Special: Ad- und Spyware auf Ihrem Rechner

Verseuchte Freeware

Spyware, Badware und Crimeware schleusen sich über vorgebliche Freeware heimlich auf Ihren PC. Unser Ratgeber-Special klärt über die gefährlichen Tools auf und zeigt, wie Sie sich schützen.

Manche Utilities sind nur auf den ersten Blick völlig unbedenklich. Betrachtet man sie genauer, stößt man auf Funktionen, die nicht jeder gutheißt. Mehr noch: Dank„Hacker-Paragraf“ § 202c StGB sind bestimmte Utilities seit geraumer Zeit rechtlich besonders problematisch. Aber wer macht sich wobei überhaupt strafbar? Welche kostenlosen Programme darf man aus dem Internet herunterladen und welche nicht? In welcher Freeware verbergen sich Gefahren? Wir liefern die aktuelle Rechtslage, geben einen Überblick über populäre illegale Tools und sagen, welche Software in Ihrem eigenen Interesse nicht auf den Rechner gehört.

Die Inhalte im Überblick:

Ad- und Spyware auf Ihrem Rechner

VERSEUCHTE FREEWARE

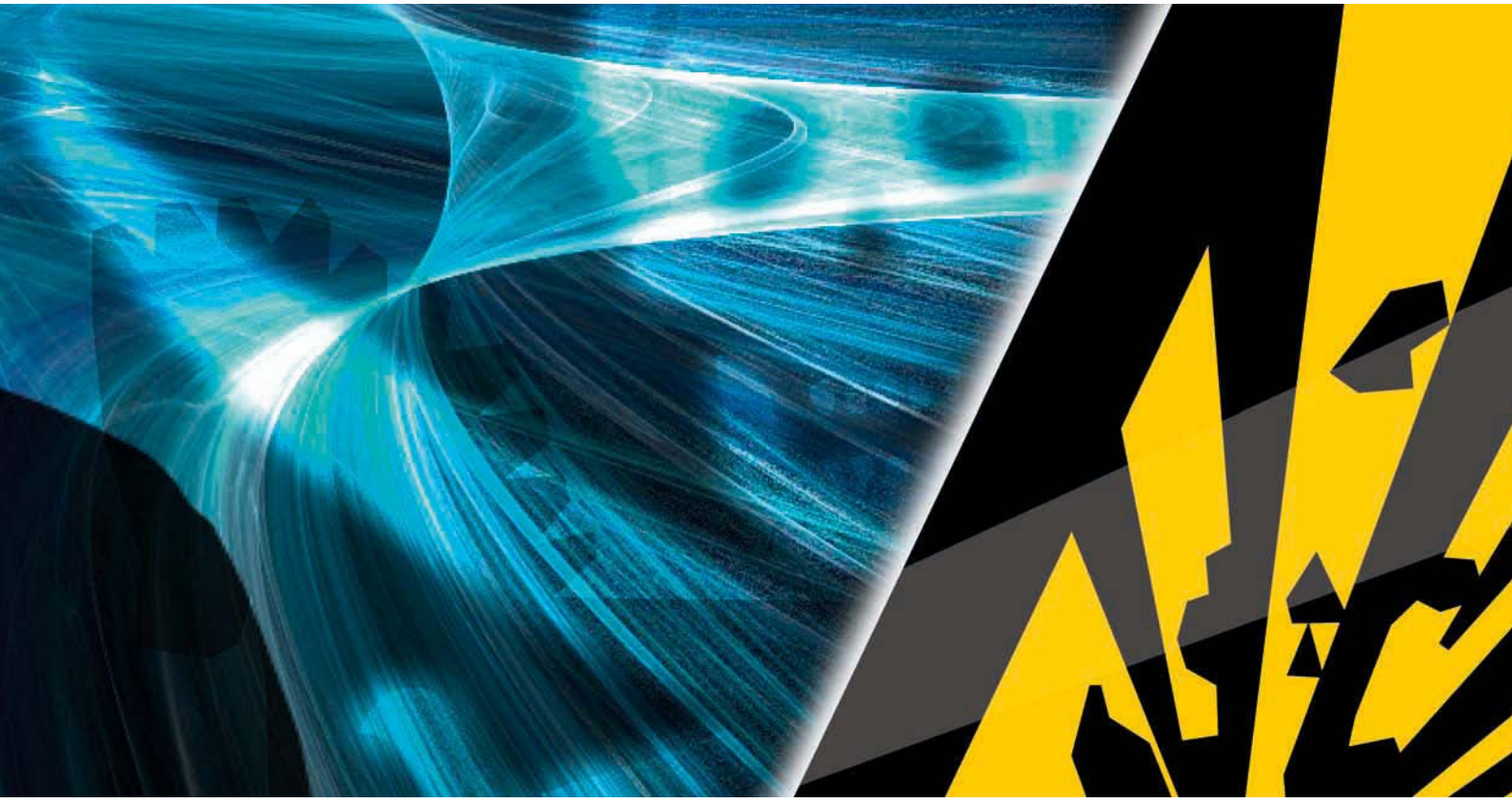
Spyware, Badware und Crimeware schleusen sich über vorgebliche Freeware heimlich auf Ihren PC. Wir klären über die gefährlichen Tools auf und zeigen, wie Sie sich schützen.

Von **Arne Arnold**

FREEWARE-PROGRAMME SIND BELIEBT. Schließlich leisten die kostenlosen Tools oft genauso viel wie Kaufprogramme, strapazieren aber nicht den Geldbeutel. Früher finanzierte sich manche Freeware über Werbemodule, die etwa Banner innerhalb des Programms anzeigten. Nach und nach wurden die Werbemodule aber immer neugieriger: Sie zeichneten auf, welche Websites der Anwender besucht und welche Begriffe er in Suchmaschinen eingibt. Die meisten Benutzer wollten das nicht und mieden solche werbefinanzierte Freeware, die dann mit der Zeit auch nicht mehr angeboten wurde.

Seit einiger Zeit sind viele Anwender jedoch nicht mehr so sensibel, was ihre Privatsphäre angeht. Das haben auch Freeware-Programmierer mitbekommen, und schon integrieren sie wieder etliche Zusatzmodule in ihren Programmen, über deren Notwendigkeit man streiten kann …

Außerdem gibt's jede Menge Abzocker-Programme, die vorgeben, das System kostenlos zu schützen, in Wirklichkeit aber den Anwender dazu erpressen, eine kostenpflichtige Version zu kaufen. Dass die kei-



nen nennenswerten Nutzen hat, erfährt der Anwender nicht. Wir berichten über den aktuellen Stand bei werbefinanzierter Freeware, Ad- und Spyware sowie allen anderen potenziell unerwünschten Modulen. Und natürlich erfahren Sie auch, wie Sie sich vor den Gefahren schützen können.

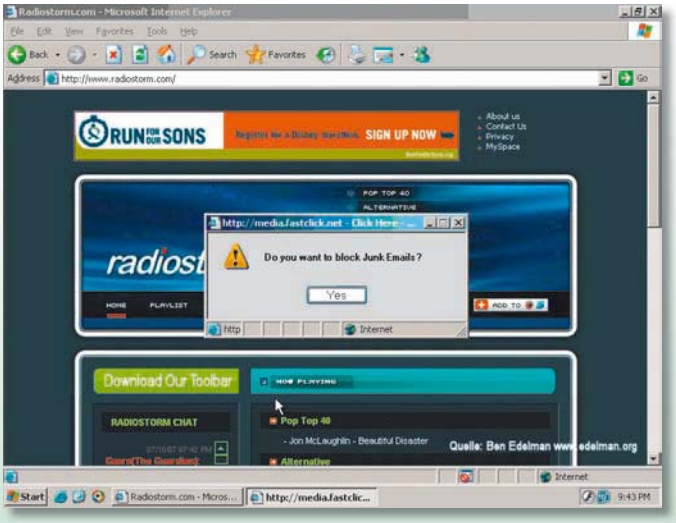
Verseuchte Freeware

Infektion erwünscht

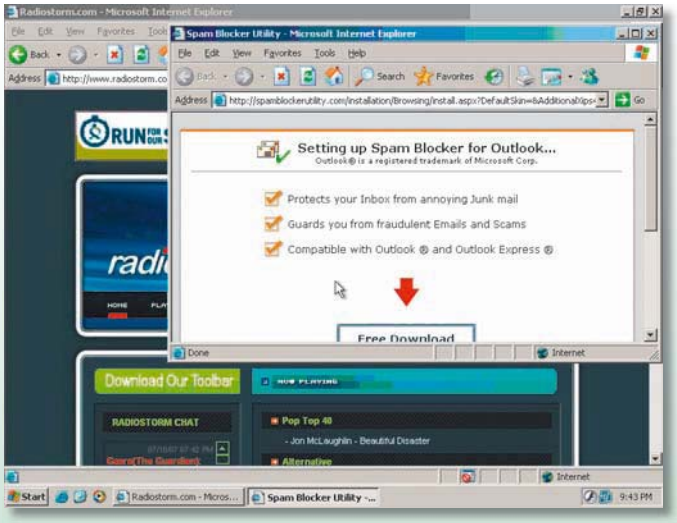
Der Begriff „werbefinanzierte Freeware" hat einen negativen Beigeschmack, der die meisten Anwender davon abhält, ein solches Programm zu nutzen. Darum achten clevere Programmierer genau darauf, dass ihr Tool nicht in diese Ecke gestellt wird.

Firefox: Sehr clever sind etwa die Macher von Mozilla Firefox. Sie integrierten in die Symbolleiste des Browsers ein Suchmaschinen-Eingabefeld, das standardmäßig auf Google eingestellt ist. Die meisten Anwender empfinden das als Service, als nützliche Funktion – nicht aber als das, was es für Mozilla in erster Linie ist: die Finanzierung ihrer Organisation über Werbung. Denn dieses Suchfeld stellt die Haupteinnahmequelle für Mozilla dar. Und das geht so: Firefox übermittelt den Suchbegriff an Google und kennzeichnet ihn als eine Anfrage, die von diesem Browser kommt. Das erkennen Sie an der Adresszeile, die Firefox aufruft: Dort steht am Ende „rls=org.mozilla:de:official & client= firefox". Klicken Sie im weiteren Verlauf auf Werbung, verdient daran nicht nur Google, sondern auch die Mozilla Corporation – und das nicht schlecht. Die Corporation gibt es seit 2005, sie ist eine hundertprozentige Tochter der Non-Profit-Organisation Mozilla Foundation. Als solche muss sie ihre Ein- und Ausgaben bekannt machen. Im Jahr 2005 verdiente Mozilla ganze 50,5 Millionen Dollar über die Kooperation mit Suchmaschinen – vornehmlich Google –, im Jahr 2006 waren es 61,5 Millionen. Vor diesem Deal mit Google lagen die Gesamteinnahmen deutlich darunter. Im Jahr 2004 beliefen sie sich auf 5,8 Millionen Dollar, im Jahr davor auf nur 2,4 Millionen. Den Report können Sie über **www.pcwelt.de/a3e** als PDF-Datei (55 KB) herunterladen. ›

Verseuchte Freeware: Der kostenlose Divx-Player kommt huckepack mit der Google-Toolbar. Mit der Installation der Software auf Ihrem Rechner verdienen viele Leute einen Haufen Geld



Neugierige Toolbar kommt mit einer Freeware: Auf dieser Website soll ein Werbe-Pop-up für einen Spamblocker zum Klicken verführen



Werbung im Browser: Wer auf das Pop-up klickt, landet schnurstracks auf der Download-Site für den Spamblocker

Unsere Meinung: Wir finden, gegen das Suchfeld in der Symbolleiste lässt sich eigentlich wenig einwenden. Es erhöht den Bedienkomfort, und wenn Mozilla daran verdient, geht das auch in Ordnung. Schließlich speichert Mozilla dabei keine anwenderbezogenen Daten. Anders sieht das aber bei etlichen Toolbars aus.

Toolbars: Verseuchung geduldet

So schnell wie eine aggressive Seuche verbreiten sich in letzter Zeit Suchmaschinen-Toolbars via Installationsprogramme von Freeware. Die Toolbars integrieren sich in den Internet Explorer oder Firefox. Sie stecken also nicht in der Freeware, sondern nur mit im Installationspaket.

Die gute Nachricht: Wer bei der Installation aufpasst, kann das Aufspielen der Toolbar abwählen – zumindest seriöse Freeware-Anbieter bieten diese Möglichkeit. Viele Anwender dulden aber, dass die zusätzlichen Suchfunktionen installiert werden, da mit den meisten dieser Toolbars auch ein gewisser Nutzen verbunden ist.

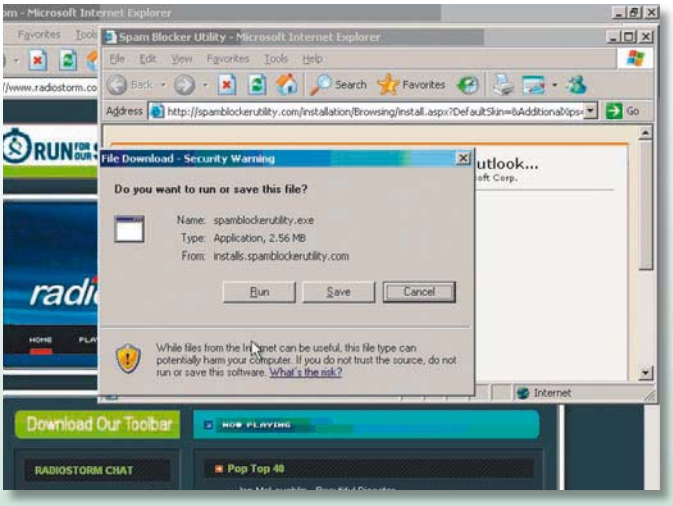
Ein Beispiel für die Toolbar-Freeware-Bündelung ist der Divx-Player, der selbst in der Shareware-Version Divx für Windows 6.7 noch mit der Google-Toolbar im Installationspaket kommt. Diese bringt als Funktion etwa die Integration von Google-Diensten wie „Text & Tabelle“ oder eine Rechtschreibprüfung mit. Einen Überblick über alle Funktionen gibt's über **www.pcwelt.de/b37**.

Gerade die Google-Toolbar steht aber in der Kritik von Datenschützern. Wer hier Funktionen wie Page Rank, Rechtschreibprüfung, Auto Link oder Wort-Übersetzung aktiviert, erklärt sich damit einverstanden, dass sein Surfverhalten an Google übermittelt wird.

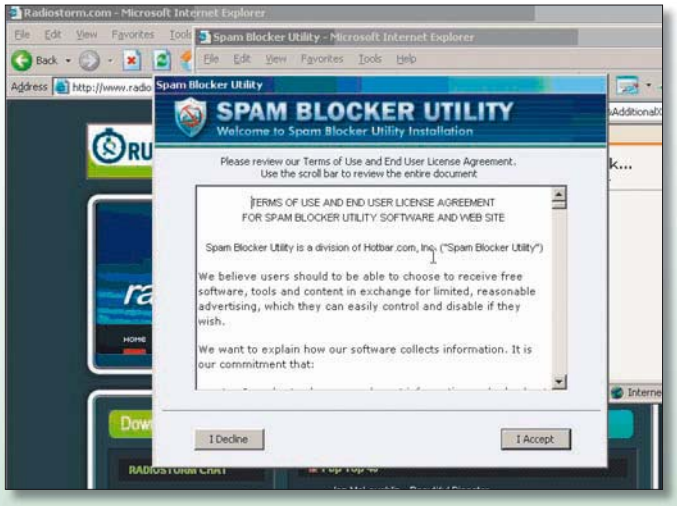
Unsere Meinung: Man kann Google zugute halten, dass der Konzern viel darüber verrät, was er speichert. Infos finden sich etwa auf der Datenschutzseite zur Toolbar (über **www.pcwelt.de/3dd**) und seit November 2007 auch als Video-Channel auf Youtube (**www.youtube.com/googleprivacy**). Trotzdem schätzen viele Anwender Googles Datenmacht und -sammlung als gefährlich ein und meiden die Toolbar.

Ad- & Spyware: Unerwünscht

Die Grenze zwischen nützlicher Such-Toolbar und spionierendem Browser-Plug-in ist unscharf. Nur für Anwender, die lieber



Software herunterladen: Das standardmäßige Download-Fenster des Browsers wird für den Spamblocker angezeigt



Ziemlich verwirrend: Nach dem Start der Installationsdatei erscheinen auf dem Bildschirm sogar Lizenzbedingungen

nicht verraten wollen, welche Websites sie besuchen, ist die Grenze klar: Toolbars von Suchmaschinen selbst sind meist noch akzeptabel, fast alle anderen Plug-ins mit Sucheingabe sind es nicht.

Beispiel Zango-Toolbar: Diese Toolbar kommt ebenfalls huckepack mit anderer Software. Diese wird teilweise recht aggressiv per Werbe-Pop-up angeboten, wie die Abbildung auf der vorherigen Seite zeigt.

Wer sich die Zango-Toolbar auf seinem Rechner installiert, bekommt Pop-ups angezeigt, die laut Zango auf die Suchbegriffe des Anwenders abgestimmt sind. Zumindest macht der Hersteller kein großes Geheimnis aus seiner Datensammelwut. Auf der Website erklärt er potenziellen Werbekunden, wie das System und damit das Geschäftsmodell funktioniert.

Badware: Je beliebter eine Freeware ist, umso interessanter ist sie für Programmierer von Werbemodulen. Und wenn die Freeware-Macher auch noch bereit sind, solche Module einzubauen, dann gibt's das Tool oft in mehreren verseuchten Versionen. Stopbadware.org, eine Organisation einer Universität und mehrerer Firmen, hat es sich zur Aufgabe gemacht, verseuchte Freeware zu finden (**www.stopbadware.org**). Als verseucht (also Badware) gilt für die Organisation jedes Programm, das auf dem PC des Anwenders Dinge macht, die der Anwender nicht wünscht.

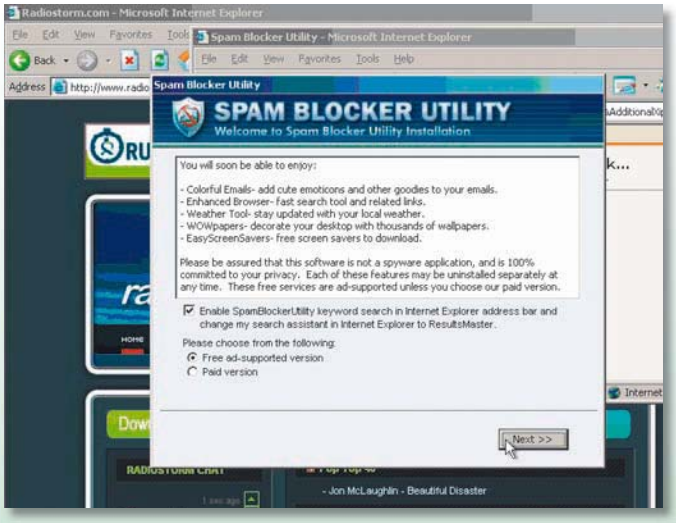
Der Begriff Badware umfasst damit Ad- und Spyware, aber auch noch weitere nervige Programme. Die Organisation veröffentlicht eine Liste mit Programmen, die sie als Badware einstuft.

Kazaa: Auf der Liste findet sich etwa die verbreitete Tauschbörsen-Software Kazaa. Stopbadware.org hat das Tool heruntergeladen und analysiert. Das Ergebnis: Kazaa kommt mit sieben weiteren Tools, um die der Anwender nicht gebeten hat. Dazu zählen Topsearch und Altnet Peer Points Manager (beide unter **www.altnet.com**), Cydoor (**www.cydoor.com**) oder RX Toolbar (**www.searchenginebar.com**).

Fast MP3 Search Plug-in: Ein weiteres Beispiel ist ein kleines Plug-in für den Internet Explorer, das man sich laden soll, um kostenlos an MP3-Musik zu kommen. Auf der Download-Website wurde unter anderem behauptet, dass niemand verfolgen kann, was man über das Plug-in herunterlädt. Eine Analyse ergab, dass eine ganze Reihe von Werbe- und Badware-Tools enthalten sind. Mit dabei waren etwa Tag A Saurus, Stop Zilla, Mirar Toolbar, UC more Search Accelerator, Command, Deluxe Communications, Enhanced Ads by Think-Adz removal, Internet Optimizer, Network Monitor, Related Page, Search Bar, Target Saver, Think-Adz Search Assistant Removal, Toolbar 888, Smitfraud-C und Windows Overlay Components. Alles Komponenten, die ein PC-Anwender gewöhnlich nicht auf seinem PC haben will.

Jessica Simpson Screensaver: Als letztes Beispiel von Stopbadware.org haben wir Jessica Simpson Screensaver herausgesucht. Er integriert einen Bildschirmschoner mit rund 40 Fotos von der Sängerin und Schauspielerin Jessica Simpson. Es ist möglich, dass es einen solchen Bildschirmschoner auch unverseucht gibt. Doch die Version, die Stopbadware.org gefunden hat, enthielt unter anderen diese Komponenten: Better Internet/Best Offers Network, Begin 2 Search, Dollar Revenue, Dy Fu CA (auch bekannt als Money Tree), e 2 give, Ezula, Get Mirar, Hotsearchbar, Media Motor, Prutect, Safesurfing, Web Hancer, Win AD, Wind Updates und Zango.

Liste von Stopbadware.org: Die Organisation Stopbadware.org gibt regelmäßig einen Bericht über unerwünschte Programme heraus. Zu jedem Tool gibt's eine genaue Analyse mit Angaben, wann der Code heruntergeladen wurde, was er vorgibt zu sein – und welche unerwünschten Bestandteile enthalten sind. Die Infos finden Sie auf **www.stopbadware.org/home/reports**.



So wird der PC zugemüllt: Wer „Free ad-supported Version" mit „Next" bestätigt, bekommt die Zango-Toolbar auf den Rechner

Betrugs-Software

Tuning-Software zockt Sie ab

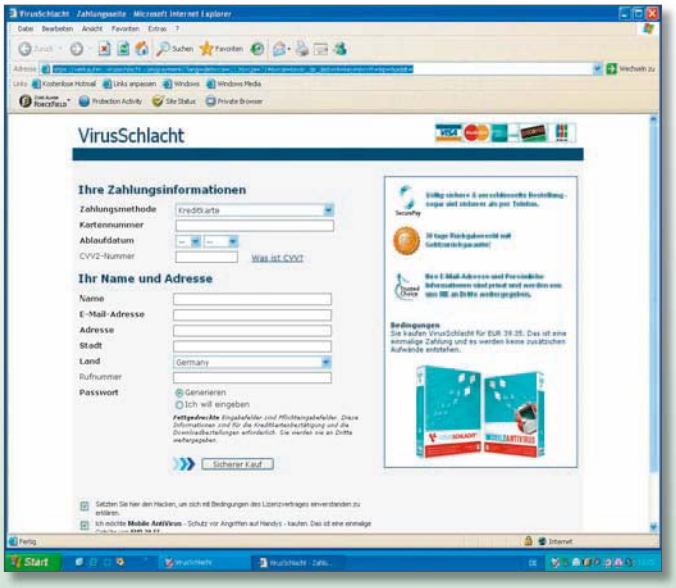
Im Jahr 2007 tauchten extrem viele Betrugsprogramme (Crimeware) auf. Das sind Tools, die versuchen, dem Anwender unter Vorspiegelung falscher Tatsachen das Geld aus der Tasche zu ziehen. Die Betrüger pro- ›

IM ÜBERBLICK Kostenlose Schutz-Tools

Programm	Kategorie	Windows	Internet (Download)	Seite
Ad-Aware 2007 Free 7.0.2 1) 2)	Ad- und Spyware-Jäger	2000, XP, Vista	**www.lavasoft.de** (19 MB)	–
Antivir PE Classic 7.0 1)	Antiviren-Programm	2000, XP, Vista	**www.free-av.de** (17 MB)	–
McAfee Siteadvisor 2.5	Website-Analyse	98/ME, 2000, XP, Vista	**www.siteadvisor.com** (1,7 MB)	110
Moka 5 1.0 1) 2)	virtueller PC	XP	**www.moka5.com** (45 MB)	111
Netcraft Toolbar 1.1 2)	Website-Analyse	2000, XP, Vista	**http://toolbar.netcraft.com** (3 MB)	110
Spbybot Search & Destroy 1.5.1 1)	Ad- und Spyware-Jäger	98/ME, 2000, XP, Vista	**www.spybot.info/de** (7 MB)	–
Windows Defender 1.5	Ad- und Spyware-Jäger	XP	**www.pcwelt.de/3d8** (5 MB)	–
WISO Internet Security 3)	PC-Sicherheitspaket	2000, XP, Vista	**www.buhl.de** (35 MB)	–

1) gratis für private Nutzung 2) englischsprachig 3) 180-Tage-Testversion Vollversion 39,95 Euro

So läuft der Nepp: Auf der Site eines vorgeblichen Optimierungs-Tools kommt ein Pop-up, das auf ein folgendes Download-Fenster hinweist



Angebliche Gratis-Antiviren-Software: Wer die Bedrohung beseitigen will, muss die Vollversion des Tools kaufen – für 40 Euro

bieren das beispielsweise mit vorgeblicher Tuning-Software oder Schein-Updates.

Schritt 1: Beim Surfen erscheint ein Pop-up, das einer Windows-Systemmeldung ähnelt. Darin wird behauptet, dass Ihr System nicht optimiert sei und sich die Leistung Ihres PCs erhöhen lasse. Es wird vorgeschlagen, kostenlos ein Tool zu installieren.

Schritt 2: Wer auf „OK“ klickt, gelangt auf die Website von Syskontroller, die eher einem Programm nachempfunden ist als einer Website. Der Button „SOFORTDO SCANNEN“ zeigt einen von mehreren Übersetzungsfehlern. Dieser wurde aber ein paar Tage, nachdem der Screenshot entstanden ist, bereits ausgemerzt.

Schritt 3: Wer auf den Button klickt, bekommt wieder ein Pop-up auf seinem Bildschirm zu sehen, das wiederum einer Systemmeldung nachempfunden ist. Es leitet den Besucher an, im folgenden Dialog – das wird ein normaler Datei-Download sein – auf „Ausführen“ zu klicken.

Schritt 4: Wer der Anweisung folgt, bekommt als Nächstes ein kleines Programmfenster angezeigt, in dem sich die Installation der Betrugs-Software starten lässt. Vermutlich um sich in einer gerichtlichen Auseinandersetzung besser verteidigen zu können, gibt es in diesem Fenster sogar einen Link zu den „Geschäftsbedingungen“. Von der Installation einer Tuning-Software ist in dem Fenster übrigens gar keine Rede. Dort heißt es: „Bitte, klicken Sie auf Fortsetzen, um Ihren PC vor allen Bedrohungen zu schützen“.

Schritt 5: Als Nächstes installiert sich die „Tuning-Software“ Syskontroller, die umgehend mit einer Systemprüfung beginnt. Die ist äußerst schnell erledigt und präsentiert dann angeblich gefährliche Systemfehler, die es gar nicht gibt.

Schritt 6: Um diese Fehler zu beseitigen, soll der Anwender die Vollversion kaufen. Wenn er auf „Sofort reparieren“ klickt, landet er auf dem Online-Shop von Syskontroller und soll 34,95 Euro bezahlen.

Sicherheits-Tool erpresst Sie

Die Masche mit der Tuning-Software (oben) gibt’s auch mit Sicherheits-Software. Hier ist der Druck auf den Anwender sogar noch um einiges höher. Denn die angeblichen Antispyware- oder Antiviren-Programme behaupten, sie hätten schädlichen Code auf dem PC gefunden.

Wieder bietet ein Tool seine Dienste an. Nach der Installation des Antiviren- oder Antispyware-Programms meldet dieses, es seien gefährliche Dateien auf dem Rechner und zur Beseitigung müsse der Anwender die Vollversion des Programms kaufen.

Einige dieser Abzock-Programme bringen übrigens die gemeldeten Schädlinge selber mit. Andere Abzocker gehen nicht ganz so weit – sie erfinden die Schädlinge einfach. Auch wenn Sie ein solches Programm auf ein frisch installiertes System aufspielen, wird es also behaupten, der Rechner sei verseucht.

Einige der Programme begnügen sich übrigens nicht mit der einmaligen Kauf-Aufforderung. Stattdessen platzieren sie sich im Infobereich neben der Uhr und melden sich stündlich mit der Warnung, dass der Rechner verseucht und der Kauf der Vollversion für die Reinigung nötig sei. So wird nach und nach Druck auf den Anwender aufgebaut und laufend erhöht.

Betrug erkennen

Richtig installieren & Filter einsetzen

Gegen Toolbar-verseuchte Freeware: Vor Programmen wie Toolbars, die sich bei der Installation eines anderen Utilitys aufdrängen, schützen Sie sich recht einfach. Man muss sich nur daran gewöhnen, bei der Installation alle Optionen des Assistenten gründlich zu studieren. Das Häkchen für die Zusatzinstallation der Toolbar entfernen Sie dann.

Gegen Abzock-Tools: Schwieriger wird es bei Abzock-Tools, die selbst für Profis nicht immer leicht zu erkennen sind. Generell helfen Website-Filter wie die **Netcraft-Toolbar** oder **McAfee Siteadvisor**. Beide sind kostenlos, und es gibt sie sowohl für den Internet Explorer als auch für Firefox. Beide Tools sollen Sie warnen, wenn Sie versehentlich auf die Website eines Betrügers geraten. So kommen die angeblichen Antispyware-Tools gar nicht erst auf Ihren Rechner.

Betrüger oder schlechtes Programm

Die schlechte Nachricht: Website-Filter warnen nicht vor jeder Website, auf der an-

gebliche Antispyware-Programme Sie ausnehmen wollen. Der Grund: Einige der Tools beseitigen tatsächlich ein paar „Schädlinge". Sie melden etwa harmlose Cookies als gefährliche Spyware. Die kostenpflichtige Vollversion löscht dann alle Cookies. Manche Utilities beseitigen sogar ein paar Viren. Den Machern der Abzocker-Tools kann man also nur vorwerfen, dass sie ein ganz schlechtes Programm verkaufen. Ob das strafbar ist, ist allerdings sehr ungewiss. Entsprechend werden die Websites dieser Programme von den Filter-Tools nicht immer als gefährlich gekennzeichnet. Bei Grenzfällen bleiben aber alle Website-Filter stumm.

Internet: Google-Fundstellen checken

Auf der sicheren Seite sind Sie natürlich, wenn Sie nur Tools ausprobieren, die vorher etwa von PC-Magazinen geprüft wurden. Doch wenn Sie gerne viele neue Tools ausprobieren, reichen diese Informationen vielleicht nicht.

Bevor Sie also ein Tool installieren – vor allem, wenn es sich über ein Pop-up angeboten hat –, sollten Sie zuerst über eine Suchmaschine detaillierte Hintergrundinfos dazu einholen. In eindeutigen Fällen kommen gleich als Erstes Links zu Anleitungen, wie man das Programm wieder los wird. Dann ist klar, dass es sich um keine erwünschte Software handelt. Denn die Abzocker-Tools haben zudem die Eigenschaft, sich sehr tief und widerstandsfähig ins System einzuklinken. Um sie wieder zu entfernen, bedarf es also oft einer Hilfestellung. In manchen Fällen tauchen aber auch die Website zum Programm selbst und sogar ein paar Einträge in Download-Archiven auf. Dann sollten Sie ein paar von den Sites lesen, die eine Anleitung zum Entfernen des Tools geben, um ein Gefühl zu bekommen, ob es ein bösartiges Tool ist.

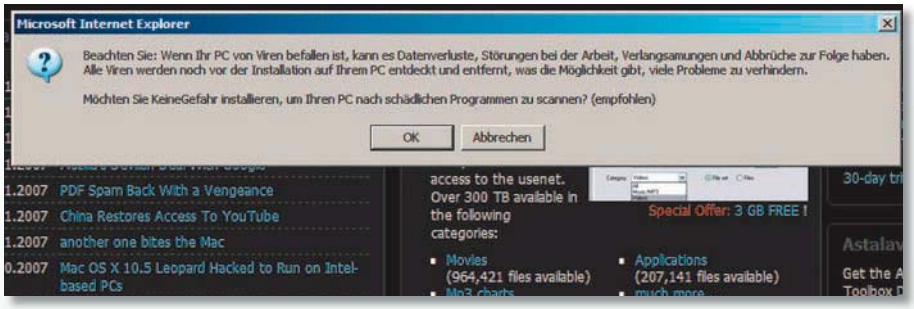
Verzwickt wird es, wenn Sie bereits ein zwielichtiges Programm installiert haben und nachträglich darüber Infos einholen. Dann kann es vorkommen, dass Sie auf Websites stoßen, die Ihnen fürs Entfernen ein Tool anbieten, das Sie kaufen müssen. Das kann dann ein seriöses Programm sein, es kann sich aber auch um ein Abzocker-Tool handeln. Hier empfiehlt es sich ebenfalls, mehr Infos einzuholen.

Wichtig: Wenn der Tool-Name zwei- oder mehrteilig ist, dann geben Sie ihn in Anführungszeichen ein. Sonst werden zu viele irrelevante Treffer angezeigt.

Infektion vermeiden

Den solidesten Schutz für Ihren PC erhalten Sie, wenn Sie damit gar nicht erst ins Internet gehen. Das klappt tatsächlich – dank Virtualisierungs-Software. Sie installiert einen virtuellen PC, mit dem Sie online gehen. Sollten sich tatsächlich unerwünschte Programme einschleusen, bleibt Ihr eigentliches System davon unberührt.

Moka 5 macht Virtualisierung sogar ganz einfach. Nach der Installation laden Sie sich über das Programm ein Betriebssystem zum Surfen herunter – etwa das Fearless Browser genannte Linux-System. Fachkenntnisse sind dafür nicht nötig. Allerdings brauchen Sie eine Breitband-Anbindung: Für Fearless Browser sind schon 165 MB fällig, für ein Ubuntu-System gehen rund 765 MB durch die Leitung.



Aufmerksamkeit erwecken: Ein Pop-up auf einer Website empfiehlt dem Anwender, seinen Rechner nach Viren durchsuchen zu lassen , um ihn später zum Kauf einer Vollversion zu bringen

Seriöse Aufmachung: Wer auf das Virenscan-Pop-up geklickt hat, landet auf der Website eines vorgeblichen Antiviren-Tools, die den Anwender mit einer vertrauenserweckenden Optik empfängt

Scheinbare Bedrohnung: Nach einem „Scan" des Systems stuft das Tool harmlose Cookies als mittlere Bedrohung ein und verunsichert dadurch den Anwender

Diese Tools gehören nicht auf Ihren PC!

Foto: © ktsdesign – Fotolia.com

Checken Sie Ihren PC auf inoffizielle Tools. Falls eines der von uns vorgestellten Programme ohne Ihre explizite Zustimmung auf dem Rechner installiert ist, sollen Sie schnellstens aktiv werden.

Von **Ramon Schwenk**

ES GIBT PROGRAMME, DIE ALLE ALARMGLOCKEN schrillen lassen, sofern Sie sie auf Ihrem PC entdecken. Zwar sind es allesamt Utilities, die nützliche Dienste leisten – etwa wenn Sie Sicherheitslücken in Netzwerken aufspüren oder vergessene Codes für komprimierte Dateien herausbekommen wollen. In den falschen Händen können sie aber Schaden anrichten oder sind gar zu kriminellen Zwecken zu gebrauchen. Denn die hier vorgestellten Tools haben auch einige Risiken und Nebenwirkungen. Wenn eines der von uns genannten Programme ohne Ihr Wissen auf Ihrem PC landet, ist Gefahr im Verzug. Möglicherweis versucht ein Mitbenutzer, der Zugang zum Rechner hat, Daten auszuspionieren.

Wir raten Ihnen: Entfernen Sie die problematischen Programme schnellstens von Ihrem System.

Sogar das Herunterladen ist manchmal gesetzeswidrig

Einige Utilities demonstrieren Ihnen, wie unsicher Windows ist. Die Kennwort-Knacker des Herstellers Nirsoft beispielsweise lesen Kennwörter aus Programmen wie Outlook, Thunderbird, Instant Messenger oder dem Windows-Netzwerk aus. Freilich lässt sich ein solches Tool auch zum illegalen Ausspionieren von Codes auf anderen Rechnern nutzen. Tools wie dieses unterstreichen, dass es fahrlässig ist, Zugangsdaten in Programmen zu speichern.

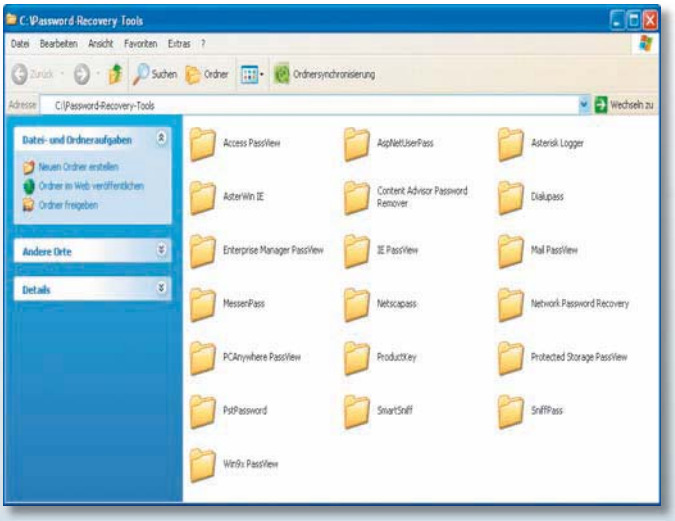
Eines der Programme, die wir Ihnen vorstellen (Any DVD), dürfen Sie nicht herunterladen. Auch wenn Sie einen gebrauchten Rechner erwerben und das Tool entdecken, sollten Sie es schnellstens löschen.

Bitte beachten Sie: Aus rechtlichen Gründen verzichten wir in diesem Artikel auf den gewohnten Service, Web-Adressen zu den einzelnen Tools anzugeben!

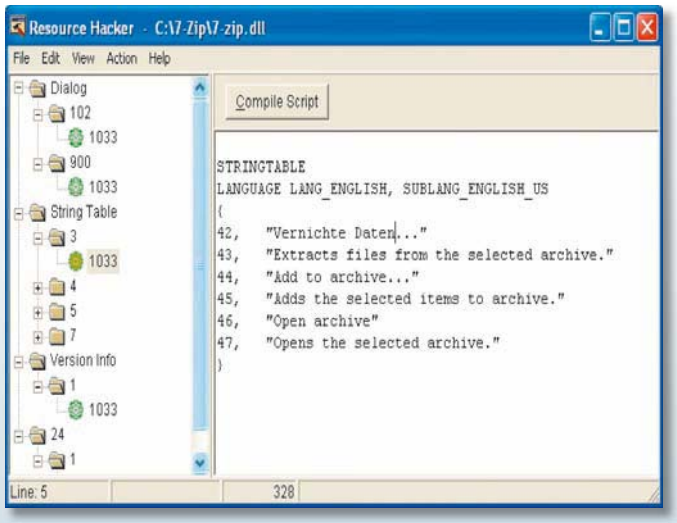
iPod-Knacker Jhymn entfesselt iTunes-DRM

Apple arbeitet beim iTunes Music Store mit einem Kopierschutz auf Basis von Digital Rights Management (DRM). Er haftet den heruntergeladenen Songs an und verhindert unter anderem, dass sich Musikstücke mit jeder Software nutzen lassen. Vielmehr sind Käufer zwingend auf die Abspiel-Software iTunes von Apple angewiesen.

Das kostenlose Tool Jhymn (Java Hear Your Music aNywhere) macht aus rechtmäßig im Music Store erworbenen Tracks MP3-Dateien ohne DRM. Sie lassen sich nach einer Konvertierung vom Apple-eigenen AAC-Format mit jeder Software abspielen, archivieren und auf jeden mobilen



Zugangsschutz umgehen: Der Hersteller Nirsoft bietet ein ganzes Arsenal an kostenlosen Kennwortknackern an



EXE-Dateien frisieren: Mit dem Resource Hacker kann man ausführbare Dateien editieren und dadurch beispielsweise Menübefehle fälschen

MP3-Player überspielen. Mit dem Tool lassen sich nur eigene Songs entdonglen, denn die Software ist zum Schutz vor Missbrauch an die Online-Anmeldung zum iTunes-Store geknüpft. Inzwischen hat Apple die Programmierer der Software übrigens durch eine Unterlassungserklärung aufgefordert, das Tool nicht mehr zum Download anzubieten.

Passwort-Entschlüsseler gratis für jeden Zweck

Sie schützen vertrauliche Geschäftsunterlagen und private Zugänge mit Passwörtern. Ein Kennwort fürs Homebanking, eins für den Freemail-Dienst, eins für die Anmeldung beim Messenger, eins für Web-Foren – es ist schwierig, sich alle seine Kennwörter zu merken. Praktisch ist da die Merkfunktion für regelmäßig genutzte Passwörter in vielen Anwendungen und Tools.

Wir möchten Sie warnen: Diese Schutzvorrichtungen sind einfach zu knacken. Die gespeicherten Daten lassen sich mit den Knack-Tools von Nirsoft einfach und sekundenschnell auslesen. Und: Die Passwortknackprogramme von Nirsoft halten das, was der Hersteller verspricht. Eine schnörkellose Bedienerführung, ein paar Klicks, und schon zeigt die Software die gewünschten Kennungen im Klartext an.

EXE-Dateien mit dem Resource Hacker manipulieren

Das, was Sie von einem Programm in Dialogen und Menüs auf dem Bildschirm zu sehen bekommen, lässt sich mit dem kostenlosen Resource Hacker in vielen Fällen ganz einfach verändern. Das Problem: Windows-Software ist nicht fälschungssicher.

Mit dem Tool Resource Hacker lässt sich die Oberfläche von Windows-Programmen manipulieren. Man kann Menüs, Dialogboxen und Hotkeys ändern, ergänzen oder entfernen. Außerdem ist es möglich, im Programm integrierte Icons zu tauschen.

Heimtückisch ist die Software, weil sich mit ihrer Hilfe Programmpunkte gefährlich umfunktionieren lassen, etwa indem der verhängnisvolle Kontextmenübefehl zum Löschen von Daten mit einer angeblich harmlosen Funktion beschriftet wird.

Wichtig: Die Lizenzinfos der meisten Programme verbieten die Manipulation ihres Codes. Bei unsachgemäßem Gebrauch von Resource Hacker kann die bearbeitete Software irreparabel beschädigt werden.

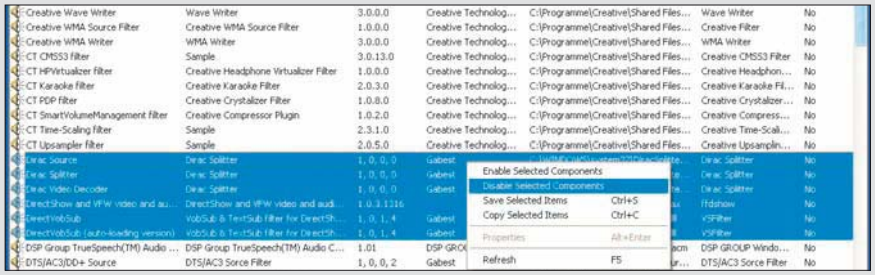
Perfect Keylogger Lite ist Gift

Das kleine einfach zu bedienende Utility Perfect Keylogger Lite zeichnet alle Tastatureingaben am Rechner auf. So finden etwa neugierige Dritte heraus, was Sie am PC machen, welche Programme Sie nutzen und auf welchen Web-Seiten Sie surfen. Das Tool kann sich gut vor den Blicken eines PC-Anwenders verstecken und ihn so unbemerkt überwachen. Sogar für den Taskmanager von Windows XP ist das Programm unsichtbar. Erst ein spezieller Taskmanager wie der kostenlose **Process Explorer** (**www.microsoft.com/sysinternals**) fin-

SO ENTFERNEN SIE NERVIGE CODECS wieder vom System

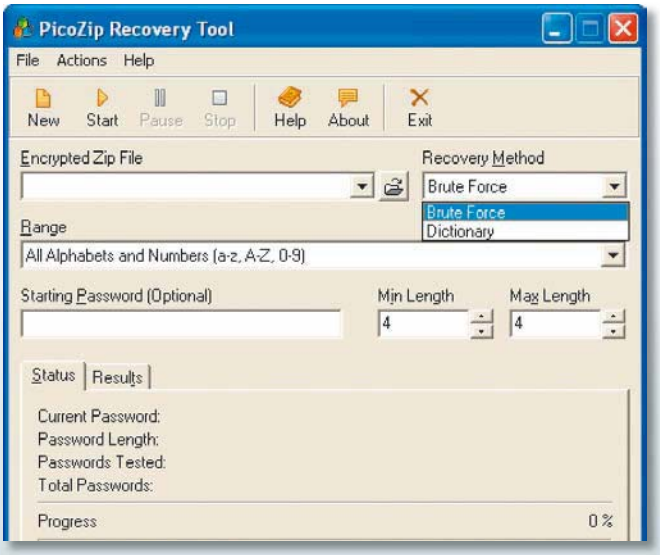
Zum Sichten und De-Installieren von Codecs ist die Freeware **Mmcompciew 1.10** empfehlenswert (**www.nirsoft.net**).

Das kostenlose Aufräumprogramm scannt die in der Registry verknüpften Codec-Module und zeigt sie in einer Tabelle an. Per Rechtsklick auf einen Eintrag lassen sich Codecs gezielt entfernen. Auch ohne Software werden Sie unterwünschte Codecs wieder los. Gehen Sie dazu in den Geräte-Manager unter „Audio, Video- und Gamecontroller, Audiocodecs/Videocodecs“.



Codec-Wahnsinn stoppen: Das kostenlose Aufräumprogramm Mmcompciew zeigt die im Betriebssystem installierten Codec-Module an und hilft bei der De-Installation

›



Passwort-Entschlüsseler: Picozip Recovery Tool kann vergessene Kennwörter im Klartext anzeigen, lässt sich allerdings auch zum illegalen Knacken von geschützten Dateien verwenden

det das Tool und zeigt es als Task an. Legal darf das Tool nur auf dem eigenen Rechner zum persönlichen Schutz eingesetzt werden und auch nur dann, wenn man sich den PC nicht mit jemandem teilt.

Der DVD-Kopierschutzknacker aus fernen Landen

Viele Anwender dürften sich schon einmal darüber geärgert haben, dass bei fast jeder DVD zunächst ein langweiliger Urheberrechtshinweis und die Werbung des Filmverleihers zu sehen sind. Any DVD ermöglicht es, direkt zu den Menüs oder zum Hauptfilm zu springen, also die lästigen und überflüssigen Einspielungen vor dem Film zu übergehen. Zudem gibt es DVDs, bei denen sich die Untertitel nicht unterdrücken lassen. Mit Any DVD gehört auch das der Vergangenheit an.

Außerdem ignoriert die Software Kopierschutzmechanismen wie Macrovision oder CSS – das ist eindeutig illegal. Dadurch lassen sich verschlüsselte DVDs kopieren – der Anwender registriert nicht mal, dass der Datenträger kopiergeschützt ist. Das Anbieten des Tools ist in Deutschland verboten.

Universal-Sniffer als Spürhund für lokale Netzwerke

Der Netzwerk-Sniffer Wireshark speichert und analysiert den Netzwerkverkehr. Das Tool kommt mit allen gängigen Protokollen zurecht. Es unterstützt unter anderem TCP/IP, IPX/SPX, SMB und Netbios. Das Utility eignet sich legal gut für die detaillierte Analyse bei Netzwerkproblemen. Allerdings sollten Sie es auch nur dafür einsetzen. Das Abhören des Netzwerkverkehrs ist in den meisten Fällen verboten. Wenn Sie den Verdacht haben, dass Sie mit Wireshark abgehört werden, können Sie das übrigens mit Administrations-Tools herausfinden.

Verschlüsselte ZIP-Dateien mit Software aufsperren

Viele Anwender schützen persönliche Dateien in ZIP-Archiven mit einem Kennwort. Der Passwortschutz sorgt jedoch nur für eine trügerische Sicherheit: Angreifer können ZIP-Passwörter leicht aushebeln.

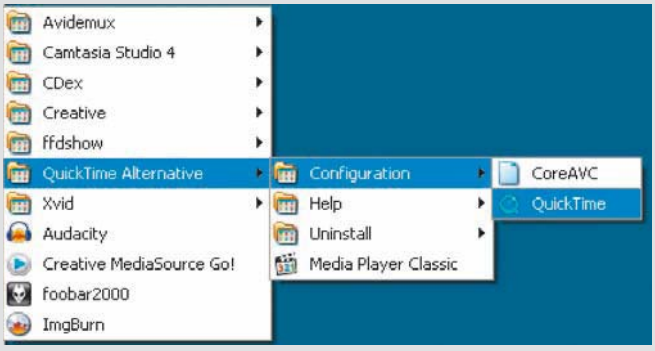
Beim Entsperren kommen Nachschlüssel wie das Picozip Recovery Tool zum Einsatz. Die Software analysiert die geschützte Datei und findet das benötigte Code-Wort heraus. Dazu attackiert das Knackprogramm die Datei mittels Brute-Force-Methode je nach Prozessorgeschwindigkeit mit bis zu mehreren tausend Zeichenkombinationen pro Sekunde, bis schließlich das Kennwort gefunden ist.

Codes im Netzwerk abhören

Die Passwörter von Mail- und FTP-Programmen enttarnt die kostenlose Software Sniff Pass ganz einfach. Das Tool belauscht dazu den Netzwerkverkehr. Aus den empfangenen und gesendeten Daten liest die Freeware Passwörter von Web- und FTP-Servern sowie von POP3-, IMAP4- und SMTP-Konten heraus. Sie werden vom Browser, dem FTP-Client und Mailprogrammen wie Outlook (Express), Thunderbird oder The Bat notwendigerweise unverschlüsselt übertragen. Problematisch ist Sniff Pass vor allem, wenn das Tool unbemerkt im Netzwerk eingesetzt wird. Da es ohne Installation läuft, kann es ein Angreifer von einem USB-Stick starten. Sobald Sie eine Web-, FTP- oder Mailverbindung aufbauen, hat er ihre Passwörter.

ORIGINAL ODER FÄLSCHUNG Alternative-Versionen

Musik und andere Audiodateien gibt es auf vielen Websites nur im Real- oder Quicktime-Format – etwa bei Amazon in der Musikabteilung zum Probehören der Titel. Wer sich dafür die fetten Original-Player wegen gelegentlicher Pop-ups und Protokollfunktionen nicht installieren möchte, weicht auf die englischsprachigen Alternative-Tools aus. **Real Alternative** und **Quicktime Alternative** sind praktische Alternativen für die ressourcenfressenden Player von Real (Real Player) und Apple (Quicktime). Die Pakete enthalten die nötigen Codecs, um Dateien in den jeweiligen Formaten wiedergeben zu können. Installiert wird dazu neben den entsprechenden Codecs auch der kostenlose Media Player Classic. Er kommt für die Wiedergabe von Film- und Musik-Stream sowie zum Abspielen lokal gespeicherter Dateien zum Einsatz und ist anders als die Original-Player nicht mit allerlei Zusatzfunktionen vollgestopft. Real Alternative unterstützt unter anderen Musikdateien im RA-, RM-, RMVB-, RAM-, RPM- und SMI-Format und kann auch in Web-Seiten eingebettete Musikdateien abspielen. Quicktime Alternative spielt die bei Apple üblichen Audio- und Videoformate ab. Zusätzlich bringen die Alternative-Packs Plug-ins für den Internet Explorer, für Firefox und für Opera mit. Herunterladen lassen sich die kostenlosen Pakete von der Website **www.codecpackguide.com**.



Quicktime-Alternative: Das Abspielen der Apple-Codes erfolgt über den mitgelieferten Media Player Classic

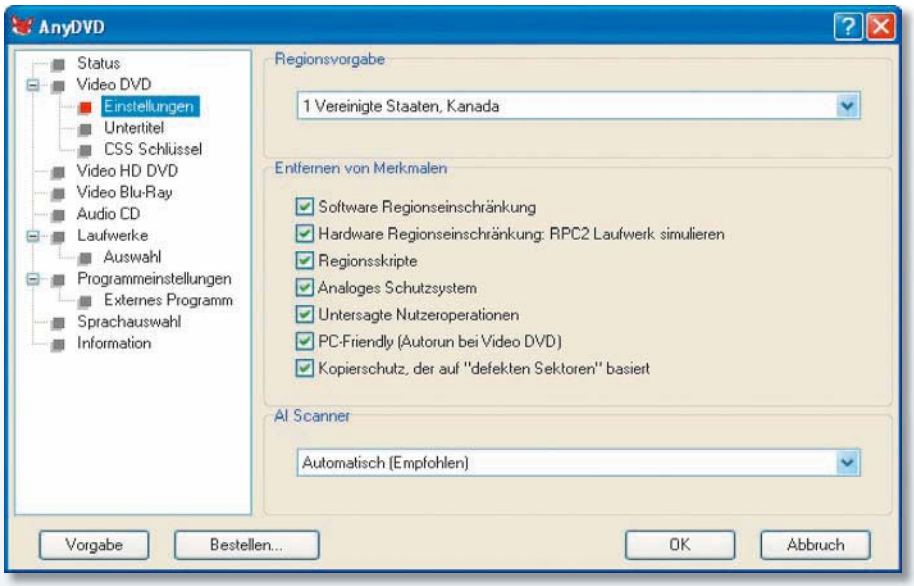
Benutzerkonten-Knacker für Windows XP und Vista

Offline NT Password & Registry Editor knackt Passwörter von Windows-Benutzerkonten. Die kleine Software mit dem langen Namen erlaubt das Löschen oder Ändern der Anmeldekennwörter von allen gespeicherten Benutzern einer Windows-Installation. Das gilt für Windows 2000, XP und Vista. Die Software ist nützlich, wenn Sie Ihr Kennwort vergessen haben und sich nicht mehr bei Windows anmelden können. Die Manipulation des Benutzerkontos kann auch schiefgehen. Wenn es beim Löschen des Passworts zu einem Schreibfehler kommt, wird Windows nicht mehr starten. Außerdem: Ändert man das Passwort eines Benutzers, der seine Dateien mit der Verschlüsselungsfunktion von Windows 2000 oder XP geschützt hat, lassen sich die Daten erst wieder entschlüsseln, wenn man das ursprüngliche Passwort eingibt. Sie sollten das Programm also nur in Notfällen einsetzen und auch nur die Passwort-Knackfunktion nutzen.

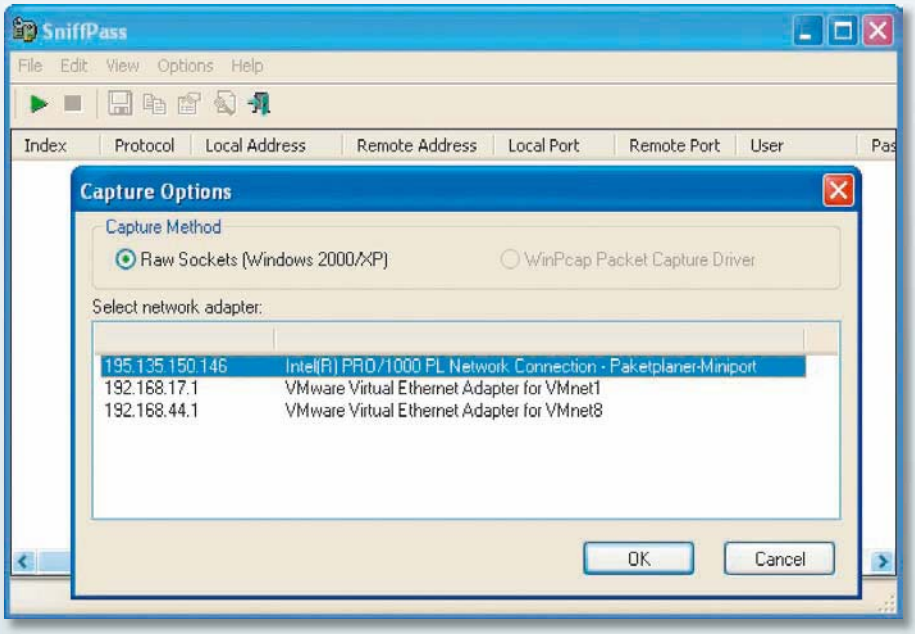
Codec-Packs: Vorprogrammiertes Wirrwar für Player

Wer seinen Rechner nicht mit zahlreichen Wiedergabe-Tools wie Divx, Apple Quicktime & Co. zumüllen möchte, greift auf ein Codec-Pack zurück. Darin sind die gängigsten Module für die Wiedergabe von Film und Ton enthalten, beispielsweise Divx, MPG 4, Ogg Vorbis und Xvid. Per Internet-Suchmaschine finden sich verschiedene Zusammenstellungen. Durch solche Pakete können Sie auch auf den Real- und den Quicktime-Player verzichten. So machen Sie mit nur einer Installation Ihren PC zum Abspielgerät für eine Vielzahl von Medienformaten. Das Codec-Pack liefert, was Sie für gängige Multimedia-Dateien benötigen. Mit einer Installation ist Ihr PC fit für fast jede Video- oder Audiodatei – jedenfalls theoretisch. In der Praxis ergeben sich allerdings mehrere Probleme: Oft ist der Inhalt eines Codec-Packs zumindest teilweise veraltet, und Windows wird häufig mit unnützen Codecs verstopft, die Sie gar nicht benötigen. Außerdem überschreiben manche Pakete ohne Rückfrage auf der Festplatte bereits vorhandene Codecs.

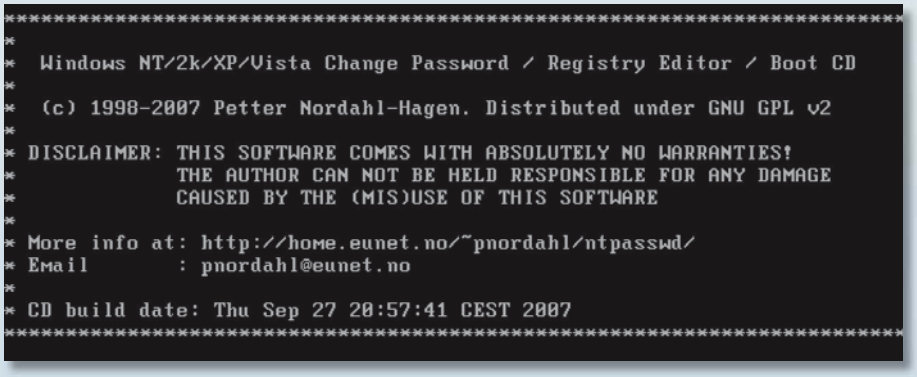
Die Codec-Packs enthalten auch kostenpflichtige Codecs. Ob der Herausgeber dafür die erforderlichen Genehmigungen hat, ist für den Nutzer nicht erkennbar.



Hierzulande illegal: Die Shareware Any DVD ist ein Treiber, der nach der Installation im Hintergrund automatisch und unbemerkt eingelegte DVD-Filme entschlüsselt



Spürhund mit TCP/IP-Nase: Der kostenlose Kennwort-Späher Sniff Pass fängt im lokalen Netzwerk übertragene Passwörter für Mailzugang, FTP-Server und so weiter ab



Kontoverwaltung austricksen: Offline NT Password & Registry Editor wird über eine Boot-CD gestartet und überschreibt Benutzer- sowie Administratorkennwörter in Windows-Systemen

VERBOTENE HACKER-TOOLS

Was darf man aus dem Internet herunterladen und was nicht? Hier die aktuelle Rechtslage und ein Überblick über 15 populäre illegale Tools.

Von **Hendrik Becker**

Hacker-Tools, Kopierschutzknacker, Freischalt-Cracks: Was ist erlaubt, was ist verboten? Waren Tools zum Belauschen des Netzwerkverkehrs vor eineinhalb Jahren noch legal zu bekommen, kann man sich heute schon beim Download strafbar machen (siehe Kasten auf dieser Seite).

Der Paragrafentext lässt aber einige Fragen offen. Denn es ist zum Beispiel gar nicht immer eindeutig zu bestimmen, wann ein Hacker-Tool ein Hacker-Tool ist. So offensichtlich, wie die Rechtslage scheint, ist sie also keineswegs – und sie kann sich morgen auch schon wieder ändern.

Wann wirkt ein Kopierschutz?

Schon seit 2003 sind Programme verboten, die den „wirksamen technischen" Kopierschutz von Werken umgehen, welche dem Urheberrecht unterliegen (siehe Kasten auf Seite 60). Auch hier fehlen konkrete Leitlinien, so dass möglicherweise auch harmlose Tools als illegal angesehen werden könnten. Die Definition, ob ein Programm oder ein Programmteil einen „wirksamen technischen" Kopierschutz umgeht, bleibt den Gerichten überlassen – jeder Richter kann hier anders urteilen.

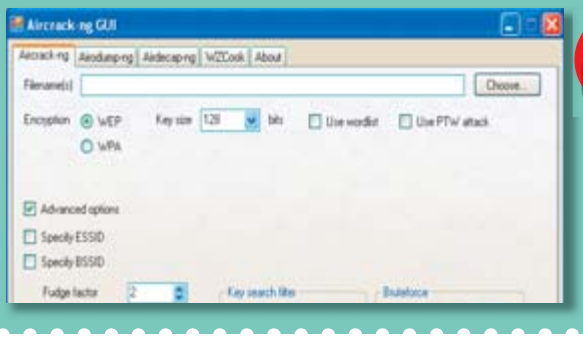
Überblick über illegale Tools

Wir haben 15 Programme in ihren aktuellen Versionen als Beispiele herausgesucht, deren Einsatz nach derzeitigem Stand der Dinge wohl als illegal angesehen werden muss – wenngleich sich einige Tools in Teilen des Funktionsumfangs wohl auch sinnvoll und legal einsetzen lassen. Wir raten davon ab, diese Tools aus Graubereichen des Internets herunterzuladen. Denn es gibt Trittbrettfahrer, die verseuchte Versionen verbreiten und Trojaner und Würmer gleichen Namens lancieren. Sie schaffen es sogar, ihre Download-Seiten weit vorne bei Google zu platzieren.

RECHT: HACKER-TOOLS

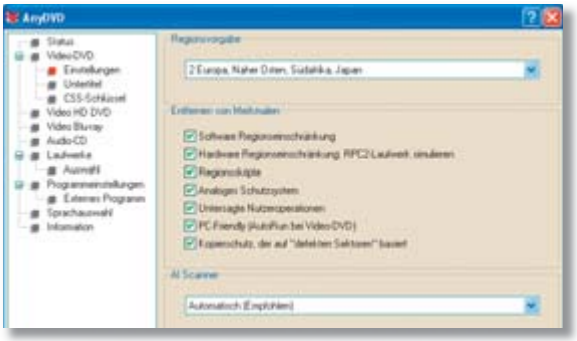
Deutschland hat im August 2007 EU-Vorgaben zur Bekämpfung von Computerkriminalität umgesetzt. Der Paragraph 202c des Strafgesetzbuches hält unter „Vorbereiten des Ausspähens und Abfangens von Daten" fest: Wer eine Straftat nach § 202a (Ausspähen von Daten) oder § 202b (Abfangen von Daten) vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. **Ist ein Zugangsschutz jedoch sehr schwach** – wie bei der Outlook-Maildatenbank –, stellt sich die Frage, ob er überhaupt als Zugangssicherung im Sinne von § 202a angesehen werden kann. Hierüber wird erst Klarheit herrschen, wenn eine höchstrichterliche Instanz ein Urteil getroffen hat.

Foto: getty images/David King



Aircrack-ng 1.0-rc1

WLANs sollte man tunlichst verschlüsseln, damit kein Fremder Schindluder treiben kann. Das alte WEP-Verfahren ist dafür allerdings ungeeignet: Die neue Version von Aircrack-ng ermittelt binnen Sekunden den Schlüssel eines WEP-geschützten Funknetzes. Schlüssel des sichereren WPA-Verfahrens kann Aircrack-ng nur durch Ausprobieren sämtlicher Buchstaben- und Zahlenkombinationen herausbekommen. Das dauert lange und ist bei komplexen Passwörtern sogar aussichtslos.

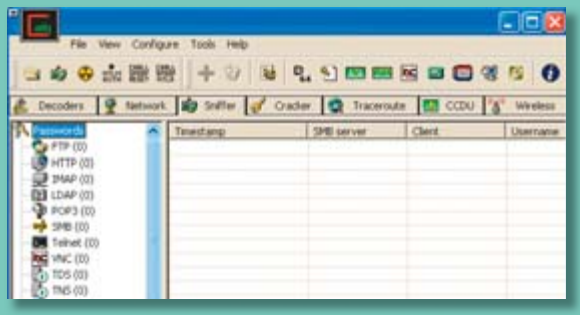


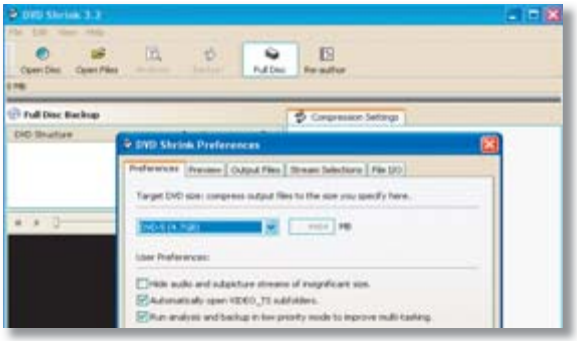
2 Anydvd (HD) 6.4.5.0

Anydvd klinkt sich ins Betriebssystem ein und entschlüsselt im Hintergrund Video-DVDs. In der neuen Version wurde der Knack-Algorithmus weiter verfeinert. Die HD-Variante von Anydvd unterstützt auch Blu-Ray und HD-DVD. Durch den Einsatz von Anydvd sieht es für Player-Software und Kopier-Utilities so aus, als wäre der Film unverschlüsselt. Dadurch wird es möglich, die DVD entweder 1:1 zu kopieren oder das Videomaterial von einem legal erhältlichen Recodier-Tool herunterrechnen zu lassen, etwa von der Shareware Clonedvd 2 (*www.elby.ch*).

3 Cain & Abel 4.9.17

Mit Cain & Abel lässt sich Datenverkehr in einem lokalen Netz belauschen. Das Tool ist in der Lage, die Zuordnungstabelle im Router oder Switch so zu ändern, dass es die Datenpakete abfangen kann. Über einen Trick lassen sich auch verschlüsselte HTTPS-Verbindungen belauschen. Cain & Abel zeigt nicht den rohen Datenverkehr an, sondern pickt sich die für Hacker relevanten Informationen heraus, zum Beispiel Benutzernamen, Passwörter und VoIP-Gespräche.



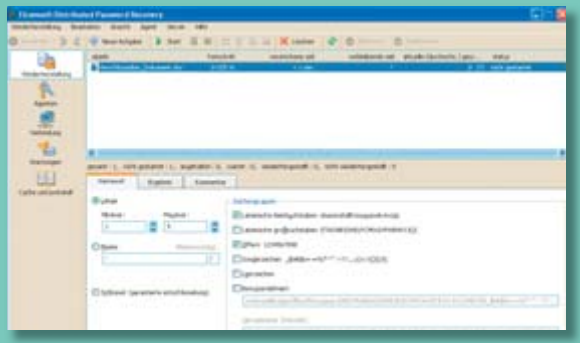


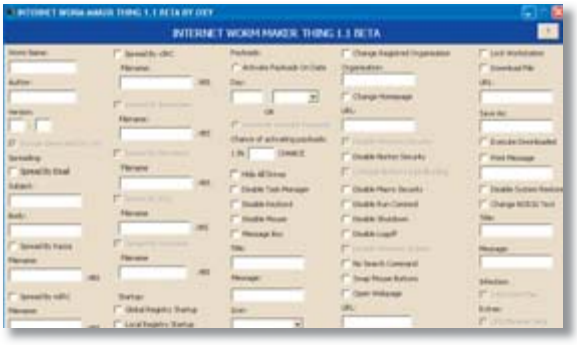
4 DVD Shrink 3.2.0.15

Mit DVD Shrink lassen sich manche kopiergeschützte DVDs duplizieren. Dabei umgeht die Software die unsichere CSS-Verschlüsselung und einige zusätzliche Schutzmethoden. Mit aktuellen Verfahren kommt DVD Shrink nicht zurecht, ebenso wenig wie mit HD-DVDs und Blu-Ray-Disks. Beliebt ist das Programm, weil es DVD-9-Filme auf DVD-4-Rohlingen unterbringt, indem es die Bit-Rate herunterschraubt und nicht benötigte Tonspuren sowie Extras weglassen kann. DVD Shrink entfernt auch den Regionalcode und eventuelle Restriktionen in der DVD-Benutzerführung.

5 Distributed Password Recovery

Elcomsoft Distributed Password Recovery 2.60.176 ist ein Hochleistungs-Tool zum Entschlüsseln von Passwörtern. Das Besondere an der Software: Sie kann die Rechenleistung von Grafikkarten mit Nvidias GPU Geforce 8 und 9 einbeziehen. Diese Graphical Processing Units sind bei Kryptografie-Berechnungen aktuellen CPUs mehrfach überlegen. Zudem ist das Programm in der Lage, die Berechnung im Netzwerk zu verteilen. Das Tool kann unter anderem Office-Dokumente und Windows-Passwörter knacken.





6 Internet Worm Maker Thing 1.1

Mit diesem Baukasten für Internet-Würmer kann sich ein Täter erschreckend einfach einen Schädling zusammenklicken. Damit ist das Tool eindeutig illegal. Der Täter bestimmt, welche Aktionen der Wurm durchführen soll. Dazu zählen neben harmloseren Dingen wie dem Vertauschen der Maustasten auch gefährlichere, zum Beispiel das Deaktivieren von Antiviren-Programmen und das Nachladen von Dateien. Auch die wurmtypischen Verbreitungs-Optionen sind vorgesehen. Wer einen Wurm in Umlauf bringt, muss mit ernsthaften rechtlichen Konsequenzen rechnen.

›

7 Offline NT PW & Registry Editor

Offline NT Password & Registry Editor erfüllt nur einen simplen Zweck, den aber sehr effektiv: Es ermöglicht, das Anmelde-Passwort von Windows XP und Vista auszuhebeln. Der Rechner muss über ein CD/DVD- oder ein Diskettenlaufwerk verfügen, über das er gebootet werden kann, denn das Tool kommt in Form eines bootfähigen CD- und Disketten-Images. Darin verbirgt sich ein Mini-Linux auf Kommandozeilen-Basis. Mit ein paar Eingaben ist das XP- oder Vista-Passwort entweder geändert oder gelöscht. Das ursprünglich gesetzte Passwort lässt sich nicht ermitteln.

8 Ophcrack Live-CD 2.0.1

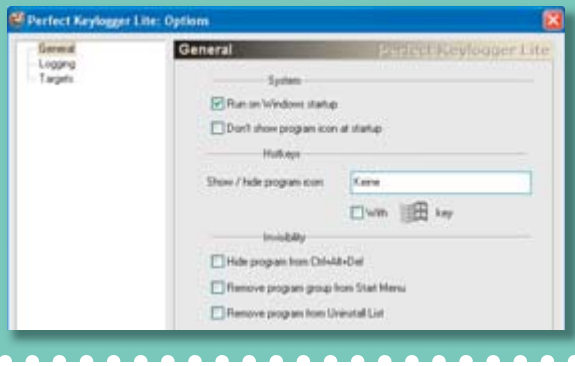
Die Ophcrack Live-CD ist eine Alternative zum Offline NT Password & Registry Editor. Der Unterschied liegt darin, dass man damit die gesetzten Passwörter nicht löschen und ersetzen, sondern ermitteln und anzeigen lassen kann. Ophcrack wird insbesondere dann eingesetzt, wenn jemand Zugang zu einem fremden PC erlangen will, ohne dass der Besitzer dies hinterher bemerkt. Das Tool nutzt die relativ neue Methode des Passwort-Knackens per Rainbow Tables.

9 Passware Kit Enterprise 8.3

Passwörter wiederherstellen und Dokumente entschlüsseln – darauf ist das kostenpflichtige Passware Kit Enterprise spezialisiert. Enthalten sind 25 Module, die jeweils für ein Dateiformat, eine Anwendung oder ein Software-Paket bestimmt sind. So lassen sich die Passwörter von Office-Dokumenten ebenso finden wie die von PDF-Dateien oder Datenbanken. Je nach Dokumentformat, Komplexität des Kennworts und verfügbarer Rechenleistung kann die Suche Wochen oder Monate dauern.

10 Perfect Keylogger Lite 1.15

Keylogger wie dieser werden benutzt, um Tastaturanschläge anderer Personen aufzuzeichnen. Dadurch lassen sich PC-Aktivitäten nachvollziehen und Passwörter ausspähen. Damit das Opfer nichts von der Abhöraktion bemerkt, lässt sich Perfect Keylogger Lite unsichtbar schalten. Nur mit dem richtigen Tastaturkürzel kann derjenige, der das Programm installiert hat, es wieder sichtbar machen und die Protokolldatei einsehen. Darin steht, in welchem Programm um welche Uhrzeit welche Tastatureingaben gemacht wurden.

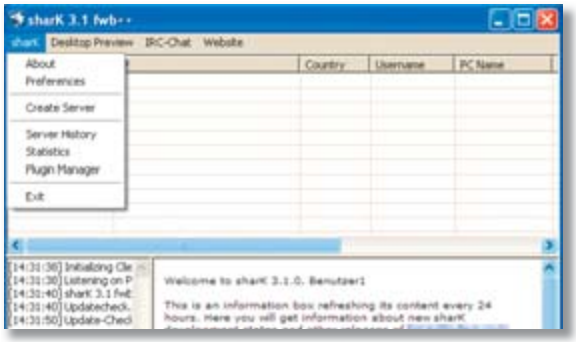


11 Protected Storage Passview 1.63

Im Bereich Protected Storage in der Windows-Registrierdatenbank werden Benutzernamen und Passwörter von bestimmten Anwendungen verschlüsselt und zum Teil zusätzlich noch versteckt abgelegt. Die Software Protected Storage Passview kann die sehr schwache Verschlüsselung knacken, die Zugangsdaten anzeigen und sie gesammelt in eine Textdatei speichern. So macht das Programm zum einen Login-Daten sichtbar, die im Internet Explorer gespeichert sind – also Passwörter für Websites. Zum anderen zeigt es die in Outlook und Outlook Express hinterlegten Login-Daten für Mailpostfächer an.

12 Pst Password 1.11

Dieses Tool knackt den Passwortschutz von Outlook 97, 2000, XP, 2003 und 2007. Wenn die Mail-Software auf dem System installiert ist, ermittelt das Tool selbständig, wo die Mail-Datenbank(en) mit der Endung .PST liegen. Wenn Outlook nicht installiert ist, lässt sich eine PST-Datei, die zum Beispiel von einem anderen Rechner stammt, manuell öffnen. Da der Passwortschutz in den aufgeführten Outlook-Versionen sehr schwach ist, benötigt das Tool keine lange Rechenzeit.



13 Shark 3.1

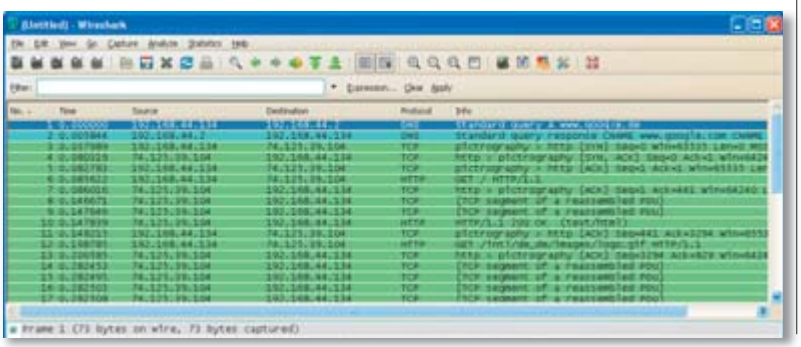
Rechner übers Internet fernsteuern – das ist der Einsatzweck von Shark. Anders als legale Remote-Desktop-Software wie Ultravnc ermöglicht Shark das aber auch ohne Kenntnis und Einwilligung des Nutzers, der vor dem entfernten PC sitzt. Die Server-Komponente von Shark tarnt sich auf vielerlei Arten, um unerkannt zu bleiben. Der Angreifer kann sie so seinen Opfern unbemerkt unterschieben, zum Beispiel per Mail oder als nützliches Programm getarnt über Web-Seiten. Die Server melden sich in regelmäßigen Abständen beim Angreifer und warten auf seine Befehle.

14 Vista Loader 3.0.0.1

Für Windows Vista existieren mehrere Cracks, die das Betriebssystem illegalerweise ohne gültige Lizenz nutzbar machen. Aber nur die neue Version von Vista Loader umgeht auch die Kopierschutztechniken von Vista SP1. Der Crack macht sich die Tatsache zunutze, dass Microsoft aktivierungsfreie Lizenzschlüssel an große PC-Hersteller ausgibt. Diese funktionieren aber nur, wenn Vista das jeweilige Hersteller-Bios auf dem PC vorfindet. Vista Loader täuscht daher dem Betriebssystem durch einen Treiber das passende Bios vor.

15 Wireshark 1.0.2

Mit Wireshark (früherer Name: Ethereal) lässt sich der komplette Netzwerkverkehr eines PCs protokollieren und analysieren. Auch andere PCs im Netz können belauscht werden, allerdings nur, wenn die Rechner über Hubs verbunden sind. Hubs kommen heutzutage eher selten vor, in aller Regel trifft man Switches an, die den Datenstrom geräteweise trennen. Wireshark zeigt jedes übertragene Paket einzeln an. Über die Kontextmenü-Funktion „Follow TCP Stream“ lässt sich die komplette TCP-Verbindung nachvollziehen, in der das gewählte Paket vorkommt.



RECHT: KOPIERSCHUTZ

Seit dem Inkrafttreten des neuen Urheberrechtsgesetzes im Jahr 2003 ist es in Deutschland nicht mehr erlaubt, Kopierschutzmaßnahmen zu umgehen (§ 95 a Abs. 1 Urheberrechtsgesetz). Nicht nur der Vorgang ist strafbar, sondern bereits Herstellung, Einfuhr, Verbreitung und Verkauf von Kopierschutzknackern, ebenso wie deren Bewerbung (§ 95 a Abs. 3 Urheberrechtsgesetz). Programme, die zum Umgehen von Kopierschutz angeboten werden, dürfen daher nicht mehr über deutsche Websites vertrieben werden. Die Anbieter operieren nun vom Ausland aus. Ein Download von ausländischen Servern dürfte aber bereits eine rechtlich unzulässige Einfuhr im Sinne des Gesetzes sein – so die Auffassung von Rechtsanwalt Johannes Richard (*www.internetrecht-rostock.de*).

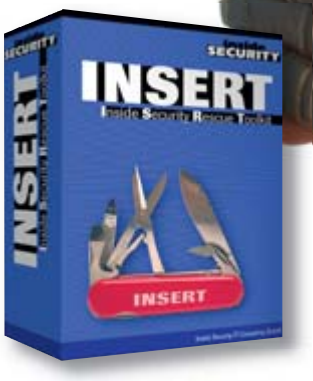
Mittlerweile ist bei Juristen umstritten, ob die unsichere CSS-Verschlüsselung von Video-DVDs überhaupt ein wirksamer Kopierschutz im Sinne des Urheberrechtsgesetzes ist.

Achtung Strafverfolgung!

LÖSCHEN SIE DIESE TOOLS

Dank „Hacker-Paragraf“ § 202c StGB sind bestimmte Utilities seit einigen Monaten rechtlich besonders problematisch. Momentan ist noch unklar, wer sich wobei strafbar macht.

Von **Ramon Schwenk**



Insert: Die Mini-Linux-Distribution enthält viele Werkzeuge zur Netzwerkanalyse, Computer-Forensik, Virensuche und Datenrettung

SEIT AUGUST GIBT ES DEN NEUEN „Hacker-Paragrafen“ 202c Strafgesetzbuch (StGB). Demnach sind Herstellung, Verkauf, Überlassung, Beschaffung oder Verbreitung von Passwörtern oder Software, die dafür ausgelegt ist, Daten auszuspähen oder abzufangen, strafbar. Das Gesetz ist allerdings extrem umstritten.

1. Was hinter dem Rundumschlag steckt

Anfang Juli 2007 verabschiedete der Bundesrat das neue Gesetz zur Bekämpfung von Computerkriminalität mit dem Ziel, das Hacken von Computeranlagen und Programmen schärfter bestrafen zu können. Seit die Norm am 11. August veröffentlicht wurde, ist die Verwirrung groß. Denn der „Hacker-Paragraf“ § 202c StGB trifft nicht nur die bösen Jungs.

Das Gesetz kriminalisiert auch Programme für Administratoren und Sicherheitsexperten – etwa Portscanner und Netzwerk-Testprogramme. Die Verunsicherung ersteckt sich weiter auf Web-Seiten-Betreiber, Software-Hersteller und Anwender. Momentan ist noch weitgehend unklar, wer sich wobei tatsächlich strafbar macht.

202c – drei Ziffern, ein Buchstabe. Doch dieser Zusatz zum StGB könnte die IT-Sicherheit um Jahre zurückwerfen. Denn in Absatz 1, Unterpunkt 2 heißt es „Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.“

„Sanktioniert wird insbesondere das Herstellen, Überlassen, Verbreiten oder Verschaffen von ‚Hackertools‘, die bereits

SOFTWARE Keys downloaden

Etliche Websites im Internet, beispielsweise **www.astalavista.com** bieten Lizenzschlüssel (Seriennummern, Keys) fürs Freischalten von fast jeder Software an.

So gefährlich ist es: Unter gewissen Umständen ist es legal, wenn Sie sich von dort einen Key besorgen.

Zu den Voraussetzungen einer zulässigen Nutzung zählt unter anderem, dass Sie den Key eigentlich schon erworben haben, ihn aber nach einem Verlust nicht umgehend vom Hersteller ersetzt bekommen.

Unter Umständen müssen Sie zumindest zivilrechtliche Ansprüche fürchten.

nach Art und Weise ihres Aufbaus darauf angelegt sind, illegalen Zwecken zu dienen.“ (Originaltext BMJ-Pressemitteilung).

2. Über das Ziel hinausgeschossen

„Besserer Schutz vor Hackern, Datenklau und Computersabotage“, das soll der aktualisierte § 202 StGB laut Bundesministerium der Justiz (BMJ) bringen. Damit will Bundesjustizministerin Brigitte Zypries „letzte Lücken im deutschen Strafrecht schließen“. Das sind laut Bundesministerium der Justiz „Regelungslücken vor allem im Bereich des ‚Hacking‘, das heißt dem ‚Knacken‘ von Computersicherheitssystemen und der Computersabotage“. (Originaltext BMJ-Pressemitteilung).

Das Gesetz hat also nach Willen und Interpretation des BMJ direkte Auswirkung auf die „Verbreitung“ und „Verschaffung“ von Software, die sich prinzipiell (auch) für illegale Handlungen nutzen lässt. Damit sind aber neben den tatsächlichen Übeltätern vor allem Sicherheitsexperten, Programmierer und Internet-Seiten als Verbreiter, Überlasser und Hersteller betroffen.

In der Praxis heißt das, dass jedes Programm, das sich unter Umständen für eine illegale Aktion einsetzen lässt, potenziell verboten ist. In den Verschwörungstheorien hat der § 202c noch eine andere Funktion. So mutmaßte der Chaos Computer Club bereits im Mai, dass damit der Weg für den Bundestrojaner freigeräumt werden soll. Denn wenn keine Sicherheitslücken mehr gefunden werden dürfen, kann man diese auch nicht flicken.

3. Finger weg: Das ist ab sofort gesetzlich verboten

Die Auswirkungen der neuen Gesetzeslage sind weitreichend: Bislang durften in Deutschland beheimatete Websites Sicherheits-Tools und Rettungsprogramme anbieten, deren Verbreitung nun möglicherweise verboten ist. Möglicherweise deshalb, weil niemand so genau weiß und sicher sagen kann, ob ein einzelnes Programm nun tatsächlich zu den in § 202c StGB gemeinten Programmen gehört oder nicht. Betroffen sind unter anderem:

Passwort-Knacker: Utilities, mit denen Sie selbst überprüfen können, ob verschlüsselt gespeicherte Daten sicher und die genutzten Passwörter ausreichend sind. Verboten weil: Hacker verwenden solche Tools zum Knacken von chiffrierten Dateien.

System-Recovery-CDs: Rettungs-CDs sowie Erste-Hilfe-Systeme für USB-Sticks, mit denen Sie im Falle einer nicht mehr startfähigen Windows-Installation an Ihre Daten herankommen und Reparaturversuche unternehmen können. Verboten weil: Mit System-Recovery-CDs kommen Unbefugte ohne Benutzer- oder Administratorkennwort an die auf Festplatte gespeicherten Daten heran.

Auditing-Tools: Systemprogramme, die Sie starten und die das Betriebssystem systematisch auf Sicherheitslücken wie fehlende Hotfixes untersuchen und die sich als mögliches Schlupfloch für Angreifer eignen. Verboten weil: Auch Hacker verwenden solche Programme, um ihre Attacken auf PC-Systeme vorzubereiten.

Netzwerk-Sniffer: Ein Sniffer fängt Netzwerkpakete ab und bietet Funktionen zur Analyse der Datenpakete an. So lassen sich der Datenverkehr im Netzwerk untersuchen, den Ursachen von Übertragungsfehlern auf die Spur kommen und Gefahrenbereiche aufspüren. Verboten weil: Bösartige Zeitgenossen mit einem Sniffer Datenpakete abfangen und den Datenverkehr einschließlich der darin übertragenen Passwörter ausspähen können.

Port-Scanner: Diese Programme untersuchen eine von Ihnen eingegebene IP-Adresse oder einen IP-Adressbereich systematisch auf offene Ports hin und zeigen eine Liste aller ansprechbaren Port-Adressen an. Verboten weil: Port-Scanner hefen beim Aufspüren angreifbarer Systeme für die Vorbereitung einer Internet-Attacke.

LAN-/WKAN-Checker: Netzwerk-Tools, die testen, ob Ihre Netzeinstellungen sicher sind und Ihr eigenes Netzwerk oder Wireless LAN unangreifbar ist. Verboten weil: Damit lassen sich Zugriffsmöglichkeiten auf anfällige, schlecht geschützte oder ungeschützte Netzwerke ermitteln.

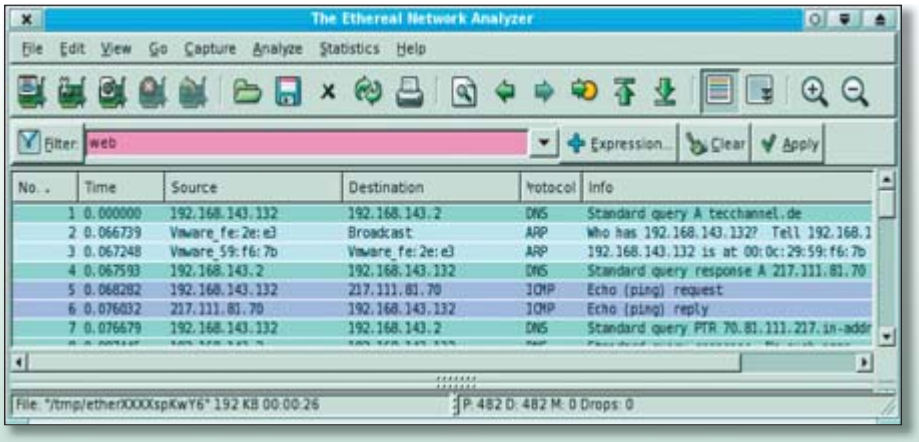
Seriennummern-Tools: Solche Programme enthalten entweder eine Datenbank mit gestohlenen echten beziehungsweise gefälschten Seriennummern oder eine Suchmöglichkeit für entsprechende Software-Codes im Internet. Mit den Seriennummern lassen sich sich Programme ohne Lizenz entsperren. Verboten weil: Inoffizielle Seriennummern umgehen die Sicherheit- und Sperrfunktionen in Software.

Programme der aufgeführten Genres dürfen wir Ihnen bis zur Klärung der Sachlage durch richterliche Urteile auch nicht mehr auf Heft-DVD anbieten, da wir uns strafbar machen würden, wenn wir die Software verbreiten würden.

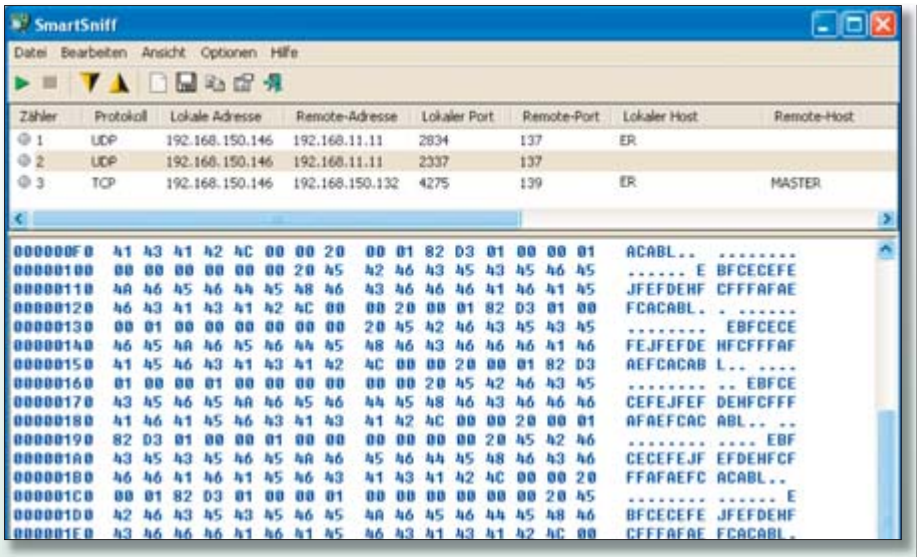
4. Windows-Tools: Diese Tools sind juristisch umstritten

Die folgende Liste der unter dem Licht von § 202c StGB problematischen und mögli- ›

ÜBERBLICK Verbotene Tools



Finger weg von Backtrack: Die populäre Linux-Distribution für Rettungsmaßnahmen in Form einer Live-CD umfasst Sicherheits-Software, die auch Kennwörter knacken und Daten bespitzeln kann



Datenverkehr bespitzeln: Mit einem Netzwerk-Sniffer protokollieren Sie über die LAN-Verbindung übertragene Datenpakete mit, darunter auch den Inhalt von Dokumenten und Zugangs-Codes

Bewerten von Kennwörtern: Das Tool Proactive Password Auditor von Elcomsoft hilft Netzwerke sicherer zu machen, indem es die Kennwörter der Konten überprüft

cherweise verbotenen Programme erhebt keinen Anspruch auf Vollständigkeit. Vielmehr soll sie als Warnung dienen.

Advanced <x> Passwort Recovery: Die Tools des Herstellers Elcomsoft umgehen die Passwortsperren in Anwendungen und Dokumenten wie Office, Mail-Clients, Adobe Acrobat und anderen Programmen.

Backtrack: Backtrack ist eine Rundum-Sicherheits-Linux-Distribution für Sicherheitsspezialisten mit einem großen Tool-Arsenal für Netzwerk- und PC-Checks.

Insert Linux: Das Rettungs-Toolkit auf Linux-Basis mit grafischer Oberfläche bietet Lesezugriffe auf Festplatten und kann Kennwörter knacken.

Free Password Recovery: Die gut gemachten Freeware-Tools von Nirsoft knacken Passwörter von Instant Messengern, Mail-Clients, Datenbanken, Browsern und hinter Sternchen verdeckte Codes.

Nessus: Der Network Security Scanner sucht und findet Sicherheitslücken, die Hacker für Angriffe verwenden könnten.

Netstumbler: Das Tool sucht in der Umgebung nach Funknetzwerken und findet WLANs auch dann, wenn sie ihre SSID-Kennung verstecken.

Sniff Pass: Das Gratis-Tool fängt im Netzwerk übertragene Kennwörter für die Protokolle POP3, IMAP4, SMTP, FTP und HTTP ab und zeigt Sie in einer Tabelle an.

Steganos Hacker Tools: Das Toolkit umfasst eine Zusammenstellung der bekanntesten Angriffs- und Knackprogramme.

Superscan: Das Tool überprüft, welche Dienste ein mit TCP/IP oder UDP arbeitendes System anbietet.

Wireshark: Ein Tool, das Netzwerke erkundschaftet und die vorhandenen Einstellungen analysiert.

5. Die Wirkung des Gesetzes ist gleich null

Während sich die Betreiber von in Deutschland gehosteten Websites an den § 202c StGB halten müssen, brauchen sich international ansässige Websites um die nationale Regelung nicht zu scheren.

Die Folge: Hacker-Tools werden im Web weiterhin verbreitet und sind auch für Anwender hierzulande von den Hersteller-Websites oder per Suchmaschine zu finden und herunterladbar. So verwundert es kaum, dass sich versierte Anwender und Administratoren trotz der neuen Gesetzeslage die problematischen Tools beschaffen, mit denen sie ihre eigenen Systeme auf Sicherheitslücken prüfen

6. Das ist wichtig für Website-Betreiber

Wer sich jetzt nicht strafbar machen möchte, entfernt in einem Akt unfreiwilliger Selbstzensur sämtliche Inhalte und Verweise auf möglicherweise riskante Software. Hersteller von Software sollten prüfen, den Betrieb ins benachbarte Ausland zu verlagern.

Die Situation ist absurd, denn ohne jegliche Änderung auf der WebSeite läuft das Angebot einfach in dem Land weiter, wo es nicht strafbar ist.

Zwar gibt es Beispiele, bei denen ein Hersteller demonstrativ auch die Domain-Endung wechselt, um gegen § 202c publikumswirksam zu protestieren, notwendig ist das aber eigentlich nicht. Schließlich kann eine Webseite mit Domain-Endung .de auch auf einem Server in der Schweiz betrieben werden.

„HACKER-PARAGRAF" Das ist brisant

Seit dem 11.8.2007 macht sich derjenige strafbar, der gemeinhin als „Hacker-Tools" bezeichnete Software herstellt, sie anderen überlässt, sie verbreitet oder sich selbst welche beschafft. Dabei sind mit „Hacker-Tools" alle Programme gemeint, mit denen das Ausspionieren oder Manipulieren fremder Computer oder Netzwerke möglich ist.

Es geht also um Programme, die illegalen Zwecken dienen können. Das große Problem: Legitime Werkzeuge, die etwa Administratoren brauchen, um Rechner auf Sicherheitslücken zu überprüfen, unterscheiden sich oft nicht von denen, die Kriminelle nutzen, um in fremde Rechner oder Netze einzudringen. Und damit sind auch sie illegal.

Umstrittene Programme

Gute Tools, böse Tools

In diesem Artikel lesen Sie

- **warum** manche Tools – nicht nur aus juristischer Sicht – umstritten sind
- **welche** Argumente die Gegner anführen
- **was** Sie wissen müssen, falls Sie eins der vorgestellten Utilities einsetzen wollen

Manche Utilities sind nur auf den ersten Blick völlig unbedenklich. Betrachtet man sie genauer, stößt man auf Funktionen, die nicht jeder gutheißt. Einige dieser Tools stellen wir hier vor. Von **Daniel Behrens**

Unter den Hunderttausenden Tools, die Sie aus dem Internet herunterladen können, gibt es einige, die nicht über alle Zweifel erhaben sind. Sie lassen sich zwar, teilweise unter bestimmten Voraussetzungen, völlig straffrei verwenden. Trotzdem sind sie jeweils einem Personenkreis oder einer Interessengruppe ein Dorn im Auge. Einige der Hilfsprogramme so sehr, dass sie die Verbreitung haben verbieten lassen oder dies am liebsten tun würden.

Ebay versuchte, Bietagenten vollständig zu verbieten

Beispiel Ebay: Das Auktionshaus sieht es gar nicht gern, wenn die Anwender automatische Biet-Software wie **Biet-o-Matic** nutzen. Denn diese ist darauf getrimmt, erst in letzter Sekunde ein Gebot abzugeben. Die Folge: Der Preis für eine Ware schaukelt sich nicht in ungeahnte Höhen. Da Ebay prozentual am erzielten Verkaufspreis beteiligt ist, fällt die Provision entsprechend niedriger aus. Dementsprechend hat das Auktionshaus in seinen AGB den Einsatz solcher Tools verboten und ging rechtlich gegen die Anbieter von automatischer Biet-Software vor. Vor Gericht musste Ebay aber eine Schlappe hinnehmen.

Aufnahme-Software: Dorn im Auge der Musikindustrie

Ein weiteres Beispiel ist das Mitschneiden von Web-Radio. Die Musikindustrie drängt

KOPIERSCHUTZ Knacken verboten

Das Kopieren mit technischen Mitteln geschützter Medien ist gesetzlich verboten. Sind Video-DVDs etwa per CSS-Codierung kopiergeschützt, dürfen Sie nach dem aktuellen Urheberrecht keine Sicherheitskopien mehr erstellen, da Sie hierzu den Kopierschutz überwinden müssen. Programme, die einen Kopierschutz umgehen, sind daher in der Regel als unzulässig anzusehen. Doch es gibt einen Ausweg: Schneiden Sie den Film während des Abspielens auf dem Bildschirm digital mit, und brennen Sie das Ergebnis auf eine DVD. Das ist nicht verboten, da zum Abspielen des Films die Codierung nicht umgangen wird. Das hierfür erforderliche Programm heißt Hypercam (*www.hyperionics.com*). Das englischsprachige Tool ist eigentlich dafür gedacht, Bildschirminhalte von Präsentationen aufzuzeichnen. Das einfach gestrickte Tools schneidet aber auch einen frei wählbaren Bildausschnitt einschließlich Ton und mit Filminhalten in guter Qualität mit. Starten Sie denFilm mit Ihrem gewohnten DVD-Abspielprogramm und danach die Software Hypercam. Legen Sie dann den gewünschten Bildausschnitt fest. Wählen Sie danach die Bild- und Tonqualität, und sorgen Sie mit der entsprechenden Einstellung dafür, dass der Ton ebenfalls aufgezeichnet wird. Als Frame Rate sollten Sie einen Wert zwischen 10 und 25 wählen, die „Frame Compression Quality" sollte zwischen 50 und 100 Prozent liegen. Die Aufnahme starten und stoppen Sie mit <F2>.

schon seit langem darauf, dass ein Verbot von „intelligenter Aufnahme-Software" ins Urheberrechtsgesetz aufgenommen wird. Damit meint sie Utilities wie **Clipinc.fx**, die Web-Radio nicht nur aufnehmen, sondern auch Schnittmarken empfangen und die Aufzeichnung titelgenau in einzelne MP3s zerteilen kann. Bisher ist sie mit ihrem Ansinnen auf taube Ohren gestoßen.

Besondere Vorsicht geboten bei „Hacker-Tools"

Tatsächlich verboten ist es, mit speziellen Tools fremde Daten aus einer „nichtöffentlichen Datenübermittlung" abzufangen und „besonders gesicherte Daten" auszuspähen. Das entsprechende Gesetz („Hackerparagraph") trat Mitte 2007 in Kraft, allerdings sind bisher noch keine Urteile bekannt, aus denen ersichtlich wäre, welche Hacker-Tools nun genau gemeint sind. Straffrei können Sie Passwort-Knacker und Netzwerk-Sniffer auf jeden Fall noch immer dann einsetzen, wenn die Daten, auf die Sie zugreifen möchten, von Ihnen stammen oder für Sie bestimmt sind – Stichwort „eigene Daten, eigener PC".

Dies waren nur einige Beispiele für sinnvolle Tools, die manche als „böse" ansehen könnten. Viele weitere Programme stellen wir Ihnen auf den folgenden Seiten vor. ›

Im Überblick Gute Tools, böse Tools

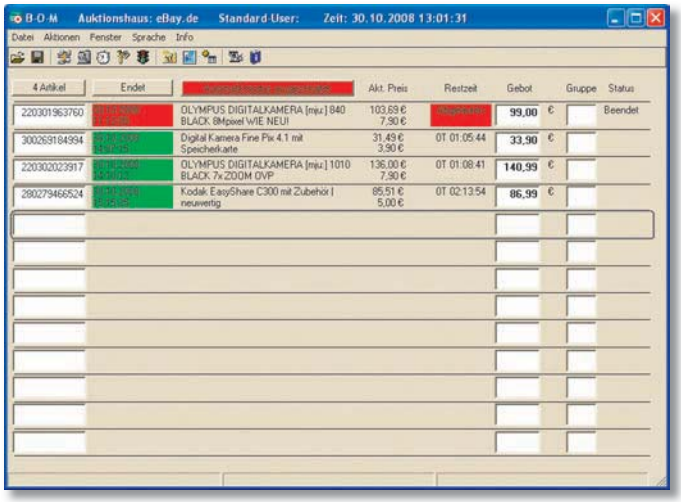
Programm	Beschreibung	Windows	Sprache	Internet	Preis
Biet-o-Matic 2.8.3	Ebay-Bietagent	95/98/ME, 2000, XP, Vista	Deutsch	*www.bid-o-matic.org*	gratis
Clipinc.fx Lite	Web-Radio-Aufnahme-Tool	XP, Vista	Deutsch	*www.clipinc.de*	gratis
Craagle 1.91	Seriennummer-Such-Tool	XP	Englisch	– [1]	gratis
Cyberghost VPN	Internet-Anonymisierer	XP, Vista	Deutsch	*www.cyberghostvpn.com*	ab 0 Euro
FLV Player 2.0.25	spielt FLV-Videos ab	2000, XP, Vista	Englisch	*www.martijndevisser.com*	gratis
Freeware PDF Unlocker 1.0.4	hebt PDF-Beschränkungen auf	2000, XP	Englisch	– [1]	gratis
Gamejack 6.0.946 [2]	Kopierschutz-Knacker für Spiele	2000, XP	Deutsch	*www.my-sad.com*	26,99 Euro
Gpg4win 1.1.3	Verschlüsselungs-Tool-Sammlung	2000, XP, Vista	Deutsch	*www.gpg4win.org/index-de.html*	gratis
IE7 Pro 2.4	IE-Add-on mit Werbefilter	2000, XP, Vista	Deutsch	*www.ie7pro.com*	gratis
µTorrent 1.8.2	Bit-Torrent-Client	98/ME, 2000, XP, Vista	Englisch / Deutsch	*www.utorrent.com*	gratis
Orbit Downloader 2.8.7	Download-Manager	2000, XP, Vista	Deutsch	*www.orbitdownloader.com*	gratis
PC-WELT Google-Hack-Suche 1.0	Spezial-Suchanfragen	2000, XP, Vista	Deutsch	*www.pcwelt.de/scripts*	gratis
Spy Agent 6.31	Überwachungs-Software	2000, XP, Vista	Englisch	*www.spytech-web.com*	56,49 Euro
Tunebite Platinum 6 [2]	entfernt Kopierschutz legal	XP, Vista	Deutsch	*www.tunebite.com*	29,90 Euro
Video Cache View 1.25	archiviert Videos von Youtube & Co.	2000, XP	Englisch	*www.nirsoft.net*	gratis
Wireshark 1.0.6	Netzwerk-Analyse	2000, XP, Vista	Englisch	– [1]	gratis
Word Password 11.0	Passwort-Knacker	95/98/ME, 2000, XP, Vista	Englisch	– [1]	46,41 Euro
Yamipod 1.7	iPod-Kopier-Tool	XP, Vista	Englisch	*www.yamipod.com*	gratis

1) Verbreitung in Deutschland möglicherweise unzulässig 2) Testversion auf CD

Biet-o-Matic: Ebay-Gebote erst in letzter Sekunde abgeben

Wer bei Ebay zu früh auf einen Artikel bietet, treibt den Preis unnötig hoch. Denn je mehr Zeit bis zum Ende der Auktion bleibt, desto mehr Gebote sind möglich. Nicht selten kommt es dann zu einem Bieterwettstreit. Die Kunst besteht also darin, sein Gebot erst in letzter Sekunde abzugeben. Das geht normalerweise nur, wenn man selbst vor dem PC sitzt. Und sogar dann verpasst man meist den idealen Zeitpunkt – schließlich geht es um Sekunden. Beide Probleme löst das Tool Biet-o-Matic: Es steigert erst kurz vor Ablauf der Auktion(en) mit. Sie geben dazu die Artikelnummer(n) sowie das jeweilige Maximalgebot ein und aktivieren den „Automatikmodus". Zuvor müssen Sie dem Tool Ihre Ebay-Anmeldedaten anvertrauen, was ein gewisses Risiko darstellt.

Umstritten, weil: Ebay verbietet das Benutzen von automatischer Biet-Software in seinen AGB und ist auch schon gegen deren Hersteller vorgegangen. Letztendlich unterlag das Auktionshaus aber.



Zum Ärger von Ebay: Biet-o-Matic steigert erst in letzter Sekunde vor Ablauf bei einer Auktion mit. Das hilft, den Preis niedrig zu halten

Clipinc.fx Lite: Schneidet Web-Radios mit und exportiert einzelne Titel als MP3

Web-Radios bieten in der Regel keine Aufnahmefunktion. Hier hilft Clipinc. Nach der Installation beginnt das Tool, fortlaufend in einer 3-Tages-Schleife die von Ihnen ausgewählten Sender mitzuschneiden – auch dann, wenn die Clipinc-Bedienerführung gerade nicht geöffnet ist. Von einem Server des Herstellers ruft es die Informationen ab, wann die betreffenden Sender welche Titel gespielt haben. Die so gekennzeichneten Lieder können Sie per Kontextmenübefehl „Speichern unter" als MP3 exportieren. Um die permanente Aufzeichnung auszusetzen, klicken Sie auf das Clipinc-Symbol im Systray und wählen „Aufnahme anhalten".

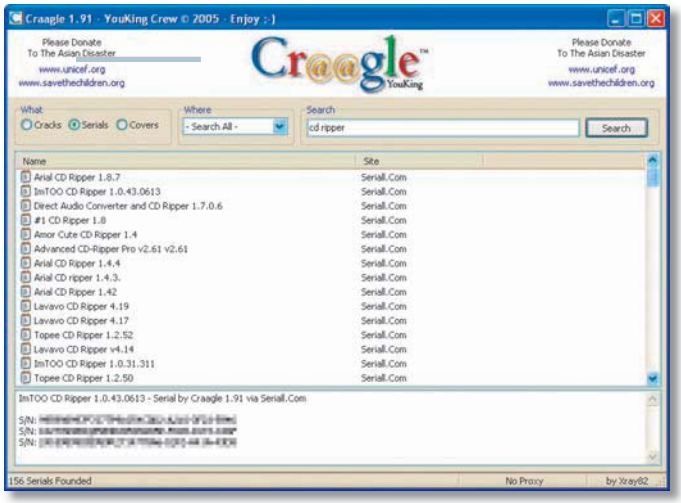
Umstritten, weil: Die Musikindustrie behauptet, wer einen Song in guter Qualität mitgeschnitten habe, kaufe ihn nicht mehr. Die Rechteinhaber versuchen daher seit geraumer Zeit, ein Verbot „intelligenter Aufnahme-Software" herbeizuführen – aber bisher erfolglos.

Die Musikindustrie will's verbieten: Clipinc nimmt Web-Radios auf und zerteilt den Stream anhand von Schnittlisten titelgenau in einzelne MP3s

Craagle: Sucht im Internet nach Seriennummern, ohne dass Sie dafür dubiose Seiten öffnen müssen

Wer Windows regelmäßig neu installiert, stand bestimmt schon einmal vor dem Problem: Für ein gekauftes Programm, das Sie dringend benötigen, ist die Seriennummer nicht mehr auffindbar. Man könnte zwar versuchen, sich an den Hersteller zu wenden – nicht immer ist das aber von Erfolg gekrönt. In solch einem Fall ist es durchaus legal, sich selber zu helfen – zum Beispiel mit Seriennummern aus dem Web. Diese werden zuhauf auf speziellen Seiten veröffentlicht, die aber häufig mit anstößigen Werbebannern versehen sind und/oder versuchen, Ihnen Malware unterzuschieben. Das Tool Craagle durchsucht einschlägige Websites, ohne dass Sie diese im Browser öffnen müssen.

Umstritten, weil: Mit Craagle könnten auch Software-Piraten nach Seriennummern suchen. Zudem lässt das Tool die Suche nach illegalen Cracks zu. Manche Virenscanner melden Craagle als „potentiell unerwünschtes Programm" oder Spyware.



Missbrauchsgefahr durch Software-Piraten: Wer seine Seriennummer verloren hat, kann mit Craagle im Web nach Ersatz suchen

Cyberghost VPN: Anonymisiert die Internet-Verbindung

Privatsphäre und Datenschutz sind Ihr gutes Recht. Wenn Sie im Web surfen, hinterlassen Sie aber auf jedem Server Ihre aktuelle IP-Adresse. Sie gibt Aufschluss darüber, wo und über welchen Provider Sie sich eingewählt haben. Sollten Sie aus irgendeinem Grund unschuldig ins Fadenkreuz von Internet-Ermittlern gelangen, ist die IP-Adresse Ausgangspunkt zur Identitätsfeststellung. Cyberghost VPN leitet Ihren gesamten Datenverkehr über Anonymisierungs-Server des Anbieters – unter dessen IP-Adresse. Da er keine Protokolle speichert, ist eine Rückverfolgung ausgeschlossen. 10 GB Datenverkehr pro Monat sind kostenlos, allerdings mit gebremster Geschwindigkeit. Das Premium-Paket mit 2000er-Bandbreite und mehr Volumen gibt es ab 5,83 Euro pro Monat.

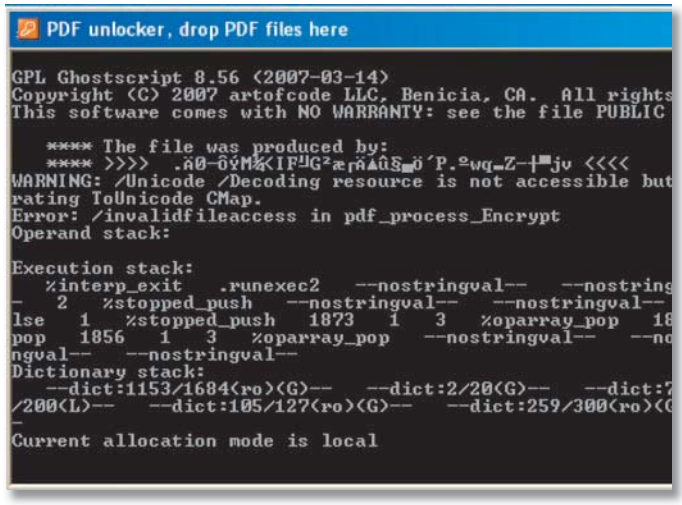
Umstritten, weil: Kriminelle könnten Cyberghost VPN missbrauchen, um unerkannt illegale Dateien zu tauschen oder Internet-Straftaten auszuüben.

Unerkannt online: Cyberghost VPN anonymisiert die Internet-Verbindung – auch Straftäter könnten so aber unbehelligt bleiben

Freeware PDF Unlocker: Hebt Beschränkungen und Passwortschutz in PDF-Dateien auf

PDF-Dateien können mit Benutzer-Restriktionen belegt sein. Der Ersteller kann verhindern, dass Anwender die Inhalte über die Zwischenablage in eine andere Anwendung übertragen oder ausdrucken. Zusätzlich lassen sich PDFs mit einem Passwort versehen. PDF Unlocker hebt viele derartige Beschränkungen auf. Bei der Installation legt es ein Desktop-Icon an. Zieht man eine PDF-Datei darauf, öffnet sich kurz die Kommandozeile. Wenn es keine Probleme gibt, spuckt PDF Unlocker eine ungeschützte Kopie des PDFs aus, erkennbar an dem Dateinamenszusatz „_noPW“. Manche Passwort-geschützten PDFs kann das Tool nicht umwandeln.

Umstritten, weil: Rechtlich gesehen könnte man solche Benutzerbeschränkungen als Kopierschutz einordnen. Dann wäre eine Verbreitung von PDF Unlocker strafbar, die private Nutzung hingegen nicht. Wenn Sie allerdings mit dem Tool den Passwortschutz eines Dokuments aufheben, könnte das unter Strafe stehen.

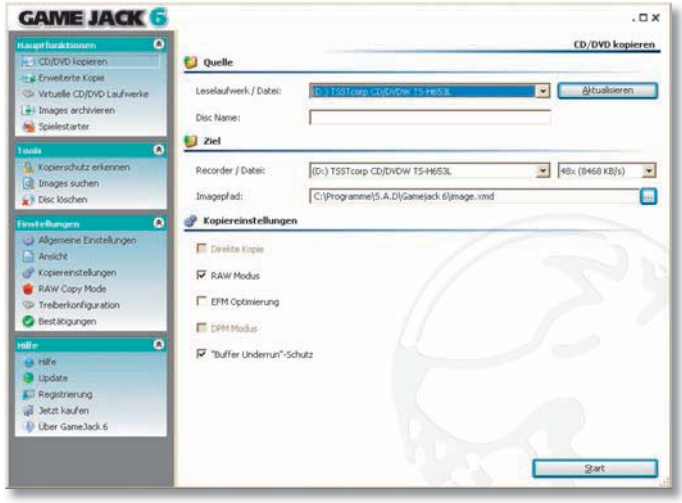


Freeware PDF Unlocker: Das Tool befreit PDF-Dateien von Beschränkungen, die zum Beispiel das Ausdrucken verhindern

Gamejack: Fertigt Sicherungskopie auch von kopiergeschützten Spiele-CDs/-DVDs an

Backups von Spiele-CD/DVDs lassen sich mit einem einfachen Brennprogramm meistens nicht erstellen, da die Spielehersteller ausgefeilte Kopierschutztechniken verwenden. Die Lösung für das Problem ist Gamejack. Das Tool versucht zunächst eine Bit-gleiche Kopie des Datenträgers inklusiver sämtlicher Schutz-Merkmale anzufertigen. Das schlägt fehl, wenn das Laufwerk manche Kopierschutz-Informationen nicht schreiben kann. Dann gibt es die Option, ein Abbild der CD/DVD auf der Festplatte abzulegen. Dieses bindet Game Jack als virtuelles Laufwerk ein und emuliert Kopierschutz-Merkmale. Dadurch wird dem Spiel vorgegaukelt, dass es sich um einen Original-Datenträger handelt.

Umstritten, weil: Anders als bei Musik-CDs und Film-DVDs dürfen Sie von Spielen auch dann eine Kopie anlegen, wenn sie kopiergeschützt sind. Allerdings nur eine einzige und auch nur für sich selbst. Das Tool kann aber auch mehrere Kopien erstellen.



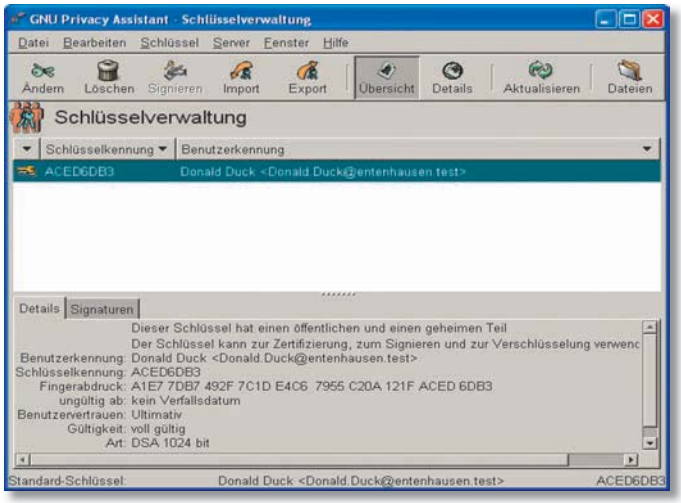
Sicherungskopie erlaubt: Den Kopierschutz von Spiele-CDs/DVDs dürfen Sie umgehen – aber nur ein einziges Mal pro Exemplar

›

Gpg4win: Mails und Dateien einfach und sicher verschlüsseln

Die meisten Anwender verschicken ihre Mails unverschlüsselt und haben vertrauliche Dokumente ungeschützt auf der Festplatte liegen. Was die Mails betrifft, so sollte man wissen, dass diese auf ihrem Weg zum Empfänger mehrere Stationen durchlaufen und an jeder einzelnen abgefangen und gelesen werden könnten. Dateien auf der Festplatte könnten durch einen Trojaner in falsche Hände gelangen. Mit Gpg4win schlagen Sie beide Fliegen mit einer Klappe: Die Tool-Sammlung unterstützt neben der Mail- auch die Dateiverschlüsselung. Eine gut gemachte Schritt-für-Schritt-Anleitung („Einsteigerhandbuch“) und ein „Durchblickerhandbuch“ für Fortgeschrittene liegen im PDF-Format bei.

Umstritten, weil: Mit Gpg4win könnten auch Straftäter ihre Kommunikation und Web-Piraten ihre illegalen Dateien verschlüsseln. Das führt die staatlich verordneten Abhörschnittstellen der Mail-Provider und die geplanten Online-Durchsuchungen ad absurdum.

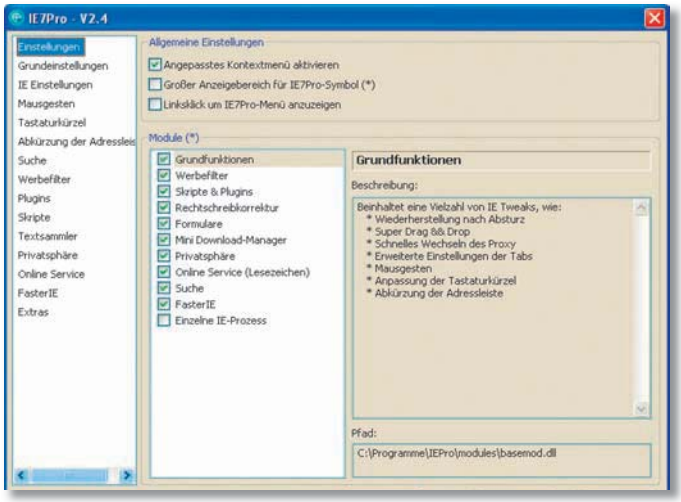


Schützt private Geheimnisse, aber auch Pläne Krimineller: Gpg4win verschlüsselt nicht nur Mails, sondern auch Dateien auf der Festplatte

IE7Pro: Filtert (fast) jede Werbung aus Web-Seiten heraus

IE7Pro ist ein Add-on für den Internet Explorer ab Version 6.0. Es erweitert den Browser um zahlreiche Funktionen. Für viele Anwender am interessantesten ist der integrierte Werbeblocker. Er filtert ziemlich zuverlässig Reklame aus Web-Seiten heraus. Über einen Rechtsklick auf das IE7Pro-Symbol in der Statusleiste und die Option „Diese Seite nicht filtern“ erstellen Sie eine Ausnahme. Werbemittel, die IE7Pro übersehen hat, klicken Sie auf der Web-Seite mit der rechten Maustaste an und wählen „Diese Grafik filtern“. Besonders hartnäckige Anzeigen im Flash-Format werden Sie los, indem Sie den „Flash-Blocker“ aktivieren. Erwünschte Flash-Anwendungen wie die Player auf manchen Videoportalen werden dann allerdings ebenfalls nicht geladen.

Umstritten, weil: Viele Websites finanzieren sich durch Werbung. Der massenhafte Einsatz von Werbeblockern würde viele Betreiber in den Ruin stürzen oder sie zwingen, Gebühren zu verlangen.

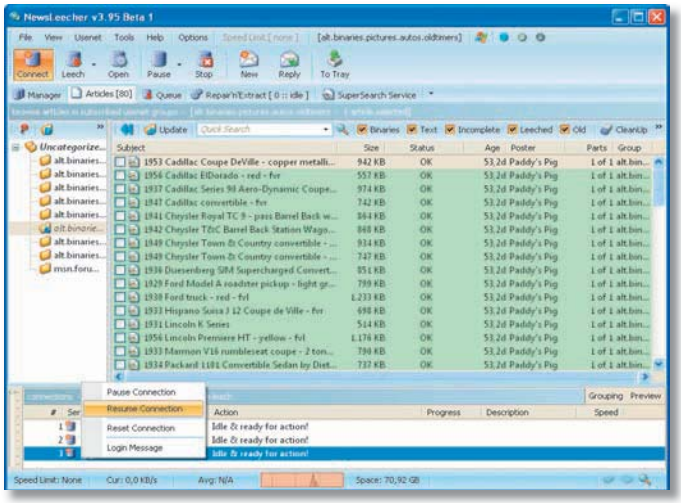


Freut Surfer, ärgert werbefinanzierte Sites: Das Internet-Explorer-Add-on IE7Pro besitzt unter anderem einen ausgefuchsten Werbefilter

Newsleecher: Durchsucht Newsgroups, findet Dateien und lädt sie auf die Festplatte

Um auf einen Newsserver zuzugreifen, benötigen Sie ein Newsreader-Tool, das die einzelnen Beiträge anzeigen kann. Doch nicht jeder Newsreader unterstützt das Laden von Dateien. Newsleecher arbeitet mit beliebig vielen Newsservern zusammen, hebt alle neuen Postings farbig hervor und lädt Dateien und Textnachrichten herunter. Die Funktionsausstattung ist fein: Der Anwender kann von mehreren Servern gleichzeitig laden, parallele Verbindungen aufbauen, was sich positiv auf die Übertragungsgeschwindigkeit auswirkt, und einen Zeitplaner sowie die Suchfunktionen nutzen. Letztere ist kostenpflichtig und erleichert mittels Volltextindex und Filtern das gezielte Auffinden von Dateiinhalten.

Umstritten, weil: Programme wie Newsleecher reichen zusammen mit einem unbeschränkten News-Zugang aus, um Tag für Tag mehrere Gigabyte Software, Videos und Sounds zu laden. Neben Gratis-Inhalten lassen sich damit auch Raubkopien laden.

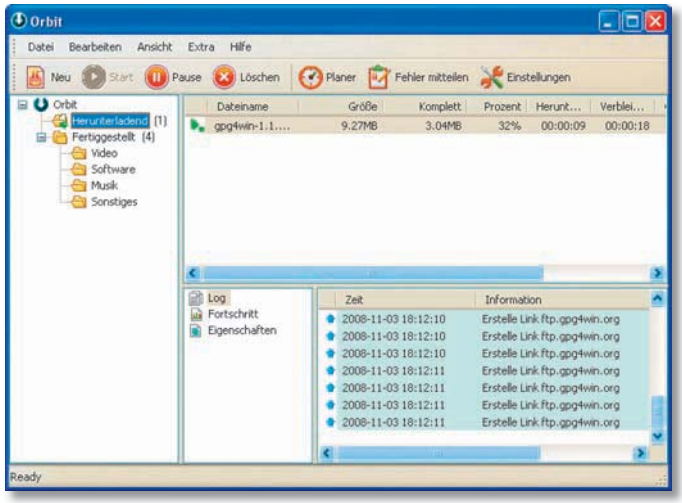


Spezialist für Dateien: Newsleecher lädt Dateien aus Newsgroups in mehreren Parallel-Threads mit Maximaltempo auf Festplatte

Orbit Downloader: Beschleunigt langsame Downloads deutlich

Manche Downloads aus dem Web ziehen sich ewig hin. Grund dafür ist, dass der betreffende Server überlastet ist oder die Bandbreite pro Verbindung beschränkt. Orbit Downloader hilft in beiden Fällen. Das Tool versucht, andere Server zu finden, die die gleiche Datei anbieten, in der Fachsprache auch „spiegeln“ genannt. Um Geschwindigkeits-Begrenzungen zu umgehen, stellt Orbit Downloader statt nur einer gleich mehrere parallele Verbindungen zu jedem Server her und fordert über jede nur einen Teil der Datei an. Die deutschsprachige Bedienerführung lässt sich über „View, Language, Deutsch“ aktivieren.

Umstritten, weil: Wenn ein Download-Server-Betreiber die Bandbreite pro Verbindung beschränkt, so tut er das nicht ohne Grund. Er möchte damit allen Anwendern die gleiche Maximal-Geschwindigkeit anbieten. Wer diese Beschränkung umgeht, verlangsamt unter Umständen die Dateitransfers anderer Benutzer.

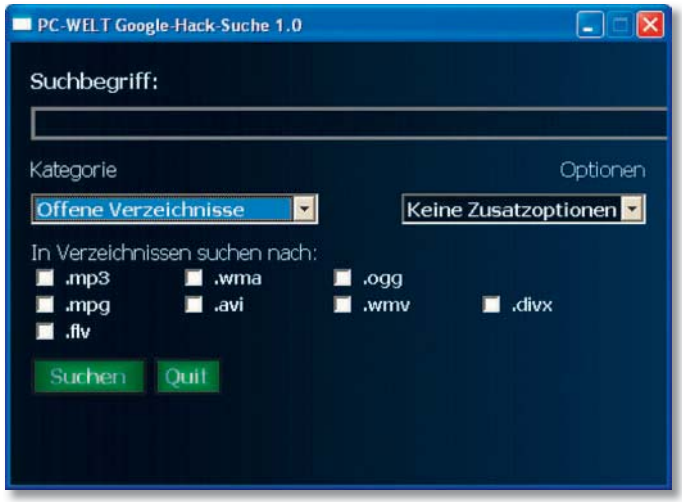


Schneller downloaden: Orbit Downloader benutzt saubere und schmutzige Tricks, um den Transfer zu beschleunigen

PC-WELT Google-Hack-Suche: Spürt per Google geheime Dateien auf

Im Suchindex von Google finden sich zahlreiche Dokumente und Dateien, die eigentlich nicht für die Öffentlichkeit bestimmt sind. Ob kommerzielle MP3-Dateien, Bücher im PDF-Format oder vertrauliche Briefe und Tabellen – es gibt nichts, was es nicht gibt. Meistens liegt es an einer falschen Server-Konfiguration, dass Googles Suchroboter dort auf private Daten zugreifen können. Um gezielt danach zu fahnden, genügt es, die passenden Suchparameter zu benutzen. Unser Tool „PC-WELT Google-Hack-Suche“ kennt die interessantesten Abfragen und führt sie per Mausklick aus. Bei einigen gilt: Sie können einen Suchbegriff eingeben, um die Ergebnisse weiter einzuschränken, müssen es aber nicht.

Umstritten, weil: Web-Piraten könnten das Tool beziehungsweise die speziellen Google-Suchabfragen missbrauchen, um gezielt nach Musik- oder Filmdateien zu suchen. Diese könnten urheberrechtlich geschützt sein.



Spürhund: Das PC-WELT-Tool hilft dabei, über Google-Spezialabfragen geheime Dateien und offene Server-Verzeichnisse zu finden

Spy Agent: Überwachungs-Software für Eltern und Chefs

Eltern möchten gerne wissen, was ihr Nachwuchs am PC treibt, Chefs am liebsten ganz genau erfahren, wie viel Zeit ihre Mitarbeiter mit privatem Internet-Surfen oder Solitär-Spielen verbringen. Mit einer Überwachungs-Software wie Spy Agent lassen sich diese Informationsbedürfnisse stillen. Sie läuft auf Wunsch unsichtbar im Hintergrund und protokolliert detailliert alle PC-Aktivitäten. Dazu zählen sämtliche Tastenanschläge, Programmaufrufe, empfangene und gesendete Mails, aufgerufene Websites, Chats sowie geöffnete Dateien. Außerdem speichert Spy Agent wiederholt Screenshots des gesamten Bildschirminhalts. Der Überwacher kann über ein Tastaturkürzel und ein Passwort die Protokolle einsehen – oder lässt sie sich regelmäßig per Mail schicken.

Umstritten, weil: Das Tool könnte auch zur Überwachung von Mitarbeitern eingesetzt werden, die sich damit nicht einverstanden erklärt haben. Das wäre illegal.

Nicht immer legal: Mit Spy Agent können Eltern und Chefs lückenlos nachvollziehen, was Nachwuchs oder Angestellte am PC getrieben haben

›

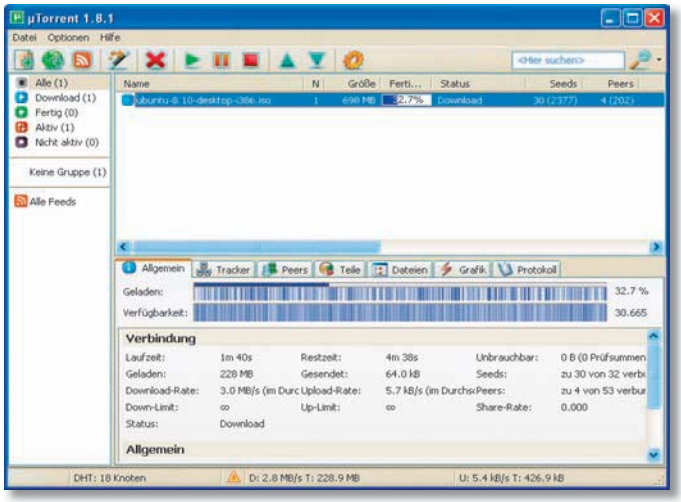
Tunebite Platinum: Entfernt Kopierschutz von Musik und Videos

Manche Musikdateien, die Sie bei Download-Shops wie Musicload.de oder über iTunes kaufen, sind mit einem Kopierschutz versehen. Dieser schränkt den Käufer eklatant ein. Die Shareware Tunebite entfesselt kopiergeschützte Songs auf zwei legale Weisen: Wenn der Schutz eines Songs das Brennen als Audio-CD zulässt, nutzen Sie den virtuellen Brenner „Audials Tunebite CD-R". Im Anschluss öffnet sich Tunebite und konvertiert die virtuelle CD in MP3-Dateien. Wenn ein Brennen nicht (mehr) möglich ist, nutzen Sie das zweite Verfahren, bei dem Tunebite kopiergeschützte Songs während der Wiedergabe als freie MP3-Datei aufzeichnet. Mit dem gleichen Prinzip kann es auch DRM-geschützte Filme entfesseln.
Umstritten, weil: Die Verfahren, die Tunebite nutzt, sind rechtlich nicht zu beanstanden, da der Kopierschutz selbst nicht geknackt wird. Trotzdem sind solche Tools der Musik- und Filmindustrie natürlich ein Dorn im Auge.

Geschützte Dateien entfesseln: Tunebite nutzt unter anderem die legale Hintertür der „Wiederaufnahme", um den Kopierschutz aufzuheben

µTorrent: Dateien mit Bit-Torrent-Technik blitzschnell herunterladen

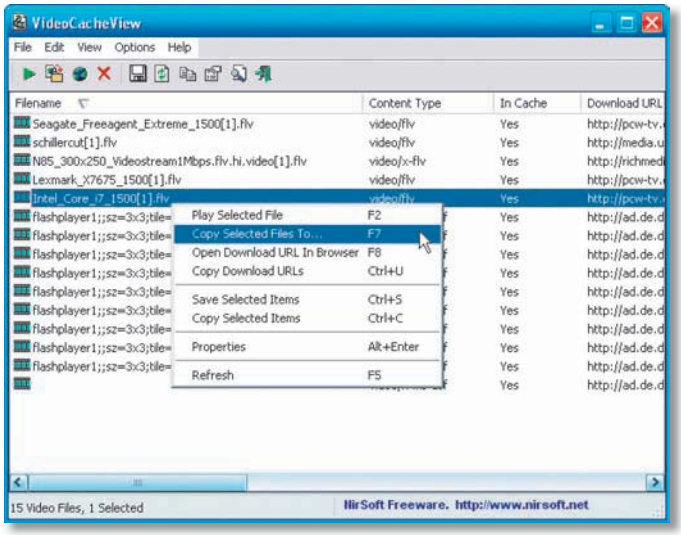
Wenn es darum geht, große Datenmengen an ein großes Publikum zu verteilen, kommt oft das Bit-Torrent-Verfahren zum Einsatz. Es funktioniert nach dem Prinzip einer Tauschbörse, aber immer nur auf eine Datei bezogen. Wer etwas herunterlädt, gibt währenddessen die bereits empfangenen Fragmente für andere frei. Die normalerweise weitgehend ungenutzte Upload-Bandbreite jedes Surfers kommt anderen zugute. Das Ergebnis: Alle profitieren von einer hohen Geschwindigkeit. Um Dateien per Bit Torrent herunterzuladen, benötigen Sie ein Programm wie µTorrent. Eine große Zahl an legalen Dateien, die über Bit Torrent zum Download angeboten werden, ist über *www.youtorrent.com* zu finden.
Umstritten, weil: Es gibt einige Web-Piraten, die illegal kopierte Software, Musik oder Filme mit Hilfe des Bit-Torrent-Verfahrens schnell und weitgehend anonym verbreiten. Daher ist es in die Kritik geraten.



Schnell und effizient: Große Dateien werden häufig nur über das Bit-Torrent-Verfahren zum Download angeboten

Video Cache View: Archiviert Videos von Youtube & Co.

Youtube, Sevenload & Co. sind beliebt wie nie zuvor. Viele Anwender haben den Wunsch, besonders originelle Videos, die sie beim Stöbern in den Videoportalen gefunden haben, zu archivieren oder auf ihr Handy zu kopieren. Diese Funktion bieten die meisten Dienste nicht an. Es ist trotzdem möglich, an die Videodateien zu kommen. Was viele nicht wissen: Sie liegen nach der vollständigen Wiedergabe bereits auf der Festplatte – und zwar als temporäre Dateien im Zwischenspeicher („Cache") des Browsers. Das Tool Video Cache View macht es Ihnen einfach, sie dort zu finden und zu kopieren. Die meisten Videoportale verwenden das FLV-Videoformat. Um es abzuspielen, nutzen Sie zum Beispiel den **FLV Player** . In ein anderes Format konvertieren Sie es mit dem kostenlosen Dienst *www.media-convert.com*.
Umstritten, weil: Youtube & Co. sind nicht erfreut über Tools wie Video Cache View. Sie hätten es lieber, wenn Sie zum erneuten Anschauen eines Videos wieder auf die Website kommen würden.

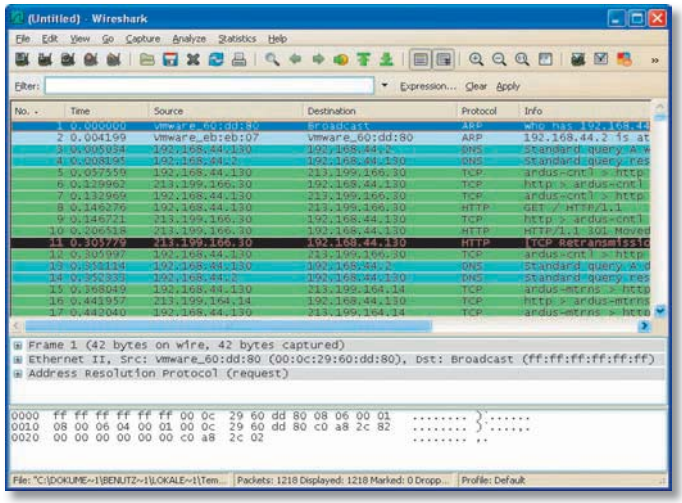


Video Cache View: Mit dem Tool können Sie bequem Videos von Youtube & Co. auf Festplatte, Handy und andere Geräte kopieren

Wireshark: Schneidet den kompletten Netzwerkverkehr mit

Wireshark protokolliert alle ein- und ausgehenden Daten der Netzwerkkarte. In einer Listendarstellung sehen Sie, von welchen Adressen Pakete ankommen und wohin Ihr PC welche aussendet. Per Klick auf einen Eintrag erscheint der Inhalt des Datenpakets. Um es in Zusammenhang mit den anderen, dazugehörigen Paketen zu sehen, wählen Sie „Follow TCP Stream“. Binärdaten, zum Beispiel von Bildern oder verschlüsselten Daten, können Sie ohne weitere Hilfsmittel nicht rekonstruieren. Ein großer Teil an Internet-Übertragungen läuft jedoch im lesbaren Ascii-Format ab – und das meist unverschlüsselt. Beispiele dafür sind HTML-Code, in Web-Formulare eingegebene Daten sowie Mailinhalte und -passwörter.

Umstritten, weil: Wireshark kann auch Daten des angeschlossenen Netzwerks mitschneiden, wenn dieses über Hubs statt moderne Switches zusammengeschaltet ist. Es könnte also zum illegalen Ausspähen fremder Daten missbraucht werden.



Verkehr im Blick: Mit Wireshark sehen Sie Datenpaket für Datenpaket, was bei Ihrem PC und in Ihrem Netz über die Leitung geht

Word Password & Co.: Hebeln den Passwortschutz von Office-Dokumenten und anderen Dateien aus

Word-Dokumente lassen sich im „Speichern“-Dialog über „Extras, Sicherheitsoptionen“ per Passwort verschlüsseln. Dumm allerdings, wenn man das Kennwort vergisst. Dann hilft „Word Password“ weiter. Das Tool bietet für Dokumente, die mit Word bis Version 2003 erstellt wurden, mehrere Knackmethoden an. Bei der „Brute Force Attack“ probiert es alle erdenklichen Buchstaben- und Zahlenkombinationen aus. Je nach Länge des Passworts und Rechenleistung kann das mehrere Tage, Wochen oder gar Monate dauern. Schneller funktioniert die „Dictionary“-Suche, bei der das Tool nur Begriffe aus einem Wörterbuch testet. Die Demoversion sucht nur nach Kennungen mit bis zu drei Stellen. Der Hersteller bietet auch Passwort-Knacker für andere Dateiformate an.

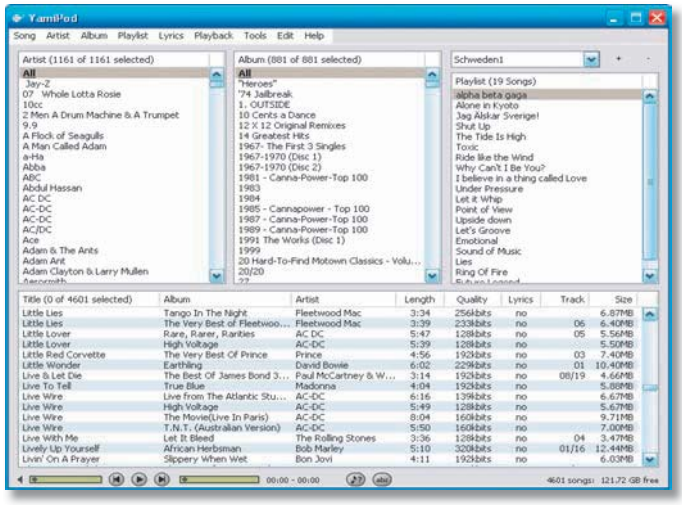
Umstritten, weil: Wenn man mit dem Tool Schutzmaßnahmen von Dokumenten knackt, ohne dazu berechtigt zu sein, macht man sich strafbar.

Retter in der Not: Wer das Passwort zu einer Word-Datei vergessen hat, kann dieses Tool darauf ansetzen, es herauszufinden

Yamipod: Kopierfunktion für iPod/iTunes problemlos nachrüsten

iTunes hat einige Beschränkungen. Die tiefgreifendste ist, dass sich Lieder zwar zum iPod hin übertragen lassen, aber von dort nicht wieder zurück auf den PC. Yamipod ist eine schlanke Alternative zu iTunes, die diese Einschränkung nicht hat. So können Sie nach einem Datenverlust der PC-Festplatte zumindest Ihre Musik zurückkopieren. Wer allerdings das Podcast-Verzeichnis von Apple ansehen und Musik oder Videos im Apple Store kaufen möchte, benötigt weiterhin iTunes. Yamipod muss nicht installiert werden. Am besten kopieren Sie die EXE-Datei auf den Speicher Ihres iPods, damit Sie das Tool immer dabei haben.

Umstritten, weil: Apple dürfte nicht erfreut sein über die Existenz von Yamipod. Irgendeinen Grund wird das Unternehmen ja gehabt haben, die Kopierfunktion in iTunes wegzulassen. Welcher das sein mag, darüber kann man nur spekulieren. Eine gesetzliche Verpflichtung, diese Funktion auszuklammern, gibt es jedenfalls nicht.



Yamipod: Mit dem Tool verwalten Sie die Musik auf Ihrem iPod und können Musik vom Player auf den PC kopieren – mit iTunes geht das nicht

Unseriöse Anbieter vertreiben Toolbars, die sich ins System einnisten, den Browser manipulieren und aggressiv kommerzielle Websites bewerben. Eine De-Installation ist oft nur mit Tricks möglich.

Von **Hartmut Pelitz**

Ärger mit Symbolleisten meistern

Problemfall Toolbars

GEHT ES NACH DEM WILLEN VON Google, Skype, Ebay, MSN, Yahoo und vielen weiteren Dienstleistern, ist Ihr Desktop mit einer Vielzahl von Symbolleisten zugekleistert. Toolbars wie die von MSN oder Google binden sich direkt in den Internet Explorer ein, andere arbeiten augenscheinlich nur auf dem Desktop. Viele Unternehmen haben Toolbars inzwischen als Marketinginstrument erkannt und bieten mehr oder weniger nützliche Werkzeugleisten gespickt mit Schnittstellen zur eigenen Websites und zu Online-Diensten an.

Aufgabe der Toolbars ist meist ein Direktzugriff auf die Suchfunktionen der jeweiligen Website, ohne auf die entsprechende Seite wechseln zu müssen. Sie geben den gewünschten Suchbegriff in das Eingabefeld der Toolbar ein – und bekommen dann die Treffer im Browser präsentiert.

So landen Toolbars im System

Die meisten Toolbars bekommen Sie als nur wenige hundert KB große EXE-Datei zum Herunterladen angeboten, die per Doppelklick gestartet wird und die die Installation übernimmt. Es gibt auch Online-Installationen, bei der das manuelle Herunterladen entfällt. Mit einem Klick starten Sie den Installationsvorgang, bei dem Sie eine Sicherheitsmeldung des Browsers bestätigen müssen. Bei beiden Varianten müssen Sie den Internet Explorer anschließend neu starten, um die Leiste zu sehen. Bei Windows XP mit Service Pack 2 oder Vista fängt der im Internet Explorer eingebaute Pop-up-Blocker neue Browser-Erweiterungen ab. Damit die Toolbar-Installation klappt, müssen Sie die Einrichtung zulassen.

Einige Toolbars laufen als eigenständiges Programm, die meisten Toolbars sind allerdings fest mit dem Internet Explorer verknüpft. Die Leisten können – sobald Sie den Browser gestartet haben – jederzeit mit einem beliebigen Server im Internet Verbindung aufnehmen, ohne dass Sie davon etwas mitbekommen. Sogar eine Desktop Firewall ist wirkungslos, denn je nach Toolbar läuft die Software im Browser, der als eine Art Tunnel ins Web fungiert. Haben Sie dem Internet Explorer das Recht zugeteilt, auf das Internet zuzugreifen, hat die Symbolleiste automatisch dasselbe Recht. Dazu kommt der Nerv-Faktor: Bei der Arbeit mit mehreren Toolbars geht schnell die Übersicht verloren, schließlich beansprucht jede Leiste Platz auf dem Monitor. Immerhin können Sie manche der Leisten bei Nichtbenutzung im Internet Explorer mit dem Befehl „Ansicht, Symbolleisten“ ein- und wieder ausblenden.

Sicherheitsbedenken beim Einsatz von Toolbars

Ein ernst zu nehmendes Sicherheitsprogramm ist die in manchen Toolbars eingebaute Spyware. Eine Spyware-Toolbar teilt jedem Anwender eine ID-Nummer zu und übermittelt diese zusammen mit Hinweisen zu den vom Anwender durchgeführten Aktionen an den jeweiligen Hersteller: Besuchte Seiten, angerufene Produktinformationen, gekaufte Artikel und so weiter lassen sich auf diese Weise übermitteln. Bedenklich: Auch eine verschlüsselte SSL-Verbindung ist in speziellen Fällen nicht sicher, da die Leiste hinter dem verschlüsselten Kanal sitzt. Alles, was der Anwender im Brow-

ser sieht, kennt auch der Internet Explorer und damit genauso die Toolbar. Um sich vor Browser-Leisten mit Spyware zu schützen, empfehlen wir Ihnen, im Anschluss an jede Toolbar-Installation zur Sicherheit einen zuverlässigen Spyware-Scanner wie das für Privatnutzer kostenlose Sicherheits-Tool Ad-Aware (unter **www.lavasoftusa.com**) laufen lassen.

Wer den IE unter Windows XP mit SP2 oder Vista benutzt, kann sich über die installierten Browser-Erweiterungen einfach einen Überblick verschaffen. Der Add-on-Manager befindet sich im Internet Explorer unter „Extras, Add-Ons verwalten". Damit erhalten Sie Einblick darin, welche Zusatzmodule und Toolbars für den IE auf Ihrem System installiert sind – und welche der Browser momentan verwendet. Einzelne Elemente lassen sich per Mausklick deaktivieren und so zum Beispiel eine lästige Spyware-Toolbar abschalten.

Ein weiteres Problem: Manche Toolbars lassen sich nicht problemlos parallel installieren. Für absturzfreies Arbeiten müssen Sie inkompatible Add-ons de-installieren.

Protected Mode für den IE 7

Um den Internet Explorer besser abzuschirmen, schuf Microsoft beim in Vista eingebetteten Internet Explorer 7 unter anderem den „geschützten Modus" (Protected Mode). Der Browser wird mit geringen Rechten ausgeführt, um den Zugriff auf das Dateisystem, die Registry und andere Bereiche einzuschränken. Schreibzugriff besteht nur im temporären Verzeichnis. Damit soll es Angreifern nicht mehr möglich sein, Schwachstellen des Browsers auszunutzen und beispielsweise die Startseite zu verändern oder vom Anwender unbemerkt zusätzliche Toolbars zu installieren. Der geschützte Modus lässt sich für jede Zone einzeln aktivieren oder deaktivieren. In der Standardeinstellung ist er nur für vertrauenswürdige Sites deaktiviert. Für das Internet, das lokale Netzwerk und eingeschränkte Sites ist er aktiv. Für optimale Sicherheit ist es empfehlenswert, diese Voreinstellungen beizubehalten.

Browser-Hijacker aufspüren

Toolbars, die Sie über den Add-on-Dialog nicht loswerden, müssen Sie mit Hilfe von Spezial-Tools entfernen. Dabei hilft Ihnen die Freeware Hijack This (unter **www.trendsecure.com**).

Tipp: Manche Spyware-Programme haben einen eingebauten Wächter, der den Aufruf von Hijack This verhindert. Ist das bei Ihnen der Fall, benennen Sie die Programmdatei einfach um, etwa in Saubermann.COM. Den ersten Teil des Namens können Sie frei wählen, die Datei-Endung COM ist jedoch zwingend.

Nach dem Start von Hijack This führen Sie mit einem Klick auf die Schaltfläche „Do a system scan and save a logfile" einen Suchvorgang auf Ihrem Rechner durch.

Das Tool erzeugt einen Bericht, der alle laufenden Prozesse auflistet. Die Log-Datei liefert anhand einer Buchstaben-Zahlen-Kombination am Zeilenanfang Hinweise auf die Art des Programms: „R" steht für die Start- und Suchseite des Internet Explorers. In der Gruppe O1 bis O23 zeigt Hijack This, welche Zusatzmodule und Active-X-Controls sich im Internet Explorer eingenistet haben. Außerdem erfahren Sie, welche Malware beim Systemstart automatisch aktiv wird. Um herauszufinden, ob es sich bei den Programmen tatsächlich um schädliche Software handelt, schlagen Sie den ID-Code auf der Website **www.castle cops.com/CLSID.html** nach.

Automatische Sicherheitsanalyse

Eine besser verständliche Auswertung des Protokolls von Hijack This erhalten Sie, wenn Sie die Datei zur Analyse auf die Website **www.hijackthis.de** hochladen. Dazu kopieren Sie den Inhalt des Protokolls über die Zwischenablage in das große Eingabefeld auf der Web-Seite, oder Sie starten den Upload der Log-Datei mit „Durchsuchen".

Die Analyse starten Sie mit einem Klick auf „Auswerten". Lassen Sie die Option „Besucherbewertungen anzeigen" in jedem Fall eingeschaltet, damit der Dienst Infos zu den Funden auf Basis von Erfahrungsberichten anderer Hijack-This-Nutzer liefert.

Für eine detaillierte Analyse veröffentlichen Sie Ihre Protokolldatei unter **http://forum.hijackthis.de**. Dort begutachten erfahrene Hijack-This-Nutzer die Suchergebnisse und geben Tipps, wie Sie die Malware wieder loswerden. Hierfür fügen Sie Ihr Protokoll einfach in einem neuen Diskussionsbeitrag unter „Support" im Forum „HijackThis Logfiles" ein. ●

Huckepack-Installation: Wer nicht aufpasst, installiert mit der aktuellen Version des populären Bildbetrachters Irfan View auch gleich die kostenlose Toolbar von Google mit

Unerwünschte Toolbars aufspüren: Eine Online-Analyse der Protokolldatei von Hijack This liefert eine Übersicht über mögliche Malware auf Ihrem Rechner

Tuning-Tools sind gefährlich: Oft trennt Sie nur ein einziger Klick von einem defekten System. Wo genau die Probleme liegen und welche der viel gepriesenen Utilities besonders gefährlich sind, erfahren Sie hier.

Von **Tim Kaufmann**

Foto: © JL – Fotolia.com

So richten Tuning-Tools Schaden an

Kaputt geklickt

Sie löschen jede Menge Dateien und verbiegen Windows bis an seine Grenzen: Tuning-Tools rücken kritische und unkritische Änderungen gleichermaßen in greifbare Nähe. Am Beispiel von **SAD Tuneup Utilities** (*www.tuneup.de*) – einem der populärsten und erfolgreichsten deutschsprachigen Tuning-Helfer für Windows – zeigen wir Ihnen, wo die potenziellen Gefahren beim Systemoptimieren mit Tools liegen.

Tuning-Tools wie die Tuneup Utilities unterstützen den Anwender mit zahlreichen Tipps, aufschlussreichen Hilfetexten und warnen vor potenziell gefährlichen Funktionen. Gefahrloses Tuning setzt aber immer zwei Faktoren voraus: ein solides Tuning-Tool und einen Nutzer, der entsprechende Hilfen auch berücksichtigt. Wer vorschnell in der Oberfläche umherklickt und Hilfetexte bestenfalls überfliegt, der ist auf dem besten Weg zu einem System, das sich unerwartet verhält oder sogar beschädigt wird.

Stört manchmal: Automatische Defragmentierung

Die verschiedenen Tuneup-Funktionen stehen Ihnen in sechs Kategorien zur Verfügung. Los geht es mit der Rubrik „Leistung steigern“. Deren erstes Hilfsmittel heißt „Tuneup Drive Defrag“ und ist eine Defragmentierung für die Festplattenlaufwerke Ihres Rechners.

Damit eine Festplatte Dateien speichern kann, wird sie durch ein Dateisystem – bei Windows XP und Vista üblicherweise NTFS – in Tausende gleich große Datenblöcke unterteilt. Weil jeder Datenblock nur wenige Kilobyte umfasst, werden größere Dateien beim Speichern auf mehrere Datenblöcke verteilt. Windows achtet dabei aber nicht darauf, dass jede Datei in benachbarten Datenblöcken landet, sondern belegt einfach die nächstbesten freien Blöcke. Solche fragmentierten, also nicht in aufeinander folgenden Datenblöcken gespeicherte Dateien lassen sich nur verzögert laden.

Tuneup Drive Defrag startet eine Defragmentierung auf Wunsch manuell oder automatisch. Letzteres kann zu unerwünschten Nebenwirkungen führen. Einmal eingerichtet, gerät nur allzu schnell in Vergessenheit, dass regelmäßig Samstags um 16 Uhr die Defragmentierung startet. Dann kann es zu Leistungsengpässen kommen, beispielsweise weil man beispielsweise just zu dieser Zeit ein grafiklastiges Spiel startet oder Videos in HDTV aufnehmen will. Verlorene Spiele und ruinierte TV-Aufnahmen können die Folge sein.

Zweifelhafte Hilfe: Arbeitsspeicher optimieren

Tuneup Utilities’ zweites Doping-Mittel für den Rechner ist der „Tuneup Memory Optimizer“, der freien Arbeitsspeicher gewinnen soll. Die Menge des Arbeitsspeichers, die nach dem Start des Betriebssystems verbleibt, ist neben der Geschwindigkeit von CPU, Grafikkarte und Festplatte einer der vier Faktoren, die maßgeblich über die Gesamtgeschwindigkeit eines Rechners bestimmen. PCs, die über viel freies RAM verfügen, können viele Programme und Anwendungsdaten verfügbar behalten. Rechner mit wenig verfügbarem RAM verwen-

den die Auslagerungsdatei auf der Platte als Merkzettel. Zugriffe auf die Auslagerungsdatei sind deutlich langsamer als solche auf echten Arbeitsspeicher. Deshalb arbeitet es sich auf Rechnern, die reich an freiem RAM sind, schneller.

Unter XP bietet Tuneup Utilities zwei verschiedene Möglichkeiten, den Arbeitsspeicher zu optimieren. Zum einen können Sie im Rahmen des „AutoOptimize“ eine Untergrenze freien RAMs vorgeben. Wird diese erreicht, sorgt Tuneup Utilities automatisch für mehr freien Arbeitsspeicher. Alternativ rufen Sie die manuelle Optimierung auf, beispielsweise bevor Sie eine RAM-intensive Anwendung wie Photoshop starten.

Wie so manche Automatik fällt auch die an und für sich gute Auto-Optimize-Funktion dem Nutzer gelegentlich in den Arm. Durch die mit der Optimierung einhergehende Auslagerung wird die Festplatte belastet. Geschieht das zu einem Zeitpunkt, wo die Festplatte ohnehin schon gut ausgelastet ist, kann dies den Rechner ausbremsen. Speziell bei Tuneup Utilities kommt hinzu, dass sich die Optimierung auch per Tastenkombination <Strg>-<Alt>-<O> aufrufen lässt. Unter Umständen ruft der Nutzer so die Optimierung durch eine Verwechslung mit einer anderen Tastenkombination zu einem unerwünschten Zeitpunkt auf. Es wäre sinnvoller, wenn der Hotkey manuell freigeschaltet werden müsste. Er ist nach der Installation von Tuneup Utilities jedoch standardmäßig eingeschaltet.

Registry optimieren ohne Prüfroutine

Weiter geht die Optimierung mit Registry Defrag, das laut Hersteller den Speicherverbrauch der „Registrierung“ senkt und Defekte in der „Registrierung“ behebt. Mit „Registrierung“ meint Tuneup Utilities die Registrierungsdatenbank. Die Registry besteht aus zwei Teilen, von denen einer allgemeine Konfigurationsdaten und einer die benutzerspezifischen Infos aufnimmt. Auf der Festplatte findet sich die Registry in Form mehrerer Dateien wieder, den Hives. Durch nicht gründlich arbeitende Uninstall-Funktionen und Programm- oder Systemabstürze kann es zu überflüssigen und unvollständigen Einträgen in der Registry kommen – ein Effekt, der mit dem Alter einer Windows-Installation voranschreitet.

Registry Defrag geht nach unseren Tests umsichtig und zuverlässig zu Werke, birgt aber prinzipbedingte Nachteile. Zum Einen müssen Sie alle Programme beenden, damit es die Registry nach Fehlern durchsuchen kann. Gehen Sie dabei langsam und gründlich vor, sonst verlieren Sie womöglich Informationen, beispielsweise in einem noch nicht gespeicherten Word-Dokument. Eine Check-Routine auf parallel laufende Programme fehlt.

Zum anderen müssen Sie auch Ihre Viren- und Spyware-Abwehrprogramme zeitweise abschalten. Nur so lässt sich ein argwöhnischer Virenschutz, der Tuneup bei der Analyse anhalten könnte, zuverlässig umgehen. Allerdings öffnen Sie damit auch potenziellen Schädlingen Tür und Tor, die während der Analyse den Rechner angreifen. Und wenn Ihr Virenscanner nicht über eine automatische Reaktivierung verfügt, bleiben Sie unter Umständen sogar noch deutlich länger ungeschützt.

Schnelloptimierung und Leistungsratgeber

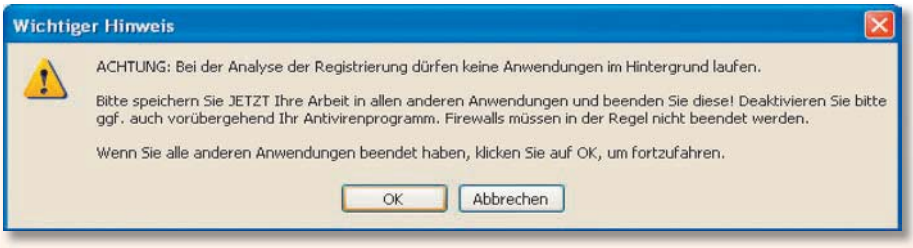
Als Nächstes geht Tuneup Utilities „Speed Optimizer“ ans Werk, das aus der Schnelloptimierung und dem Leistungsratgeber besteht. Letzterer bietet Programme, die Sie seit längerem nicht mehr oder nie verwendet haben, zur De-Installation an. So wird Speicherplatz frei. Im Fall automatisch startender Programme verkürzt sich außerdem die Startzeit des Rechners, und der RAM-Verbrauch sinkt.

Technisch interessanter ist die Schnelloptimierung, die an mehreren Punkten ins System eingreift. Sie schaltet Windows-Dienste ab und optimiert die Netzwerkeinstellungen sowie die visuellen Effekte der Windows-Oberfläche.

Überflüssige Dienste abzuschalten kann danebengehen

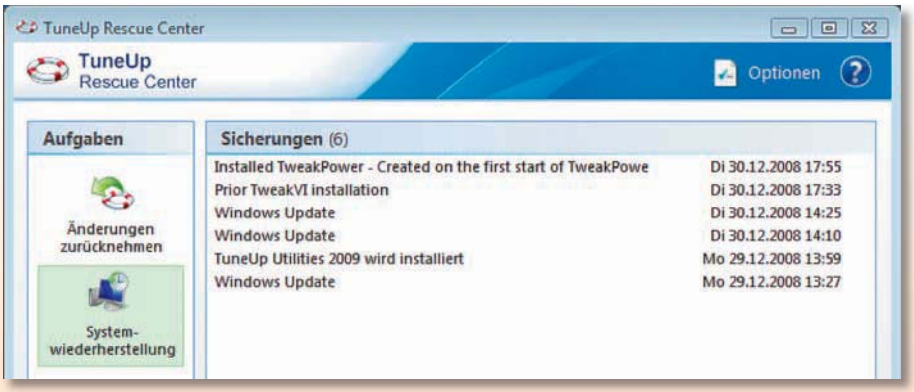
Bei den Diensten handelt es sich um automatisch mit Windows startende Module, die im Hintergrund laufen. Ein frisch installiertes Windows XP bringt über achtzig Dienste mit, bei Vista sind es einige mehr. Jeder Dienst verlängert die Zeit, die Windows zum Booten benötigt, belegt RAM und strapaziert die CPU. Von daher ist es plausibel, dass Tuneup Utilities & Co. überflüssige Dienste abschalten wollen, um den Rechner zu beschleunigen.

Kritisch ist unter Umständen die Auswahl der zur Deaktivierung vorgeschlagenen Dienste. Tuneup geht hier sehr vorsichtig vor und schaltet lediglich den Web-Client-Dienst aus, der die Anzeige von ›



Gefährlich: Nur bei abgeschaltetem Virenscanner lässt sich die Registry optimieren

Gelungene Aktion: Tuneup Utilities beschreibt die vom Programm zum Abschalten vorgeschlagenen Windows-Dienste mit einem ausführlichen Informationstext



Einstellungen widerrufen: Mit Funktionen wie dem Tuneup Rescue Center erleichtert die aktuelle Generation von Tuning-Tools die Rücknahme unerwünschter Änderungen

FTP- und Sharepoint-Ordnern im Arbeitsplatz ermöglicht. Entdeckt Tuneup Utilities nur ein einziges Benutzerkonto auf dem PC, dann schlägt es außerdem den Secondary Logon zum Abschalten vor, der für die Funktion „Ausführen als" zuständig ist. Ebenfalls ein Pluspunkt: Beide Dienste werden von Tuneup Utilities in den Modus „Manuell" versetzt. So kann Windows sie bei Bedarf anschalten – die Funktionen sind also nicht ganz aus der Welt.

Viel hilft nicht viel

Andere Tuning-Tools lösen das weniger elegant. Nach dem Motto „Viel hilft viel" schlägt **Ashampoo Win Optimizer** (*www.ashampoo.de*) auf demselben Testsystem mit Windows XP gleich acht Dienste zum Abschalten vor, darunter auch Nützliches wie den Sitzungs-Manager für Remote-Desktop-Hilfe. Eine ähnlich detaillierte Aufklärung über den damit einhergehenden Funktionsverlust wie bei Tuneup Utilities sucht man bei Win Optimizer vergeblich. Weniger versierte Anwender drehen deshalb unter Umständen mehr Diensten den Hahn ab, als gut ist. Die Fehlersuche gestaltet sich dann recht komplex, denn Fehlermeldungen weisen nur selten auf abgeschaltete Dienste als Ursache hin. Kaum ein weniger erfahrener Anwender führt schon einen Fehler, der womöglich erst ein paar Tage später auftritt, auf Anhieb auf einen nicht gestarteten Dienst zurück.

LAN oder Internet – beides geht nicht

Auch die Netzwerkeinstellungen verbessert das Tool. Zu den vorgeschlagenen Maßnahmen der Schnelloptimierung zählen Änderungen der TCP/IP-Parameter MTU (Maximum Transmission Unit) und RWIN (Receive Window). Andere Tools verändern auch die Werte für MSS (Maximum Segment Size) und TTL (Time to live).

Tuning-Tools wie Tuneup Utilities unterstellen, dass der Nutzer den Großteil seiner Daten mit dem Internet austauscht, und optimieren die TCP/IP-Einstellungen entsprechend. Für die überwiegende Zahl aller Nutzer trifft das sicherlich zu. Wer aber regelmäßig große Datenmengen durch das lokale Netzwerk jagt, der ist mit den für das Internet optimierten Einstellungen weniger gut aufgehoben. Der Online-Datentransfer wird auf Kosten der Leistung beim Netztransfer optimiert. Das ist ein Zusammenhang, auf den Nutzer der Software nicht in genügendem Ausmaß aufmerksam gemacht werden.

Tipp: Gute Tuning-Tools erkennen Sie auch daran, dass Sie unter Vista keine Veränderungen an den TCP/IP-Einstellungen vornehmen. Vista optimiert diese Parameter nämlich selbständig, Tuning-Maßnahmen kommen ihm dabei allenfalls in die Quere.

Tückisch: Speicherplatz gewinnen

Ist die Leistungsoptimierung abgeschlossen, bietet Tuneup Utilities die Rückgewinnung von Speicherplatz auf der Festplatte an. Nach einem Klick auf die Schaltfläche „Speicherplatz gewinnen" analysiert das Programm zunächst den Festplatteninhalt und generiert dann eine Übersicht potenziell überflüssiger Inhalte.

DIESE 10 PROGRAMME SIND GIFT

Die folgende Liste nennt die Programme, mit denen sich weniger versierte, unachtsame Anwender leicht das System zerschießen können.

Tuneup Utilities 2009: Die System-Suite (*www.tuneup.de*) macht folgenreiche Tuning-Maßnahmen so leicht verfügbar, dass technisch weniger interessierten Nutzern wichtige Details nicht rechtzeitig bewusst werden.

X-Setup Pro: Die deutschsprachige Oberfläche des überaus umfangreichen System-Tools (*www.xq-setup.de*) steht nur mit einem separaten Download zur Verfügung. Das erhöht die Gefahr von Missverständnissen und unabsichtlichen Tuning-Maßnahmen.

Tweak XP und Tweak Vista: In der in Teilen recht unübersichtlichen Programmoberfläche fällt es schwer, vorgenommene Änderungen wieder rückgängig zu machen (*www.totalidea.com*).

Ashampoo Win Optimizer: Mit dem Modul Startup Tuner legt der Nutzer unter Umständen für die reibungslose Funktion des Rechners wichtige Autostart-Programme lahm (*www.ashampoo.de*).

Tweak Power: Wer mit dem integrierten Port-Scanner nicht richtig umzugehen weiß, macht sich bei Administratoren und anderen Internet-Nutzern schnell unbeliebt (*http://kurtzimmermann.com*).

Tweak RAM: Nach der Installation ruft Tweak RAM (*www.elcor.net*) eine Website auf, die das Vorhandensein kritischer Systemfehler suggeriert und zum Download weiterer Programme des Anbieters auffordert.

Riva Tuner: Ohne ausreichendes Hintergrundwissen kann der Einsatz von Riva Tuner (*http://downloads.guru3d.com*) Ihre Grafikkarte durch Übertaktung dauerhaft beschädigen.

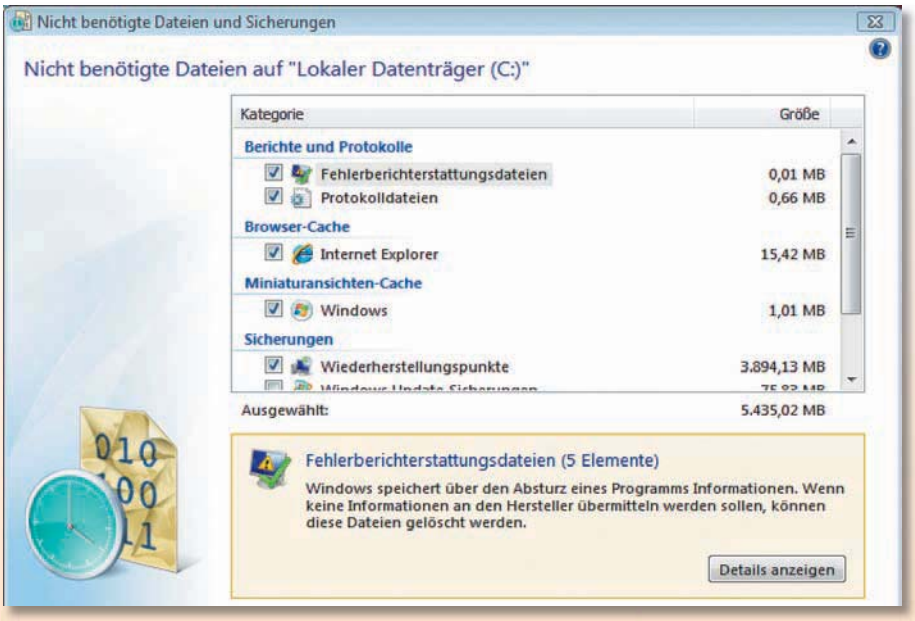
Nlite und Vlite: Beide Tools (*www.german-nlite.org und shttp://vlite.net*) erstellen individuelle Setup-CDs für Windows XP und Vista. Zwischen einer perfekten Installation und einem nicht starteten oder instabilen System liegt bei der Konfiguration oft nur ein einziger Mausklick.

PC Decrapifier: Die Software (*http://pcdecrapifier.com*) soll neue Rechner von unerwünschten Demoversionen befreien. Zuweilen gerät dabei aber auch absichtlich installierte Software unter die Räder. So wird eine erneute Installation der betreffenden Programme fällig.

Eusing Free Registry Cleaner: Wer im Tool (*www.eusing.com*) bei der Auswahl, welche verwaisten Verknüpfungen, fehlerhaften Pfadangaben und fehlerhaften DLLs das Programm beseitigen soll, einen Fehler macht, fegt mitunter noch benötigte Bibliotheksdateien vom Rechner.

Die Liste besteht aus zwei Kategorien namens „Nicht benötigte Dateien und Sicherungen“ und „Windows-Funktionen“. Ein Klick auf einen dieser Einträge zeigt, welche Inhalte sich dahinter verbergen. Zu den nicht benötigten Dateien zählt Tuneup Utilities beispielsweise den Inhalt des Browser-Caches und temporäre Dateien. Wer diese Dateien löscht, macht in der Regel nichts falsch. Kritischer sind die ebenfalls zum Löschen vorgeschlagenen Wiederherstellungspunkte, Windows-Update-Sicherungen und – bei Vista – das Backup des Service Pack 1. Sie machen neunzig Prozent der auf unserem Vista-Testsystem zur Vernichtung vorgeschlagenen Dateien aus und laden deshalb ganz besonders zum Löschen ein.

Wer sich davon aber blenden lässt und deshalb Tuneup Utilities warnende Hinweise überliest, der beraubt sich zugleich vieler Reparaturmöglichkeiten. Zumindest die Wiederherstellungspunkte sollten Sie aufheben, um so beim Auftreten von Fehlern – etwa durch frisch installierte Software oder Windows Updates – bequem zu einem früheren Zustand des Systems zurückkehren zu können.



Ausgehebelte Sicherheit: Wer die bei wichtigen Systemänderungen erstellten Wiederherstellungspunkte leichtfertig löscht, der riskiert seine Reparaturmöglichkeiten

Windows-Funktionen entfernen mit Nebenwirkungen

Tuneup Utilities entfernt auf Wunsch sogar ganze Windows-Funktionen. Unter Vista enthält die entsprechende Funktion den Vorschlag, den „Energiesparmodus Ruhezustand“ auszuknipsen. Im Ruhezustand ist der PC gänzlich ausgeschaltet, verbraucht also keinen Strom. Beim Einschalten wird aber nicht der normale Boot-Vorgang aufgerufen. Stattdessen lädt der PC Windows so, wie Sie es verlassen haben – inklusive aller gestarteten Programme, geöffneter Web-Seiten und Dokumente.

Die dazu notwendigen Daten bezieht Windows aus einer speziellen Datei, die so groß ist wie der Arbeitsspeicher des Rechners. Schalten Sie diesen Energiesparmodus ab, wird die Datei gelöscht und freier Speicher auf der Festplatte gewonnen. Tuneup Utilities weist auf diese Zusammenhänge hin. Weniger versierten Nutzern entgeht aber unter Umständen, dass eine Änderung am Ruhezustand sich auf alle Nutzer des Rechners auswirkt und das unerwartete Verhalten des Rechners etwa die übrigen PC-Nutzer verwirren kann. Ähnliches gilt auch für die Funktionen zum Austauschen von Programm- und Laufwerks-Icons, die Tuneup Utilities ebenfalls mitbringt. Was für den einen Nutzer eine willkommene Abwechslung bedeutet, kann den PC für andere Anwender unbenutzbar machen.

VORSICHT FALLE Die 10 gefährlichsten Tweaks

Unsere Top 10 informiert Sie über die zehn größten Tuning-Fallen im Zusammenhang mit Tweak-Tools.

Platz 10: Rechner schnell herunterfahren. Beim schnellen Herunterfahren bleibt Programmen unter Umständen nicht genug Zeit, um Informationen ordnungsgemäß zu speichern. Datenverlust droht!

Platz 9: Prefetch-Cache löschen. Durch Löschen des Prefetch-Caches verzögert sich nur der nächste Boot-Vorgang beziehungsweise der erste Aufruf eines Programms, denn Windows muss die Prefetch-Dateien dann erst neu erzeugen.

Platz 8: XP Superfetch-Modus aktivieren. Wer versucht, den in XP angeblich vorhandenen Superfetch-Modus à la Vista zu aktivieren, der beschädigt höchstens die Registry seines Rechners.

Platz 7: Dokumente und Einstellungen verschieben. Der Ordner „C:\Dokumente und Einstellungen“ enthält alle Einstellungen und Dateien der Benutzer. Wer ihn verschiebt, riskiert insbesondere unter XP gravierende Fehlfunktionen.

Platz 6: Firefox und Internet Explorer tunen. Auf Wunsch laden Firefox und Internet Explorer Daten über mehrere parallele Verbindungen vom Webserver. Das beschleunigt den Seitenaufbau, aber manche Seiten sind danach unerreichbar.

Platz 5: Netzwerkeinstellungen tunen. Im besten Fall winkt eine minimal flottere Internet-Verbindung, mit etwas Pech geht danach gar nichts mehr.

Platz 4: Speicher defragmentieren. Den Arbeitsspeicher zu defragmentieren bringt allenfalls kurzfristigen Nutzen, belastet die Festplatte aber enorm.

Platz 3: Systemwiederherstellung abschalten. Die Systemwiederherstellung belegt einige Gigabyte Speicherplatz – und sie ist Ihre Versicherung. Wenn das System beschädigt wurde, versetzen Sie es damit in einen früheren Zustand zurück.

Platz 2: Windows-Updates deaktivieren. Windows-Updates können zuweilen nerven. Wer sie deswegen deaktiviert, handelt sich aber gravierende Sicherheitsprobleme ein.

Platz 1: Übertakten. Programme wie Riva Tuner ermöglichen das Übertakten der Grafikkarte. Dabei wird diese außerhalb ihrer Spezifikation betrieben und kann zerstört werden.