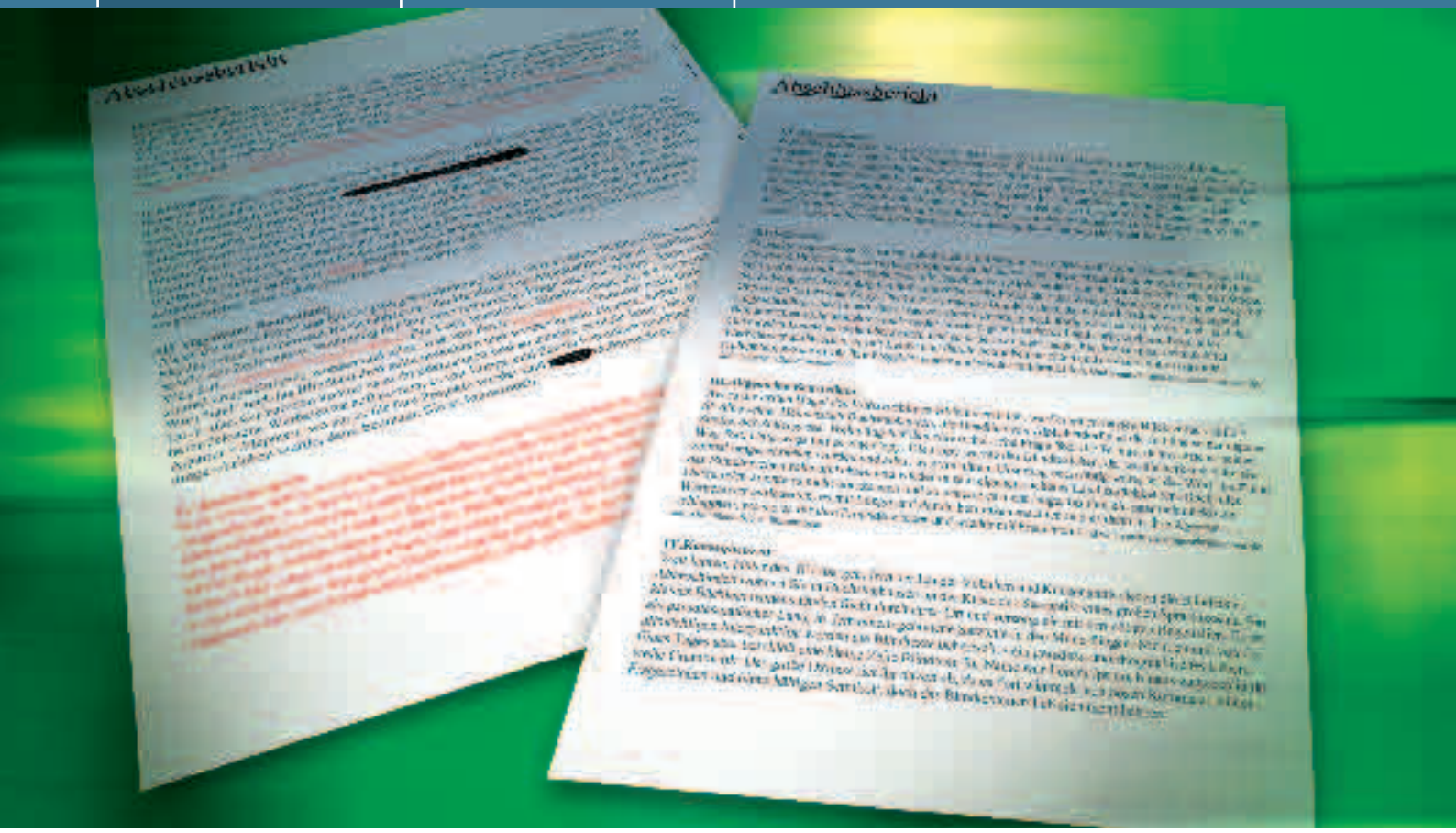
Bevor Sie einen gebrauchten Datenträger verkaufen oder auch nur entsorgen, sollten Sie ihn einmal komplett überschreiben. Denn dann kann selbst ein Rettungslabor nichts wiederherstellen. Eine Software, die das zuverlässig erledigt und auch alle Datenverstecke aufspürt, ist der Eraser (auf Heft-CD, genaue Anleitung ab 91).

Der Eraser bindet sich in das Kontextmenü des Windows Explorer ein und steht auf diese Weise jederzeit zur Verfügung. Er vernichtet sowohl den Freispeicher als auch existierende Ordner und Dateien. Zur Erklärung: Beim „Freispeicher“ handelt es sich um den Bereich der Platte, in dem sich keine aktuellen Dateien befinden. Allerdings liegen dort sämtliche aus dem Papierkorb gelöschten Dateien.

Tipp: Um das Löschen zu beschleunigen, sollten Sie zuvor im Eraser die Methode der Datenvernichtung ändern. Voreingestellt ist das dreifache Überschreiben, was allerdings unnötig Zeit kostet. Stellen Sie in den „Preferences Erasing“ die Arbeit des Tools auf die Methode „Pseudorandom Data“ um, erledigt der Eraser das Überschreiben in einem Drittel der Zeit.



Daten-Zerstörer tunen: Ändern Sie im Eraser die Methode, mit der er die Daten vernichtet. Ist er richtig eingestellt, arbeitet er gleich dreimal so schnell.



VERSTECKTE INFOS FINDEN

Was Word & Co. verraten

Dokumente von Microsoft Office und OpenOffice.org können Informationen enthalten, die andere Benutzer besser nicht sehen sollten. So finden und löschen Sie versteckte Randbemerkungen.

Das altbekannte Versprechen „What you see is what you get“ stimmt zumindest bei Word, Excel und PowerPoint, aber auch bei OpenOffice.org nicht ganz: Die Dokumente, die Sie mit diesen Programmen speichern, enthalten weit mehr Informationen, als auf dem Bildschirm angezeigt werden. Und das kann fatale Folgen haben.

AUF EINEN BLICK

→ Versteckte Informationen

Alle Tools auf CD

OpenOffice.org 2.1: Umfangreiche Office-Suite mit neuen Funktionen ◎ Office

PDFCreator: Wandelt Word-Dokumente in PDF-Dateien um ◎ Office

Stellen Sie sich vor, Sie schicken einem Kunden ein Angebot in Form einer Word-Datei. Der Kunde ruft zurück und fragt, warum Sie den Preis in letzter Minute noch erhöht und ihm den Kommentar eines Ihrer Kollegen verschwiegen haben, der auf ein mögliches Problem mit dem Produkt hinweist? Diese Informationen hat er nicht von einem redseligen Mitarbeiter in Ihrem Unternehmen erhalten, sondern aus versteckten Informationen innerhalb des Word-Dokuments.

Aber nicht nur die Dokumente der Textverarbeitung weisen diese Sicherheitslücke auf, sondern auch Excel- und PowerPoint-Dateien sowie die Files von OpenOffice.org. Alle diese Programme speichern in ihren Dokumenten unter anderem Kommentare, Änderungen, die Namen aller Personen, die das Dokument verändert haben, und das Datum der letzten Bearbeitung der Datei.

In den letzten Jahren gab es mehrere spektakuläre Fälle, in denen Word-Dokumente Informationen preisgaben, die die Verfasser lieber für sich behalten hätten: Im Februar 2003 veröffentlichte die britische Regierung ein Dossier, das die Gefahren beschrieb, die angeblich von Irak ausgingen. Kurz darauf stellte sich heraus, dass ein Großteil der vermeintlichen Geheimdienst-Informationen aus einer im Internet veröffentlichten Arbeit eines Studenten stammten. Anhand des Bearbeitungsprotokolls in der Word-Datei konnte man genau sehen, welche Beamten des britischen Außenministeriums und des Premierministeramts welche Beiträge geliefert hatten.

Im Oktober 2005 veröffentlichte die UNO-Kommission, die den Mord am libanesischen Premierminister Hariri untersuchte, ihren Abschlussbericht ebenfalls im Word-Format. Aus politischen

Illustration: S. Schönberger

Gründen wurden vor der Freigabe des Dokuments Erkenntnisse gelöscht, denen zufolge Syrien in den Mord verwickelt war. Die gelöschten Passagen ließen sich rekonstruieren, da sie noch in der Word-Datei enthalten waren, was zu internationalen Spannungen führte.

Selbst in PDF-Dateien kann man teilweise noch versteckte Informationen finden: Im März 2005 wurde die im Irak entführte italienische Journalistin Giuliana Sgrena freigelassen. Auf dem Weg zum Flughafen wurde ihr Auto von amerikanischen Soldaten beschossen, wobei ein Dolmetscher ums Leben kam. Der offizielle Untersuchungsbericht war als PDF-Datei erhältlich, in der die Namen der in den Vorfall verwickelten Soldaten geschwärzt waren. Dazu hatte man in der Word-Datei, aus der das PDF entstand, den Texthintergrund auf Schwarz gesetzt. Allerdings ließ sich der gesamte Text einfach aus der PDF-Datei herauskopieren, sodass die Namen wieder lesbar waren.

Versteckte Informationen in MS-Office löschen

Häufig wird empfohlen, Word-Dateien nicht im DOC-, sondern im RTF-Format zu speichern oder die gesamte Textdatei zu kopieren und in ein leeres Word-Dokument einzufügen. Dabei solle man nur darauf achten, dass die abschließende Absatzmarke, die in Word Formatierungen und verschiedene versteckte Infos enthält, von der Markierung ausgeschlossen bleibt. Doch keine dieser beiden Methoden ist wirklich sicher: Denn RTF-Dokumente können genauso wie DOC-Dateien Überarbeitungen speichern, die sich wieder sichtbar machen lassen. Und beim Kopieren eines Word-Texts in eine leere Datei werden auch die Kommentare aus dem Originaldokument übernommen.

Immerhin können Sie in Word über „Extras | Optionen | Sicherheit“ die Optionen „Beim Speichern persönliche Daten aus Dateieigenschaften entfernen“ aktivieren und „Warnung anzeigen, bevor eine Datei, die Überarbeitungen oder Kommentare enthält, gedruckt, gespeichert oder versendet wird“ ausschalten. Dann werden Sie wenigstens informiert, wenn ein Dokument Infos enthält, die Sie wahrscheinlich nicht weitergeben wollen. Die Funktion zum Löschen der persönlichen Daten, also etwa Ihres Benutzernamens, finden Sie übrigens auch in den Programmen Excel und PowerPoint. Sie sollten sie auf jeden Fall aktivieren.

Microsoft Office selbst bietet keine Möglichkeit, Überarbeitungen und Kommentare in einem Dokument nachträglich zu entfernen. Für Office XP und 2003 stellt Microsoft jedoch ein kostenloses „Add-In zum Entfernen verborgener Daten“ zur Verfügung. Das Tool wird bei der Installation ins „Datei“-Menü von Word, Excel und PowerPoint eingebunden und kann auf Wunsch auch über die Befehlszeile ausgeführt werden, sodass es sich auch für die Batch-Bereinigung mehrerer Dokumente eignet. Rufen Sie dazu in der Eingabeaufforderung von Windows die Datei OFFRHD.EXE auf.

Sie erhalten das Programm mit dem Dateinamen RHDTool.exe kostenlos auf der Microsoft-Website (**www.microsoft.de**). Suchen Sie dort nach „Add-In zum Entfernen verborgener Daten“ oder „Office Remove Hidden Data“. Laden Sie das Tool herunter, und installieren Sie es.

Um die versteckten Daten zu entfernen, speichern Sie Ihr Dokument zunächst. Dann rufen Sie im Menü „Datei“ den Befehl „Remove Hidden Data“ auf. Geben Sie einen neuen Dateinamen ein, und klicken Sie auf „Next“. Sobald die Daten gelöscht sind, klicken Sie auf „Finish“.

Verborgene Inhalte in OpenOffice.org löschen

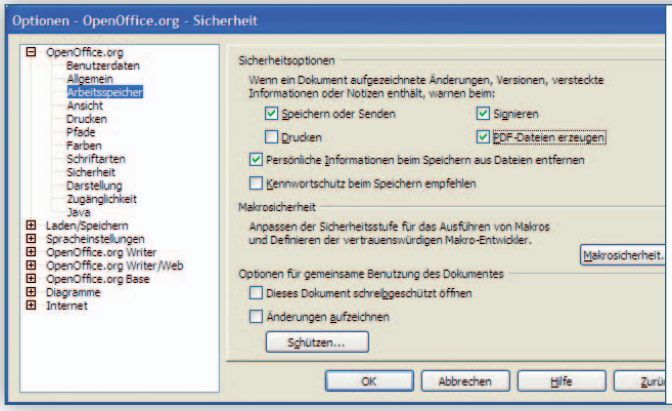
Ähnlich wie in Microsoft Office können Sie auch in OpenOffice.org das Speichern persönlicher Daten, gelöschter Textstellen etc. unterbinden und sich warnen lassen, wenn ein Dokument verborgene Infos enthält: Dazu rufen Sie in einer der OpenOffice.org-Anwendungen „Extras | Optionen“ auf und öffnen das Register „Sicherheit“. Aktivieren Sie „Persönliche Informationen beim Speichern aus Dateien entfernen“ sowie die Optionen „Speichern oder Senden“ und „PDF-Dateien erzeugen“ (unter „Wenn ein Dokument aufgezeichnete Änderungen ... warnen beim:“). Die Einstellung gilt anschließend für alle OpenOffice.org-Programme. Damit vor der Weitergabe einer Datei zusätzlich die Einträge in ihren Eigenschaften gelöscht werden, rufen Sie „Datei | Eigenschaften“ auf und klicken im Re- →

KNOW-HOW

Was Microsoft Office alles preisgibt

Dokumente aus Word, Excel und PowerPoint können etliche versteckte Informationen enthalten – mit dem RHD-Tool lassen sie sich entfernen:

- Kommentare
- die Namen des Autors und der Bearbeiter des Dokuments
- den Benutzernamen
- persönliche Informationen (aus den Dokument-Eigenschaften)
- Überarbeitungs-Markierungen
- gelöschte Textabschnitte
- ältere Dokumentversionen (aus dem Dialog „Datei | Versionen“)
- VBA-Makros sowie Beschreibungen und Kommentare aus Makros (sofern Sie nicht über „Extras | Optionen | Sicherheit | Makrosicherheit“ die hohe Sicherheitsstufe für die Ausführung von Makros aktiviert haben)
- die ID des jeweiligen Dokuments, die vom Befehl „Extras | Änderungen nachverfolgen“ genutzt wird, um das Originaldokument zu identifizieren
- den Verteiler („Datei | Senden an“)
- Den E-Mail-Header
- die Scenario-Kommentare
- die UID von Office-97-Dokumenten



OpenOffice.org: Entfernen Sie beim Speichern die persönlichen Daten aus Ihren Dokumenten.

gister „Allgemein“ auf „Löschen“. Damit setzen Sie die Bearbeitungsdauer auf „0“ und die Versionsnummer auf „1“. Schalten Sie zudem die Option „Benutzerdaten verwenden“ aus, damit der Autorenname nicht im Dokument gespeichert wird.

Ein Addin zum Entfernen von versteckten Infos gibt es für OpenOffice.org nicht. In diesem Office-Paket können Sie die Änderungen Ihrer Kollegen lediglich akzeptieren oder verwerfen – dazu dient der Befehl „Bearbeiten | Änderungen“. Ansonsten gilt das Gleiche wie für Microsoft Office: Geben Sie Ihre Dokumente lieber in Form von PDF-Dateien weiter.

PDF-Dateien anlegen mit OpenOffice.org

Um ein Dokument von OpenOffice.org als PDF-Datei zu speichern, öffnen Sie die Datei und rufen den Befehl „Datei | Exportieren als PDF“ auf. Anschließend geben Sie den gewünschten Dateinamen ein und klicken auf „Speichern“.

Es erscheint ein Fenster mit den PDF-Optionen. In ihm können Sie in OpenOffice.org ab Version 2.0.4 beziehungsweise in Star Office 8 ab Update 4 die Sicherheitseinstellungen anpassen: Im Register „Sicherheit“ aktivieren Sie „Rechtevergabe“, klicken auf „Rechte-Passwort setzen“ und geben ein Kennwort ein. Damit niemand außer Ihnen die Einstellungen ändern kann, sollten Sie ein hinreichend kompliziertes Passwort wählen.

Schalten Sie dann die Option „Inhalt kopieren erlauben“ aus – dann lässt sich der Text in der PDF-Datei später nicht in die Zwischenablage kopieren. Außerdem können Sie Ausdrucke untersagen und/oder das Einfügen von Änderungen und Kommentare unterbinden. Klicken Sie zum Schluss auf „Exportieren“.

PROFI-TIPP

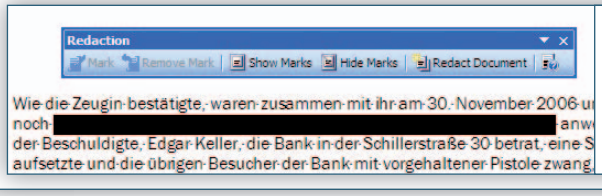
Word Redaction: Wörter richtig schwärzen

Für Behörden, Organisationen und Firmen, die vor der Weitergabe von Dokumenten einzelne Textstellen schwarz einfärben müssen, bietet Microsoft mit Word Redaction ein Add-in für Word 2003 an. Es genügt nämlich nicht, nur den Hintergrund und die Textfarbe auf Schwarz zu setzen: Das kann der Empfänger rückgängig machen – und außerdem den Text kopieren und etwa in den Windows-Editor einzufügen, sodass der geschwärzte Text wieder sichtbar wird.

Sie finden Word Redaction auf der amerikanischen Website **www.microsoft.com** unter dem Suchbegriff „Word Redaction“. Sie können es ausschließlich zusammen mit Word 2003 verwenden, zudem setzt es auch das .NET Framework 1.1 voraus.

Laden Sie das Add-in herunter. Dabei ist eine Office Validation, also eine Online-Überprüfung der Gültigkeit Ihrer Office-Installation, erforderlich. Leider ist das Programm ausschließlich in englischer Sprache verfügbar. Beenden Sie Word, und installieren Sie Word Redaction. Rufen Sie die Textverarbeitung anschließend wieder auf. Sie enthält nun die neue Symbolleiste „Redaction“ , die Sie über den Befehl „Symbolleisten“ im Menü „Ansicht“ ein- und ausblenden können. Markieren Sie den Textabschnitt, den Sie schwärzen wollen, und klicken Sie auf den Button „Mark“. Anstelle eines schwarzen Balkens erscheint – vorerst – lediglich eine graue Hinterlegung, sodass der Text noch lesbar ist. Sobald Sie alle Textstellen markiert und mit „Mark“ behandelt haben, klicken Sie auf „Redact Document“. Word erzeugt nun eine Kopie des Dokuments, in der alle zuvor markierten Stellen mit einem schwarzen Balken überschrieben sind. Diese Balken lassen sich aus dem neuen Dokument nicht mehr entfernen. Zur Vorsicht sollten Sie die veränderte Datei daher unter einem neuen Namen sichern. Je nachdem, an wen das Dokument gehen soll, greifen Sie später entweder zur Original- oder zur geschwärzten Version der Datei.

Beim Schwärzen erzeugt das Tool einen Balken, der genauso lang ist wie der geschwärzte Text – auf diese Weise bleiben die Zeilenumbrüche erhalten. Allerdings kann ein aufmerksamer Leser aus der Länge der Balken unter Umständen Rückschlüsse auf die Inhalte des „zensierten“ Texts ziehen. So kann man insbesondere bei einzelnen Wörtern erraten, was hinter den Balken verborgen ist.



Zensurbalken: Die Word-Erweiterung Redaction versieht Textstellen, die Sie verbergen wollen, mit einem schwarzen Balken.

PDF-Files anlegen mit Microsoft Office

Das Office-Paket von Microsoft kann erst ab der kommenden Version 2007 PDF-Dateien erzeugen. Es gibt jedoch einige kostenlose Tools, mit denen sich aus jeder Windows-Anwendung heraus PDF-Dokumente anlegen lassen. Eins davon ist PDFCreator, das Sie unter **www.pdfforge.org** erhalten. Entscheiden Sie sich für die Version inklusive Ghostscript, und installieren Sie beide Programme.

PDFCreator wird unter Windows als Drucker eingerichtet, an den Sie aus einer beliebigen Anwendung heraus Dokumente schicken und so ins PDF-Format umwandeln können. Um eine PDF-Datei zu erzeugen, rufen Sie einfach den Befehl „Datei | Drucken“ auf und wählen als Gerät „PDFCreator“. Bestimmen Sie den Druckbereich, und schließen Sie den Dialog mit „OK“. Das Dokument wird nun in die Druckwarteschlange von PDFCreator aufgenommen. Es erscheint ein Fenster, in das Sie den Dokumenttitel und – wenn Sie wollen – den Autorennamen, das Thema sowie Stichwörter eingeben. Außerdem können Sie an dieser Stelle das Erstellungs- und Änderungsdatum verändern. Diese Infos machen Sie später im Windows Explorer über die „Eigenschaften“ der Datei sichtbar.

Wichtig ist der Button „Einstellungen“. Um zu verhindern, dass der Empfänger der PDF-Datei Textabschnitte oder Bilder über die Zwischenablage übernehmen kann, klicken Sie in PDFCreator auf „Eigenschaften“, öffnen unter „Formate | PDF“ das Register „Sicherheit“ und aktivieren „Sicherheit benutzen“. Wenn Sie ausschließen wollen, dass andere Benutzer die Inhalte der PDF-Datei in die Zwischenablage kopieren, aktivieren Sie die Option „Verweigere Benutzern: Text und Bilder zu kopieren“. Außerdem können Sie ihnen die Möglichkeit verbauen, die PDF-Datei auszudrucken.

Sollen nur ausgewählte User die PDF-Datei öffnen dürfen, aktivieren Sie „Passwörter erforderlich zum Öffnen“, am besten wählen Sie außerdem „Verschlüsselungsgrad: Hoch“. Nach dem Klick auf „Speichern“ fordert PDFCreator Sie zur Eingabe des Kennworts auf. Nur wer das Passwort kennt, kann die Datei später im Acrobat Reader öffnen und die Inhalte einsehen.

Franz Grieser

DATEN REGELMÄSSIG SICHERN

Die richtige Backup-Strategie

Gefahr für Ihre Daten droht nicht nur durch Viren und Hacker – auch ein plötzlicher Ausfall der Festplatte kann katastrophale Folgen haben. Davor bewahrt Sie eine überlegte Backup-Strategie. CHIP zeigt Ihnen, wie Sie individuelle Daten und ganze Laufwerke sichern und wiederherstellen.

Windows XP hält einige Bordmittel zur Datensicherung bereit. Darüber hinaus gibt es – unter anderem auf der Heft-CD – kostenlose Zusatztools, die Sie bei Ihren Backup-Aktivitäten unterstützen. Daneben finden sich auch auf dem Freeware- und Shareware-Markt zahlreiche interessante Anwendungen, die Ihre Daten sichern und überdies komprimieren.

Die meisten dieser Programme konzentrieren sich auf das Sichern einzelner Daten und Verzeichnisse, nicht aber auf das Backup kompletter Laufwerke – geschweige denn bootfähiger Systemlaufwerke. Für eine solche Aufgabe setzen Sie am besten ein kommerzielles Programm ein. CHIP zeigt Ihnen am Beispiel von Acronis True Image Home, wie Sie ein komplettes Laufwerk auf CD, DVD oder einen externen Datenträger sichern.

Bevor Sie mit der Sicherung beginnen, sollten Sie überlegen, was Sie überhaupt sichern möchten. Ein Backup der kompletten Festplatte inklusive der installierten Programme empfiehlt sich bei einer großen Menge an Anwendungen und komplexen Installationen, da sonst eine Neuinstallation viel Zeit verschlingt.

Haben Sie auf Ihrer Festplatte bestimmte Bereiche und Strukturen angelegt, auf denen Sie Ihre Daten speichern, so lohnt sich an dieser Stelle eine spezifische Sicherung einzelner Verzeichnisse oder Laufwerke. Dabei sollten Sie vor allem wichtige Dokumente, Ihre Musik-, Video- oder Fotosammlung sowie das Postfach Ihres Mailprogramms samt Kontaktliste nicht vergessen.

Die Antwort auf die Frage, wohin Sie Ihre Daten am besten sichern, hängt vor allem von der Menge der Daten ab und von der Zeit, die das Sichern beansprucht. Eine kurzfristige Datensicherung können Sie mit einem USB-Stick oder einem RW-Medium vornehmen, mittelfristige Datenhaltung sollte auf einer DVD erfolgen. Für sehr große Datenmengen schließlich kommen externe Festplatten oder Bandlaufwerke in Frage.

AUF EINEN BLICK

Alle Tools auf CD

TrayBackup: Legt individuelle Sicherungskopien an ⊙ **Windows**

Z-DBackup: Sichert und verschlüsselt bequem Ihre Daten ⊙ **Windows**

Foto: Alex-, Photocase.com; Illustration: S. Schönberger

Komplett oder Zuwachs: Die richtige Backup-Strategie

Grundsätzlich lassen sich zwei Vorgehensweisen unterscheiden: die Komplett- und die Zuwachssicherung. Die Komplettsicherung berücksichtigt alle Dateien – ob sie sich seit der letzten Sicherung verändert haben oder nicht. Die Zuwachssicherung legt nur eine Kopie jener Daten an, die sich entweder seit der letzten Komplettsicherung oder der letzten Zuwachssicherung verändert haben.

Die Zuwachssicherung unterscheidet sich in differenziell und inkrementell: Die differenzielle Sicherung benötigt länger für das Backup der Daten, da es immer alle geänderten Daten seit der letzten Komplettsicherung berücksichtigt. Das Vorgehen hat jedoch den Vorteil, dass lediglich zwei Dateien zur Rücksicherung notwendig sind: die letzte Komplettsicherung und die letzte differenzielle Datensicherung.

Bei der inkrementellen Sicherung ist das Backup schneller erledigt, da sie nur die geänderten Daten seit der letzten Sicherung berücksichtigt – ob dies eine Komplettsicherung oder eine inkrementelle Sicherung war. Dafür dauert die Rücksicherung länger, da Sie neben der letzten Komplettsicherung auch alle inkrementellen Sicherungen wieder einspielen müssen.

Sichern mit XP-Bordmitteln: MS-Backup

Microsoft hat Windows XP mit einem Backup-Programm ausgestattet, das Ihnen die wesentlichen Arbeiten bei der Datensicherung abnimmt. Es ist allerdings so gut versteckt, dass es nicht gleich ins Auge springt – es trägt den Namen „Sicherung“ und verbirgt sich unter „Zubehör | Systemprogramme“. Sollte es in Ihrem System nicht vorhanden sein, installieren Sie es über Ihre Windows-XP-CD nach – die Dateien befinden sich im Ordner VALUEADD/MSFT/NTBACKUP. Beginnen Sie die Installation durch den Start des Programms NTBACKUP.MSI. Zum Einstieg ins Programm steht Ihnen der Sicherungsassistent zur Verfügung, der Sie schrittweise durch die Funktionen des Programms führt.

MS-Backup eignet sich besonders zum Sichern von Dateien und Verzeichnissen. Wählen Sie als Quelle für die Sicherung „Dateien und Einstellungen“, und treffen Sie im nächsten Schritt Ihre Auswahl mit der Option „Elemente für die Sicherung selbst auswählen“. Im folgenden Fenster wählen Sie die Verzeichnisse und Dateien, die archiviert werden sollen.

Mit der Eingabe des Speicherorts und des Namens der Sicherung könnten Sie die Definition dieses Backup-Jobs abschließen – unter „Erweitert“ finden Sie zusätzliche Konfigurationsmöglichkeiten für Ihre Datensicherung.

Im ersten Fenster wählen Sie den Sicherungstyp aus. Er steht standardmäßig auf „Normal“ – an dieser Stelle können Sie sich auch für eine inkrementelle oder differenzielle Sicherung entscheiden.

Eine Datensicherung erfüllt nur dann ihren Zweck, wenn sie bei einer Rücksicherung funktioniert. Oftmals wird monatelang gesichert – und im Ernstfall stellt sich heraus, dass die Backup-Datei defekt ist. Überprüfen Sie daher grundsätzlich nach einer Sicherung die Daten, auch wenn dies etwas Zeit beansprucht.

Bei einer normalen Sicherung fragt MS-Backup, ob die vorhandene Sicherungskopie ersetzt oder ergänzt werden soll. Die Antwort hängt sehr vom Umfang des festgelegten Backups ab.

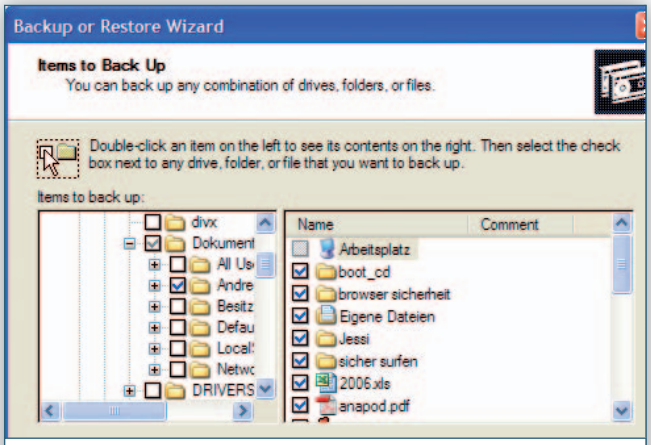
Zuletzt geben Sie noch den Zeitpunkt der Sicherung an und speichern den Auftrag. Wenn Sie die Datensicherung nicht sofort starten, können Sie einen passenden Zeitpunkt und darüber hinaus auch einen Zeitplan für regelmäßige Sicherungsläufe angeben.

Nach dem Crash: Gesicherte Daten wiederherstellen

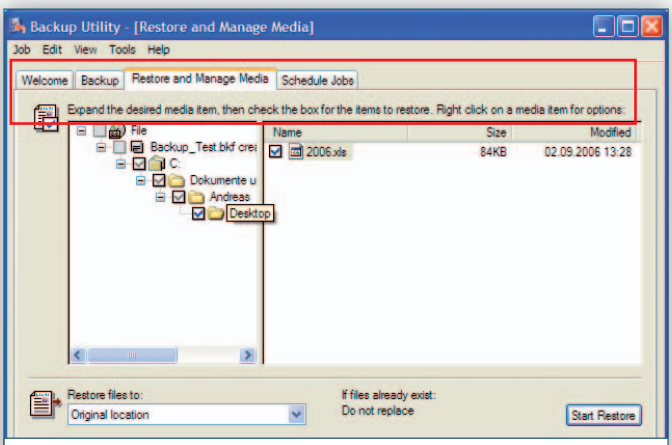
Das Rücksichern der Daten ist entweder über einen Assistenten oder im direkten Zugriff über die Registerkarte „Wiederherstellen“ möglich. In einer Liste sehen Sie alle Backup-Jobs und die zugehörigen Speichermedien. Wählen Sie die verschwundenen oder zerstörten Informationen aus und bestätigen Sie die Wiederherstellung. Vergessen Sie auch nicht, zuvor die notwendigen Zusatzoptionen zu setzen. Geben Sie an dieser Stelle den Ort an, wohin die Daten zurückgespielt werden sollen, und legen Sie zusätzlich das Vorgehen für den Fall fest, dass dort bereits eine Datei existiert.

Bei größeren Projekten: Daten synchronisieren

Das Backup mit dem Microsoft-Tool ist ideal, um Dateien und feste Strukturen zu sichern und bei Bedarf wiederherzustellen. Wenn Sie allerdings gerade an einem →



MS-Backup: Mit Bordmitteln von Windows XP können Sie einzelne Dateien oder ganze Ordner und Laufwerke sichern.



MS-Backup: Beim Zurückspielen der Sicherung können Sie entweder einzelne Dateien oder ganze Laufwerke wiederherstellen.

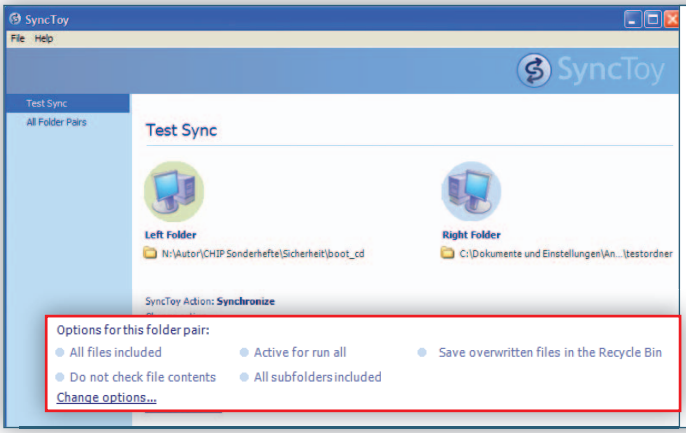
größeren Dokument arbeiten, beispielsweise an einer Diplomarbeit, ist dieses Verfahren recht unflexibel. In solchen Fällen empfiehlt sich ein USB-Stick – und eventuell auch mehrere Rechner, auf denen das Dokument und die Bilder gespeichert und bearbeitet werden sollen. Dabei soll der USB-Stick dazu dienen, auf allen Computern stets den aktuellsten Stand der jeweiligen Datei zur Verfügung zu haben. Bei diesem Unterfangen hilft Ihnen das Tool SyncToy (**www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx**), das zu den Microsoft PowerToys gehört und gratis zu haben ist. Zum Betrieb des Synchronisationstools ist allerdings das .NET-Framework ab Version 2.0.50727 erforderlich – ansonsten verweigert SyncToy die Installation.

Zur Synchronisation müssen Sie zuerst ein Ordnerpaar definieren, das Sie abgleichen möchten. Im nächsten Schritt legen Sie fest, was Sie mit den beiden Ordnern vorhaben – und zum Abgleich der beiden Ordner wählen Sie schließlich den Befehl „Synchronize".

Nachdem Sie dem Ordnerpaar noch einen Namen gegeben haben, können Sie mit dem Synchronisieren starten. Im Hauptfenster können Sie noch verschiedene Optionen zur Synchronisation auswählen, etwa die Dateitypen oder die Unterordner. Gerade zu Beginn Ihrer Synchronisationsarbeit sollten Sie sicherheitshalber auch die ersetzten Dateien im Abfalleimer liegen lassen.

Mit „Preview" starten Sie einen Testabgleich, und SyncToy zeigt Ihnen, welche Dateien wie synchronisiert werden. „Run" startet schließlich den Kopiervorgang.

Das Ordnerpaar und die vorgenommenen Einstellungen legt SyncToy zur erneuten Verwendung ab. Eine Übersicht über alle Ordnerpaare finden Sie im Menüpunkt „All Folder Pairs" auf der linken Navigationsleiste.



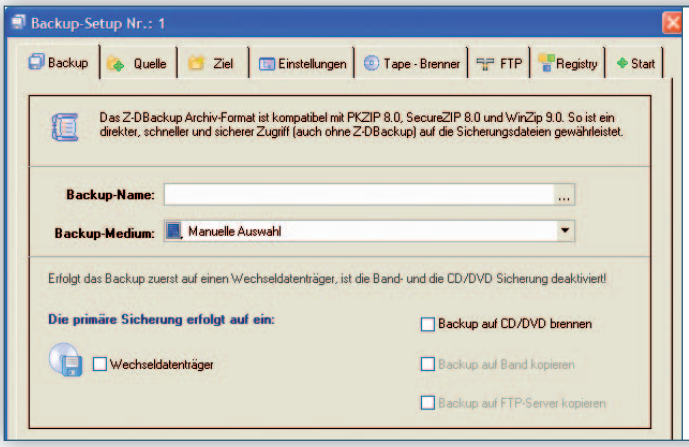
SyncToy: Im Auswahlfenster des zu synchronisierenden Ordnerpaares legen Sie weitere Eigenschaften fest.

Z-DBackup & Co: Weitere kostenlose Alternativen

Reicht Ihnen MS-Backup nicht aus, sollten Sie sich zunächst einige Freeware-Tools ansehen, die Sie bei der Datensicherung unterstützen.

Z-DBackup: Eines der interessantesten von ihnen ist Z-DBackup (**www.z-dbackup.de**), das sowohl für Anfänger als auch für ausgesprochene Experten eine Vielzahl von Funktionen zur Verfügung stellt. Einsteiger in Sachen Datensicherung können sich für die ersten Schritte Unterstützung bei den Assistenten des Programms suchen. Aber auch Backup-Profis werden an dem Produkt Gefallen finden.

Über die grafische Oberfläche kann man zahlreiche Optionen setzen. Bei der Auswahl der Sicherungsziele lässt Z-DBackup so gut wie keine Wünsche offen: CDs, DVDs und Speicherkarten werden ebenso unterstützt wie externe Festplatten oder Netz- und Bandsicherungslaufwerke.



Z-DBackup: Ein Backup-Vorgang lässt sich bei Z-DBackup ganz einfach über die grafische Oberfläche vorbereiten.

Vor dem Start des Backups legen Sie noch fest, ob die Daten in komprimierter und verschlüsselter Form abgelegt werden sollen.

Eine interessante Funktion ist die Sicherung von Dateien aus dem laufenden Betrieb heraus. Diese sind normalerweise gesperrt und lassen sich aus diesem Grund nicht sichern. Das Plugin Z-OpenLock entsperrt sie jedoch und erlaubt so das Backup der Daten, ohne dass der laufende Betrieb beeinflusst wird.

KWs Datenbackup: Das zweite Backup-Tool kann zwar durch seinen Funktionsumfang, nicht jedoch durch seine Benutzerfreundlichkeit glänzen. KWs Datenbackup (**www.vontis.de/kwsdb/soft_db.html**) erfüllt zwar im Hinblick auf die Datensicherung fast jeden Wunsch, ist allerdings – nicht zuletzt durch das Fehlen von Assistenten – für Einsteiger ziemlich schwierig zu bedienen. Ein Studium der umfangreichen (fast fünf MByte!) Hilfe-Datei hilft an dieser Stelle jedoch in den meisten Fällen weiter.

Das Programm kann die Sicherung entweder direkt ausführen oder unauffällig im Hintergrund arbeiten. Das Backup der Daten lässt sich mithilfe von Skripten automatisieren. Gerade bei großen Datenmengen hilft die Funktion des automatisierten Löschens von Daten dabei, dass man den Überblick nicht verliert und immer die aktuellsten Daten im Blick hat. KWs Datenbackup unterstützt – ebenso wie Z-DBackup – die wesentlichen Sicherungsverfahren und die gebräuchlichsten Speichermedien.

TrayBackup: Eins der bekanntesten Backup-Produkte der Freeware-Szene ist Backitup – mittlerweile abgelöst durch TrayBackup (**http://traybackup.de/**). Das Tool besticht durch eine umfangreiche Liste

von Funktionen, sodass es sich keineswegs vor seinen kommerziellen Konkurrenten verstecken muss.

Bevor Sie mit der Datensicherung mit TrayBackup beginnen, legen Sie über die Filterregeln fest, welche Datentypen von der Sicherung ausgeschlossen sind. Auf diese Weise sparen Sie Zeit und Speicherplatz. Was die Speichermedien betrifft, bietet TrayBackup eine breite Palette an – vom ZIP-Laufwerk über CD und DVD bis hin zur Netzwerksicherung finden eine Vielzahl unterschiedlicher Datenträger Unterstützung.

Aufgrund seines Funktionsumfangs und des Fehlens von Assistenten ist das Programm Backup-Einsteigern nicht unbedingt zu empfehlen. Sind Sie jedoch bereits ein wenig geübt in der Materie, dann werden Sie mit TrayBackup viel Freude haben.

Andreas Hitzig

MINI-WORKSHOP: ACRONIS TRUE IMAGE HOME

Komplettsicherungen anlegen

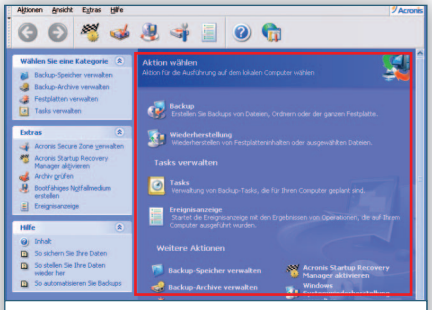
Mit dem Sichern eines kompletten Systemlaufwerks sind Freeware-Tools überfordert. Für diese Aufgabe sollten Sie ein kommerzielles Programm wie Acronis True Image Home einsetzen.

In diesem Mini-Workshop zeigen wir Ihnen, wie Sie mit diesem Tool ein Image Ihrer Systempartition anlegen. Alternativen zu Acronis True Image Home sind etwa Norton Ghost 10 oder Norton Save & Restore von Symantec (**www.symantec.com/de/de/home_homeoffice/index.jsp**).

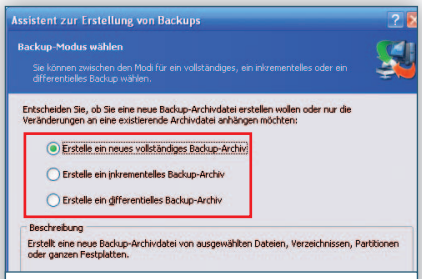
Acronis True Image Home ist rund 100 MByte groß und steht unter **www.acronis.de/homecomputing/download/trueimage/** zum Download bereit.

1 Laufwerk auswählen: Nach der Installation wählen Sie mit dem Backup-Assistenten das oder die Laufwerke aus, das/die Sie sichern wollen. Wenn Sie eine Komplettsicherung eines oder mehrerer Laufwerke planen, wählen Sie bei der Frage nach dem Backup-Typ die Option „Meinen Computer“. Im nächsten Fenster sehen Sie alle zur Verfügung stehenden Festplatten und die darauf enthaltenen Laufwerke. Nach der Auswahl der Laufwerke geben Sie noch den Speicherort an.

2 Backup-Strategie definieren: Nun legen Sie Ihre Backup-Strategie fest. Sichern Sie Ihr System zum ersten Mal, sollten Sie ein ganz neues Backup anlegen und sich ab der zweiten Sicherung für ein inkrementelles oder differenzielles Backup entscheiden. Unter den Backup-Optionen finden Sie eine Reihe von Einstellungen für das Komprimieren der Daten, den Schutz des Backup-Archivs



True Image: Die Sicherungen verwalten Sie bei Acronis True Image Home über eine gelungene grafische Oberfläche.



True Image: Beim ersten Backup legen Sie eine vollständige Sicherung an. Danach genügen auch Teilsicherungen.

und weitere Steuerungsmöglichkeiten. So können Sie etwa vor und nach der Sicherung ein Skript aktivieren, das beispielsweise ein Image auf ein Netzwerklaufwerk kopieren könnte, oder vor dem Backup bestimmte Verzeichnisse mit temporären Daten löscht.

3 Komprimierungsrate festlegen: Beim Ändern der Komprimierungsrate können Sie beobachten, dass ein Zusammenhang zwischen der Größe der Sicherungsdatei und der Backup-Zeit besteht: Je höher die Komprimierung ausfällt, desto kleiner wird die Datei, und desto länger dauert die Datensicherung. Wenn Sie während der Datensicherung mit Ihrem Rechner arbeiten wollen, sollten Sie die Backup-Priorität nicht zu hoch setzen, da ansonsten zu viele Systemressourcen für das Backup reserviert werden.

Das direkte Kopieren von Acronis True Image Home auf einen externen Datenträger erleichtert Ihnen das Rücksichern der Imagedatei, falls Ihr Betriebssystem komplett ausgefallen ist. Es wird auf der ersten CD oder DVD installiert und steuert den restlichen Ablauf der Rücksicherung.

Wenn Sie bei der Auswahl des Laufwerks eine Festplatte gewählt haben, fragt Sie das Tool, ob das Archiv geteilt werden soll und wie groß die einzelnen Dateien sein sollen. Eine feste Größe bietet sich dann an, wenn Sie die Daten später auf einem externen Datenträger speichern möchten.

4 Gesicherte Daten zurückspielen: Ob die Daten auf einer zusätzlichen Festplatte oder auf externen Datenträgern gesichert wurden, hat Einfluss auf den Vorgang des Zurückspielens. Wenn Sie einen oder mehrere Datenträger mit True Image Home inklusive Bootloader angelegt haben, ist das Rücksichern eines Laufwerks einfach. Legen Sie den ersten Datenträger ins Laufwerk, und starten Sie Ihren PC neu. Achten Sie darauf, dass im BIOS Ihr CD- oder DVD-Laufwerk als primäres Bootlaufwerk angegeben ist.

Beim Wiederherstellen haben Sie die Wahl, das komplette Laufwerk oder nur einzelne Dateien oder Ordner zurückzusichern. Wählen Sie die entsprechende Option aus, und bestimmen Sie das Ziel der Sicherung. In den erweiterten Optionen können Sie auch an dieser Stelle zusätzliche Parameter setzen. Falls Sie die Daten ins ursprüngliche Verzeichnis zurückspielen, müssen Sie klären, wie das Tool mit bereits vorhandenen Daten umgehen soll. Den Rest übernimmt das Backup-Programm für Sie.

5 Booten mit Acronis: Haben Sie die Daten zuerst auf eine Festplatte kopiert und erst danach auf CD oder DVD, fehlt Ihnen das Bootprogramm von Acronis. Das lässt sich auf zwei unterschiedlichen Wegen hinzufügen: Wählen Sie aus dem Menü „Extras“ die Option „Bootfähiges Notfallmedium erstellen“, und folgen Sie den Anweisungen des Assistenten. Sie können aber auch auf einer Festplatte einen exklusiven Bereich für die Sicherung einrichten und parallel dazu einen Bootmanager installieren. Dies geschieht über die Funktion „Acronis Startup Recovery Manager aktivieren“. Damit ist auch eine Wiederherstellung möglich, wenn eine Partition zerstört wurde. Bei einem Festplatten-Crash hilft dieses Vorgehen allerdings nicht weiter.

True Image: Im Recovery Manager legen Sie einen Bereich auf einer Festplatte fest, der als Speicher dienen soll.

GECRASHTES WINDOWS BOOTEN

XP-Notfall-CD vorbereiten

Wenn Windows schon beim Booten streikt, hilft meist eine Notfall-CD weiter. Wir zeigen Ihnen, wie Sie das Betriebssystem auf einer Notfall-CD oder einem USB-Stick installieren und mit Treibern und Analysetools ausstatten.

Notfall-CDs kommen meist dann zum Einsatz, wenn bei einem installierten Betriebssystem Probleme auftreten – etwa weil sich ein Virus eingenistet hat oder Windows nicht mehr bootet. Oft lassen sich solche Probleme bereits mit den Werkzeugen beheben, die in Windows ohnehin enthalten sind – aber die sind nur dann erreichbar, wenn auch das Betriebssystem funktioniert.

Ein Ausweg aus dieser Zwickmühle bietet sich in Form einer Live-Installation von Windows. Dabei wird das System so weit abgespeckt, dass es auf eine CD oder einen USB-Stick passt und von dort auch booten kann. Wir zeigen Ihnen in diesem Artikel, wie Sie eine solche Live-CD anlegen und um einige sinnvolle Analysetools erweitern.

1 Boot-Reihenfolge einstellen

Jeder Rechner besitzt eine vordefinierte Boot-Reihenfolge, die Sie über das BIOS Ihres Rechners ändern können. Die zuständigen Einstellungen erreichen Sie, während der PC hochfährt. Welche Taste Sie dann drücken müssen, steht im Handbuch Ihres Rechners und wird zudem oft auch mit einer BIOS-Meldung angezeigt. Je nach Hersteller des BIOS müssen Sie dann entweder die Taste [Entf] oder [F1] drücken. In welchem Menü Sie anschließend die Boot-Reihenfolge einstellen, ist ebenfalls abhängig vom Hersteller und von der Version Ihres BIOS – auch hier hilft ein Blick ins Handbuch weiter.

Über die Auswahl der verfügbaren Einstellungen erfahren Sie auch, ob das Booten von einem USB-Speichermedium möglich ist oder ob der Computer lediglich CD, Diskette und Festplatte als Startlaufwerke akzeptiert. Teilweise können Sie diese Liste durch ein BIOS-Update erweitern. Ob eine neuere Version verfügbar ist und welche Funktionen sie bietet, erfahren Sie auf der Website des Mainboard-Herstellers.

2 Vorbereitungen treffen

Zum Zusammenstellen einer Live-CD benötigen Sie verschiedene Software- und Hardware-Komponenten: eine originale Installations-CD von Windows XP, einen CD-Brenner, einen CD-Rohling und eine Brennsoftware wie etwa Nero.

Zudem sollten Sie das Service Pack 2 für Windows XP herunterladen und gleich in die Boot-CD integrieren. Rufen Sie dazu die Microsoft-Homepage auf (**www.microsoft.com/germany**), geben Sie dort ins Suchfeld den Begriff „Servicepack“ ein, und laden Sie die Version „Windows XP Service Pack 2-Netzwerkinstallationspaket für IT-Spezialisten und Entwickler“ herunter. Darüber hinaus müssen Sie sich ein Programm zum Anlegen einer Windows-Boot-CD beschaffen. Es gibt mittlerweile mehrere Tools dieser Art, wir verwenden für diesen Workshop das kostenlose Bart's PE Builder V3.1.10a (**www.nu2.nu/pebuilder**). Mit dieser Software und den erwähnten Zutaten stellen Sie eine Boot-CD zusammen, die Windows mit einer Bildschirm-Auflösung von 800 x 600 startet, einen Zugriff aufs Netzwerk bietet und die Dateisysteme FAT, NTFS und CDFS unterstützt.

Da die Boot-CD aus einer Imagedatei auf der Festplatte gebrannt wird, sollten auf Ihrer Festplatte noch mindestens 500 MByte frei sein. Je nach Anzahl und Umfang der Analyse- und Zusatztools, die Sie

Foto: M. Fiorito

AUF EINEN BLICK

Alle Tools auf CD

Bart's PE Builder: Legt Live-CDs von Windows an ◎ Windows

ZoneAlarm: Blockiert Schädlinge aus dem Internet ◎ Security

mit auf die CD packen wollen, sollten Sie entsprechend mehr Platz einplanen. Die Imagedatei finden Sie später übrigens im gleichen Ordner, in dem Sie auch Bart's PE Builder installiert haben.

3 Boot-CD zusammenstellen

Installieren und starten Sie Bart's PE Builder, und stellen Sie in dem Programm das Laufwerk oder den Ordner mit den Installationsdateien von Windows XP ein. Den Pfad tragen Sie entweder manuell ein oder geben ihn über die Schaltfläche mit den drei Punkten an. Auf Wunsch sucht PE Builder auch selbstständig nach den Files (Befehl: „Quelldateien | Suchen"). Das kann allerdings eine Weile dauern, da die Software zunächst die komplette Festplatte scannt. Anschließend weisen Sie das Tool im Bereich „Bootmedium" an, dass es zunächst ein Image der Windows-Boot-CD erzeugen soll.

Wenn auf Ihrer Windows-CD das Service Pack 2 nicht integriert ist, nehmen Sie es über „Quelldateien | Slipstream" in die Boot-CD auf. Markieren Sie zudem das Kontrollkästchen „Quelle ist nicht beschreibbar". Sobald Sie die Einstellungen bestätigt haben, beginnt PE Builder mit der Extraktion der benötigten Dateien von der CD und kombiniert sie mit den aktuelleren Versionen des Service Pack 2.

4 Mit Plugins arbeiten

Bereits mit den Standardfunktionen des Windows PE auf der Boot-CD können Sie viele Probleme einer beschädigten XP-Installation lösen. Mit der Integration von Plugins lassen sich die Möglichkeiten jedoch noch deutlich erweitern.

Schon in Bart's PE Builder ist eine Reihe von nützlichen Zusatzprogrammen enthalten. Damit die Installationsdatei des Programms jedoch nicht zu groß wird, hat sich der Entwickler dazu entschlossen, für einige weitere Tools lediglich das Installationsskript beizulegen. In der Liste der Plugins sind sie daher zwar verzeichnet, aber nicht aktiviert. Ein komplettes Verzeichnis des Lieferumfangs von Bart's PE Builder gibt es unter der Adresse **www.nu2.nu/pebuilder/plugins**.

Wenn Sie eines der Plugins nutzen möchten, für welches nur die Installationsdatei vorhanden ist, benötigen Sie weitere Daten, die Sie sich aus dem Internet herunterladen können. Wie Sie die Software in die Boot-CD aufnehmen, erfahren Sie auf der erwähnten Plugin-Seite oder nach Anklicken der Hilfe-Schaltfläche. Wir zeigen Ihnen am Beispiel des Virenscanners Stinger von McAfee und der Ad-Aware von Lavasoft, wie Sie sie in die Windows-PE-CD einbauen.

5 Plugins integrieren

Zahlreiche Freeware-, Open-Source- und kommerzielle Programme eignen sich für die Integration in eine Windows-Live-CD. Sollten Sie auf der Suche nach speziellen Anwendungen sein, lohnt sich ein Blick auf die deutsche Seite von Bart's PE Builder (**www.nu2german.de/pluginn.shtml**) oder ins deutsche Forum zu der Software (**http://pebuilder.de**). Dort sind zu vielen Programmen gleich mehrere Plugins verzeichnet.

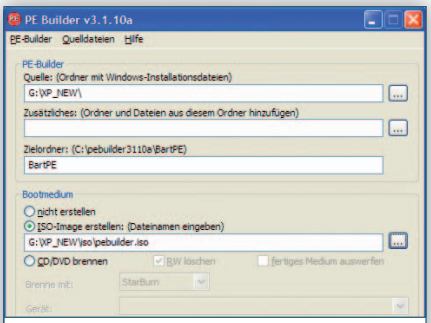
Stinger und Ad-Aware sind bereits für die Integration in die CD vorbereitet. Sie benötigen lediglich noch einige zusätzliche Dateien. Für Ad-Aware laden Sie sich von der Lavasoft-Homepage (**www.lavasoft.de**) die Freeware-Version herunter und installieren sie auf dem XP-Rechner. Führen Sie anschließend ein Update übers Internet aus, und kopieren Sie die beiden Dateien defs.ref und ad-aware.exe in den Ordner \plugin\adawarese\files.

Stinger ist auch ohne Installation lauffähig. Holen Sie sich die aktuelle Version von der Homepage von McAfee (**http://vil.nai.com/vil/stinger**), und speichern Sie sie im Verzeichnis \plugin\stinger. Weitere Informationen zur Integration von Stinger finden Sie unter **www.nu2.nu/pebuilder/pluginhelp/stinger.htm**, für Ad-Aware unter **www.nu2.nu/pebuilder/pluginhelp/adawarese.htm**.

6 Plugins nachladen

Falls PE Builder das gewünschte Tool nicht anbietet, können Sie auch externe Programme in die Live-CD einbinden. Wie das geht, zeigen wir Ihnen am Beispiel der Anti-Spyware Spybot - Search & Destroy, des Virenscanners Antivir und der Firewall ZoneAlarm Free.

Recht einfach ist die Integration von Spybot, da der Entwickler selbst ein Plugin zur Verfügung stellt. Sie können es unter **www.safer-networking.org/files/peplugin.zip** herunterladen. Legen Sie in Bart's PE Builder einen neuen Ordner auf →



3 Quelle und Ziel: Auf dem Haupt-Programmfenster von PE Builder geben Sie an, wo die Originaldateien von Windows liegen.

der gleichen Ebene an, auf der auch die anderen Plugin-Verzeichnisse liegen, und entpacken Sie dort die ZIP-Datei. Fügen Sie das Programm anschließend mit dem Plugin-Manager Ihrer Live-CD hinzu.

Von AntiVir gibt es zwar kein offizielles Plugin vom Hersteller, dafür jedoch eine Reihe von Eigenentwicklungen. Problemlos funktioniert hat im Test das Plugin aus dem Bart's-PE-Builder-Forum. Nach dem Entpacken nehmen Sie das Programm einfach über den Plugin-Manager in die CD auf. Stoßen Sie auf Probleme, sehen Sie sich die Forenbeiträge an, die sich mit dem Plugin beschäftigen. Viele Fragen klären sich bereits, wenn Sie die Beiträge unter **http://pebuilder.de/htopic,1525,avira.html** und **http://pebuilder.de/htopic,1584,avira.html** lesen.

7 Firefox nachrüsten

Auch die Live-CD von Windows XP enthält standardmäßig den Internet Explorer als Browser. Trotzdem müssen die Fans von Firefox nicht auf ihren Open-Source-Browser verzichten. Die erforderlichen Skripte, um das Programm über Bart's PE Builder in die Live-CD aufzunehmen, finden Sie auf der Homepage unter der Adresse **www.nu2.nu/pebuilder/firefox**. Das dort angebotene Installationspaket enthält die Version 1.5.0.1 des Browsers. Beim Betrieb von der Live-CD aus müssen Sie allerdings einige Einschränkungen hinnehmen. So ist beispielsweise die Startseite nicht individuell einstellbar, zudem ist auch eine Reihe von Funktionen nicht erreichbar. Dazu zählt etwa, dass Sie kein Update des Programms und seiner Erweiterungen vornehmen können.

Außerdem lassen sich die Suchseiten nicht frei konfigurieren, Sie können den Speicherort für heruntergeladene Dateien nicht auswählen und müssen auf eine Reihe von Warnmeldungen verzichten. Grund ist einfach, dass die einmal gebrannte Live-CD anschließend nicht mehr beschrieben werden kann. Darüber hinaus ist der Browser jedoch uneingeschränkt einsatzfähig und bietet Ihnen die gewohnte Arbeitsumgebung.

8 Zusätzliche Treiber einbinden

Die PE-Version von Windows unterscheidet sich in ihrer Treiberausstattung nicht von einer normalen Windows-XP-Installation. Sie kommt daher mit sämtlichen Geräten zurecht, die auch von XP automatisch und ohne die Hilfe der Treiber anderer Hersteller erkannt werden. Funktioniert eine Hardware-Komponente also mit den Standardtreibern von Windows XP, so sind auch bei der Live-CD keine Schwierigkeiten zu erwarten.

Falls Windows zur Kommunikation mit einem bestimmten Gerät einen zusätzlichen Treiber benötigt, fügen Sie ihn in Bart's PE Builder dem Installationsverzeichnis hinzu. Wie das funktioniert und was Sie dabei beachten müssen, lesen Sie in englischer Sprache unter der Adresse **www.nu2.nu/pebuilder/help/english/drivers.htm**.

9 Image anlegen und brennen

Sobald Sie alle Teile für die Windows-Live-CD zusammengetragen haben, können Sie die Imagedatei anlegen. Bart's PE Builder lässt Ihnen auf seiner Einstiegsseite die Wahl, ob es das Image zunächst auf der Festplatte speichern oder direkt auf CD brennen soll.

Besser ist es, die Daten zunächst auf der Festplatte abzulegen. Denn auf diese Weise können Sie es mithilfe eines Programms zum Lesen von ISO-Dateien wie etwa Virtual Clone Drive (**www.slysoft.com**) vorab schon einmal testen. Doch wenn dieser Test erfolgreich verläuft, steht dem Brennvorgang nichts mehr im Wege.

Um mit den Imagedaten eine Live-CD anzulegen, eignet sich nahezu jedes aktuelle Brennprogramm. Wir zeigen Ihnen am Beispiel von Nero Express, was zu tun ist. Rufen Sie das Programm auf, markieren Sie „Image, Projekt, Kopie" und klicken Sie auf „Disk-Image oder gespeichertes Projekt". Wählen Sie das erzeugte Image aus, stellen Sie den gewünschten Brenner ein, und klicken Sie zum Schluss auf „Brennen". Sobald der Vorgang beendet ist, besitzen Sie eine individuell zusammengestellte Windows PE Boot-CD.

PROFI-TIPP

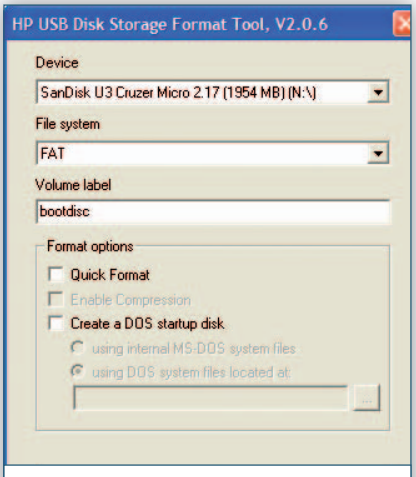
Windows XP von USB-Stick booten

Die Live-Version von Windows XP lässt sich nicht nur von CD starten, sondern auch von einem USB-Stick. Voraussetzung ist allerdings, dass im BIOS des PCs die USB-Schnittstelle für Boot-Vorgänge angeboten wird und Sie einen kompatiblen USB-Stick haben. Er muss mindestens 256 MByte Speicherkapazität besitzen. Abhängig von den zusätzlichen Tools, die Sie in die Live-Version aufnehmen wollen, empfiehlt sich jedoch die Verwendung eines größeren Sticks. Außerdem sollte das Mainboard den USB-2.0-Standard unterstützen. Das ist zwar nicht zwingend erforderlich, beschleunigt jedoch den Boot-Vorgang und das Arbeiten mit Windows PE.

Formatieren Sie den USB-Stick am besten mit dem Dateisystem FAT, das von nahezu allen BIOS-Versionen als Dateisystem zum Booten akzeptiert wird. Verwenden Sie dafür aber nicht den Windows Explorer, sondern das Tool HP USB Disk Storage Format (**ftp://ftp.compaq.com/pub/softpaq/sp27001-27500/sp27213.exe**).

Legen Sie anschließend mit dem Programm pe2usb eine RAM-Disk an. Sie starten es über die Eingabeaufforderung („Start | Ausführen | cmd"). Geben Sie dort den Befehl „pe2usb x:" ein, wobei Sie für „x:" den Laufwerksbuchstaben Ihres USB-Sticks einsetzen. Kopieren Sie dann von Laufwerk C: auf Ihrer Festplatte die Dateien boot.ini, ntldr und ntdetect.com auf den Stick. Für einen ersten Test genügt das: Schließen Sie den Stick an, starten Sie den PC neu, und versuchen Sie, vom Stick zu booten.

Falls der Test erfolgreich war, führen Sie die Schritte zum Anlegen einer Windows-Live-CD wie im Artikel beschrieben durch. Legen Sie zum Schluss jedoch kein Boot-Medium an, sondern kopieren Sie lediglich die Dateien aus dem Ausgabeverzeichnis komplett auf den USB-Stick, und booten Sie erneut.



Formatieren: Richten Sie auf Ihrem USB-Stick das Dateisystem FAT ein – das akzeptieren fast alle BIOS-Versionen.

10 Distributionen verwenden

Bequemer als das Zusammenstellen einer eigenen Live-CD sind fertige Distributionen auf Windows-PE-Basis, etwa Ultimate Boot CD for Windows. Sie liefert eine Anzahl von Tools zur Systemanalyse und für den Kampf gegen Schädlinge mit. Welche Programme darin enthalten sind, zeigt die Übersicht auf der Homepage **www.ubcd4win.com**.

Ultimate Boot CD bietet bereits vorinstalliert einen Netzwerk-Support, Diagnosetools für Hardware und Software und kann auf FAT-, FAT32-, NTFS- und CDFS-Laufwerke zugreifen. Darüber hinaus sind auch mehrere Virenscanner und Tools zum Entfernen von Malware in der Distribution enthalten.

Die Installation läuft ähnlich ab wie bei Bart's PE Builder. Sie benötigen die gleichen Zutaten und zusätzlich eben Ultimate Boot CD for Windows. Laden Sie die Installationsdatei herunter, entpacken Sie sie, und geben Sie dem Zielverzeichnis einen Namen ohne Leerzeichen – im Beispiel verwenden wir \ubcd4win.

Legen Sie die Installations-CD von Windows XP ins Laufwerk, oder kopieren Sie deren Verzeichnisse auf die Festplatte. Starten Sie das Programm UBCD4WinBuilder.exe aus dem Installationsverzeichnis, und überspringen Sie die Suche nach den Installationsdateien – wo die Originaldaten von Windows XP lagern, wissen Sie ja bereits. Falls das Service Pack 2 noch nicht integriert ist, holen Sie das nach, wie oben beschrieben.

Ein Klick auf „PlugIns" zeigt die Stärke von Ultimate Boot-CD – eine lange Liste bereits verfügbarer Anwendungen. Sollten Sie immer noch Programme vermissen, können Sie sie, wie oben beschrieben, übernehmen. Plugins, die Sie nicht benötigen, markieren Sie und entfernen sie mittels „Enable/Disable". Den aktuellen Status des Plugins sehen Sie im Feld „Enabled". Im letzten Schritt stellt Ultimate Boot CD for Windows eine individuelle CD zusammen, die Sie anschließend entweder brennen oder auf einen USB-Stick kopieren können.

11 Ausweichen auf Linux

Neben Windows PE gibt es auch eine Reihe von Linux-Distributionen, mit denen sich ein streikender Computer wieder zum Leben erwecken lässt. Anders als die Live-CD von Windows XP werden sie jedoch bereits vorgefertigt im Internet angeboten und müssen nur noch auf CD oder DVD gebrannt werden. Beispiele dafür sind etwa Knoppix STD (**http://s-t-d.org**), Ultimate Boot-CD (**www.ultimatebootcd.com**) oder Knoppix (**www.knop per.net/knoppix**).

Das Zusammenstellen einer individuellen Boot-CD ist also dank Bart's PE Builder nicht allzu kompliziert. Wenn Sie eine fertige Lösung suchen, sind Sie mit Ultimate Boot CD gut beraten. In diesem Fall müssen Sie sich nur noch für eine der beiden Versionen (Linux oder Windows) entscheiden, das Image herunterladen und mit einem beliebigen Brennprogramm auf CD oder DVD kopieren.

Andreas Hitzig

NOTFALLPAKET MIT VOLLVERSION

Daten retten mit DiskRecovery & Co.

Datei weg, Partition zerstört, System kaputt? Keine Bange: CHIP mutiert für Sie zum Superman und rettet Ihre Daten. Ob sich die beschädigten Dateien auf der Festplatte, einer DVD oder einer Speicherkarte befinden – mit den Programmen auf der Heft-CD lässt sich alles zurückholen.

Wenn es auf einem Schiff „Mann über Bord!“ heißt, sollte man schnell den Rettungsring werfen. Wenn es bei Ihrem PC „Daten weg!“ heißt, können Sie ab sofort zur Heft-CD greifen. Denn ganz gleich, ob es sich um Fotos auf einer Speicherkarte, Dokumente auf der Festplatte oder Daten auf kaputten DVDs handelt: Unsere Tools rekonstruieren nahezu alle Dateien, die versehentlich gelöscht oder beschädigt wurden. Voraussetzung ist lediglich, dass die Daten noch nicht überschrieben wurden.

Für jedes Szenario geben wir Ihnen in diesem Artikel einen Workshop an die Hand. Sollte die einfache Rettungsaktion einmal versagen, gibt es weiterführende Tipps. Zusätzlich haben wir clevere, kleine Tools in das Paket gesteckt, die dafür sorgen, dass der Daten-GAU gar nicht erst eintritt. Sie sichern wichtige Files einfach vorher – zum Teil automatisch (siehe Kasten auf 113).

AUF EINEN BLICK

Rettung bei gelöschter Partition

Tool: DiskRecovery 3.0 Personal
Info: www.oo-software.de

Haben Sie eine Partition versehentlich gelöscht, neu formatiert oder teilweise überschrieben? Mit DiskRecovery sind die enthaltenen Dateien trotzdem nicht verloren. Denn es handelt sich dabei um ein Spezialtool für Profis, das sogar beschädigte Dateien wiederherstellt und auch außerhalb von Partitionen nach gelöschten Files sucht. Die Professional Edition von DiskRecovery kostet daher auch stolze 300 Euro.

Auf der Heft-CD finden Sie dagegen die Vollversion der Personal Edition. Sie liegt normalerweise bei 50 Euro, bietet jedoch denselben Funktionsumfang wie die Profi-Ausführung. Die einzige

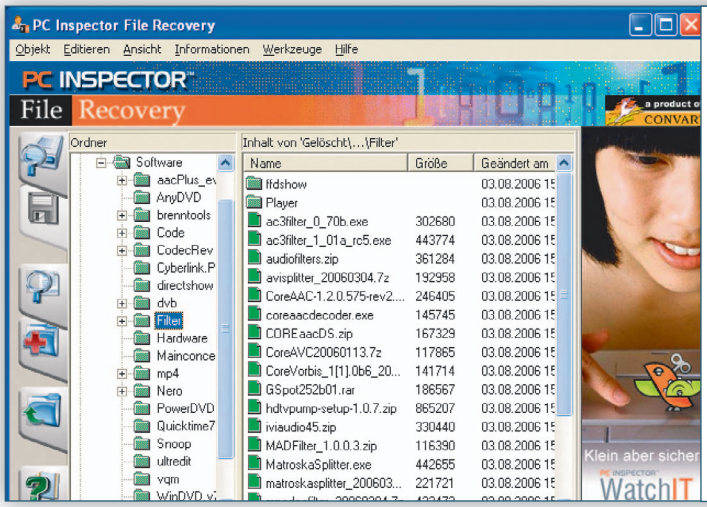
Foto: Warner Bros., „Superman returns“

Einschränkung ist, dass sie lediglich das Wiederherstellen von maximal 50 Dateien pro Suchlauf erlaubt. Ideal, wenn Sie nur bestimmte Dateien retten wollen.

Partition auswählen: Starten Sie DiskRecovery über „Start | O&O Software | O&O DiskRecovery“. Im Startmenü klicken Sie auf „Weiter“. Im nächsten Fenster markieren Sie das Laufwerk, auf dem Sie gelöschte Dateien wiederherstellen wollen. Befinden sich die Files auf einer gelöschten Partition, entfernen Sie das Häkchen vor „nicht partitionierte Bereiche ausblenden“. Klicken Sie auf „Weiter“. Bei den „Erweiterten Einstellungen“ sollten Sie ebenfalls alle Voreinstellungen unverändert belassen. Es sei denn, Sie suchen nach einer gelöschten Datei, die größer als 512 Bit ist – sich also nicht in der MFT (Master File Table) des Dateisystems befindet. Dann können Sie das Häkchen vor „Deep Scan“ der MFT entfernen, die Suche läuft anschließend ein wenig schneller ab.

Suchparameter definieren: Klicken Sie auf „Weiter“, und geben Sie im nächsten Menü die „Dateitypen“ an, die Sie wiederherstellen wollen. Normalerweise sind alle Typen, die DiskRecovery erkennen kann, bereits markiert. Wenn Sie aber beispielsweise nur AVI-Files retten wollen, drücken Sie „deselektieren“ und setzen vor „AVI“ ein Häkchen. Alternativ dazu wählen Sie „Filtern nach Dateigruppe“ und aktivieren im Menü die Option „Film“. Jetzt spürt DiskRecovery auch MPEG- und WMV-Files auf. Bestätigen Sie mit „OK“.

Dateien wiederherstellen: Nach einem Klick auf „Weiter“ startet DiskRecovery den Suchvorgang. Je nach Größe der Partition kann er mehrere Minuten dauern – rechnen Sie mit zwei Minuten pro Gigabyte. Anschließend zeigt das Programm das Ergebnis nach Dateitypen sortiert an. Da Sie nur 50 Dateien pro Suchlauf retten können, klicken Sie zunächst auf „Alle markieren“ und anschließend auf „deselektieren“. Jetzt sind alle Häkchen entfernt, sodass Sie sich in aller Ruhe die Dateien aussuchen können, die Sie im ersten Durchgang retten wollen. Danach klicken Sie auf „Weiter“. Im nächsten Fenster definieren Sie ein Verzeichnis, in welches DiskRecovery die geretteten Dateien ablegen soll. Nach einem Klick auf „Weiter“ startet die Software den eigentlichen Rettungsvorgang.



Dateien retten: PC Inspector File Recovery zeigt nach dem Scan alle gelöschten Dateien an. Nun können Sie sie einfach wiederherstellen.

TIPP Wenn sich die Daten, die Sie retten wollen, auf der Systempartition befinden, sollten Sie anders vorgehen. Denn Windows beschreibt diese Partition bei jedem Start mit neuen Daten. Es besteht daher die Gefahr, dass das Betriebssystem genau die Files überschreibt, die Sie retten wollen. Besser geeignet ist in diesem Fall Instant Disk Recovery, das Sie ebenfalls auf der Heft-CD finden. Dieses Tool ist nur im Arbeitsspeicher aktiv und tastet die Partition nicht an. Legen Sie die CD ein, und rufen Sie vom Menü aus „Instant Disk Recovery“ auf. Nach Eingabe Ihrer Seriennummer legt das Programm los.

TIPP Bei exotischen Dateiformaten wie etwa MP4 oder AAC muss DiskRecovery normalerweise passen, da es sie nicht automatisch erkennen kann. Doch Sie können den Funktionsumfang erweitern: Legen Sie einfach selber eine Dateisignatur an, also ein Code-Muster, anhand dessen DiskRecovery den Typ identifizieren kann. Das Muster lässt sich in der Regel mit einem Hex-Editor herausfinden – ideal für Einsteiger ist die Freeware HxD (auf Heft-CD). Beispiel AAC-Dateien: Wenn Sie in HxD über „Datei | Öffnen“ einige AAC-Files laden, sehen Sie, dass die ersten vier Hexadezimal-Werte darin immer „FF F1 59 80“ heißen. Diese Werte tragen Sie in DiskRecovery ein.

Verlorene Files zurückholen

Tool: PC Inspector File Recovery

Info: www.pcinspector.de

Sie müssen nicht gleich in die Luft gehen, wenn Sie versehentlich Dateien aus dem Windows-Papierkorb gelöscht haben. Die Freeware PC Inspector ist für solch einfache Fälle der ideale Partner. Denn die Dateien sind auf der Festplatte immer noch vorhanden, Windows vermerkt in der Partitionstabelle nur, dass sie gelöscht wurden. Die Informationen über Namen, Länge und Typ bleiben ebenso erhalten wie die Blockadressen der Festplatte, an denen sich die Bits der Datei befinden. PC Inspector File Recovery muss daher lediglich die Partitionstabelle scannen, etwa die Master File Table von NTFS, und nach dem Vermerk „gelöschte Datei“ suchen. In der Tabelle findet das Tool auch alle weiteren Daten, die es benötigt, um ein File wiederherzustellen.

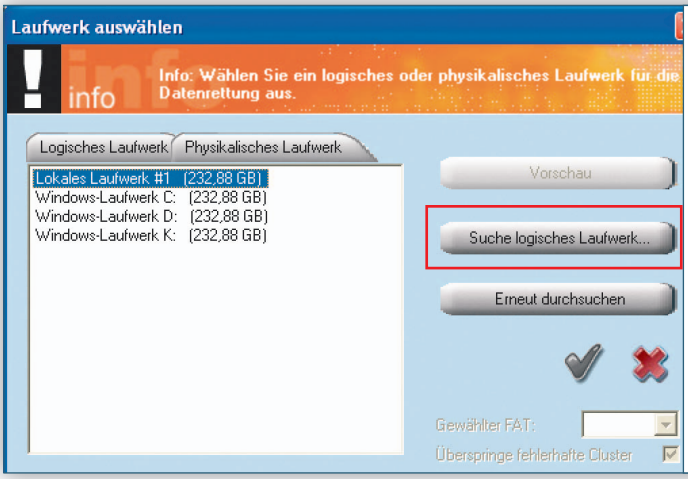
Laufwerk auswählen: Im Hauptfenster von PC Inspector File Recovery klicken Sie links oben auf das Icon „Laufwerk auswählen“. Im folgenden Fenster sehen Sie unter „Logisches Laufwerk“ die vorhandenen Partitionen. Markieren Sie das Laufwerk, das das Tool nach gelöschten Dateien durchsuchen soll. Bestätigen Sie Ihre Auswahl mit einem Klick auf das grüne Häkchen. Danach startet das Programm die Analyse.

Dateien wiederherstellen: Das Ergebnis zeigt PC Inspector File Recovery kurz darauf in einer Explorer-Ansicht. Sobald Sie im linken Fenster den Ordner „Gelöscht“ öffnen, sehen Sie rechts alle Dateien aufgelistet, die das Tool zur Wiederherstellung anbietet. Um eine einzelne Datei oder einen Ordner zu retten, markieren Sie sie oder ihn im rechten Fenster und starten über das Kontextmenü die Funktion „Speichern unter“. Im nächsten Fenster geben Sie ein Verzeichnis an, in dem PC Inspector die Datei ablegen soll.

TIPP Um beispielsweise nur gelöschte Word-Dokumente wiederherzustellen, setzen Sie die Suchfunktion von PC Inspec- →

tor ein. Mit einem Klick auf das Lupensymbol öffnen Sie die Suchmaske. Im Feld „Name“ können Sie auch Wildcards verwenden, also etwa „*.doc“ eingeben, um alle Word-Dokumente aufzuspüren. Die Treffer finden Sie dann im Explorer-Fenster im Ordner „Durchsucht“.

TIPP Ist die Partitionstabelle defekt oder der Eintrag einer gelöschten Datei dort schon überschrieben, starten Sie über PC Inspector File Recovery eine tiefer gehende Suche. Dazu wählen Sie im Hauptfenster die Option „Verlorene Dateien finden“ aus. Jetzt erscheint ein Fenster, in dem Sie per Schieberegler den Cluster-Bereich einstellen, in dem die Software suchen soll. Vorgegeben ist normalerweise die gesamte Partition, sodass Sie hier nichts machen müssen. Sobald Sie auf das grüne Häkchen klicken, startet die Suche.



Laufwerk suchen: Im PC Inspector File Recovery können Sie auch Laufwerke aufspüren, die Windows gar nicht mehr anzeigt.

Gelöschte Fotos aufspüren

Tool: PC Inspector Smart Recovery

Info: www.pcinspector.de

Digitalknipser leben gefährlich: Sie schießen Tausende von Fotos und löschen sie genauso schnell wieder, denn sie brauchen ja Platz für neue. Unter Umständen vernichten sie dabei auch Bilder, die sie behalten wollen. Wie gut, dass sich PC Inspector Smart Recovery darauf spezialisiert hat, Fotos von externen Medien wiederzubeschaffen, etwa von SD-Cards, Memory Sticks und Micro Drives.

Fotos retten: Legen Sie die Speicherkarte am besten in ein Lesegerät ein, und starten Sie Smart Recovery. Über „Laufwerk auswählen“ geben Sie an, unter welchem Laufwerksbuchstaben Windows die Kamera oder das Lesegerät ins System eingebunden hat. Unter „Dateityp auswählen“ ist im Normalfall „JPG“ eingestellt. Sie können aber auch nach anderen Multimedia-Typen suchen lassen. Dazu klicken Sie in das Dropdown-Menü darunter und wählen beispielsweise „TIFF“ aus. Jetzt legen Sie noch den „Speicherort“ fest, in dem das Tool die geretteten Dateien ablegen soll. Nach einem Klick auf „Start“ beginnt die Software mit der Arbeit. Die Rettungsaktion kann recht lang dauern – etwa zwei Stunden pro Gigabyte auf einer Smart Media Card.

TIPP Falls das Ergebnis nicht zu Ihrer Zufriedenheit ausgefallen ist, können Sie über „Datei | Einstellungen“ die „intensive Suche“ zuschalten.

TIPP Lassen Sie die Funktion „Medium überprüfen“ mitlaufen. Auf diese Weise sehen Sie schon beim Scannen, ob ein Hardwaredefekt vorliegt: Unter „Lesefehler“ zeigt das Tool an, wie viele Sektoren auf der Karte beschädigt sind. Sie wissen dann, ob Sie die Karte besser ausmustern sollten, um einem zukünftigen Datenverlust vorzubeugen.

Beschädigte CDs & DVDs auslesen

Tool: IsoBuster

Info: www.smart-projects.net

Zerkratzt, korrodiert, gelöscht – CDs und DVDs sind empfindliche Medien, bei denen immer ein plötzlicher Datenverlust droht. So kann es passieren, dass Sie eine ältere DVD mit Urlaubsfotos einlegen – und Windows liest und liest stundenlang, doch das Explorer-Fenster bleibt leer. Aber auch wenn das Betriebssystem die Fotos nicht mehr findet, sind sie dank IsoBuster noch lange nicht verloren.

CD/DVD einlesen: Legen Sie die Scheibe mit den verschwundenen Daten in das Laufwerk Ihres PCs ein, und öffnen Sie per Doppelklick IsoBuster. Das Tool liest den Datenträger beim Start automatisch ein. Wenn die Software danach in der Ex-

PROFI-TIPP

Wie Profis Daten schneller retten

Für Anwender, die mit dem Aufbau einer Festplatte vertraut sind, haben wir zwei weitere, leistungsstarke Tools auf die Heft-CD gepackt: Testdisk und Photorec. Bei beiden handelt es sich um Open-Source-Programme, die Sie über die Eingabeaufforderung steuern. Zum Installieren entpacken Sie einfach die ZIP-Archive der Tools auf die Festplatte. Gehen Sie dann auf „Start | Ausführen“, und öffnen Sie durch die Eingabe von „cmd“ die Eingabeaufforderung. Navigieren Sie dann zu dem Ordner, der die beiden entpackten Programme enthält.

Testdisk: Das Tool findet gelöschte Partitionen mit den Dateisystemen FAT32, NTFS und ReiserFS und stellt sie wieder her. Doch Vorsicht: Da Testdisk den Master Boot Record (MBR) ändert, kann es auch intakte Partitionen überschreiben.

Zum Start rufen Sie die Datei testdisk_win.exe auf und wählen unter „Select a media“ die Festplatte aus. Bestätigen Sie die Auswahl mit „Proceed“. Jetzt fragt das Tool nach dem „partition table type“ – bei einem PC lautet er „Intel“. In der folgenden Auswahl gehen Sie auf „Analyse“. Testdisk vergleicht nun die Daten auf der Platte mit den Einträgen im MBR. Stößt es dabei auf eine gelöschte Partition, können Sie deren Attribut ändern, beispielsweise von „D“ für „deleted“ in „L“ für „logical“. Um gelöschte Partitionen zu finden, die im MBR nicht mehr eingetragen sind, steht die erweiterte Suche zur Verfügung. Danach können Sie die Attribute nochmals ändern und mit „Write“ den MBR überschreiben.

Photorec: Die Software hat sich auf die Wiederherstellung gelöschter Fotos spezialisiert, sie rettet aber auch andere Dateitypen wie etwa ZIP-Archive. Rufen Sie photorec_win.exe auf, und wählen Sie ein Medium aus. Bestätigen Sie dann mit „Proceed“. Geben Sie den Typ der Partitionstabelle an – normalerweise ist es „Intel“. In der nächsten Anzeige markieren Sie das Laufwerk und gehen auf „Search“, um die Suche zu starten. Das Tool stellt gelöschte Dateien automatisch wieder her und speichert sie im Ordner \recup_dir. Den finden Sie im Programmverzeichnis der photo-rec_win.exe.

plorer-Ansicht des Hauptfensters keine Ergebnisse anzeigt, durchsuchen Sie zunächst die verschiedenen Dateisysteme, die sich in der Regel auf einer CD/DVD befinden. Klicken Sie dazu im linken Fenster auf das „ISO“- beziehungsweise „UDF“-Symbol.

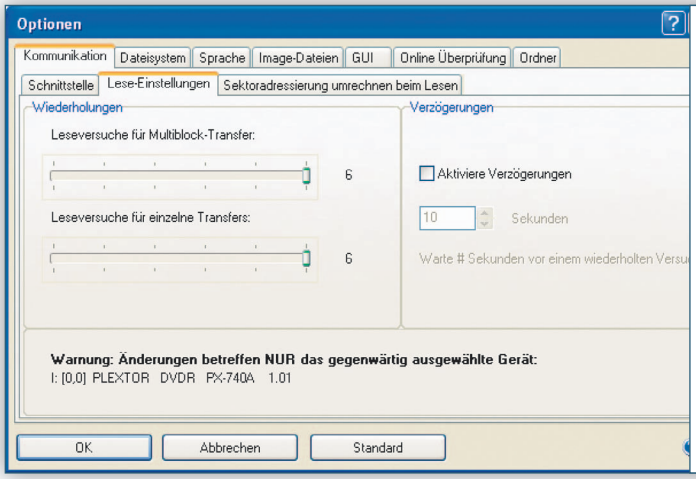
Falls das auch nicht hilft, ist ein zusätzlicher RAW-Scan erforderlich. Hierzu klicken Sie auf das CD/DVD-Symbol im linken Fenster und öffnen über die rechte Maustaste das Kontextmenü. Wenn Sie auf „Suche verlorene Dateien und Ordner“ klicken, spürt das Tool auch Files in einem defekten Dateisystem auf.

Dateien wiederherstellen: In der Explorer-Ansicht zeigt IsoBuster die gefundenen Dateien getrennt nach Dateisystemen an. Falls Sie einen RAW-Scan durchführen mussten, gehen Sie auf „Dateien gefunden über ihre Signatur“. Markieren Sie im rechten Fenster alle Files, die Sie retten möchten, und starten Sie über das Kontextmenü die Funktion „Extrahieren“.

TIPP Lässt sich ein Datenträger nur schwer einlesen, klicken Sie in IsoBuster auf das CD/DVD-Symbol und wählen über das Kontextmenü den Befehl „Eine verwaltete IBP/IBQ Image-Datei anlegen“ an. Mit dieser Einstellung extrahiert das Programm alle Daten von der CD oder DVD in eine Imagedatei auf der Festplatte. Dieses File können Sie dann wieder in IsoBuster öffnen und die Datenrettung auf diese Weise von der Festplatte starten. Diese Methode schont nicht nur die Mechanik Ihres CD- oder DVD-Laufwerks, sondern auch den ohnehin schon angegriffenen Rohling. Außerdem läuft die Suche nach den beschädigten Dateien deutlich schneller ab als auf CD oder DVD.

TIPP Haben Sie die verlorenen Dateien auch mit der eben beschriebenen Image-Analyse nicht entdeckt, gibt es noch eine weitere Möglichkeit. Legen Sie die beschädigte Scheibe erneut ins Laufwerk, und erhöhen Sie danach in IsoBuster über „Optionen | Kommunikation | Lese-Einstellungen“ die „Leseversuche“ von „3“ auf „6“. Jetzt versucht das Tool sechsmal, einen beschädigten Block auf der DVD auszulesen. Aber haben Sie viel Geduld: Der Vorgang kann bei dieser Einstellung schon mal ein paar Stunden dauern. Deshalb sollten Sie zu diesem Mittel nur dann greifen, wenn Sie auf die verlorenen Daten wirklich angewiesen sind.

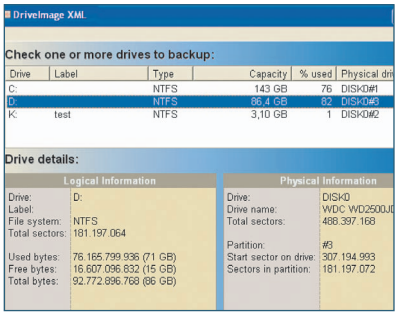
Markus Mandau



Mehrfach probieren: IsoBuster kann bei einem korrupten Sektor auf CD oder DVD bis zu sechs Leseversuche starten.

VORSORGE-TOOLS

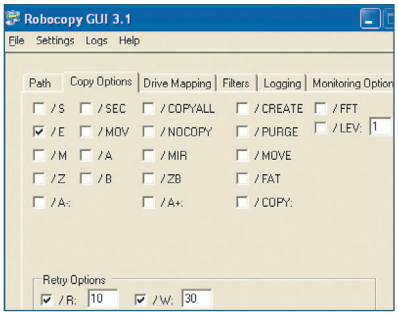
Datenverluste von vornherein verhindern



1 DriveImage XML 1.18

Das Image-Programm sichert Partitionen und stellt sie wieder her. Neben der Imagedatei legt es auch ein XML-File als Inhaltsverzeichnis an. Mit dessen Hilfe können Sie ein gespeichertes Image öffnen, um einzelne Dateien wiederherzustellen. Wenn Sie die Systempartition sichern wollen, binden Sie das Tool in Bart's PE Builder (**www.nu2.nu**) ein, um das Image bootfähig zu machen.

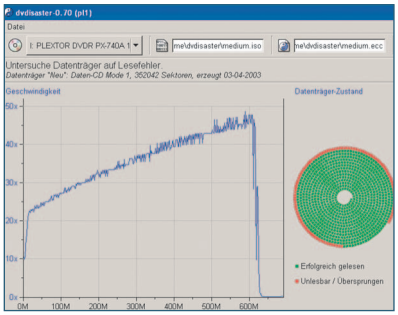
Info: www.runtime.org



2 Robocopy GUI 3.1.1

Das rasend schnelle Backup-Tool wird nur per Kommandozeile gesteuert. Kombinieren Sie es deshalb mit der Freeware Robocopy GUI, die allerdings ein installiertes .NET Framework voraussetzt. Die Bedienoberfläche bringt zudem eine Dokumentation zu Robocopy mit. Mit dessen Hilfe treffen Sie auch schnell die Einstellungen für ein zeitgesteuertes, inkrementelles Backup im Hintergrund.

Info: www.gotdotnet.com



3 Dvdisaster 0.70

Das Tool versichert Sie vor Datenverlusten bei CDs und DVDs, indem es eine verbesserte Fehlerkorrektur anlegt. CDs und DVDs besitzen zwar bereits eine integrierte Fehlerkorrektur. Doch die sorgt nur dafür, dass trotz kleiner Kratzer noch alle Daten lesbar sind. Bei größeren Schäden versagt sie, Dvdisaster aber nicht. Das Tool legt seine Fehlerkorrektur als zusätzliche, separate Datei auf der Festplatte ab.

Info: www.dvdisaster.de

Das nächste CHIP-Sonderheft — Ab 19. März

Umsteigen auf Vista

Endlich ist es so weit: Das neue Windows ist da. Das nächste CHIP-Sonderheft macht Sie mit sämtlichen Neuheiten von Windows Vista vertraut und hilft Ihnen beim sicheren Umstieg.

→ Der leichte Einstieg

Die wichtigsten Fragen zu Vista, die richtige Version wählen, Update oder Neuinstallation, alle Neuheiten

→ Vista perfekt einrichten

Die neue Oberfläche konfigurieren, Vista-Treiber finden, Netzwerk aufbauen, Internet einrichten

→ Vista sichern & tunen

Alle Sicherheitsfeatures komplett erklärt, die besten Registry-Tweaks für Vista, die wichtigsten Shortcuts, die ersten Tipps & Tricks

www.chip.de/vista

Foto: Microsoft

Impressum

Redaktionsleiter Sonderhefte: Andreas Vogelsang (verantwortlich für den Inhalt)
Redaktion: Manuel Schreiber
Freie Mitarbeiter: Isolde Durchholz (Schlussredaktion), Roland Freist (Redaktion)
Autoren dieser Ausgabe: Stephan Goldmann, Franz Grieser, Andreas Hentschel, Andreas Hitzig, Thomas Hümmler, Peter Klau, Markus Mandau, Valentin Pletzer, Michael Schweizer
Leserservice CHIP-Sonderhefte: sonderhefte@chip.de
Grafische Gestaltung: Isabella Schillert (CvD), Steffi Schönberger (Titel, Grafikleitung)
Bildagentur/Syndication: Sabrina Stange (Projektmanagerin); Calina Amann, Tel. (089) 746 42-150, www.chipimages.de
EBV: Jürgen Bisch, Gisela Zach
Bildredaktion: Kersten Weichbrodt (Ltg.), Gertraud Janas-Wenger, Gabi Koller
Zentrale Hardware: Dr. Ingo Kuss (Ltg.), Sepp Reitberger (Stellv.), Andreas Ilmberger (Ltd.), Daniel Wolff (Ltd.), Klaus Baasch, Gerhard Bader, Tomasz Czarnecki, Christian Friedrich, Werner Gaschar, Martin Jäger, Peter Krajewski, Thomas Littschwager, Monika Masek, Loys Nachtmann, Torsten Neumann, Nicole Ott, Gunnar Troitsch
CHIP-CD/-DVD: Anja Laubstein (Ltg.), Bastian Stein (Manager), Alfred Stumpf (Ltg. Produktion)
Geschäftsführer: Josef Zach
Verlagsleiter CHIP-Sonderhefte: Jürgen Hiller
Anzeigenleitung CHIP-Sonderhefte: Anke Huber (verantwortlich für den Anzeigenteil)
Herstellung: Dieter Eichelmann, Verlags-Herstellung, Vogel Services GmbH, D-97082 Würzburg
Verlag: Vogel Burda Communications GmbH, Poccistraße 11, D-80336 München, Tel. (089) 746 42-0, Fax: (089) 74 60 56-0
Die Inhaber- und Beteiligungsverhältnisse lauten: Alleinige Gesellschafterin ist die Vogel Burda Holding GmbH mit Sitz in Poccistraße 11, D-80336 München

Anzeigenverkauf:
PLZ 0, 1, 2, 3
Key Account Manager: Paul Schlier, Tel. (04642) 96 54 99, Fax (04642) 96 51 86
PLZ 4, 5, 6
Key Account Manager: Hartmut Wendt, Tel. (089) 746 42-392, Fax -325
Mediaberater: Andreas Krumm, Tel. (089) 746 42-464, Fax -325
Mediaberater: Alto Mair, Tel. (089) 746 42-197, Fax -325
PLZ 7, 8, 9
Key Account Managerin: Katharina Dursch, Tel. (089) 746 42-116, Fax -325
Mediaberater: Marcel Pelders, Tel. (089) 746 42-526, Fax -325
Zentrale Anzeigenverwaltung und Disposition:
Linda Anders, Tel. (089) 746 42-529, Fax -300,
Sabine Maurer, Tel. (089) 746 42-252, Fax -300 E-Mail: anzeigen@chip.de
Vertrieb Einzelverkauf:
Burda Medien Vertriebs GmbH, Arabellastraße 23, D-81925 München
Digitale Druckvorlagenherstellung:
Vogel Services GmbH, D-97082 Würzburg
Druck: AVD Goldach, CH-9403 Goldach