

Tipps & Tricks

CD

Vollversion: McAfee Sicherheitspaket

Personal Firewall Plus 2006 7.0, Antispyware 2006 2.0, Spamkiller 2006 7.0

Vollversion: Steganos Hacker Tools 7

Garantiert viren- und trojanerfreie Hacker-Tools plus Hacker-Workshops & Videos

Weitere Software auf CD:

Password-Knack-Suite

15 geniale Entschlüsselungs-Tools
für verloren gegangene Kennwörter

Tools aus dem Giftschränk

Die besten Tools zum anonymen Surfen,
geheime WLAN-Knacker & DVD-Kopierer

**Usenet-
Zugang gratis!**

3 Monate unzensuriert
und schnell
Dateien saugen

Hacken! Knacken! Tauschen!

Saugen mit Highspeed

So laden Sie täglich zig
Gigabyte: **BitTorrent** und
Newsgroups – die letzten
echten Tauschbörsen

Privatsphäre schützen

Keine Chance für **Rootkits**,
Bots und **Keylogger**.
Die 30 aktuellsten Risiken
– und wie Sie sich schützen

Raubkopier-Report 2007

Verbotene **Programme** und
Filme aus dem Ausland: Das
sind die Strafen, so arbeiten
die Fahnder

Auf Heft-CD: Vollversionen von Steganos und McAfee

Mit der Premium-Vollversion Steganos Hacker Tools 7 lernen Sie die Arbeitsweise von Hackern detailliert kennen. Mit dabei sind Profi-Tools zum Herz-und-Nieren-Check von PCs und Netzwerken. Eine tolle Ergänzung ist das McAfee-Sicherheitspaket mit Firewall, Spam- und Spyware-Scanner.



PLUS: QEMU-Puppy Linux 2 und Passwort-Knack-Suite

Mit null Risiko sicher surfen komplett ohne Virenschutz – mit QEMU-Puppy Linux geht das ganz einfach. Die Surf-Umgebung in Form einer virtuellen Maschine starten Sie ohne vorherige Installation. Viren, Trojaner und Hackangriffe können Ihnen so nichts anhaben. Wenn Sie Puppy Linux schließen, sind alle Änderungen verworfen. Lohnenswert: Die 15 Kennwort-Knack-Tools.

Service für die Heft-CD

Falls Sie einen Defekt der Heft-CD vermuten, wenden Sie sich für Ersatz bitte direkt an den PC-WELT-Leserservice, Tel. 0711/ 7252277. Mail: shop@pcwelt.de. Österreich: Tel. 01/2195560. Schweiz: Tel. 071/31406-15.

Haftungsausschluss: Das Installieren der auf Heft-CD bereitgestellten Software erfolgt auf eigene Gefahr.

PC-WELT übernimmt keine Gewährleistung oder Haftung für die Funktionsfähigkeit und etwaige Schäden, die durch die Installation entstehen können. Die Haftung für mittelbare Schäden oder entgangenen Gewinn ist ausgeschlossen.



Szenengeflüster

Die Warez- und Cracker-Szene ist aktiver denn je. Das klassische Filesharing ist zwar tot, längst aber gibt es neue Tauschkanäle für Software, Filme und MP3s.

Vorsicht Falle Jeden gefassten Raubkopierer stellt die Software- und Filmindustrie medienwirksam an den Pranger und kriminalisiert in Kinospots pauschal alle Internet-Nutzer. Darüber kann die Szene nur milde lächeln – erwischen lassen sich in der Regel nur noch unbedarfte Frischlinge. Die ehemals sehr populären Tauschbörsen sind tatsächlich am Ende. Zu groß ist hier die Gefahr, in eine Falle zu tapen, die Industrie und Behörden auf der Jagd nach Raubkopierern aufgestellt haben.

Tauschkanäle Aktuell ist vor allem das Usenet die populärste Anlaufstelle für Software, Bilder, E-Books, Filme und Musik – so genannte Binaries. Neben freien Inhalten werden hier auch urheberrechtsgeschützte Dateien angeboten. Doch auch das Web und Bit-Torrent-Seiten sind ewig sprudelnde Quellen an interessantem Content – entsprechende Maßnahmen zum eigenen Schutz vorausgesetzt.

Techniken Das Aushebeln von Kopierschutztechniken bei Film-DVDs und Audio-CDs ist verboten. Doch ebenso wie das Freischalten von Software oder der Empfang von Pay-TV ohne Bezahlung ist das Clonen von Inhalten für viele offenbar nach wie vor ein Volkssport. Kaum hat die Industrie eine angeblich sichere und unknackbare Technik erfunden, gibt's entsprechende Cracks und Anleitungen zum Umgehen der Sicherungen. PC-WELT ist tief in die Welt der Hacker und Kopierer eingetaucht und fasst in diesem Special die Tricks der Profis für Sie zusammen.

Viel Spaß – und bleiben Sie auf der sicheren Seite!

Wolfgang Koser

Wolfgang Koser
Stellvertreter des Chefredakteurs



Heft-CD



Auf CD: Steganos Hacker Tools 7 8

Hacker, Cracker, Script-Kiddies, Phisher – lernen Sie die Methoden und Werkzeuge der Szene kennen, und finden Sie mit diesen Tools Sicherheitslücken auf Ihrem System

Kopieren & Tauschen

Raubkopier-Report 2007 10

Das Katz-und-Maus-Spiel zwischen Crackern und Verfolgern geht in die nächste Runde

Drei Monate gratis saugen 16

Bedienen Sie sich drei Monate lang – kostenlos aus mehreren tausend Newsgroups

Sprudelnde Datenquelle 20

Gigabyte-weise Software, Videos und Musik laden Sie im Maximaltempo aus Newsgroups

Diese Kopien sind noch erlaubt 26

Wir sagen Ihnen, was Sie kopieren dürfen, ohne in Konflikt mit dem Gesetz zu kommen

Raubkopierer im Visier 30

Unser Strafverfolgungsreport zeigt: Auch kleine Fische werden zunehmend kriminalisiert

Die aktivste Tauschbörse 34

Bit Torrent ist die letzte Filesharing-Plattform und trotz Beschränkungsversuchen

Hardcore gratis 40

Tausende unzensurierte Pornovideos und Sexbilder gibt's gratis und ohne Jugendschutz

Laden Sie, was Sie wollen 46

Immer mehr Websites versuchen, mit Schutzmechanismen Downloads zu unterbinden

Knacken

Alles knacken 52

Neue Windows-Tools hebeln den Kopierschutz von Musikdateien und Filmen aus

Tools aus dem Giftschränk 58

Es gibt viele hochwirksame Utilities, die in den falschen Händen Schaden anrichten können

Jede Software gratis nutzen 62

Ob Shareware oder Demo – so gut wie jede Testversion lässt sich als Vollversion freischalten

Rootkit-Finder 66

Rootkits sind schädliche Programme der ganz fiesen Art, vor denen Sie sich schützen sollten



Kopieren & Tauschen

Brandaktuelle Kinofilme, Software, CDs, DVDs und Seriennummern – nach wie vor ist im Web fast alles zu haben. Doch die Raubkopier-Szene kommt durch rigorose Ermittler immer mehr in Bedrängnis.

ab Seite 10



Knacken

Mit neuen Kopierschutzmethoden versucht die Industrie, das Kopieren von Musik, Filmen und Programmen zu erschweren. Doch von Premiere HD über Blue-Ray bis hin zu Seriennummern lässt sich alles freischalten.

ab Seite 52



Hacken

Sie wollen Passwörter am PC decodieren und persönliche Daten ausspähen? Lesen Sie, mit welchen Tricks Hacker arbeiten und wie Sie Ihre Abwehr so effektiv wie möglich gestalten.

ab Seite 88



3 Sicherheits-Tools von McAfee

Alles drin im McAfee-Sicherheitspaket: Rundumschutz für Ihren Windows-PC erhalten Sie mit dem Internet-Verbindungswächter McAfee Personal Firewall Plus 2006, dem automatischen Spionagekiller McAfee Antispyware 2006 2.0 und dem Werbeblocker McAfee Spamkiller 2006. **auf CD**

HD geknackt	70
Der Kopierschutz von HD-DVD, Blu-Ray und Premiere HD schien unüberwindlich	
Wie Katz und Maus	74
Mit WGA wollte Microsoft Raubkopien vorbeugen. Die Technik entpuppt sich als Flop	
1a Raubkopien aus dem Web	78
Profis finden Download-Links für illegale Software in Russland und China	
Debranding für das Handy	82
Wer sein Mobiltelefon knackt, entkommt der Kostenfalle durch Provider-Branding	
Einbruch mit Nachschlüsseln	84
Office, Mailkonten, Messenger – für fast jeden Kennwortschutz gibt es Knack-Software	

Hacken

Hacker greifen an	88
Hacker nutzen potenzielle Schwachstellen von Computersystemen für Online-Attacken	
Hacken lernen im Schnellkurs	92
Intensivkurse versprechen, Sie in einer Woche zum Hacker auszubilden – wir waren dort	
Geschützte Privatsphäre	94
Eine Menge Leute interessieren sich für Ihre Daten – dagegen sollten Sie was tun	
Die Abzocker-Mafia im Web	98
Geschenke, Schnäppchen ... wenn ein Angebot klasse klingt, müssen Sie auf der Hut sein	
Diagnose: Viren tot!	106
Hat sich Ihr PC einen Virus oder Trojaner eingefangen, dann sollten Sie schnell handeln	
Bot-Armeen greifen an	110
Auf tausenden PCs warten gefährliche Tools auf das Kommando für ein Bombardement	
Großer Lausangriff	112
Keylogger sind hinterhältige Tools zur unsichtbaren Überwachung und Protokollierung	
Sicher bleibt es unsicher	116
In den kommenden Monaten sind einige schwerwiegende Bedrohungen zu erwarten	
Sicherheits-Mythen entlarvt	120
Hartnäckig halten sich eine Reihe von halb-wahren Behauptungen zur PC-Sicherheit	

Rubriken

Editorial	5
Impressum/Inserentenverzeichnis	123
Vorschau	124



Tools aus dem Geheimkoffer

Untergrund-Tools satt, 15 Kennwortknacker, ein Hacker-Labor mit Software, Workshops und Trainings-Videos von Steganos sowie das McAfee-Sicherheitspaket – das bietet die Heft-CD.

Von **Ramon Schwenk**

Wer im Internet einfach drauflos lädt, Tauschbörsen nutzt oder auf problematischen Web-Seiten surft, lebt gefährlich. Die Heft-CD enthält alle nötigen Programme, die Ihren PC sicherer machen. Hacker und Angreifer haben dann keine Chance mehr, in Ihren Rechner einzudringen. Viren und Würmer beißen sich an dem virtuellen Schutzschild des McAfee-Sicherheitspakets die Zähne aus.

Mit der Vollversion Steganos Hacker Tools 7 können Sie Ihren PC optimal durchchecken und feststellen, ob er auch wirklich

gegen Hackerangriffe immun ist. Dabei kommen echte Untergrund-Programme zum Einsatz, nicht etwa harmlose Software-Placebos.

Virtuelles Hacker-Labor: Steganos Hacker Tools 7

Die Vollversion Steganos Hacker Tools 7 verspricht spannende Einblicke in die Welt der Hacker, ohne dass Sie Angst um Ihren eigenen Rechner haben müssen. Die Workshops, Grundlagen-Infos und garantiert Malware-freien Tools werden durch Video-

Shows ergänzt, in denen die wichtigsten Tricks der Hacker detailliert erklärt werden. Gezeigt wird beispielsweise, wie War Driver kabellose Netzwerke aufspürt und deren Zugangs-codes knackt, welche Passwortcracker Hacker gerne einsetzen oder wie Scan-Techniken zum Aufspüren von System-Schwachstellen genutzt werden. In den Grundlagen erfahren Sie mehr zu den Motiven der Hacker und zu potenziellen Gefahren auf der Datenautobahn. Die Workshops zu Themen wie Data Mining zeigen, was mit einfachsten Mitteln online über einzelne Personen herausgefunden werden kann. Darüber hinaus enthält die Vollversion eine ausgewählte Sammlung wirkungsvoller Hacker-Tools.

So machen Sie die Steganos Hacker Tools 7 einsatzbereit

Steganos Hacker Tools 7 läuft unter Windows 98/ME, 2000 und XP. Über die Oberfläche der Heft-CD entpacken Sie die ZIP-Datei zunächst in einen von Ihnen festgelegten Ordner. Doppelklicken Sie anschließend auf die Datei Index.HTM in diesem Ordner. Nun öffnet sich ein Browser-Fenster. In der linken Navigationsleiste navigieren Sie zwischen den Grundlagen, Themen, Tools und einem Glossar mit den wichtigsten Begriffen. Im Fenster rechts werden die jeweiligen Inhalte angezeigt.

McAfee-Sicherheitspaket: Alles drin für mehr Schutz

Das McAfee-Sicherheitspaket besteht aus drei Vollversionen, die Ihren Windows-PC optimal vor Online-Gefahren schützen.

Mit **McAfee Personal Firewall Plus 2006** in der Version 7.0 können Sie den ein- und ausgehenden Datenverkehr über eine eingängige Oberfläche kontrollieren und reglementieren. Die Software verhindert, dass Hacker auf Ihren PC zugreifen können, und schützt so Ihre persönlichen Daten, Fotos, Dokumente und Ihre Online-Kommunikation. Anhand von leicht lesbaren Activity Maps ermittelt das Tool den Ausgangspunkt eines potenziell feindlichen Angriffs.

McAfee Antispyware 2006 2.0 spürt unerwünschte Eindringlinge wie Spyware, Trojaner, Dialer und Cookies auf, bevor diese Ihre persönlichen Daten erfassen oder in Ihre Privatsphäre eintauchen und Ressourcen Ihres Rechners anzapfen können. Die Software alarmiert Sie bei der Entdeckung schädlicher Programme.

McAfee Spamkiller 2006 hält Ihren Posteingang frei von Werbemüll. Das Programm unterstützt außerdem das Filtern von Phishing-Mails, mit denen versucht wird, Ihre persönlichen Daten zu entwenden.

McAfee-Vollversionen installieren

Die drei Tools von McAfee laufen unter Windows 98/ME, 2000 und XP. Ein Assistent führt Sie durch die Installation. Bei Personal Firewall Plus sollten Sie abschließend die Verwendung des McAfee Security Centers anstelle der XP-Sicherheitszentrale bestätigen. Anschließend startet die Produktregistrierung. Stellen Sie eine Internet-Verbindung her, und tragen Sie Ihre persönlichen Daten in die vorgesehenen Felder ein. Dank der kostenlosen Online-Updates ist Ihr PC durchgängig für 12 Monate vor den neuesten Bedrohungen geschützt.

Kennwörter dechiffrieren mit der Passwort-Knack-Suite

Die Passwort-Knack-Suite bietet 15 kostenlose Decodierprogramme für verloren gegangene Kennwörter. Unter anderem lassen sich damit Passwörter aus Messenger-Programmen (MSN Messenger, Windows Messenger, Yahoo Messenger, Trillian, Miranda, Gaim), Mailprogrammen (Outlook/Outlook Express, Eudora, Thunderbird, Hotmail), DFÜ-, RAS-, VPN-Zugängen, Netzwerkverbindungen, PST-Postfachdateien, dem Internet Explorer einschließlich Version 7.0 und WEP- und



Geheime Tools auf der Heft-CD: Rechner durchsuchen, Passwörter knacken, PCs fernsteuern und WLAN-Spionage sind nur einige der Themen, für die wir Software bieten

WPA-Kennwörter aus Windows im Klartext anzeigen. Die Gratis-Tools stammen aus der Software-Schmiede Nirsoft (www.nirsoft.net) und verfügen teilweise über eine deutschsprachige Bedienoberfläche mit der Möglichkeit, die enttarnten Codes zu speichern oder in die Zwischenablage zu legen.

Wichtig: Die Programmdateien der Hacker-Tools befinden sich aus Sicherheitsgründen in einer verschlüsselten Datei. Um das Archiv entpacken zu können, müssen Sie das Passwort „pcwelt“ eingeben.

Achtung: Fehlalarm

Einige der Tools von der Heft-CD können eine Alarmmeldung Ihrer Virenabwehr-Software auslösen. Passwort-Knackprogramme beispielsweise werden von mancher Sicherheits-Software als unerwünscht bewertet, obwohl sich derartige Tools auch ganz legal zum Recovern vergessener Codes nutzen lassen. Konkrete Gefahr geht von den Programmen nur bei missbräuchlicher Verwendung aus. Bewahren Sie daher im Falle eines Alarms Ruhe, und lesen Sie die Bildschirmmeldung aufmerksam durch.

Haftungsausschluss: Die Tool-Sammlung auf Heft-CD dient ausschließlich Informationszwecken. Der Missbrauch der Utilities ist strafbar. Weder der Verlag noch die Hersteller der Tools haften für eventuell entstehende Schäden – das gilt auch für unberechtigten Zugriff auf EDV-Systeme.

So nutzen Sie die PC-WELT-CD

Wenn Sie die CD einlegen, erscheint ein Hinweisfenster. Falls nicht, starten Sie die Datei PCWSTART.EXE im Hauptverzeichnis der CD. Im Starter wählen Sie, ob Sie die CD mit dem PC-WELT-Browser oder mit Ihrem Standard-Browser betrachten möchten. Der PC-WELT-Browser ist die komfortabelste Methode – die Software lässt sich damit bequem installieren. Die Software lässt sich nach verschiedenen Kriterien sortieren. ☒

Heft-CD: Das sind die Highlights

Vollversion Steganos Hacker Tools 7

Damit finden Sie heraus, wie gut Ihr PC tatsächlich vor Attacken aller Art geschützt ist

Vollversion McAfee Sicherheitspaket

Für Rundum-Schutz sorgen McAfee Personal Firewall Plus 2006 7.0, McAfee Antispyware 2006 2.0 und McAfee Spamkiller 2006 7.0

Passwort-Knack-Suite

15 Gratis-Tools, die alles knacken: Mailprogramme, Messenger, WLAN, IE und mehr

Tools aus dem Giftschränk

Programme, die verboten gehören

QEMU-Puppy Linux 2

Mit Puppy Linux als virtuellem PC surfen Sie risikolos auf Problem-Websites

Newsgroups leersaugen

Mit speziellen Such- und Saug-Utilities zapfen Sie Newsgroups als schnelle Quelle für Foto-, Video- und Software-Downloads an

Die besten Rootkit-Finder

Enttarnen und beseitigen Sie ohne Ihr Wissen installierte Rootkits, bevor etwas passiert

Utilities zur Virenentfernung

Hijack This 2.00, Starter 5.6, The Cleaner 4.2



Raubkopier-Report

Die Musikindustrie jammert über die vielen Schwarzkopien, Film- und Software-Produzenten beklagen Milliardenverluste durch illegal kopierte DVDs und Programme – das Thema Raubkopie ist topaktuell.

Von **Simone Gissler**

Raubkopierte Software, Musik, Filme, Bücher und Zeitschriften – das Internet hält alles bereit, was sich die Fange-meinde wünscht. Faustregel: Was digital vorliegt oder sich digitalisieren lässt, das wird auch hemmungslos kopiert. Eine vorhandene Kopiersperre, vor allem bei Video-DVDs und PC-Spielen an der Tagesordnung, ist dabei kein längst kein Hindernis mehr. Auf der Suche nach der heißen Ware nutzen moderne Internet-Piraten Spezialsuchmaschinen, weichen auf Google China aus, wenn sie mit der deutschsprachigen Variante nicht weiterkommen, und recherchieren in Foren und Newsgroups.

Kopieren, was das Zeug hält

Die Business Software Alliance (BSA), ein Konsortium von Software-Firmen, bezifferte die weltweiten Verluste durch Raubkopien in der Vergangenheit auf rund 33 Milliarden US-Dollar jährlich, was ungefähr der Wirtschaftskraft Kroatiens entspricht. Diese Zahl stammt aus einer Studie des Institutes International Data Corporation (IDC, www.idc.com). IDC ermittelt durch Umfragen und Analysen die Anzahl von Computerprogrammen, die ein gewöhnlicher Rechner braucht – sowohl klassische Anwendungen als auch PC-Spiele. Diese Zahl rechnet IDC dann auf alle PCs weltweit um und vergleicht sie mit

der Anzahl der tatsächlich verkauften Programme. Weil nach dieser Theorie mehr Software benötigt als verkauft wird, gilt die Differenz als Raubkopien.

Diese Zahlen sind jedoch mit Vorsicht zu genießen, weil niemand mit Sicherheit festlegen kann, wie viel Software ein PC normalerweise braucht. Zudem kann keiner sagen, ob die Raubkopierer wirklich alle Programme kaufen würden, die sie kopieren. Geschäftsführer Holger Flöttmann der Software-Firma Ascaron: „Es ist unmöglich, konkrete Zahlen zu nennen. Aber es gilt als sichere Erkenntnis, dass auf jedes verkaufte Spiel mehrere Raubkopien kommen.“

pier-Report Kopieren & Tauschen



Überblick Software-Diebe	
Inhalt	Seite
Kopieren, was das Zeug hält	10
Raubkopien gab es immer	11
Kopiersperren bringen wenig	12
So gut wie keine Hemmungen	12
Das sind die Gelegenheitskopierer	13
Strafverfolger hangeln den Profis hinterher	13
Große Jagd und geringe Abschreckung	14
Ermittler wollen grenzüberschreitend arbeiten	14
Wege aus der Krise	15
Kästen	
Sind Raubkopierer Verbrecher?	12
Statusreport der GVV	13
„Wert der Musik geht verloren“	14
Datei-Integrität sicherstellen	15

Die Verlustzahlen sind also ein theoretischer Wert, den die Hersteller zur Veranschaulichung des Problems nutzen. Dieses Problem dreht sich nicht um Peanuts, denn die Entwicklung beispielsweise von Anwendungsprogrammen und hochwertigen PC-Spielen verschlingt große Summen. In Deutschland etwa kostet ein klassisches Adventure-Spiel rund 500.000 Euro, auf den internationalen Markt ausgelegte Projekte sind noch teurer – bis zu 8 Millionen Euro sind keine Seltenheit. Wenn sich ein Titel nicht gut verkauft, verzeichnet der Hersteller Verluste im sechsstelligen Bereich.

Raubkopien gab es von Anfang an

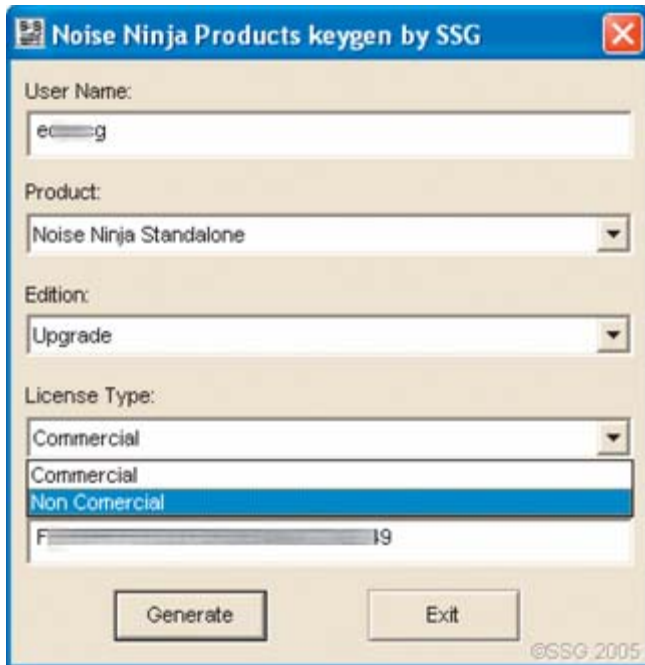
Dass Raubkopien ein nachhaltiges Problem sind, weiß die Software-Branche seit ihren Kindertagen. Für den populären C64 etwa war der Umlauf der Schwarzprogramme gigantisch, auf jedes verkaufte Exemplar großer Spiele kamen Dutzende Raubkopien. Auf Schulhöfen kursierten Pakete aus Disketten samt Handbüchern. Im Bereich Amiga und Atari ST ruinierten die Kopien Fir-

men, deren Programme populär waren – obwohl sie fast niemand gekauft hatte. In der PC-Ära versprachen neue Datenträger eine Lösung. Zwar erwies sich die CD kurzfristig als wirksames Mittel gegen Raubkopien, weil viele Programme zu groß für Disketten und die Brenner anfangs teuer waren. Doch zwei bis drei Jahre später sanken die Preise für Brenner und Rohlinge, nun ließen sich die Silberscheiben beliebig vervielfältigen. Beim Technologiesprung auf die DVD verschlief die Spielbranche das natürliche Kopierschutz-Potenzial, die Masse der Spiele auf DVD kam fast zeitgleich mit erschwinglichen Brennern und Rohlingen. Zudem ermöglichen seit der Jahrtausendwende Online-Tauschbörsen und schnelle DSL-Anschlüsse den

bequemen Austausch kopierter Software, Videos und Musik über das Internet. Dass eine Software häufig kopiert wird, heißt nicht zwangsläufig, dass sie sich deshalb schlecht verkauft. So quollen die Tauschbörsen über mit Kopien des Rollenspiels Oblivion, trotzdem stand es über Monate in den Top Ten der Verkaufsranglisten. Auch Windows, MS Office und die Grafik-



Alles drin: „All in One“-Pakete enthalten die geknackten Programme eines Herstellers – meist hübsch aufbereitet



Key-Generatoren: Cracker veröffentlichen Tools, die beliebig viele Seriennummern zu einer Software ausspucken

programme von Adobe gehen in großen Mengen über die Ladentheke, obwohl sie permanent in Newsgroups kursieren. Einer der Gründe ist, dass Raubkopierer im Vergleich zu ehrlichen Käufern die Minderheit sind. Ein anderer, dass manche Anwender die Tausch- und Download-Möglichkeiten im Internet nutzen, um sich einen kosten-

liegt. Bei Standard-Software setzen die Hersteller dagegen in der Regel auf Seriennummern. Im Trend ist auch eine Online-Aktivierung des Programms, bei der die Software Daten wie Seriennummer und die PC-Konfiguration zum Server des Programmherstellers übermittelt und dieser im Gegenzug die Software freischaltet (aktiviert).

losen Eindruck von bestimmten Programmen zu verschaffen – und dann bei Gefallen Geld dafür ausgeben.

Kopiersperren bringen wenig

Um Raubkopien zu verhindern, erfand die Industrie den Kopierschutz und Seriennummern. Die Kopiersperre bestand früher aus modifizierten Disketten. Heute sind Hardware-Dongles als Kopierschutz bei hochpreisigen Spezialprogrammen üblich, bei Spielen prüft ein Verschlüsselungsprogramm, ob bei Start der Original-Datenträger im Laufwerk

Diese Maßnahmen verhindern zwar illegale Duplikate durch Gelegenheitskopierer, ein perfekter Schutz existiert aber nicht. Nach einiger Zeit kursieren geknackte Versionen der kopiergeschützten Programme ohne Kopiersperre. Seriennummernabfragen lassen sich durch Key-Generatoren austricksen. Die Kopien kommen aus der Schattenwelt der Software-Cracker. Dahinter stecken engagierte Computer-Tüftler mit dem nötigen Know-how, die an Programmen basteln. Zudem verteidigen sie die Informationsfreiheit und setzen sich dafür ein, dass jede Form von Programmcode offen zugänglich sein sollte. Cracker gehen davon aus, dass jeder Code geknackt werden kann.

Das mündet in Wettbewerbe; wer einen Code zuerst knackt, erntet Ansehen in der Szene. Und am liebsten knacken die Cracker Kopierschutz-Algorithmen. Es gibt Wettläufe, welche Gruppe eine Software oder einen Film zuerst vom Schutz befreit – bevor das Produkt in den Handel kommt.

Das schutzlose Werk stellen die Cracker dann anderen Szene-Mitgliedern zum Download zur Verfügung, um zu beweisen, dass es auch funktioniert. Das nennt man „Release“, die Software-Cracker heißen deshalb auch „Release Groups“. Bis die Produkte dieser Gruppen ihren Weg in Tauschbörsen und Newsgroups finden, vergeht meist wenig Zeit.

So gut wie keine Hemmungen

Von den Produkten der Schattenwelt profitieren weltweit Millionen von Gelegenheitskopierern, die Software, Filme und Musikstücke in Online-Tauschbörsen oder aus dem Usenet herunterladen. In der Studie „Digitale Mentalität“ analysiert das Institut für Strategieentwicklung gemeinsam mit der Universität Witten/Herdecke diese große Zahl der Nutznießer.

Die Studie klärt zunächst den Ausdruck „Eigentum“: Als Eigentum gilt ein Gegenstand, den man kauft. Mit seinem Besitz darf man dann anstellen, was man will: Wer ein Auto kauft, hat das Recht, es zu fahren. Käufer einer Computersoftware erwerben aber nur eine DVD, nicht die Software selbst. Die Rechte am Programm bleiben beim Hersteller; der Käufer bezahlt nur für die Erlaubnis, das Spiel zu benutzen. Mit Software darf man also nicht anstellen, was man will: Es ist ausdrücklich verboten, Software-Kopien weiterzugeben.

Nachgefragt: Sind Raubkopierer Verbrecher?

Dazu Rechtsanwalt Stephan Mathé (s.mathe@rode-mathe.de), Partner der Hamburger Wirtschafts- und Medienkanzlei „Rode + Mathé Rechtsanwälte“, deren Schwerpunkt in der Beratung von Unternehmen der Spielebranche liegt:

Wer eine illegale Kopie herstellt, muss mit Konsequenzen rechnen. So kann er zivilrechtlich vom Hersteller auf Unterlassung und Schadensersatz verklagt werden – was teuer werden kann. Zudem kann der Raubkopierer vom Staat mit einer Geldstrafe oder einer Freiheitsstrafe von bis zu drei Jahren bestraft werden (bei gewerbsmäßigem Handel sogar mit einer Freiheitsstrafe von bis zu fünf Jahren). Damit handelt es sich um ein Vergehen, nicht aber um ein Verbrechen.

Denn als „Verbrechen“ gelten nur Delikte, deren Mindestfreiheitsstrafe ein Jahr beträgt. Der Raubkopierer ist also kein „Verbrecher“, wohl aber ein Straftäter.



Anti-Kopierkampagne: Ein Motiv der Business Software Alliance

Zudem wirkt Kopieren nicht wie Diebstahl, weil dabei nichts geklaut wird. Denn das Original bleibt erhalten. Zudem bestiehlt der Täter niemanden direkt. Wer ein Auto klaut, dem ist klar, dass sich dessen Besitzer über den Verlust ärgert. Wer Software kopiert, bedenkt aber in der Regel nicht, dass sie dem Hersteller gehört.

Hinzu kommt, dass viele Kopierer Urheberrechtsdelikte nicht nachvollziehen können, weil sie nie einem zum Opfer gefallen sind. Die wenigsten Raubkopierer haben je selbst eine Software programmiert, die raubkopiert wurde. Weil einzelne Kopierer auch noch in der Masse untergehen, besitzen sie oft kein Unrechtsbewusstsein; sie erkennen nicht, dass sie eine Straftat begehen.

Das sind die Typen von Gelegenheitskopierern

Unter den Gelegenheitskopierern unterscheidet die Studie vier Typen:

PC-Freaks: Sie kennen sich exzellent mit Computern sowie deren Technik aus und sammeln Raubkopien. Über das Internet besorgen sie alle Programme, die sie für nützlich halten. Obwohl PC-Freaks wissen, dass sie übermäßig viel kopieren, halten sie dies nicht für eine Straftat. PC-Freaks sind meist jünger als 25 Jahre.

Hobby-Anwender: Sie sind um die 29 Jahre alt und weniger gewieft im Umgang mit Technik, sammeln aber ähnlich viele Raubkopien an wie die PC-Freaks. Sie gestehen sich allerdings selbst nicht ein, dass sie viel Software kopieren, und halten dies auch nicht für Unrecht.

Pragmatiker: Sie sind durchschnittlich 34 Jahre alt, nutzen ihren Computer zur Arbeit



Strafverfolgung: Mit Szene-Experten wollen Polizei, Industrie und private Fahnder die Ermittlungen gegen die großen Fische vorantreiben (Quelle GVU)

und begeistern sich kaum für Technik. Sie kopieren nur die diejenigen Programme, die sie auch brauchen. Viele Pragmatiker wissen, dass Raubkopieren ein Vergehen ist.

PC-Profis: Die Angehörigen dieser Gruppe sind Nutzer um die 39 Jahre, die sich mit Technik auskennen. Sie kaufen Software aber legal – auch, weil sie Raubkopieren für eine Straftat halten.

Strafverfolger hangeln den Profis hinterher

Polizei und Staatsanwaltschaft sind verpflichtet, Verstöße gegen das Urheberrecht

zu verfolgen. Hauptkommissar Jürgen Müller arbeitet beim Kommissariat 241 des Münchner Polizeipräsidiums, das sich um die Verfolgung von Internet-Kriminalität kümmert. Dazu zählen auch illegale Kopien. „Ermittlungen in der Cracker-Szene sind langwierig“, berichtet Müller. „Das ist wie bei jeder Form organisierter Kriminalität. Die Cracker wissen, wie sie sich verstecken können.“ Allerdings beschäftigt auch die Polizei Szene-Experten. Das führt immer wieder zu Fahndungserfolgen, die teils auf Hinweisen amerikanischer Behörden beruhen. Trotzdem bleibt die Szene aktiv; das

Raubkopien: Statusreport der GVU

Die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU)

zieht für das Jahr 2006 hinsichtlich der Fahndung nach Erstverursachern an der Spitze der Verbreitungskette von Raubkopien eine positive Bilanz.

Insgesamt wurden durch die GVU nach eigenem Bekunden 1843 Verfahren eingeleitet (2549 im Jahr 2005) und 1475 initiierte Verfahren abgeschlossen (1500 im Jahr 2005). Im Rahmen von Strafverfahren wurden durch die Strafverfolgungsbehörden 552.731 Gegenstände und Datenträger beschlagnahmt, davon waren rund 70 Prozent mit Filmen bespielt.

Im Visier der Verfolgung standen vor allem Tätergruppen, die für die Veröffentlichung von urheberrechtlich geschützten Werken in die illegalen Verbreitungswege verantwortlich sind. Dazu gehören die Supplier, also Personen, die Originalprodukte oder Teile hiervon wie die Video- oder

Tonspur von Filmen beschaffen. Aber auch Release Groups, deren Mitglieder diese Teile zusammenfügen und die illegalen Kopien im Internet auf so bezeichneten Top-Sites bereitstellen.

Ebenfalls im Blickpunkt der Ermittler stand die Gruppe der „Faciliators“, die das illegal erstellte Material im Internet für die massenhafte Verbreitung zur Verfügung stellen oder hierfür die technischen Voraussetzungen schaffen, sowie Personen, die illegale Kopien gegen Bezahlung auf Datenträgern oder über das Internet vertreiben.

„Durch unsere zugespitzte Vorgehensweise haben wir im Jahr 2006 zwar insgesamt weniger Verfahren eingeleitet als im Vorjahr, diese hatten aber eine wesentlich höhere Wirkung in Bezug auf die Quellen des illegalen Vertriebsnetzes“ kommentiert Ronald Schäfer, Geschäftsführer der GVU.



Im europäischen Fahnungsvisier: Industrie und internationale Ermittlungsbehörden wollen Raubkopierer künftig grenzüberschreitend verfolgen

Cracker-Netzwerk ist weltweit zu sehr verzweigt und bisweilen perfekt versteckt. Meist ermittelt die Polizei gegen kommerzielle Raubkopierer, die etwa Software in einem Online-Auktionshaus feilbieten. Alle Privatkopierer kann der Gesetzgeber nicht verfolgen. „Dazu fehlen uns die Mittel“, erklärt Müller. Falls aber konkrete Hinweise eingehen, muss die Polizei ermitteln – etwa wenn ein Software-Hersteller Anzeige erstattet. Zudem bietet die Polizei Fortbildungen für Lehrer und Referate an Schulen

an – damit die Schüler lernen, dass Raubkopieren strafbar ist. Das sind jedoch in der Regel Einzelaktionen. „Die Industrie hat mehr Mittel, gegen Privatkopierer vorzugehen“, weiß Müller.

Große Jagd und geringe Abschreckung

In Deutschland arbeitet die Industrie mit der GVV zusammen, der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen. Das ist ein eingetragener Verein, der sich aus

den Beiträgen seiner Mitglieder finanziert, darunter Software-Hersteller. Mit diesen Geldern führt die GVV Ermittlungen in der Szene durch. „Die GVV setzt Informanten ein, die aus der Szene stammen und sich als Zuträger anbieten“, führt Geschäftsführer Ronald Schäfer aus. Wenn die GVV Raubkopierer aufspürt, stellt sie Strafantrag bei der zuständigen Staatsanwaltschaft, die dann ermittelt. Zu den Maßnahmen der Industrie zählt die Aktion „Raubkopierer sind Verbrecher“, die unter anderem auf Kinospots und Plakate setzt.

Die Aussage, Raubkopierer seien Verbrecher, ist jedoch rechtlich nicht korrekt, weswegen die Kampagne in die Kritik geriet. Als Ergebnis der Proteste werden einige Spots und Plakate der Abschreckungskampagne nicht mehr veröffentlicht.

Ermittler wollen grenzüberschreitend arbeiten

Die Anti-Piraterie-Organisationen Deutschlands, Österreichs und der Schweiz haben im April dieses Jahres eine intensivere Kooperation bei der Bekämpfung von Raubkopieren von Filmen und Computerspielen vereinbart. Die drei deutschsprachigen mit der Bekämpfung von Raubkopien befassten Organisationen GVV, VAP und SAFE wollen damit Raubkopierer besser verfolgen. So wollen die Gesellschaften zukünftig noch enger bei Ermittlungen und bei Verfahren mit grenzüberschreitendem Charakter zusammenarbeiten. Im Mittelpunkt dabei steht vor allem die Problematik der grenznahen Märkte und Shopping-Center, insbesondere

IFPI: „Wert der Musik geht verloren“

Gut 14,44 Milliarden Songs haben die deutschen PC-Besitzer derzeit auf ihren Rechnern gespeichert – im Vorjahr waren es noch weniger als 9 Milliarden. Das ist das Ergebnis der aktuellen Brennerstudie der Gesellschaft für Konsumforschung (GfK, www.gfk.de), die die IFPI (der Interessenverband der Phonoindustrie, www.ifpi.de) in Auftrag gegeben hat. Aufgrund der rasant wachsenden Zahl der gespeicherten Musiktitel befürchtet die IFPI einen Wertverlust der Musik: „Weil eine Festplatte immer das gleich wiegt – egal ob 100, 1000 oder 10.000 Musikdateien darauf gespeichert sind –, geht schleichend das Gefühl für den Wert von Musik verloren“, sagt Michael Haentjes, Vorsitzender der Deutschen Phonoverbände. Laut GfK ist der Anteil derjenigen Personen über 10 Jahre, die Musik auf ihrem Rechner speichern, von 31 im Jahr 2006 auf 37 Prozent in diesem Jahr gestiegen. Im Schnitt sind 614 Titel gespeichert. Zu den 14,44 Milliarden Songs kommen noch weitere 2 Milliarden Titel auf MP3-Playern

sowie 128 Millionen Songs auf MP3-fähigen Mobiltelefonen hinzu – damit kommt die IFPI auf insgesamt 16,6 Milliarden Musiktitel.

Insgesamt wurden laut Studie im vergangenen Jahr 465 Millionen Musiktitel legal und illegal aus dem Netz heruntergeladen. 80 Prozent der befragten Personen gab dabei an, Musik über Internet-Tauschbörsen herunterzuladen, rund 14 Prozent besorgten sich kostenlose Titel – etwa freie Songs von Künstlern über deren Homepage –, und 6 Prozent kauften bei kostenpflichtigen Download-Portalen gegen Bezahlung ein.

Intelligente Aufnahme-Software, zum Beispiel das Radio-Mitschnittprogramm Clipinc (www.clipinc.de), rückt ebenfalls ins Blickfeld des Industrieverbands. Solche Tools zeichnen automatisch Web-Radiosendungen auf Festplatte auf. So kommt rasch ein ganzes Archiv zusammen. Rund 2,7 Prozent der Bevölkerung nutzen derartige Software, am aktivsten ist dabei der Personenkreis zwischen 20 und 29 Jahren.

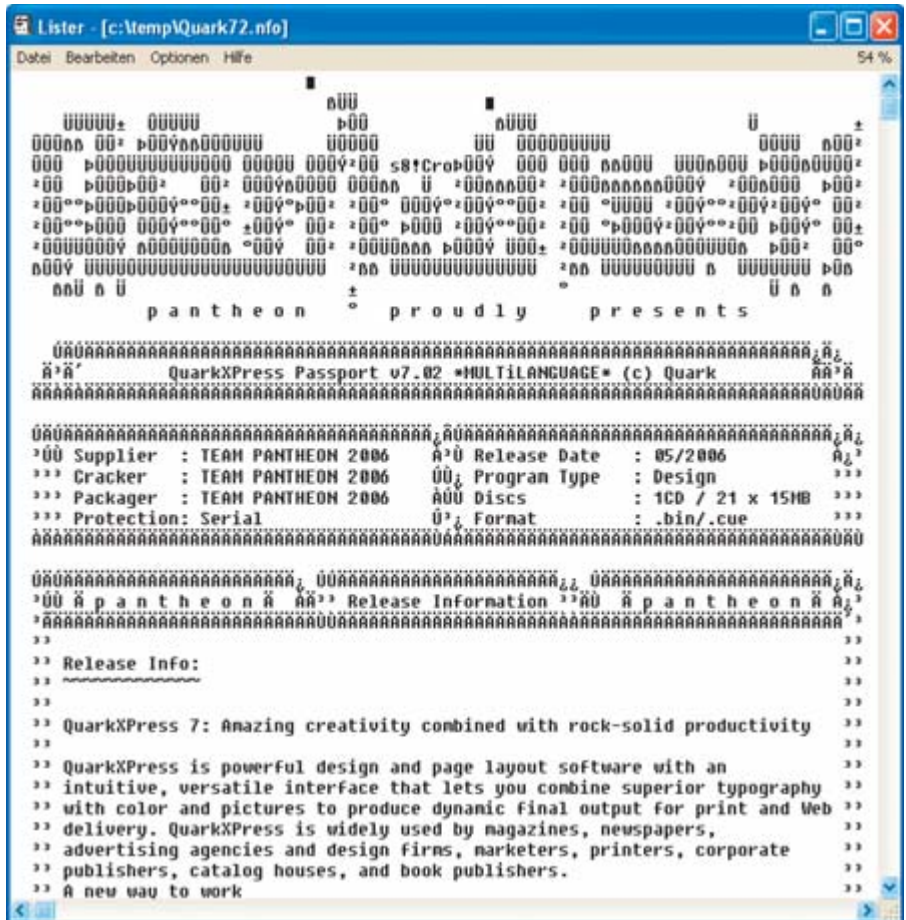
Tschechiens, auf denen illegale Kopien in großem Umfang verkauft werden und so auf die deutschsprachigen Märkte gelangen. Aber auch der umfassende Austausch von Erkenntnissen in Fällen der grenzüberschreitenden Serverpiraterie zur Verbreitung von Raubkopien über das Internet ist Gegenstand dieser Vereinbarung.

In einer gemeinsamen Erklärung stellten die Organisationen klar, dass sich der Fokus ihrer Tätigkeit auf die Ermittlung der Quellen und die Verfolgung von Personen richten wird, die an den Schlüsselstellen der illegalen Verbreitung tätig sind. Flächendeckende Massenverfahren gegen einzelne Personen wären zwar im Interesse der Rechteinhaber, sind allerdings nach wie vor nicht Teil ihrer Strategie zur Eindämmung von Urheberrechtsverletzungen. Zudem wurde eine weitergehende Abstimmung bei der Öffentlichkeitsarbeit und der gemeinsamen Aufklärung der Öffentlichkeit über den Umfang von Urheberrechtsverletzungen vereinbart.

Wege aus der Krise

Die Studie „Digitale Mentalität“ hält die von der Industrie betriebenen Abschreckungskampagnen für sinnlos. So setzen Unternehmen auf diese Weise „ihren Ruf und das Vertrauen ihrer Kunden aufs Spiel“ und sollten einen „taktvolleren und sensibleren Umgang mit dem Phänomen Raubkopieren“ pflegen. Hierzu gehöre auch, dass die Firmen ihren Kunden behutsam erklären, dass diese gekaufte Programme zwar benutzen dürfen, aber nicht besitzen. Um ihre These zu belegen, führt die Studie Lösungen für die vier Käufergruppen an.

PC-Freaks wollen, dass die Firmen sie ernst nehmen und auf ihre Kritik hören. Dann könnten sie sich entschließen, Software zu kaufen. Ein Kopierschutz-Wettrüsten bringt der Industrie nichts. Die Hobby-Anwender könnten vom Digital Rights Management (DRM) profitieren. DRM bedeutet, dass die Software per Internet freigeschaltet werden muss und nur dann Updates akzeptiert, wenn sie registriert ist. So bleiben die Hobby-Anwender auf dem neuesten Stand, ohne sich mit Technik auskennen zu müssen. In diese Richtung zielen etwa die DRM-Funktionen von Windows Vista. Versierte Anwender verstehen DRM jedoch als Hemmnis, Gängelung und sogar als Spionage, weil das bei Daten des eigenen Rechners an die Her-



NFO-Dateien: Sie enthalten Hinweise zu den auf FTP-Servern und in Newsgroups angebotenen Raubkopien, etwa Hersteller, Version und geknackter Schutz

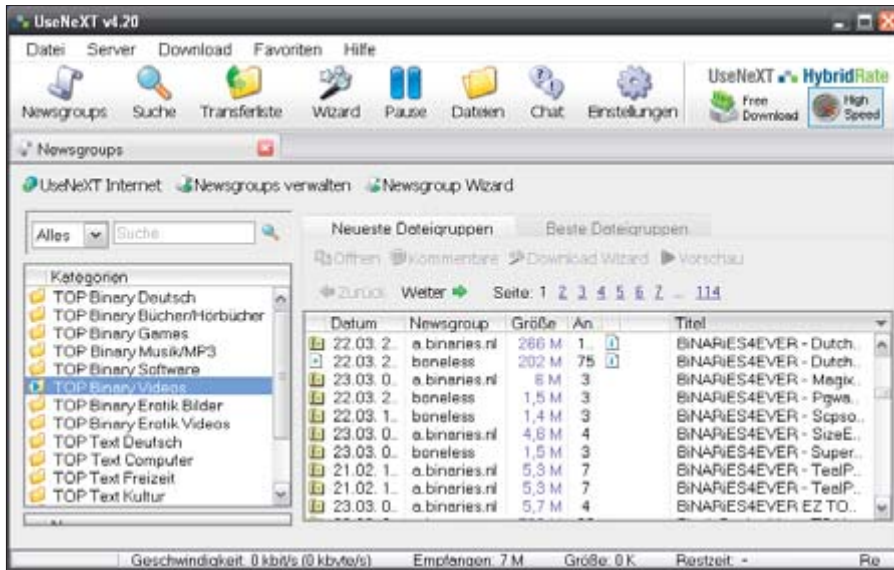
steller weitergeleitet werden. Deshalb warnt die Studie ausdrücklich, dass man den „Verbraucher nicht in Bezug auf seine Privatsphäre (...) verunsichern“ dürfe.

Pragmatiker sind meist nicht bereit, teure Software zu kaufen, könnten allerdings durch Lockangebote verführt werden. Darunter versteht die Studie Freeware, Demos oder funktional beschränkte Billig-Versi-

onen. So würden die Hersteller zwar weniger Geld verdienen, aber ihren Ruf aufpolieren, weil sie den Kundenwünschen nachkommen. PC-Profis können als Vorbild dienen, wenn man sie ehrlich behandelt. Dazu muss die Industrie auf ausgereifte Produkte setzen und auch mal Fehler zugeben. Wer Bugs verschweigt, muss sich nicht über schlechte Verkaufszahlen wundern.

Download-Check: Datei-Integrität prüfen

Mit absichtlich in Umlauf gebrachten Fakes – also defekten Dateien, die sich als echte Raubkopien ausgeben – hat die Industrie Tauschbörsen sabotiert. Die Erfolge waren zwar gering, doch partiell wurde Tauschwilligen damit das Saugen madig gemacht. Umso mehr verwundert es, dass Binär-Newsgroups bislang von Fake-Dateien weitgehend verschont wurden. Wer die dort angebotenen Datenpakete erst einmal vollständig heruntergeladen hat, braucht nur noch ein Entpackprogramm, um die Inhalte zu extrahieren. In vielen Download-Gruppen finden sich sogar MD5- und PAR-Prüfsummen. Damit lässt sich feststellen, ob die heruntergeladene Datei auch wirklich dem Original entspricht. MD5 und PAR sind Algorithmen, die aus einer beliebig langen Zeichenfolge – etwa einer Installationsdatei oder ein DVD-Image – eine eindeutige Checksumme berechnen. Parity-Dateien bieten sogar eine Reparaturmöglichkeit bei Defekten.



Drei Monate gratis saugen

Usenet-Newsgroups sind eine Fundgrube für digitale Inhalte aller Art. E-Books, Musik, Bilder, Videos: Es gibt nichts, das es hier nicht gibt. Bedienen Sie sich drei Monate lang – gratis.

Von Hermann Apfelböck

9 GB mit Highspeed, weitere hunderte von GB mit beschränkter Geschwindigkeit – so viel können Sie innerhalb von drei Monaten gratis aus dem Usenet laden, wenn Sie unsere Sonderaktion mit dem Provider Usenext wahrnehmen. Die dort gebotenen Binary Groups bieten reichlich (300 TB) Stoff – Bücher, Diskussionen, Tipps, Musik, Videos, Software ... Usenet eben ... Sie finden das Usenext-Anmeldeformular mit dem PC-WELT-Logo unter der Adresse www.pc-welt.usenext.de oder über den Link auf der PC-WELT-Seite www.pcwelt.de. Über unsere Aktion bekommen Sie einen wesentlich längeren Testzeitraum (drei Monate statt nur zwei Wochen) und ein größeres Highspeed-Volumen als beim normalen Usenext-Schnupperangebot (9 GB statt

3 GB). Das Download-Volumen im „Free Download“-Modus ist unbegrenzt – siehe Punkt 2. Für einen komfortablen Start erhalten PC-WELT-Leser gleich auf CD die notwendige Software – den leistungsfähigen Newsreader von Usenext. Er erfüllt alle Anforderungen, die an ein solches Tool gestellt werden. Wir beschreiben hier Schritt für Schritt, wie Sie an Ihren Gratis-Account kommen und diesen optimal nutzen. Wichtige allgemeine Infos zum Usenet finden Sie im Kasten ab Seite 17.

Haken? Gegenanzeigen? Keine. Sie sollten nur vor Ablauf der drei Monate per Mail oder – noch einfacher – über den Link im Mitgliederbereich von www.usenext.de kündigen (siehe Punkt 1). Es sei denn, Sie wollen mehr. Kann passieren ...

1. Anmeldung bei Usenext

Auf der Hauptseite www.usenext.de finden Sie nach einem Klick auf das PC-WELT-Logo das Anmeldeformular für unsere Sonderaktion. Nach Angabe einiger Daten und der Mailadresse werden Sie auf der Folgeseite auch nach einer Bankverbindung gefragt. Das dreimonatige Testabo kostet definitiv nichts. Sie können innerhalb dieses Zeitraums jederzeit kündigen. Sofern Sie das nicht tun, erhalten Sie nach Ablauf der drei Monate automatisch das Standard-Abo zu 7,95 Euro (10 GB Highspeed-Volumen pro Monat, 12 Monate Laufzeit). Wer seinen Usenext-Zugang tatsächlich über den Testzeitraum hinaus behalten möchte, sollte sich auf jeden Fall auch die anderen Varianten ansehen (kürzere Laufzeiten und/oder höheres Highspeed-Volumen).

Nach der Anmeldung erhalten Sie per Mail zweimal Login-Daten. Jene für die Website von Usenext benötigen Sie vor allem, um das Abo zu kündigen oder durch ein höherwertiges Bezahl-Abo zu ersetzen, die anderen für den Newsreader und damit den Zugang ins Usenet.

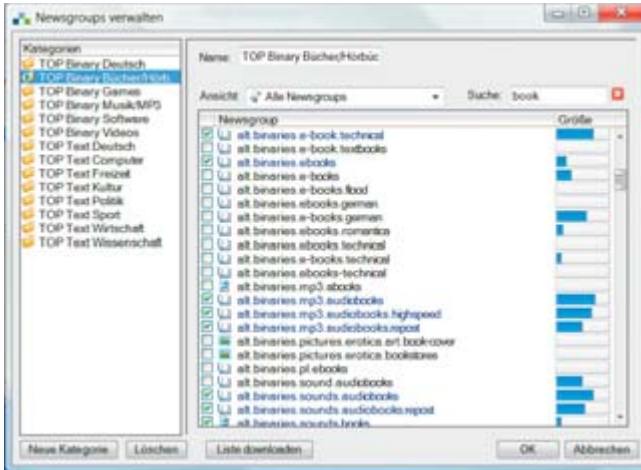
2. Installieren des Newsreaders

Mit Hilfe eines Newsreaders können Sie sich nicht nur durch die Diskussionen in den Newsgroups schmökern – Sie greifen damit auch auf die Downloads zu. Die Zugangs-Software für Usenext befindet sich in Version 4.20 auf CD. Sie können es sich natürlich auch kostenlos von der Usenext-Web-Seite holen. Die Installation setzt ein installiertes Microsoft .NET Framework 2.0 voraus (unter www.pcwelt.de/dn2, 22 MB).

Nach der Installation des Newsreaders tragen Sie darin bei den Account-Einstellungen den per Mail erhaltenen Benutzernamen („avi-<...>“) und das zugehörige Passwort ein. Nun können Sie loslegen.

Wichtig: Die Software zeigt rechts oben die Buttons „Free Download“ und „High Speed“. Im ersten Fall kommen die Downloads im Durchschnitt mit ungefähr 50 bis 100 KB/s, im zweiten mit dem Tempo Ihres DSL-Anschlusses. Das Highspeed-Volumen Ihres Test-Abos ist auf 9 GB beschränkt, der langsamere „Free Download“ (grüner Button) dagegen unbegrenzt.

Wenn Sie möglichst viel aus dem Usenet ziehen wollen, wählen Sie vor dem Download überwiegend den grünen Button. Ihr Highspeed-Volumen sollten Sie nämlich schon



Newsgruppen und kein Ende: Bevorzugte Gruppen lassen sich mühelos den voreingestellten Hauptkategorien hinzufügen

Überblick Usenet-Downloads

Inhalt	Seite
1. Anmeldung beim Provider Usenext	16
2. Installieren des Newsreaders	16
3. Navigation, Suche und Download	17
4. Weitere Newsgroups abonnieren	19
5. Externe Suche und NZB-Listen	19
Kästen	
Usenet: Das sollten Sie wissen	17

deshalb nicht vorzeitig erschöpfen, weil damit auch der „Free Download“ verfällt.

Achtung: Unter „Einstellungen, Verschiedenes“ finden Sie als vorletzten Punkt die Option „Falls eine Datei ... Highspeed Server verwenden“. In der Standardeinstellung ist diese Einstellung aktiviert. In diesem Fall wechselt der Newsreader häufig in den Highspeed-Modus, auch wenn Sie „Free Download“ gewählt haben. Wir empfehlen Ihnen daher dringend, die Option zu deaktivieren – auf diese Weise haben Sie eine wesentlich bessere Kontrolle über das kostbare Highspeed-Volumen.

3. Navigation, Dateisuche und Download

Der Newsreader startet standardmäßig mit der Newsgroups-Ansicht. In der linken Navigationsspalte sehen Sie die voreingestellten „Kategorien“, beginnend mit „TOP Binary Deutsch“. Beim Klick auf eine Kategorie sehen Sie unter „Newsgroups“ je zehn Gruppen. Wenn Sie eine der Newsgroups auswählen, sehen Sie die erste Seite mit Download-Angeboten. In großen Newsgroups erstrecken sich die Postings über zig Seiten.

Die bequemste Möglichkeit, ein einzelnes Posting zu laden, bietet der Usenext-News-

reader per Rechtsklick und „Download Wizard“. Der Programm-Wizard sammelt die RAR- und PAR-Dateifragmente eines Postings selbstständig und sorgt – sofern technisch möglich – für einen vollautomatischen Download. Bei Postings mit kleineren, vollständigen Dateien kann der Anwender nach Doppelklick auf den Eintrag auch manuell einzelne Dateien auswählen und ohne Wizard herunterladen. Wenn Sie etwas Bestimmtes suchen, ist es zu mühsam, sich durch die Gruppen und Seiten zu wühlen: Hier nutzen Sie am besten das Suchfeld oder den Button „Suche“. Im Usenext-Reader er-

Das Usenet: Was Sie darüber wissen sollten (I)

Das Usenet entwickelte sich lange vor dem Internet in den 80er-Jahren als reines Nachrichten- und Diskussionsnetz. Es ist über das Internet zugänglich, stellt aber ein eigenes, unabhängiges Netzwerk dar. Als in den frühen 90er-Jahren immer mehr Teilnehmer binäre Dateianhänge bereitstellten, wurde das Usenet zum Urahn aller Filesharing-Börsen. Wie groß das Datenvolumen im Usenet wirklich ist, weiß keiner genau – weit über 300 TB sind es allemal, da Provider wie Usenext aktuell ungefähr diese Datenmenge anbieten. Täglich kommen mit frischen Postings 500 GB bis 2 TB hinzu – auch hier schwanken die Schätzzahlen beträchtlich.

Diese riesigen Volumen und die Größe der einzelnen Downloads haben dazu geführt, dass normale Internet-Provider schon aus Kapazitätsgründen keinen Zugriff auf die Binary-Gruppen anbieten. Diese Aufgabe übernehmen spezielle, größtenteils kommerzielle Usenet-Provider. Die Angebote kosten rund 7 bis 20 Euro pro Monat (je nach Vertragslaufzeit und Download-Volumen). Die reinen Text-Newsgroups sind dagegen jedem Internet-Benutzer zugänglich, beispielsweise via Mailprogramm wie Outlook Express oder Google (Groups).

Aktualität und Verfallsdaten: Dass die Binary-Newsgroups bei den ständigen Datenzuflüssen irgendwann explodieren, verhindern die Usenet-Provider dadurch, dass sie die Postings jeweils nur wenige Tage be-

reitstellen – maximal drei bis vier Monate. Nicht nur aufgrund dieser begrenzten Bereitstellungsfristen sind Newsgroups und eben auch Binary Newsgroups ein aktueller, sich ständig ändernder Daten-Pool: Die Newsgroup-Postings reagieren umgehend auf tagesaktuelle Ereignisse – neue Zeitschriften, neu erschienene Bücher, CDs, Software. Info-Junkies, die nichts versäumen wollen, werfen daher fast täglich einen Blick mindestens in ihre favorisierten Gruppen.

Suche nach Inhalten: Gab es früher eine einfache, hierarchische Struktur mit wenigen Hauptgruppen, so ist der Überblick bei geschätzten 200.000 Newsgroups längst verloren gegangen. Die Mehrzahl ist schon vom Datenvolumen her unbedeutend oder aber eng regional oder thematisch spezialisiert. Die typischen Newsgroup-Giganten wie alt.binaries.nl oder alt.binaries.boneless bietet jeder Provider per Voreinstellung im Newsreader an. Im Übrigen bleibt es dem Usenet-Nutzer überlassen, weitere interessante Gruppen aufzuspüren und manuell zu abonnieren. Eine hierarchische Ordnung besteht zwar immer noch, die Gruppennamen sind aber nicht immer aussagekräftig. Newsreader, die eine thematische Suche über alle Gruppen beherrschen, helfen, interessante Angebote ausfindig zu machen. Weitere Unterstützung bieten Websites wie <http://alt.binaries.nl> oder www.newzsearch.com.

streckt sich diese Funktion auf Wunsch über alle Gruppen und lässt sich mit den Operatoren „AND“ und „OR“ präzisieren.

4. Weitere Newsgroups abonnieren

Die voreingestellten Kategorien und die dort enthaltenen je zehn Gruppen sind nur Startvorgaben, damit Sie sofort loslegen können. Es gibt zwei Wege, um weitere Newsgroups zu abonnieren: Der einfachere Dialog „Newsgroup Wizard“ zeigt die Top-Kategorien und bietet mit dem Button „bearbeiten“ die Möglichkeit, diesen Kategorien weitere Newsgroups hinzuzufügen. Dabei sind die angebotenen Gruppen bereits so vorsortiert, dass sie thematisch zur Kategorie passen.

Mit dem komplexeren Dialog „Newsgroups verwalten“ legen Sie mühelos eigene, neue Kategorien an oder erweitern eine bestehende Kategorie um zusätzliche Gruppen. In diesem Dialog sind Sie nicht auf thematische Vorgaben begrenzt: Über das Drop-down-Feld „Ansicht“ erreichen Sie „Alle Newsgroups“. Diese ausufernde Liste können Sie über das Feld „Suche“ thematisch filtern. Alle Newsgroups, die Sie dann per Klickbox aktivieren, landen zusätzlich in der aktuell markierten Kategorie.



Lohnt sich der Usenet-Zugang? Web-Dienste wie <http://alt.binaries.nl> zeigen rasch, was Newsgroups zu persönlichen Lieblingsthemen vorrätig haben

5. Externe Suche und NZB-Listen

Für die meisten Nutzer des Test-Abos werden die Möglichkeiten des Usenet-Readers vollkommen ausreichen. Wer garantiert nichts auslassen will oder sich ohne Newsreader über das Usenet-Angebot zu einigen Themen informieren will, kann auf <http://alt.binaries.nl> über alle Newsgroups hinweg suchen. Die Suche unterstützt den „AND“-Operator und einen Zeitrahmen zur Verfeinerung des Ergebnisses. Mit „select all“ und „create nzb“ entsteht eine Textdatei mit der Endung

NZB und allen notwendigen Informationen für den Newsreader. Diese Datei können Sie sofort oder später per Doppelklick beziehungsweise mit „Datei, NZB Datei importieren“ in die Usenet-Software laden und dann den Download starten. Die Möglichkeit, eine NZB-Datei zu erstellen, um einen recherchierten Download beispielsweise auf einen späteren Zeitpunkt zu verschieben, bietet auch der Newsreader von Usenet. Dazu markieren Sie alle relevanten Dateien und wählen anschließend im Kontextmenü „NZB Datei erstellen“.

Das Usenet: Was Sie darüber wissen sollten (II)

Anonymität und Werbefreiheit: Ein Vorteil des Usenets gegenüber Web-Tauschbörsen ist die größere Anonymität: Usenet-Provider garantieren, weder die IP-Adressen noch die Inhalte zu protokollieren, die ihre Nutzer downloaden. Lediglich die Datenmenge wird wegen des Volumentarifs protokolliert. Usenet-Nutzer, die nur downloaden und nicht selbst posten, dürfen sich daher weitgehend anonym fühlen. Werbung ist im Usenet generell verboten. Die Usenet-Provider betonen zu Recht, dass der Anwender von Pop-ups, Bannern und Dialern verschont bleibt.

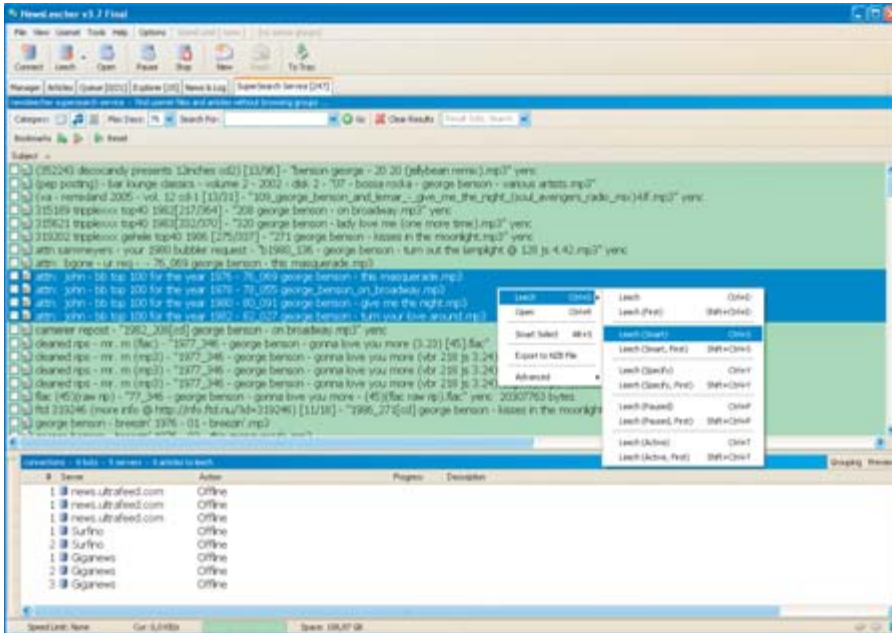
Verschwiegen wird hingegen, dass natürlich auch zunehmend mehr kommerzielle Dienste in Binary-Gruppen posten und die betreffenden Downloads erst durch eine Lizenz dieses Anbieters zu nutzen sind. Für Anwender, die darauf nicht eingehen wollen, sind diese Downloads dann natürlich wertlos.

Gesplittete Dateien und Newsreader: Binary-Newsserver akzeptieren nur Dateigrößen von 15 bis 50, selten 100 MB. Das zwingt die aktiven Usenet-Teilnehmer, große Postings entsprechend zu splitten. Technisch weniger versierte Download-Konsumenten sind mit dem Datensalat von NFOs (Info), RARs (Winrar-Archiv) und PARs (Paritätsdateien) oft überfordert. Hinzu kommen noch NZB-Dateien (Newzbin-Dateien), die die komplette Download-Liste für ein Archiv enthalten. In der Praxis reduzieren

sich aber die technischen Hürden durch einen guten Newsreader auf ein Minimum: Er kombiniert die in RAR- und PAR-Dateien enthaltenen Daten automatisch zu einem kompletten Download und importiert auch NZB-Dateien. Kleinere Angebote wie Texte, Bilder oder Audiodateien liegen hingegen unzerstückelt vor und lassen sich ohne Umweg mit einem Standard-Newsreader komplett laden.

Schrott, Viren und Illegales: Mit dem Usenet hat vor mehr als 15 Jahren etwas begonnen, was sich heute hochaktuell „Web 2.0“ nennt – zumindest in diesem Aspekt: Die Inhalte kommen von den Teilnehmern und werden nur in moderierten Gruppen mit unterschiedlicher Schärfe zensiert (gelöscht), in unmoderierten gar nicht. Folglich stehen hier technische und wissenschaftliche Inhalte neben pornografischen, seriöse neben illegalen. Usenet-Konsumenten müssen daher mitunter mit irreführenden Bezeichnungen, mit Datenmüll oder auch Viren und Trojanern in den geladenen Dateien rechnen.

Es empfiehlt sich, sofern vorhanden, vor dem Download die Kommentare zu lesen, ausführbare Downloads mit einem Scanner zu prüfen und sie in einem Konto mit eingeschränkten Benutzerrechten zu starten. Sie sollten sich dessen bewusst sein, dass Sie sich mit dem Download mancher Angebote strafbar machen könnten.



Sprudelnde Datenquelle

Ein Usenet-Provider und ein paar wenige Programme. Das reicht aus, um Tag für Tag mehrere Gigabyte Software, Videos und Sounds in Hochgeschwindigkeit zu laden.

Von **Peter-Uwe Lechner**

Klassische Peer-to-Peer-Netzwerke wie Edonkey und Gnutella sind out, Insider nutzen das riesige Angebot im Usenet (ursprünglich Unix User Network). Download und Uploads der Nutzer lassen sich nur schwer zurückverfolgen. Im Usenet sind Sie anonym unterwegs, einzig der News-Provider kennt die Identität der User. Trotz vieler Vorzüge führt das Usenet mit seinen zigtausend Newsgroups ein Schattendasein. Das liegt zum einen daran, dass die Handhabung nicht ganz einfach ist – zum anderen aber auch daran, dass man für den Zugriff auf die so genannten Binaries, also Software, Bilder, Videos und Sounds in der Regel bezahlen muss. Zwar ist bei fast bei jedem DSL-

Provider-Vertrag der Zugang zu Newsgroups enthalten. Meist sind die Gruppen, die Binaries enthalten, gesperrt oder leer. Ebenso verhält es sich mit öffentlichen Servern, die etwa Newzbot (www.newzbot.com) auflistet. Um uneingeschränkten Zugang zu Newsgroups zu bekommen, ist ein Abo bei einem Newsgroup-Provider Pflicht. Die Mitgliedschaft kostet je nach Download-Volumen um die 10 Euro monatlich.

1. Inhalte und Aktualität: Vorteil Usenet

Im Gegensatz zu den mitunter sehr langsamen P2P-Netzwerken hängt man beim Usenet direkt am Server des jeweiligen An-

bieters. Die Datenübertragung wird meist nur von der Bandbreite der Internet-Verbindung beschränkt. Per T-DSL 16000 lassen sich theoretisch über 180 GB auf Festplatte laden – ein Volumen, von dem Fileshare nur träumen können. Inhalte zum Laden gibt's reichlich: Die Newsgroups-Community ist zwar klein, die weltweiten Mitglieder sind aber so aktiv, dass pro Tag rund 3000 GB neue Daten auf den Servern landen.

2. Suchen und Finden im Usenet

Nach dem Abonnieren einer Gruppe lässt sich die interne Suche der Newsreader verwenden, um Inhalte anhand der Header zu finden. Der Header (Überschrift) ist mit dem Betreff einer Mail vergleichbar und sollte den Inhalt des Postings beschreiben. Oft werden aber unverständliche oder aussage-schwache Header gepostet, die wenig über die herunterzuladende Datei aussagen. Allerdings findet man bei vielen Files eine Datei mit der Extension NFO, die den Inhalt genauer beschreibt.

Doch welche der über 100.000 Gruppen enthält die gewünschten Dateien? Nicht immer sind Gruppennamen so eindeutig wie „alt.binaries.divx.german“. Zur Tarnung verbergen sich die wahren Schätze oftmals hinter unscheinbaren Gruppennamen ohne konkreten Bezug zum konkreten Inhalt. Mit einem einfachen Trick lassen sich gut gefüllte Gruppen aufspüren: Man lädt von Zeit zu Zeit die komplette Gruppenliste vom Newsserver und sortiert die Übersichtstabelle nach der Anzahl der Postings. Je mehr Beiträge sich in einer Binärgruppe befinden, um so höher ist die Wahrscheinlichkeit, dass es sich etwa um Videos handelt.

Darum geht's: Usenet-Basics

Bei einem Newsgroup-Provider wird ein kostenpflichtiger Zugang beantragt. Die Abrechnung erfolgt meist über Kreditkarte. Mit einer speziellen Software werden die gewünschten Newsgroups abonniert. Dateien (Binaries), die man herunterladen möchte, werden zum Download markiert. Nach der Übertragung wird mit dem Tool Quickpar überprüft, ob Dateien fehlerhaft sind und bei Bedarf eine Reparatur versucht. Danach werden die Dateiarhive entpackt.



Infoquelle fürs Usenet: Bei www.lords-of-usenet.info erfährt man, welche Postings aktuell sind (Punkt 2)

Die spezielle Websuche unter <http://binsearch.info> erlaubt das Finden nach Begriffen innerhalb der populärsten Gruppen, wobei die Betreiber der Seite schon eine entsprechende Vorauswahl getroffen haben. Auch möglich ist das Durchstöbern einer bestimmten Gruppe mit einem Klick auf den Link „browse newsgroups“. Eine integrierte Suchfunktion bieten die beiden Programme Newsleecher und Grabit gegen Aufpreis. Damit suchen Sie dann nach Dateien in einem schnellen Index, ein Abonnieren von Gruppen ist nicht notwendig. Nicht selten werden die Betreffzeilen von Postings in einer Binaries-Gruppe mit Absicht unkenntlich gemacht, stark abgekürzt oder verklausuliert. Fehlt dann auch noch die NFO-Datei, ist guter Rat teuer. Entweder man lädt alles auf Verdacht oder informiert sich über neue Posting bei speziell dafür

eingerichteten Webseiten. Bei NFO-News (www.nfo-news.com) kann man gezielt nach Filmen oder Programmen suchen und sich den Namen und die Gruppe des Postings anzeigen lassen. Die Webseite www.lords-of-usenet.info liefert entsprechende Infos nach einer kostenlosen Anmeldung.

3. Auf den richtigen Newsserver kommt's an

Bei der Auswahl des Newsservers sind drei Dinge zu beachten: Vollständigkeit der Beiträge, Vorhaltezeit (Retention) der Daten und Geschwindigkeit beim Download. Beim Verteilen der Postings durch die Server können aufgrund von Netzwerk-Störungen einzelne Beiträge verloren gehen. Bei Text-Postings fehlen dann einzelne Artikel oder ganze Threads. Auch bei Binärdaten können einzelne Teile fehlen. Viele Server garantieren eine Vollständigkeit von 99 Prozent – nachprüfen lässt sich diese Angaben allerdings nicht. Die zweite wichtige Eigenschaft eines Newsservers ist die so genannte Retention. Diese Vorhaltezeit gibt an, wie lange die Beiträge auf dem Server gespeichert werden. Dabei gilt: je länger, desto besser. Die Vorhaltezeit schwankt von Server zu Server und von Gruppe zu Gruppe. Bei Text-Postings kann sie über ein Jahr betragen,

Überblick Newsgroups

Inhalt	Seite
1. Inhalte und Aktualität: Vorteil Usenet	20
2. Suchen und Finden im Usenet	20
3. Auf den richtigen Newsserver kommt's an	21
Programme für Usenet-Downloads	
4. Binary Boy 1.96	23
5. Grabit 1.62	23
6. News File Grabber 4.5.0.2	23
7. Newsbin Pro 5.33	24
8. Newsleecher 3.9	24
9. Powergrab 2.6	25
Kasten	
Darum geht's: Usenet-Basics	20
Newsreader im Überblick	21
Binärdateien verwalten	22
News-Provider im Überblick	23
Binaries mit Grabit laden	24
Unzensuriert: Knallharte Inhalte zum Download	25

binäre Daten werden oft nur einige Tage oder Wochen gespeichert und danach gelöscht. Das obliegt dem News-Provider, einen Spitzenwert erreicht Giganews mit bis zu 120 Tagen. Welche Provider zu empfehlen sind, lesen Sie in der Tabelle „News-Provider im Überblick“ auf Seite 23.

Newsreader im Überblick

Programmname	Binary Boy 1.96 ●	Grabit 1.62 ●	News File Grabber 4.5.0.2 ●	Newsbin 5.3 ●	Newsleecher 3.9 ●	Powergrab 2.6 ●
Internet	www.binaryboy.com	www.shemes.com	www.rsbr.de	www.newsbin.com	www.newsleecher.com	www.jswnet.net
Preis für Grabit Search	18,95 Euro	kostenlos/20 Dollar lebenslange Updates	19,90 Dollar Supersearch für ein Jahresabonnement	35 Dollar inklusive	19,99 Dollar/29,99 Dollar	kostenlos
Sprache	Englisch	Englisch	Deutsch	Englisch	Englisch	Englisch
Windows	95/98/ME, 2000/XP	95/98/ME, 2000/XP	95/98/ME, 2000/XP	95/98/ME, 2000/XP	95/98/ME, 2000/XP	95/98/ME, 2000/XP
Mehrere Server	ja	ja	ja	ja	ja	nein
Parallel-Downloads	ja	ja	ja	ja	ja	ja
Anzeige von Binär-Postings	nein	ja	ja	ja	ja	ja
Download bestimmter Header	ja	ja	ja	ja	ja	nein
Neue Postings markieren	ja	ja	ja	ja	ja	nein
Newsgroup-Filter	ja	ja	ja	ja	ja	ja
Inhalte-Filter	ja	ja	ja	ja	ja	ja

Wer probeweise in das Usenet reinschnuppern möchte, kann dazu den 3-Monats-Zugang bei Usenext nutzen (siehe Seite 16). Alternativ bietet der US-Provider Giganews (www.giganews.com) für alle Tarife einen kostenlosen Zugang an, der auf drei Tage und 1 GB Download-Volumen beschränkt ist. Der Kunde muss allerdings seine Kreditkartendaten hinterlegen.

Programme für Usenet-Downloads

Um auf einen Newsserver zuzugreifen, benötigen Sie ein Newsreader-Tool, das die einzelnen Beiträge anzeigen kann. Es funktioniert im Grunde genommen wie ein Mail-

programm. Doch nicht jeder Newsreader unterstützt das Laden von Binärdateien. Programme wie Outlook Express, Xnews und Forté Agent wurden ursprünglich für das Lesen und Schreiben von Textmitteilungen entwickelt, nicht aber für Downloads. Daher ist das Laden von Dateien damit sehr umständlich. Daher sollten Sie zu Programmen greifen, die sich auf Up- und Downloads von Binaries spezialisiert haben und dazu eine Reihe nützlicher



Ohne Risiko testen: Wer bei Giganews 72 Stunden nach Vertragsabschluss kündigt, bezahlt nichts (Punkt 3)

Downloads: Binärdateien verwalten

In den Binary-Newsgroups werden große Dateien wie DVD-Rips oder Divx-Videos in der Regel im RAR-Format verbreitet. RAR zeichnet sich durch seine starke Komprimierungsraten aus und kann große Dateien vor dem Hochladen in mehrere kleinere Teile, so genannte Multi-Volumes, aufsplitten. Das ist deshalb wichtig, weil das Usenet nicht beliebig große Dateien unterstützt, sondern Dateien ab einer bestimmten Größe ablehnt. Mit dem RAR-Format kann man also eine sonst nicht über das Usenet transportierbare Datei in so kleine Stücke zerlegen, dass sie doch verschickt werden kann. Man muss jedoch alle Teilstücke eines Archivs haben, um die Datei wieder zu entpacken. Dazu verwenden Sie ein Packprogramm mit RAR-Unterstützung, etwa die Shareware Winrar (www.winrar.de, für Windows 95/98/ME, 2000/XP und Vista, 35 Euro) oder die Freeware 7-Zip (www.7zip.org, für Windows 95/98/ME, 2000/XP und Vista), beide auf CD.

Ärgerlich ist es, wenn Sie ein scheinbar vollständiges und mehrere hundert MB großes Binary auf Festplatte geladen haben und eine einzige Datei aus dem Multi-Volume-Archiv fehlt oder beschädigt ist. Das Entpacken wird dann mit einer Fehlermeldung abgebrochen.

Parity-Dateien

Besonders pfiffig ist daher die redundante Speicherung mit Hilfe von Parity-Dateien. Diese werden für einen binären Datensatz hergestellt. Für einen Satz von beispielsweise 50 RAR-Dateien erzeugt der Anwender zehn Parity-Dateien gleicher Größe. Wenn eine RAR-Datei beschädigt sein sollte oder gar ganz fehlt, kann sie aus den Parity-Dateien wiederhergestellt werden. Das beste Tool für PAR2 ist die Freeware Quickpar (www.quickpar.org.uk, für Windows 95/98/Me, 2000/XP und Vista), auf CD. Nachdem alle Dateien eines Postings auf Festplatte geladen sind, wechselt man im Windows-Explorer in das Download-Verzeichnis, das im Newsreader angegeben ist, und klickt die PAR-Datei doppelt an, um diese in Quickpar zu öffnen. Ist das Multi-Volume-RAR-Archiv vollständig, wird nach der Analyse die Meldung „Reparatur nicht erforderlich“ in einem grünen Balken angezeigt. Fehlen etwa von einem Download zwei Dateien oder sind zwei Archive beschädigt und ausreichend Wiederherstellungsinformationen in den PAR-Dateien vorhanden, erscheint die Meldung wie

„Bereit zur Wiederherstellung mit 80/196 Wiederherstellungsblöcken“. Ein Klick auf die Schaltfläche „Wiederherstellen“ genügt, um den Vorgang zu starten. Anschließend hat man einen kompletten Archivsatz, der sich etwa mit Winrar extrahieren lässt.

Repair'n'Extract

Newsleecher 3.9 bringt mit „Repair'n'Extract“ eine neue Funktion mit, die das Laden und Entpacken von Binaries geradezu revolutioniert. Nachdem alle Dateien eines Binary-Postings markiert und per Hotkey <Strg>-<D> in die Download-Warteschlange (Queue) übernommen sind, wird Repair'n'Extract im Hintergrund aktiv. Automatisch werden alle PAR-Dateien des Postings auf „Pause“ gesetzt. Jede geladene RAR-Datei wird automatisch auf Vollständigkeit überprüft. Sind alle Teile eines Postings vorhanden, entpackt Newsleecher das Archiv auf Festplatte. Sind Dateien des Postings beschädigt oder fehlen, lädt Newsleecher die PAR-Dateien automatisch nach und versucht eine Reparatur. Gelingt diese, wird das Archiv entpackt. Danach werden alle RAR- und PAR-Dateien automatisch auf Festplatte gelöscht.



Reparatur möglich: Defekte Multi-Volume-Archive lassen sich anhand von PAR-Dateien und Quickpar wiederherstellen

Funktionen bieten. Dazu zählen etwa das Laden von mehreren Servern gleichzeitig, parallele Verbindungen, Zeitplaner sowie Suchfunktionen.

4. Binary Boy 1.96

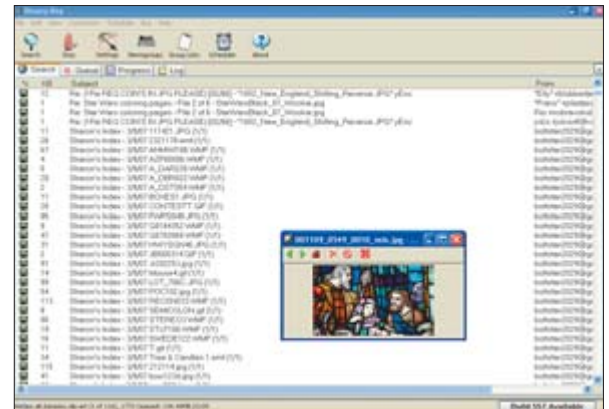
Die englischsprachige Shareware Binary Boy sucht in zuvor abonnierten Newsgroups nach Binärdateien, decodiert diese und speichert sie anschließend lokal auf Festplatte. Über die komplexen Such- und Filterfunktionen können bestimmte Stichwörter angegeben sowie Verknüpfungen über AND, OR und NOT Regeln definiert werden. Angelegte Filter lassen sich speichern und bei jeder neuen Verbindung anwenden. Die gewünschten Dateien können Sie mit Hilfe eines Planers auch zu festgelegten Zeiten laden. Sind auf dem Server nicht alle Datei-Bestandteile vorhanden, kann die Dr.-Binary-Funktion die Codierung in den meisten Fällen erfolgreich durchführen. Das Programm unterstützt nur einen News-Server, doch dafür können Sie Newsgroup-Listen erstellen und das Interessengebiet schon vor der eigentlichen Suche eingrenzen. Einzigartiges Extra: Wenn ein Posting unvollständig ist oder vom Newsserver gelöscht wurde, wird eine Verbindung zum Binary-Boy-Filesharing-Netzwerk aufgenommen und geprüft, ob ein anderer Nutzer den Artikel besitzt.

5. Grabit 1.62

Die englischsprachige Free-ware Grabit ist auf das Laden großer Mengen von Musikdateien, Bildern und Videos aus Newsgroups spezialisiert.

Die Basisfunktionen der Software sind kostenlos, die Nutzung der hilfreichen Newsserver-Suche kostet jedoch eine monatliche Gebühr ab 1,42 Euro. Bis zu acht gleichzeitige Verbindungen zu einem Server sorgen für eine hohe Auslastung der Bandbreite, falls der Usenet-Anbieter dies erlaubt. Nicht möglich ist es, ein Limit für das Download-Volumen oder eine maximale Übertragungsgeschwindigkeit vorzugeben und so nur einen Teil der Bandbreite für Downloads zu reservieren. Die Fehlersuche und -Korrektur sorgen dafür, dass die Daten ordnungsgemäß übertragen werden.

Sind Newsgroups in der Software abonniert, fordert die Aktualisierungsfunktion von Grabit automatisch eine Liste der seit dem letzten Besuch neu hinzugekommenen Dateien farblich markiert an. In den Programm-Einstellungen legt man dazu passend fest, wie viele Header die Software von einem



Verwirrend: Binaries lassen sich mit Binary Boy nur über eine Suche in zuvor abonnierten Gruppen finden (Punkt 4)

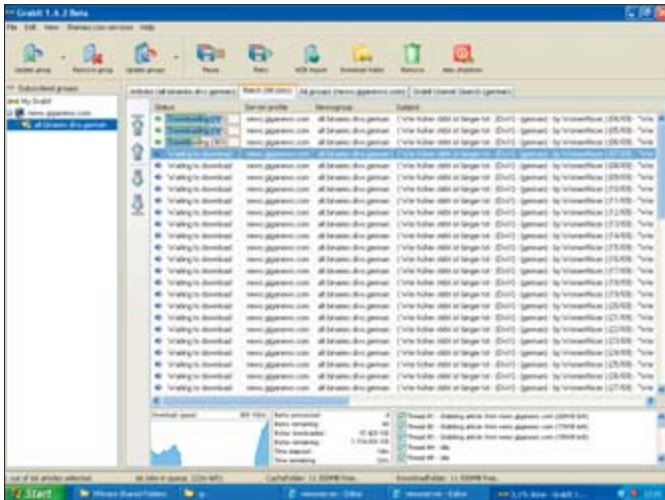
Server beziehen soll. Dank Unterstützung von NZB-Dateien lässt sich der Download von mehrteiligen Binärdateien einfach steuern. Auch ist Grabit in der Lage, nicht vollständig auf dem Server vorhandene Dateien anzuzeigen. Neben der integrierten Suche auf Newsservern durchsucht das Tool auch alle abonnierten Gruppen nach benutzerdefinierten Stichwörtern. Vielfältige Filterfunktionen helfen dabei, die Inhalte der einzelnen Newsgroups auszusortieren.

6. News File Grabber 4.5.0.2

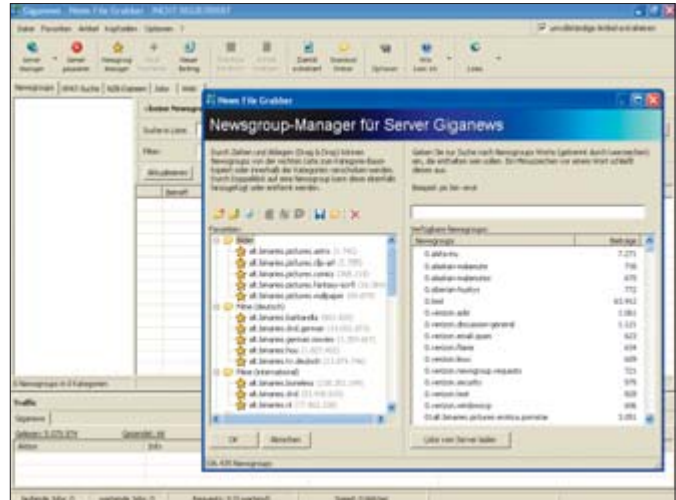
Auch die 20 Euro teure Software News File Grabber ist auf den Download von Binärdateien aus Newsgroups spezialisiert. Das Pro-

News-Provider im Überblick

Anbieter	Easynews.com	Giganews	Newsfeeds	Newshosting	Newssurfer	Premium-News	Surfino	Usenext
Internet (www.)	easynews.com	giganews.com	newsfeeds.com	newshosting.com	newssurfer.de	premium-news.com	surfino.com	usenext.de
News-Server	news.easynews.com	news.giganews.com	news.newsfeeds.com	news.newshosting.com	news.use-net-server.de	news.premium-news.net	news1.surfino.com	news.usenext.de
Tarif	9,98 Dollar für 20 GB oder 30 Tage (was zuerst erreicht wird)	25 Dollar/Mt. für Flatrate 12,95 Euro/Mt. für 25 GB 7,95 Euro/Mt. für 2 GB	4,95 Dollar/Mt. für 2 GB 9,95 Dollar/Mt. für 10 GB 19,95 Dollar/Mt. für 25 GB 24,95 Dollar/Mt. für 50 GB	10 Dollar/Mt. für 10 GB 14,95 Dollar/Mt. für Flatrate 19,95 Dollar/Mt. für Flatrate (NHXL-Tarif)	4,95 Euro/Mt. für 5 GB 6,90 Euro/Mt. für 10 GB 10,90 Euro/Mt. für 25 GB 16,90 Euro/Mt. für 50 GB 23,90 Euro/Mt. für 100 GB	12,78 Euro/Mt. für 60 GB 17,90 Euro/Mt. für 90 GB 30,17 Euro/Mt. für 150 GB	6,90 Euro/Mt. für 5 GB 9,90 Euro/Mt. für 10 GB 16,90 Euro/Mt. für 25 GB 23,90 Euro/Mt. für 50 GB 34,90 Euro/Mt. für 100 GB	7,95 Euro/Mt. für 10 GB 9,95 Euro/Mt. für 20 GB 19,95 Euro/Mt. für 20 GB
Zahlweise	Master, Visa	American Express, Discover, Master, Visa	JBC, Discover, Master, Visa	American Express, Discover, Master, Visa	Bankeinzug	Bankeinzug, Master, Visa	Bankeinzug	Bankeinzug
Anzahl Gruppen (Anbieterangabe)	Über 60.000	Über 110.000	Über 120.000	Über 120.000	Über 60.000	Über 150.000	Über 60.000	Über 60.000
Max. Verbindungen	4	10	10	8	8	8	8	8
Vorhaltezeit Binaries in Tagen	11	120	12	45/70 bei NHXL-Tarif	46	45	45	80



Übersichtlich: Die Freeware Grabit ist einfach zu bedienen und lädt Binaries in mehreren Parallel-Threads auf Festplatte (Punkt 5)



Schneller Einstieg: Ein Assistent begleitet bei News File Grabber beim Abonnieren der Newsgroups mit Binärdateien (Punkt 6)

gramm unterstützt mehrere Server mit gleichzeitigen Download-Threads und sichere Verbindungen (SSL). Verschiedene Filter erlauben etwa die Sortierung nach Größe, Datum und Poster. Newsgroups können zur besseren Übersicht in Kategorien gruppiert werden. Die Suchfunktionen sind auch auf ganze Kategorien anwendbar.

Auf Wunsch lassen sich alle Binaries einer Gruppe oder nur neue Inhalte in einem Rutsch laden und extrahieren. Dabei kombiniert das Programm auf Wunsch automatisch Multi-Part-Postings, um die Anlagen zu extrahieren. RAR-Dateien können übrigens direkt entpackt werden. Integriert ist auch die Unterstützung von NZB-Dateien.

7. Newsbin Pro 5.33

Der 35 US-Dollar teure Allrounder Newsbin Pro kann mit guter Ausstattung und vielen Extras punkten. Angefangen bei der Unterstützung mehrerer Newsserver über den inkrementellen Header-Download bis hin zur farbigen Markierung neuer Postings – die Grundausstattung der englischsprachigen Software ist tadellos. Weiterhin gibt es Auswahl- und Filtermöglichkeiten, mit denen man den Inhalt einer Newsgroup komplett übertragen kann oder gezielt einzelne Dateien lädt. Bei der Vorauswahl der gewünschten Dateien setzt die Software auf vom Anwender eingegebene Suchbegriffe und eine Dateigrößenauswahl. Ebenfalls hilfreich sind die Anzeige unvollständiger Binär-Postings sowie der eingebaute RAR-Packer, Unterstützung für NZB-Dateien und ein MP3-Organizer inklusive Tagger.

Um die vorhandene Bandbreite optimal auszunutzen, lädt das Programm Dateien in mehreren Instanzen und stellt bis zu 100 Verbindungen pro Server her. Falls nicht die ganze Bandbreite verwendet werden soll, kann eine maximale Download-Geschwindigkeit als Limit eingestellt werden. Wichtig für Newsgroup-Nutzer, deren Provider ein monatliches Download-Volumen vorgibt. In Newsbin Pro können Sie ein beliebiges Limit vorgeben. Weiteres Extra: Während der

Übertragung sehen Sie sich die geladenen Bilder in einer Vorschau an und halten einzelne Downloads auf Wunsch vorübergehend an. Lediglich eine gruppenübergreifende Suchfunktion ist nicht vorhanden.

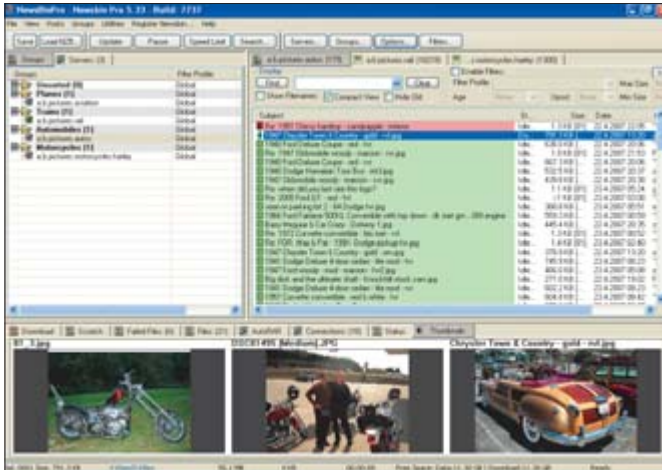
8. Newsleecher 3.9

Um die englischsprachige Software inklusive der Supersearch-Funktion für den Zeitraum von zwölf Monaten freizuschalten, sind rund 30 US-Dollar fällig. Ohne die Su-

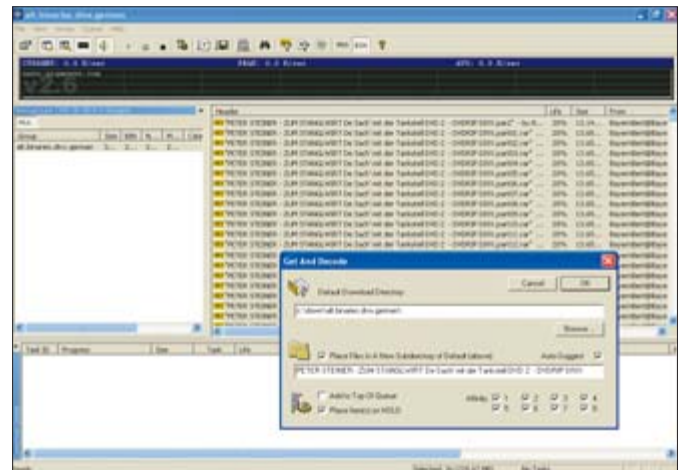
Binaries mit Grabit laden

Bei der Installation der Freeware (auf CD) übernimmt man alle Vorgaben und startet das Programm. Der Konfigurationsassistent verlangt die Eingabe der Zugangsdaten, die es vom News-Provider gibt. Nach Eingabe der Adresse des Newsservers setzt man das Häkchen vor „News (NNTP) server requires a username and password“, trägt im nächsten Dialog den Benutzernamen und das Passwort ein und klickt auf „Next“. Im folgenden Fenster ist das Häkchen vor „Retrieve group list...“ zu setzen, Grabit lädt dann automatisch die Gruppenliste vom Newsserver. Ein Klick auf „Finish“ schließt die Konfiguration ab. Die im Assistent getroffenen Einstellungen lassen sich über „Edit/Preferences“ jederzeit ändern. Nachdem Grabit die komplette Gruppenliste geladen hat, wählt man die gewünschte Gruppen aus. Hierzu reicht ein Klick auf den Button „Subscribe“, oder verwenden Sie die Tastenkombination <Strg>-<S>. Um die Liste auf Binaries zu beschränken, tippen Sie in das Feld „Only show groupnames...“ den Suchbegriff „alt.binaries“ ein. Die gewählten Gruppen zeigt das Tool im Fenster links unterhalb des Newsservers an.

Um eine Datei oder mehrere Dateien herunterzuladen, markieren Sie die gewünschte Gruppe in der Übersichtsliste und klicken auf den Button „Update group“. Das Aktualisieren kann je nach Internet-Verbindung und Anzahl der Post mehrere Minuten dauern. Ist der Vorgang beendet, werden die Inhalte der aktiven Gruppe in der rechten Fensterhälfte angezeigt. Nun wählt man einen Eintrag und klickt den „Grab selected“-Button oder nutzt die entsprechenden Befehle im Kontextmenü der rechten Maustaste. Grabit beginnt automatisch mit dem Download. Steht die Registerkarte „Batch“ im Vordergrund, lässt sich der Fortschritt der Übertragung verfolgen. Praktisch: Grabit legt für die Dateien jeder Newsgroup automatisch einen eigenen Unterordner an. Mit einem Klick auf „Download folder“ öffnet sich der Ordner mit den heruntergeladenen Dateien.



Spezialist für Bilder: Newsbin zeigt Bilder nach dem Transfer als Vorschau an und öffnet auf Doppelklick einen Viewer (Punkt 7)



Nicht mehr ganz auf der Höhe: Powergrab wirkt an vielen Stellen veraltet und ist teilweise umständlich zu bedienen (Punkt 9)

che bezahlt man 10 Dollar weniger, zu empfehlen ist das jedoch nicht. Denn gerade die schnelle Stichwortsuche in einem 140-Tage-Index mit ihren Filtern erleichtert das gezielte Auffinden von Inhalten, auf das Abonnieren und Aktualisieren von Gruppen kann dann sogar verzichtet werden. Die Software arbeitet mit beliebig vielen Newsservern zusammen, lädt Binärdateien und Textnachrichten herunter und hebt alle neuen Postings farbig hervor. Nicht vollständige Binaries werden rot als „incomplete“ gekennzeichnet. Hilfreich: Der Anwender kann genau vorgeben, wie viele neue Header das Tool vom Server laden soll. Auch in Sachen Extras schneidet das Programm mit Unterstützung von NZB-Dateien, Filterfunktionen und integrierter Vorschau gut ab. Newsleecher baut maximal 99 Verbindungen zu einem Newsserver auf und lädt Dateien auf Wunsch von mehreren Servern gleichzeitig herunter, was sich positiv auf die Übertragungsgeschwindigkeit auswirkt. Ein Download-Limit lässt sich ebenso einstellen wie die maximal erlaubte Übertragungsgeschwindigkeit. Mit dem neuen Feature „Repair’n’Extract“ werden die sonst für das Auspacken von Binaries notwendigen Tools Winrar und Quickpar überflüssig (siehe Kasten „Binärdateien verwalten“).

9. Powergrab 2.6

Die englischsprachige Freeware Powergrab fällt bei der Ausstattung gegenüber der Konkurrenz ab und besitzt lediglich grundlegende Funktionen wie die Unterstützung von speziell codierten Postings und das automatische Zusammensetzen von mehrtei-

ligen Dateien. Powergrab kann nichts mit NZB-Dateien anfangen und verbindet sich nur mit einem Newsserver. Zu diesem lassen sich dann maximal acht Verbindungen aufbauen. Die zur Verfügung gestellte Bandbreite kann pro Verbindung eingestellt werden, nicht aber ein Übertragungslimit.

Neue geladene Header markiert das Programm durch ein Icon, was die Übersicht deutlich erhöht. Schlecht sieht es bei den weiterführenden Funktionen aus. Die Suche beschränkt sich auf abonnierte Newsgroups, eine Vorschaufunktion – beispielsweise für Bilder – ist nicht integriert.

Unzensuriert: Knallharte Inhalte zum Download

In das Usenet kann jeder Dateien posten, der Zugang zu einem Server und den entsprechenden Gruppen besitzt. Eine Zensur findet – wenn überhaupt – nur beim News-Provider statt, der beispielsweise einzelne Gruppen sperrt. In den meisten alt.binaries-Gruppen finden sich auch illegale Inhalte, die Sie von Rechts wegen nicht herunterladen dürfen – auch wenn die Postings verführerisch klingen mögen. Sogar in scheinbar harmlosen Newsgroups wie alt.binaries.fonts oder alt.binaries.3d stoßen Sie möglicherweise auf urheberrechtlich geschütztes Material, das als solches aber nicht gekennzeichnet ist. Vor allem bei Schriften ist das ein Problem, denn wie soll man als Laie einen kostenlosen Font von einer einige hundert Euro teuren Profischrift unterscheiden?

Außerdem kursieren in Newsgroups angebliche Gratisprogramme, die es bei genauer Betrachtung gar nicht sind. Es handelt sich schlichtweg um Raubkopien, die ohne entsprechenden Hinweis bereitstehen. Die Installation solcher Programme kann für Sie böse juristische Folgen haben. Deshalb ist es wichtig, illegale Programme in Newsgroups rechtzeitig zu erkennen und dadurch nicht mit dem Gesetz in Konflikt zu kommen. Wer sich auf solche Downloads erst gar nicht einlassen will, kann anhand einiger Punkte mögliche Raubkopien rechtzeitig entlarven:

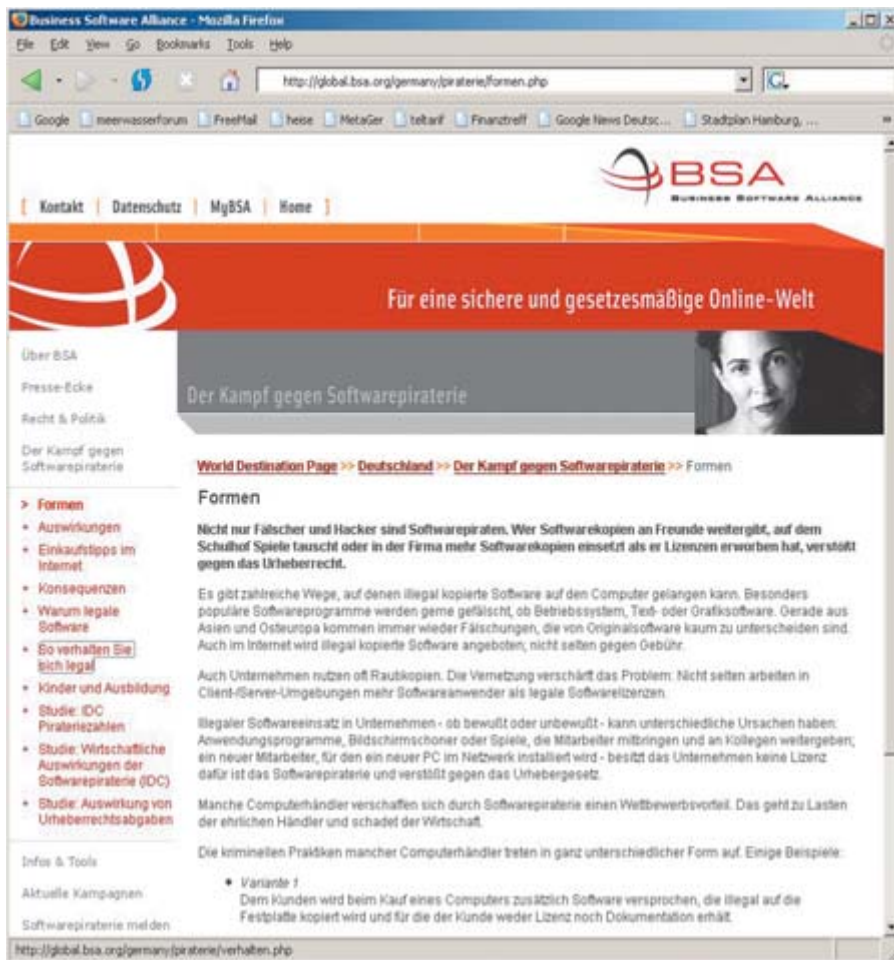
NFO-Dateien: Zusätzlich zum Programmpaket gibt es eine Datei mit der Extension NFO. Dabei handelt es sich um eine in der Raubkopierszene gebräuchliche Textdatei mit Hinweisen auf den Datei-Inhalt und Angaben zur Release Group (Gruppe, von der die Raubkopie ursprünglich stammt).

Zusammenstellungen: AIO-DVDs (All-in-one), Sammel-CDs – oder auch Compilation-CDs – mit Programmen verschiedener Hersteller sind in der Regel illegal.

Seriennummern: Datei-Archive mit dem Verweis auf beiliegende Seriennummern oder Keygens, also Tools, mit denen man sich eine gefälschte gültige Seriennummer errechnen lassen kann, sind in der Regel illegal.

Gecrackt: Vorsicht beim Hinweis „cracked“. Hier wird eine Testversion mit modifizierten EXE- und DLL-Dateien in eine lauffähige Testversion verwandelt. Auch solche Versionen sind illegal.

Gleich, ob Hollywood-Blockbuster oder Hardcore-Porno – Filme sind in der Regel Rips von Kauf-DVDs, Screener (im Kino abgefilmt) oder etwa auch illegale Kopien von Presse-DVDs.



Diese Kopien sind noch erlaubt

Das neue Urheberrechtsgesetz hat einiges verändert. Wir sagen Ihnen, was Sie noch kopieren dürfen, ohne in Konflikt mit dem Gesetz zu kommen.

Von **Rechtsanwalt Johannes Richard**

Seit September 2003 – also schon seit knapp vier Jahren – gibt es das neue Urheberrechtsgesetz. Aus rechtlicher Sicht ist die große Freiheit des nahezu unbeschränkten Kopierens von Daten seit diesem Zeitpunkt vorbei. Vorschriften legen genau fest, was noch kopiert werden darf. Verstöße stehen unter Strafe. Das Gesetz unter-

scheidet dabei zwischen Musik und Filmen sowie Computerprogrammen.

Privatkopie zulässig ...

Bei Musik und Filmen ist eine so genannte Privatkopie zulässig. Der Begriff „zulässig“ ist wichtig, da es – anders, als viele Anwender annehmen –, kein Recht auf Privatkopie

gibt. Privatkopien gibt es übrigens nur in Zusammenhang mit Musik und Filmen. Bei Software gibt es diesen Begriff nicht.

Die Privatkopie ist an mehrere Voraussetzungen geknüpft. Der Gesetzestext spricht hierbei in § 53 Urhebergesetz von „Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch“. Kopien sind daher grundsätzlich nur dann zulässig, wenn Sie als Eigentümer der CD diese entweder selbst nutzen – ein Beispiel ist die kopierte CD fürs Auto – oder aber andere Personen, die mit Ihnen, wie es im Rechtsdeutsch so schön heißt, „persönlich verbunden sind“. Hierbei handelt es sich um Familienangehörige und Freunde. Beliebig groß darf nach der Rechtsprechung der Freundeskreis jedoch nicht sein. Vor Jahren wurde von der Rechtsprechung die maximale Anzahl der Privatkopien aus wenig nachvollziehbaren Gründen auf sieben Stück festgelegt. Dies ist jedoch keine feste Größe, sondern nur ein Anhaltspunkt. Fest steht allerdings, dass eine Kopie für Arbeitskollegen oder Schulkameraden, mit denen keine engere Verbindung besteht, nicht zum privaten Gebrauch gehört. Eine Kopie für diesen Personenkreis ist keine zulässige Privatkopie.

... aber nur kostenlos

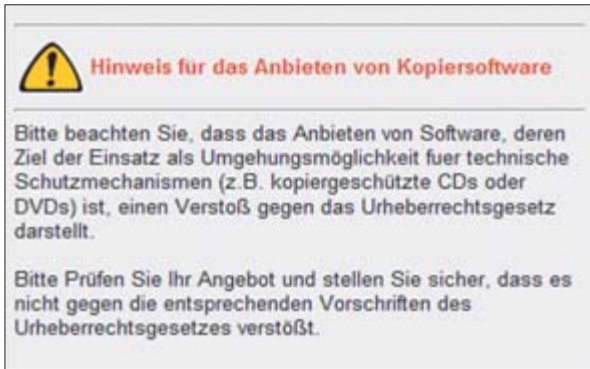
Die Kopie selbst, so lautet die Regel in § 53 Urhebergesetz, muss nicht durch den CD-Eigentümer selbst hergestellt werden. Sie kann auch durch eine andere Person erfolgen, sofern dies unentgeltlich geschieht. Die Frage der Unentgeltlichkeit hat es jedoch in sich. Eine Entgeltlichkeit, das heißt ein Gewinn des Kopierers, ist bereits dann gegeben, wenn dieser beispielsweise eine Kopie gegen Unkostenerstattung vornimmt, jedoch mehr verlangt, als der CD-Rohling tatsächlich gekostet hat.

Kopie aus Tauschbörsen

Die zulässige Privatkopie ist jedoch noch an eine weitere Voraussetzung geknüpft. Als

Unser Autor

Johannes Richard ist Rechtsanwalt in Rostock. Er ist Spezialist für das Internet-Recht und das Urheberrecht. Ausführliche Informationen finden Sie auf seiner Homepage unter www.internetrecht-rostock.de.



Vorsicht: Hinweise informieren Anbieter, die Software verkaufen, welche Kopierschutzmaßnahmen man umgeht

Vorlage für die Kopie darf keine, so das Gesetz, „offensichtlich rechtswidrig hergestellte Vorlage verwendet werden“. Diese Formulierung soll nach dem Willen des Gesetzgebers klarstellen, dass Kopien nur zulässig sind, soweit der Nutzer auf das Original oder eine zulässige Kopie einen berechtigten Zugriff hat. Rechtswidrig ist somit die Kopie einer Raubkopie.

Unter die rechtswidrig hergestellte Vorlage werden auch Vervielfältigungen aus Internet-Tauschbörsen eingeordnet. In diesem Zusammenhang ist darauf hinzuweisen, dass das Herunterladen von Kopien aus Internet-Tauschbörsen selbstverständlich nicht durch die Privatkopie gedeckt ist. Grund: Die Vervielfältigung erfolgt außerhalb eines eng begrenzten und bekannten Personenkreises.

Der Kopierschutz

Soweit die grundsätzlichen Voraussetzungen für eine Zulässigkeit der Privatkopie erfüllt sind, gibt es noch eine weitere Hürde: Das Original darf nicht mit einem Kopierschutz versehen sein. Im Juristendeutsch wird der Kopierschutz gemäß § 95 a ff. Urhebergesetz als „wirksame technische Maßnahme“ bezeichnet. Eine Definition des Kopierschutzes findet sich in § 95 a Abs. 2 Urhebergesetz. Es handelt sich somit um Technologien, Vorrichtungen und Bestandteile, die im normalen Betrieb dazu bestimmt sind, Handlungen zu verhindern oder einzuschränken, die vom Rechteinhaber nicht genehmigt sind. Beispielhaft nennt das Gesetz die Verschlüsselung, die Verzerrung, die sonstige Umwandlung oder einen Mechanismus zur Kontrolle der Vervielfältigung, die die Erreichung des Schutzziels sicherstellen sollen.

Dann ist der Kopierschutz „wirksam“

In diesem Zusammenhang stellt sich die Frage, wann technische Maßnahmen als wirksam angesehen werden können. Man könnte auf die Idee kommen, technische Maßnahmen als nicht mehr wirksam anzusehen, wenn diese geknackt sind. Die Frage, ob ein Kopierschutz überhaupt ein Kopierschutz im Sinne des Urhebergesetzes ist, wenn er mit ein-

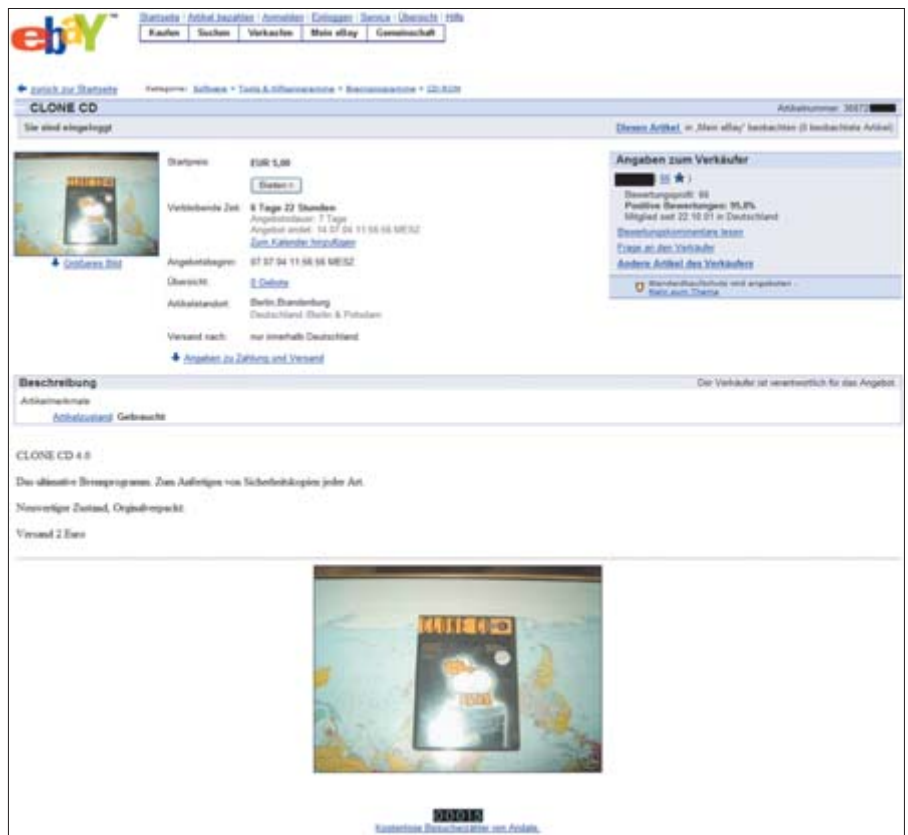
fachen Mitteln geknackt werden kann, hat der Gesetzgeber schon beantwortet. Bereits für den Gesetzesentwurf waren Kopierschutzmaßnahmen grundsätzlich auch dann wirksam, wenn ihre Umgehung möglich ist. Sonst würde es ein Wettrennen zwischen Urhebern und Hackern geben. Dies ist nicht im Sinne des Gesetzgebers. Man wird davon ausgehen können, dass nur eine völlig unfähige technische Maßnahme, die der Nutzer beispielsweise nicht einmal bemerkt, wenn er Kopien vornimmt, nicht wirksam ist.

Überblick Recht

Inhalt	Seite
Privatkopie zulässig ...	26
... aber nur kostenlos	26
Kopie aus Tauschbörsen	26
Der Kopierschutz	27
Dann ist Kopierschutz „wirksam“	27
Kopierschutz bei Audio-CDs	27
Grauzone	28
Das ist alles verboten	28
Knack-Software nicht bei Ebay verkaufen	28
Umgangener Kopierschutz – die Folgen	29
Kopien von Computerprogrammen	29
Kästen	
Mangelhafte Musik-CDs, mangelhafte Player	28
Recht: Zweiter Korb	29

Kopierschutz bei Audio-CDs

Im Einzelfall ist diese Frage nach der „Wirksamkeit“ eines Kopierschutzes jedoch schwierig zu beantworten. So gibt es CD-



Abmahnfähiges Ebay-Angebot: Abmahn-Anwälte freuen sich, wenn sie so ein Angebot sehen. Der Verkäufer erhält in der Regel in den nächsten Tagen Post



Kopierprogramm Clone CD nicht illegal? Zu diesem Ergebnis kam vor einiger Zeit ein Rechtsgutachten, das der Hersteller der verbotenen Software selbst in Auftrag gab

Brenner, die im Zusammenspiel mit normaler Brenn-Software – also ohne zusätzliche Spezial-Software – die Kopie von kopierschutzgeschützten Audio-CDs ermöglichen. Noch diffiziler wird die Frage, wenn man sich einmal anschaut, wie das Betriebssystem Linux auf viele Kopierschutzmaßnahmen für Audio-CDs reagiert – nämlich gar nicht. Es lassen sich mit Linux ohne Probleme Kopien von kopierschutzgeschützten CDs machen. Auch hier wird man jedoch annehmen können, dass grundsätzlich ein wirksamer Kopierschutz im Sinne des Gesetzes vorliegt. Zudem wird man zum Beispiel bei Audio-CDs grundsätzlich von einem Kopierschutz aus-

gehen müssen, wenn der CD-Hersteller, wozu er gesetzlich verpflichtet ist, auf der Verpackung auf das Bestehen eines Kopierschutzes hinweist.

Grauzone

Es gibt jedoch eine Grauzone, die auch bei kopierschutzgeschützten Musik-CDs eine legale Privatkopie zulässt. Es ist technisch problemlos möglich, eine kopierschutzgeschützte Musik-CD analog zu kopieren. Hierbei wird die Musik-CD normal im CD-Player abgespielt und digital über den Audio-Eingang des PCs aufgezeichnet. Eine ausdrückliche Umgehung der Kopierschutzmaßnahmen ist hier

nicht zu erkennen. Es muss jedoch darauf hingewiesen werden, dass die Legalität dieses Vorgehens noch nicht eindeutig geklärt und unter Juristen umstritten ist.

Übrigens sind viele Kopierschutzmaßnahmen schon seit längerem im Gebrauch und vielen Nutzern gar nicht bekannt. So sind alle Videorecorder und die meisten DVD-Player mit einem Kopierschutz namens Macrovision ausgestattet, der auch eine Analogkopie verhindert. Macrovision stellt ebenfalls eine wirksame technische Maßnahme dar und darf daher nicht umgangen werden.

Das ist alles verboten

Bezogen auf den Kopierschutz ist eine Menge verboten. Verboten sind die Herstellung, die Einfuhr, die Verbreitung, der Verkauf und die Vermietung von Gegenständen, mit denen der Kopierschutz umgangen werden kann. Dafür werben darf man ebenfalls nicht. Wer noch aus der guten alten Zeit ein entsprechendes Programm wie Clone-CD hat, mit dem man auch geschützte Audio-CD kopieren kann, darf dieses Programm zwar behalten, aber nicht weiter nutzen. Bereits der Besitz an sich ist jedoch verboten, wenn er gewerblichen Zwecken dient, das heißt, wenn zum Beispiel kopierte CDs mit Gewinn weiterverkauft werden. Dies ist oft schon bei den so genannten Schulhof-Kopierern der Fall, die eine ganze Schule mit den neuesten Musikstücken auf gebrannten CD versorgen.

Knack-Software nicht bei Ebay verkaufen

Diese Regelungen aus § 95 a Abs. 3 Urhebergesetz können bei Nichtbeachtung sehr schnell sehr teuer werden. Wer das hierzulande ehemals populäre Clone-CD oder ein ähnliches Programm noch hat, es aber nicht mehr benutzt, kommt leicht auf den Gedanken, die Software beispielsweise bei Ebay anzubieten. Von derartigen Verkäufen raten wir jedoch mit Nachdruck ab: Solche Programme dürfen nicht verkauft werden. Wer sie dennoch anbietet, riskiert eine Abmahnung von einer Reihe großer deutscher Musikfirmen, die Ebay regelmäßig nach solchen Angeboten durchforsten. Die Firmen verlangen in diesen Fällen eine Unterlassungserklärung. Zudem können Anwaltskosten von mehreren tausend Euro entstehen, da die Firmen mit dem Aufsetzen und

Mangelhafte CDs, mangelhafte Player

Gerade ältere CD-Player können kopierschutzgeschützte Musik-CDs zum Teil gar nicht abspielen. Der Grund: Der Kopierschutz bei Musik-CDs lässt sich nur dadurch realisieren, dass die technischen Standards der Audio-CD nicht eingehalten werden. Daher ist davon auszugehen, dass eine CD, die Sie wegen des Kopierschutzes auf Ihrem Player nicht abspielen können, mangelhaft ist und somit umgetauscht werden kann.

Daraus lässt sich jedoch nicht folgern, dass aktuelle CD-Player, die keine kopierschutzgeschützten Musik-CDs abspielen, mangelhaft sind. Das Amtsgericht Aachen hat beispielsweise mit Urteil vom 14. November 2003 (Aktenzeichen 84 C 210/03) entschieden, dass ein CD-Player nicht mangelhaft ist, wenn er keine kopierschutzgeschützten Musik-CDs abspielen kann. Eine solchen Player können Sie daher nicht umtauschen.

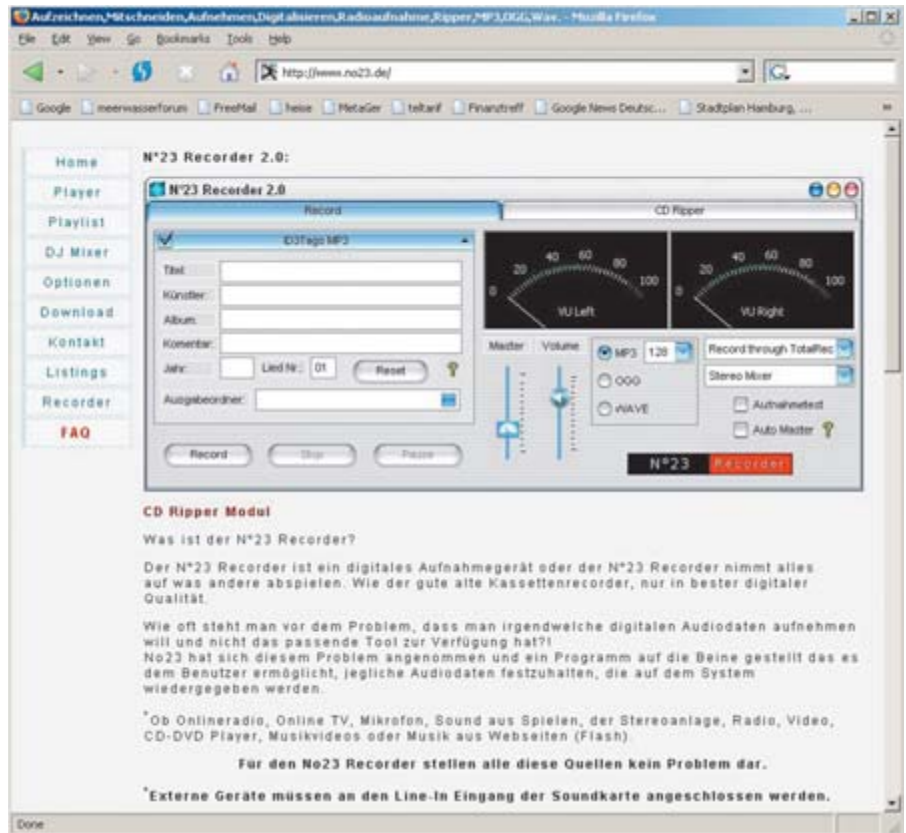
Versenden der Unterlassungserklärung in der Regel Anwaltskanzleien beauftragen. Auf die Frage, ob man in Kenntnis der Rechtslage das Programm bei Ebay angeboten hat, also absichtlich gegen das Gesetz verstoßen hat, kommt es dabei nicht an.

Umgangener Kopierschutz – die Folgen

Die Umgehung des Kopierschutzes zu privaten Zwecken ist nicht strafbar. Der Gesetzgeber wollte mit dieser Regelung eine Massenkriminalisierung vermeiden, da immer noch ein Großteil der Bevölkerung ohne Rücksicht auf Kopierschutzmaßnahmen nach eigenem Gutdünken kopiert. Voraussetzung für die Straffreiheit ist jedoch, dass es sich um eine Privatkopie handelt. Es bleibt dem Urheber allerdings unbenommen, in diesem Fall Schadensersatzansprüche geltend zu machen. Eine Frage, die in diesem Bereich wohl eher akademischer Natur ist. Die Firmen können schließlich nicht bei jeder Privatperson überwachen, was sie mit ihren gekauften CDs macht und wie viele Privatkopien sie angefertigt hat. Achtung: Unterschätzen Sie die strafrechtlichen Konsequenzen des Knackens eines Kopierschutzes nicht. Handelt es sich um keinen privaten Gebrauch, wie es bei Schulkopien schnell einmal der Fall ist, droht gemäß § 108 b Abs. 1 Urhebergesetz eine Freiheitsstrafe von bis zu einem Jahr oder Geldstrafe. Liegt ein gewerbliches Handeln



Riskant: So sieht eine Unterlassungserklärung für den erwähnten Fall aus



Analoge Aufnahme: Viele Audio-CD-Kopierschutzmaßnahmen lassen sich damit aushebeln. Unter Juristen ist die Zulässigkeit dieses Verfahrens jedoch umstritten

vor, das heißt, verdient der Täter Geld mit den Raubkopien, drohen gemäß § 108 b Abs. 3 Urhebergesetz bis zu drei Jahre Freiheitsstrafe oder Geldstrafe. Und die strafrechtliche Verfolgung ist nur eine Seite der Medaille. Der Kopierer muss sich nicht nur auf eine strafrechtliche Verurteilung, sondern auch auf erhebliche Schadensersatzforderungen der Musikindustrie einstellen. Der Verkauf eines Kopierprogramms oder eine Verbreitung über den Freundeskreis hinaus ist zudem gemäß § 111 a Urhebergesetz verboten und wird mit einem Bußgeld bestraft.

Kopien von Computerprogrammen

Alles in diesem Artikel bislang zum Thema Kopierschutz und Privatkopie. Gesagte gilt nicht für Computerprogramme. Die gute Nachricht: Die Frage nach der Umgehung eines Kopierschutzes und die sich ergebenden Rechtsfolgen gelten grundsätzlich nicht für Computerprogramme. Die schlechte Nachricht: Bei Computerprogrammen gibt es keine Privatkopie! Erlaubt ist gemäß § 69 d Urhebergesetz lediglich

eine Sicherheitskopie. Die Rechtslage ist hier nicht ganz geklärt, man wird jedoch annehmen können, dass zur Erstellung einer Sicherheitskopie auch ein Kopierschutz umgangen werden darf. Eine Sicherheitskopie ist jedoch nur eine einzige Kopie, die nicht weitergegeben werden darf. So freizügig wie mit Filmen oder Musikdateien dürfen Sie mit Computerprogrammen nicht umgehen. Daher ist der Download von geknackten Computerprogrammen immer illegal. ☒

Recht: Zweiter Korb

Seit April 2004 wird in Deutschland vom Bundesministerium der Justiz eine erneute Urheberrechtsreform („Zweiter Korb“) geplant, die die Rechte der Nutzer weiter einschränkt und die der Urheber und Rechteinhaber stärkt. Für Privatpersonen vor allem relevant ist der geplante Wegfall der Bagatelklausele, nach der nicht bestraft wird, wer urheberrechtlich geschützte Werke nur in geringer Zahl und ausschließlich zum eigenen privaten Gebrauch vervielfältigt.



Raubkopierer im Visier

Auch kleine Fische sind vor der Kriminalisierungskampagne der Industrie nicht sicher. Mit ausgefeilten Methoden stellen die Schnüffler Otto-Normal-Anwender nach.

Von **Klara Gehmach**

Vorbei die Zeiten, als Nutzer von Tauschbörsen sich noch in einem rechtsfreien Raum fühlen konnten. Seitdem die Musik-, Film- und Musikindustrie aktiv Jagd auf so genannte Raubkopierer macht, ist kaum jemand mehr davor gefeit, dass eines Tages die Polizei mit einem Durchsuchungsbefehl vor der Wohnungs- oder Bürotür steht. Polizei und Staatsanwaltschaft, vor allem aber eine gigantische Abmahnmaschinerie drohen prinzipiell nicht mehr nur den ganz großen Bösewichtern.

1. Die Industrie bangt um ihre millionenschweren Gewinne

Die deutsche Musikindustrie musste 2006 erneut einen Umsatzrückgang gegenüber dem Vorjahr hinnehmen. Die Industrie ist sich sicher: Ohne „Raubkopierer“ würde sie viel mehr Geld verdienen. Dennoch: In Deutschland wurden 2006 nach Angaben der deutschen Phonoverbände (www.ifpi.de) allein mit dem Verkauf von Musik-CDs fast 1,4 Milliarden Euro Umsatz erzielt, das sind 85 Prozent der gesamten Erlöse – für

186 Millionen Tonträger. Die Umsätze im Download-Geschäft stiegen um 40 Prozent auf rund 42 Millionen Euro. Das macht immerhin gut 25 Millionen heruntergeladene Titel und fast 2 Millionen verkaufte digitale Alben. Aber es ist auch klar, weshalb die Musiklabels besorgt sind: Laut der von den deutschen Phonoverbänden bei der Gesellschaft für Konsumforschung (GfK, www.gfk.de) in Auftrag gegebenen „Brennerstudie“ wurden 2006 766 Millionen CDs und DVDs gebrannt – und die allermeisten Privatbrenner kopieren Musik auf ihre Silberlinge.

2. „Raubkopierer sind auf alle Fälle Verbrecher!“

Eine der Strategien der Industrie ist eine beispiellose Kriminalisierungskampagne. Auch private Kopieraktivitäten sind den Musiklabels ein Dorn im Auge: „Trotz unserer Erfolge bei der Eindämmung der Internet-Piraterie blockieren die hohe Zahl illegaler Downloads und der weiter wachsende Anteil von Privatkopien nach wie vor den Turn-around“, so Peter Zombik, Geschäftsführer der deutschen Phonoverbände, Ende März 2007. Auf die Großkriminellen beschränken will man sich daher nicht.

Berühmt und berüchtigt ist die Kampagne der Zukunft Kino Marketing GmbH (www.hartabergerecht.de), die seit 2003 mit pauschalisierenden Slogans wie „Raubkopierer sind Verbrecher“ für Schlagzeilen sorgt. Tatsächlich ist der Begriff „Raubkopie“ sehr umstritten, da nach Meinung der Kritiker weder der Tatbestand des Raubes noch der des Diebstahls erfüllt ist – geschweige denn, dass ein Verbrechen vorliegt, das doch Gewalt voraussetzt. Sie sprechen daher lieber von „Schwarzkopien“.

Online-Aktivistinnen antworteten unlängst mit der Eröffnung eines Internet-Gefängnisses, wo man sich mit einer fiktiven Selbstanzeige für geringfügige Urheberrechtsverletzungen gleich selbst virtuell einsperren kann (www2.wir-haben-privat-kopiert.de) – ein gut gemachter Protest gegen diese Formen der Kriminalisierung.

3. Die Ziele und Maßnahmen der Industrie

Peter Zombik fordert als Vertreter der Musikindustrie, „jede Rechtsverletzung“ zu verfolgen – egal in welchem Umfang. Und der Vorstandschef der Phonoverbände, Michael Haentjes, kritisiert die von der Bun-

desregulierung geplante Deckelung der Abmahngebühren für Privatpersonen bei 50 Euro. Wer erwischt wird, soll bluten. Seit Jahresbeginn 2007 haben die deutschen Phonoverbände nach eigenen Angaben 15.000 Strafverfahren eingeleitet – eine Zahl, die die Interessenvertreter beliebig erhöhen können. Haentjes weiter: „Wir wollen niemanden kriminalisieren, aber die aktuelle Rechtslage zwingt uns dazu, den Weg der Strafverfahren zu gehen.“

Die deutschen Phonoverbände glauben fest daran, dass ihre Hexenjagd Erfolg verspricht. 2004 hat man dort mit der aktiven Verfolgung von Urheberrechtsverletzungen in Tauschbörsen begonnen, die Anzahl illegaler Downloads soll von rund 600 Millionen 2003 auf 374 Millionen im Jahr 2006 zurückgegangen sein. Man sieht sich in einer Vorreiterrolle, schließlich sei Musik vergleichsweise leicht zu kopieren und zu tauschen.

Der Computerspielerhersteller Zuxxez machte erstmals 2005 durch Massenanzeigen auf sich aufmerksam, er stellte auf einen Schlag 13.700 Anzeigen gegen unbekannt. In der Filmindustrie sind solche Massenanzeigen überwiegend noch umstritten – man will sich aber alle Optionen offen halten. Einigkeit kann man wohl ganz offensichtlich in einem Punkt voraussetzen: Schwarzkopierer sollen sich als Kriminelle fühlen, die erwischt werden können – nicht als Begeher eines Kavaliersdelikts.

4. Die Kooperationspartner: Internet-Detektive & Anwälte

Den Kampf gegen die Internet-Piraten ficht die Industrie nicht alleine aus. Man hat sich Partner gesucht, die mit ausgefeilter Technik und teilweise auch fiesen Tricks Schwarzkopierer aufspüren. Für sie und die kooperierenden Anwaltskanzleien ist dieses Geschäft beinahe so etwas wie eine Gelddruckmaschine. Diese Spezialisten sind zurzeit noch nicht besonders zahlreich, erzielen aber zuweilen spektakuläre Ergebnisse.

Die IFPI arbeitet mit der „Promedia Gesellschaft zum Schutze geistigen Eigentums“ (www.antipiracy.de) zusammen, die ihrerseits mit der Kanzlei Rasch kooperiert. Clemens Rasch ist auch Geschäftsführer von Promedia. Im Mai 2006 holte Promedia zum Schlag gegen Edonkey aus. Bundesweit fanden zeitgleich 130 Hausdurchsuchungen statt, rund 3500 Verdächtige waren das Ergebnis der Aktion.

Die Film- und Unterhaltungsindustrie baut auf die Zusammenarbeit mit der „Gesellschaft zur Verfolgung von Urheberrechtsverletzungen“ (GVU, www.gvu.de). Sie arbeitet mit dem weltweit agierenden Antipiracy-Netzwerk der Motion Picture Association of America (MPAA, www.mpa.org) zusammen. Die GVV konzentriert sich derzeit eher auf die großen Fische, widmet sich dazu aber auch der Überwachung von Flohmärkten und Internet-Auktionshäusern. Die GVV hat in den gut 20 Jahren ihres Bestehens mehr als 17.000 Strafverfahren angestrengt, momentan sind es rund 2500 Verfahren jährlich.

Viele Spielehersteller bedienen sich der in der Schweiz ansässigen Firma Logistep AG (www.logistepag.com), die durch eine quasi-automatische Generierung von Strafanzeigen eine fragwürdige Berühmtheit erlangt hat. Logistep arbeitet mit diversen Anwaltskanzleien zusammen; zu den Kunden der Firma gehören die Spielehersteller Zuxxez, CDV Software Entertainment AG und andere. Ebenfalls hier im Geschäft: KUV Rechtsanwälte (www.rae-su.de/antipiracy.html). Die Anwälte Karl, Urmann und Wagner gehen in Zusammenarbeit mit einem Software-Haus mit massenhaften Abmahnungen gegen Schwarzkopierer vor. Relativ neu in der Abmahnbranche ist die Firma Ipex (www.ipex-engineering.de), die Masche ist im Prinzip immer die gleiche.

Überblick Strafverfolgung

Inhalt	Seite
1. Millionenschweren Industriegewinne	30
2. „Raubkopierer sind Verbrecher!“	30
3. Maßnahmen der Industrie	30
4. Internet-Detektive & Anwälte	31
5. Schnüffeltechnologien der Ermittler	31
6. Folgen der Schnüffelaktionen	32
7. Das droht dem Anwender	32
8. Wo die Ermittler kapitulieren	33
9. So verhalten sich die Provider	33
10. Wasserzeichen statt DRM	33

5. Die Schnüffeltechnologien der Internet-Ermittler

Störmaßnahmen wie das Überschwemmen von Tauschbörsen mit fehlerhaften Dateien, wofür besonders die MPAA bekannt ist, waren in der Vergangenheit ein Weg, Dateitauern das Leben schwer zu machen. Teilweise nutzt die MPAA solche Fakefiles auch jetzt noch, aber nicht mehr zur Störung des Tauschbetriebs, sondern eher zum Sammeln von Filesharer-IP-Adressen. Heute geht es vor allem um Ermittlung, und das Hauptinstrument dazu ist immer öfter eine Spezial-Software – deren genaue Funktionsweise die Antipiraterie-Firmen aus gutem Grund streng geheim halten.



Kampagne der Zukunft Kino Marketing GmbH: Die berüchtigte Propaganda mit dem Slogan „Raubkopierer sind Verbrecher“ ist vielfach kritisiert worden (Punkt 2)



Protestbewegung: Online-Aktivisten haben ein virtuelles Gefängnis eröffnet (Punkt 2)

Ein Ermittler der Promedia soll pro Stunde rund sieben Fälle bearbeiten können. Er sichert dabei Downloads, die IP-Adresse des Tauschers, zusätzlich Screenshots. Angeblich nutzt Promedia für die Ermittlungen noch keine Multi-Clients, sondern Bearshare als Gnutella-Client. Nach eigenen Angaben erfolgen die Recherchen bislang meist manuell, in immer größerem Ausmaß jedoch auch automatisiert.

Logistep nutzt angeblich eine modifizierte Version des Clients Shareaza (www.shareaza.com) zum Aufspüren von Urheberrechtsverstößen in P2P-Netzen, die als „File Sharing Monitor“ (FSM) bekannt geworden ist. Nach Angaben der Firma übernimmt ein einziger Rechner alle Aufgaben, zugleich sei ein Knoten von drei Rechnern in der Lage, täglich mehr als zwei Millionen illegaler Down-/Uploader einzeln zu identifizieren. Mit diesem Monitoring überwacht Logistep kontinuierlich diverse P2P- und FTP-Protokolle, die etwa von Edonkey, Bittorrent, Gnutella, Emule, Limewire und vielen anderen Tauschbörsen verwendet werden.

Die Scan-Software von KUW wird im Internet mit dem Namen „Schwarze Witwe“ belegt, das Programm von Ipex nennt sich „IP-Ident“. Die Gvu hingegen setzt wie erwähnt auf gezielte Ermittlungen, um die großen Fische zu schnappen – der Einsatz einer Scan-Software ist hier nicht bekannt.

Die Technik dieser Tools funktioniert immer ähnlich: Die Scan-Software durchforstet die einschlägigen Tauschdienste nach urheberrechtlich geschützten Dateien. Und zwar nicht nach irgendwelchen, sondern nach genau denen, für die die Firma etwa vom Hersteller des jeweiligen Spiels einen Überwachungsauftrag erhalten hat. Die Identifizierung der gesuchten Dateien geschieht anhand einer digitalen Signatur. Wird das

Tool fündig, ermittelt es die IP-Adresse desjenigen, der die Datei anbietet – oder auch herunterlädt –, kurz alle verdächtigen Dateibewegungen. Im Falle des beliebten Emule wird häufig auch noch die bei der Installation des Clients generierte User-Hash (GUID) mitprotokolliert. Zudem erfasst die Software den Zeitpunkt des Tauschvorgangs.

Bei Logistep geht dann alles vollautomatisch weiter: Die Daten, die zuvor in eine Datenbank eingespeist worden sind, werden in Echtzeit an einen Rechtsanwalt übertragen, der vom Auftraggeber das Mandat hat, alle Rechtsverstöße zu verfolgen. Die Kanzlei stellt Strafantrag gegen unbekannt, die Staatsanwaltschaft muss also versuchen, denjenigen zu ermitteln, der den zur IP-Adresse gehörenden Anschluss hat. Der Anwalt beantragt dann sofort Akteneinsicht, um zivilrechtliche Forderungen gegen den Beschuldigten geltend machen zu können. Logistep informiert auch den Internet-Provider vollautomatisch per Mail und fordert ihn auf, die Verbindungsdaten des jeweiligen Anwenders länger als üblich zu speichern.

6. Die Folgen der großflächigen Schnüffelaktionen

Bei den noch mehr oder weniger gezielten Aktionen etwa der Promedia ist die Wahrscheinlichkeit, dass der Erwischte Besuch von der Polizei bekommt, relativ groß. Im Oktober 2006 beispielsweise führten die Er-

mittler in Paderborn nach entsprechenden Anzeigen durch Promedia mehrere Hausdurchsuchungen durch, unter anderem bei einer 15-Jährigen, die knapp 3000 Musiktitel in Tauschbörsen anbot. Doch die strafrechtlichen Folgen sind hier gering, viel schlimmer sind in solchen Fällen die zivilrechtlichen Folgen wegen der Urheberrechtsverletzungen.

Bei den Massenanzeigen etwa der Firma Logistep müssen die Betroffenen eine Unterlassungserklärung unterschreiben, die bei Zuwiderhandlungen mit einer Vertragsstrafe im fünfstelligen Bereich bewehrt ist. Ansonsten begnügt man sich hier häufig mit relativ geringfügigen Fixbeträgen von 200 bis 300 Euro als Schadensersatz für entgangene Lizenzeinnahmen, wovon ein Teil – und zwar der größere – Rechtsanwaltsgebühren sind.

Die Staatsanwaltschaften drohen inzwischen unter der Last der Massenanzeigen zusammenzubrechen. Die Folge ist, dass die Staatsanwaltschaften die Grenze, ab der Strafverfahren tatsächlich eingeleitet werden, massiv erhöhen.

7. Das droht dem erwischten Otto-Normal-Anwender

Im Januar 2007 beschloss die Bundesregierung den Gesetzentwurf zur Verbesserung des Schutzes geistigen Eigentums. Eine bedeutsame Änderung: Die anwaltlichen



Denunziation erwünscht: Die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen bittet auf ihrer Website auch um konkrete Hinweise von Anwendern (Punkt 5)

Kosten werden bei erstmaliger Abmahnung wegen Urheberrechtsverletzungen, die keinen kommerziellen Kontext haben, auf 50 Euro beschränkt.

Im Februar 2007 wurde ein Verfahren wegen Verletzung des Urheberrechts gegen einen 35-jährigen Familienvater gegen die Zahlung einer Geldbuße von 2300 Euro eingestellt. Aber die zivilrechtlichen Ansprüche, mit denen der Mann konfrontiert wird, dürften mehrere tausend Euro betragen. Die Haltung des Richters in diesem Fall ist symptomatisch: Da erhebliche Schadensersatzforderungen noch anstünden, sei die Einstellung des Verfahrens gerechtfertigt.

Dennoch: Werden Schwarzkopien mit kommerziellem Interesse hergestellt und vertrieben, handelt es sich um eine Straftat. Wer Kopien für den privaten Bereich herstellt, dem drohen zwar keine Straf- oder Ordnungswidrigkeitenverfahren, aber die Gefahr, sich zivilrechtlicher Ansprüche auszusetzen, besteht trotzdem. Wer bei den einschlägigen Tauschbörsen geschützte Dateien hoch- oder herunterlädt, muss mit einer Freiheitsstrafe bis zu drei Jahren rechnen – oder mit einer Geldstrafe. Macht man das professionell, kann sich die Freiheitsstrafe auf bis zu fünf Jahre erhöhen. Viele Verfahren im nicht-kommerziellen Bereich werden jedoch wegen Geringfügigkeit gegen eine Geldbuße eingestellt.

8. Wo die Ermittler weitestgehend kapitulieren

Es ist eine Frage des Aufwands, den die Ermittler betreiben können oder wollen, um Schwarzkopierer zu erwischen – möglich ist es fast immer. Es gibt jedoch zwei Bereiche, die nicht so sehr im Fokus der Internet-Detektive stehen: der Internet Relay Chat (IRC) und das Usenet.

Von den rund 60.000 Newsgroups bieten rund 100 Binärdateien an. Der Vorteil: Das Usenet gehört keinem, und es ist international. Weil der Anwender meist über einen Newsserver auf die Gruppen zugreift und nicht direkt, ist er weitestgehend anonym unterwegs – so lange der Newsserver-Anbieter keine Logfiles erstellt. Der Nachteil: Der Zugriff auf diese Binärgruppen ist praktisch nur noch über kommerzielle Newsserver möglich, die Gebühren dafür richten sich meist nach dem Transfervolumen. Deswegen wird das Usenet wohl nie eine wichtige Rolle bei den Filesharern spielen.

Viele Newsserver-Anbieter wie Usenext (www.usenext.de) oder Firstload (www.firstload.de) bewerben ihre Angebote sehr aggressiv und laden zu Urheberrechtsverletzungen praktisch ein – was bisher schon einstweilige Verfügungen der Industrie nach sich zog. Allerdings gibt es ein aktuelles Gerichtsurteil vom April 2007, in dem festgestellt wurde, ein Usenet-Zugangsanbieter müsse nicht jeden

erdenklichen Aufwand betreiben, um die Nutzung rechtswidriger Inhalte zu vermeiden. Eine Überprüfung der riesigen Datenmengen im Usenet sei unzumutbar. Im Übrigen würde die Abschaltung eines einzelnen Newsservers nicht bewirken, dass die entsprechenden Dateien komplett aus dem Usenet verschwinden.

9. So verhalten sich die Internet-Provider

Der einzige Weg, die Identität eines Filesharers zu ermitteln, führt über den Internet-Provider. Nur er kann einer IP-Adresse eine Person zuzuordnen. Erst im Februar dieses Jahres haben etwa T-Com und Arcor angekündigt, ihre Speicherpraxis ändern zu wollen. Besonders im Falle von Flatrate-Kunden sollen die Infos bereits nach wenigen Tagen wieder gelöscht werden – bislang speichert T-Com die Daten 80 Tage lang. Dies sei eine Reaktion auf die aktuelle Rechtslage, nach der die Daten nicht längerfristig gespeichert werden dürfen, wenn sie für die Abrechnung nicht vonnöten sind. Sobald diese Ankündigung umgesetzt ist, wären davon auch alle Betreiber betroffen, die den IP-Backbone der T-Com nutzen.

Die Internet-Ermittler sind davon wenig begeistert, wird doch die Strafverfolgung dadurch für sie erheblich erschwert. Es ist die Frage, ob die Staatsanwaltschaften binnen einer Woche die Herausgabe der Benutzerdaten anordnen – denn an Dritte dürfen die Provider die Daten nach wie vor nicht herausgeben. Die Rechteinhaber selbst sollen nur dann einen Auskunftsanspruch erhalten, wenn sie hieb-und-stichfest beweisen kön-

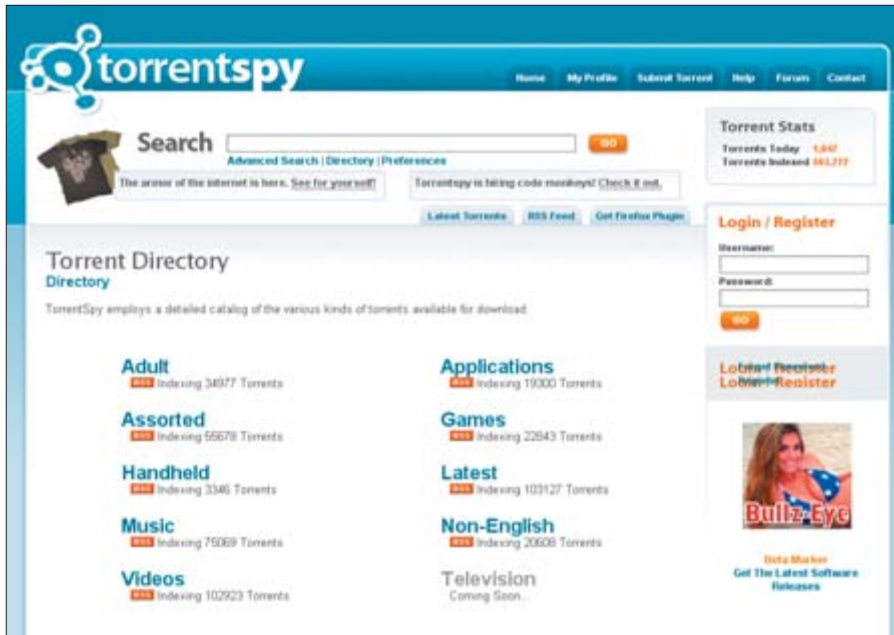


Alternative Usenet: Anbieter wie Usenext bewerben ihre Angebote aggressiv – mit Hinweis auf einschlägige Inhalte (Punkt 8)

nen, dass ihr Urheberrecht in gewerbsmäßiger Weise verletzt worden ist.

10. Die Zukunft: Digitales Wasserzeichen statt DRM

Das bisher genutzte Digital Rights Management steht vielfach in der Kritik. Per DRM geschützte Dateien lassen sich häufig nicht auf allen Geräten abspielen und verursachen auch sonst jede Menge Probleme. Das Fraunhofer-Institut SIT (Sichere Informations-Technologie) entwickelt nicht wahrnehmbare digitale Wasserzeichen als Alternative zu DRM (www.ipsi.fraunhofer.de/mediensicherheit/was_ist_watermarking.de.html). Mit dieser Technik können beispielsweise Informationen über den Kunden in digitalen Videos, Bildern oder Musikstücken untergebracht werden, die sich praktisch nicht mehr entfernen lassen. Auch in Kopien von Kopien ließe sich dann noch feststellen, wer die Datei ursprünglich gekauft hat. Der Vorteil: Die Gängelung durch DRM fiele weg, die Nutzer würden nicht mehr vorab kriminalisiert, aber schwarze Schafe könnten trotzdem erwischt werden. Im Herbst 2006 eröffnete Akuma.de, der Online-Musikshop bietet ausschließlich MP3s an, die mit digitalen Wasserzeichen geschützt sind. Dieser Technik steht eine große Zukunft bevor: Nach Apple will sich auch Musicload langfristig von Kopierschutzmethoden verabschieden und digitale Wasserzeichen einsetzen. Allerdings wollen die ganz großen Labels derzeit noch nicht auf DRM verzichten. Das Geschäft der Schwarzkopierer wird mit digitalen Wasserzeichen sicher nicht erleichtert. ☒



Die aktivste Tauschbörse

Filesharing muss nicht zwingend illegal sein oder nur illegale Inhalte verbreiten. Per Bit Torrent werden etwa auch Linux-Distris oder große Downloads wie Open Office verteilt.

Von **Peter-Uwe Lechner**

Unter dem Druck der Film- und Musikindustrie sind viele ehemals sehr populäre Tauschbörsen entweder vollständig offline oder werden kaum noch genutzt. Durchgesetzt und etabliert hat sich hingegen Bit Torrent – das Netzwerk hat sich zum wohl beliebtesten Filesharing-Dienst entwickelt. Während den klassischen Gnutella- und Edonkey-Netzen mit all ihren Clients wie Emule, Bearshare, Win Mx, Kazaa & Co. immer der Illegal-Stempel aufgedrückt war, hat vor allem die Software-Industrie die Bit-Torrent-Technologie als Verteilungswerkzeug für legale Inhalte entdeckt. So bieten Linux-Distributoren wie Open Suse und

Ubuntu neben FTP-Downloads auf ihren Webseiten Tracker für den Download ihrer DVD-ISO-Images via Bit Torrent an. In diesem Beitrag erfahren Sie alles Wissenswerte über Bit Torrent. Wir erläutern die Technik, stellen die wichtigsten Download-Tools vor und erklären, wie Sie Dateien herunterladen und für andere freigeben.

1. Selbstverständlich auch illegale Inhalte

Egal ob die neuesten Hollywood-Filme, aktuelle Alben der Stars oder die zighundert Euro teure Spezial-Software – es gibt nichts, was es nicht auch in den Tiefen des Inter-

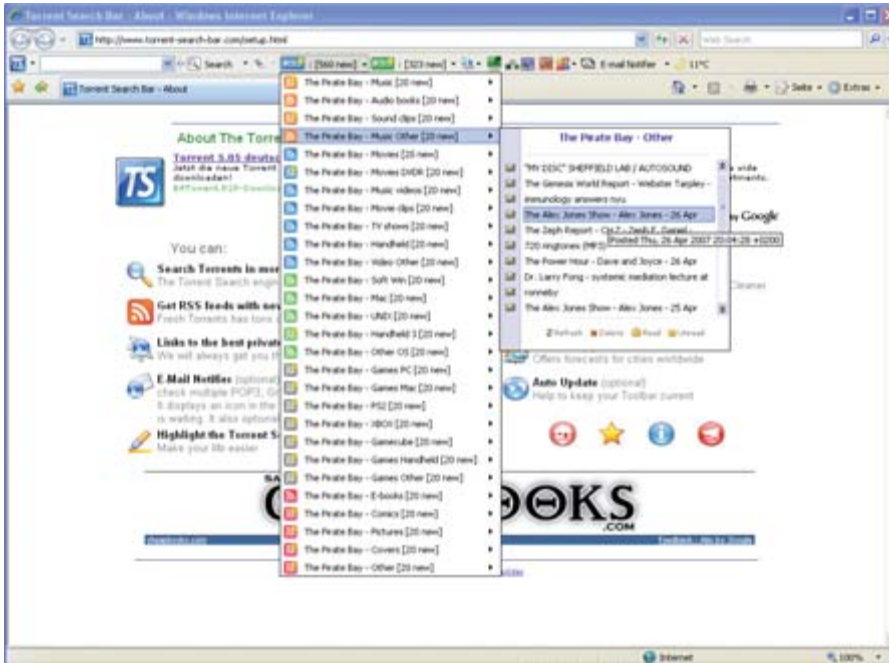
nets gibt. Immer häufiger kommt zum Tausch solcher Dateien die Bit-Torrent-Technik zum Einsatz. Die Warez-Szene unterhält eigene Download-Kanäle und hat nur wenig Berührungspunkte zu Tauschbörsen und Peer-to-Peer-Protokollen wie Bit Torrent. Filme, Musik und Software erscheinen hier später als auf Warez-Servern und im Usenet. Für gelegentliche Warez-Jäger sind Tauschbörsen allerdings die Hauptquelle für illegale Kopien. Die Industrie ist daher auf Bit Torrent nicht gut zu sprechen. Experten schätzen, dass die mit Bit Torrent getauschte Datenmenge ein Drittel des gesamten Internet-Datenvolumens ausmacht – mehr als alle anderen Tauschdienste zusammen.

2. Ganz einfach: Die Suche nach den Wunsch-Torrents

Es gibt zahlreiche Suchmaschinen im Netz, die sich auf das Auffinden von Torrents spezialisiert haben. Die wohl bekannteste bieten die Bit-Torrent-Erfinder unter www.bit.torrent.com selbst an. Die Suchmaschinen unter www.torrentspy.com und www.torrentportal.com fahnden auf Torrent-Seiten und überzeugen durch eine bessere Aufbereitung der Ergebnisse und durch eine „Advanced Search“-Funktion, bei der Sie die Suche etwa auf Musikdateien einer bestimmten Größe beschränken können. Auch das Seeder-Leecher-Verhältnis lässt sich einstellen, damit man Daten möglichst schnell auf den eigenen Rechner bekommt. In der Ergebnisliste erscheint eine Anzeige mit dem Titel „Health“. Hier sollte nach Möglichkeit einer der grünen Tracker gewählt werden, da diese ein besonders gutes Upload-Download-Verhältnis versprechen. Eine sehr gute Alternative ist die Torrent-Search-Toolbar 4.5 für die Webbrowser Firefox und Internet Explorer, die sich unter

Darum geht's: Bit Torrent

Im Gegensatz zu den Server-basierten Filesharing-Netzen von Emule, Kazaa und Co. kommt die Torrent-Technologie ohne Server aus. Jeder Client ist gleichzeitig Server. Das sorgt für schnelle Downloads und eine hohe Verfügbarkeit. Immer mehr Firmen machen sich das beispielsweise für die Verteilung ihrer Software zunutze.



Torrent-Suche leicht gemacht: Auf einen Rutsch durchforstet die Browser-Extension 32 Torrent-Verzeichnisse nach Software, Filmen und MP3-Dateien (Punkt 2)

www.torrent-search-bar.com (für Windows 95/98/ME, 2000/XP und Vista, kostenlos) installieren lässt. Über eine eigene Suchmaske können die 32 bekanntesten Torrent-Seiten wie Mini Nova, Thepiratebay, Torrent Reactor, Isohunt, Torrentspy, Torrentz und Torrentbox nach beliebigen Suchbegriffen durchstöbert werden. Über ein Aufklappmenü lassen sich von jeder Seite die 50 aktuellsten Einträge anschauen und bei Interesse anklicken. Via RSS-Feeds werden neue Inhalte in zehn Channels angezeigt. Ein anderer Weg läuft über einschlägige Websites,

die Sie bei der Eingabe von Begriffen wie „Torrent“ oder „Torrentfiles“ bei Google finden. Es kann immer wieder vorkommen, dass Torrents bereits veraltet sind und die Tracker nicht mehr unterstützt werden.

3. Gefahren: Keine Anonymität, offene IP

Wie auch in anderen Tauschbörsen ist man auch im Bit-Torrent-Netzwerk alles andere als unsichtbar. In einem Bit-Torrent-Client wird bei einer Verbindung immer die aktuelle IP-Adresse der Gegenstellen angezeigt.

Überblick Bit Torrent

Inhalt	Seite
1. Selbstverständlich auch illegale Inhalte	34
2. Ganz einfach: Die Suche nach Torrents	34
3. Gefahren: Keine Anonymität, offene IP	35
4. Die Rechtslage: Kein Kavaliersdelikt	36
Programme für Torrent-Downloads	
5. Azureus 2.5.0.4	37
6. Bitcomet 0.86	37
7. Bit Tornado 0.3.18	38
8. Shareaza 2.2.5.0	39
9. uTorrent 1.61	39
Kästen	
Darum geht's: Bit Torrent	34
Software im Überblick	35
So funktionieren Torrents	36
Eigene Dateien via Torrent verteilen	37
Torrents mit Opera und Download-Managern laden	38
Download-Ärger ersparen: Fakes erkennen	39

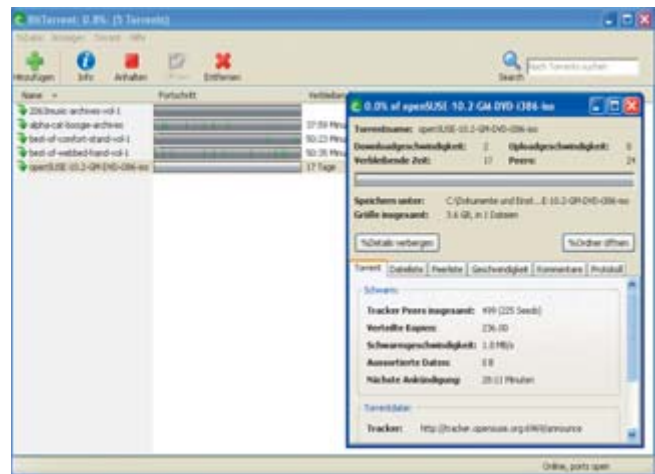
Da man automatisch beim Laden einer Datei auch gleichzeitig Anbieter ist, gerät man bei urheberrechtlich geschütztem Material leicht ins Visier der Fahnder. Außer Sie surfen über eine Anonymisier-Lösung, die Ihrer kompletten Internet-Verbindung eine Art Tarnkappe aufsetzt. Ein solcher Service ist zum Beispiel Findnot.com (www.findnot.com). Damit können Sie nicht nur anonym surfen, sondern auch anonym downloaden.

Software im Überblick: Tools für Bit-Torrent-Downloads

Programm	Azureus 2.5.0.4	Bit Torrent 5.07	Bitcomet 0.86	Bit Tornado 0.3.18	Shareaza 2.2.5.0	uTorrent 1.61
Internet	http://azureus.sourceforge.net/	www.bittorrent.com	www.bitcomet.com	www.bittornado.com	http://www.shareaza.com/	www.utorrent.com
Preis	kostenlos	kostenlos	kostenlos	kostenlos	kostenlos	kostenlos
Sprache	Deutsch	Englisch	Deutsch	Deutsch	Englisch	Deutsch
Windows	95/98/ME, 2000/XP	95/98/ME, 2000/XP	95/98/ME, 2000/XP	95/98/ME, 2000/XP	95/98/ME, 2000/XP	95/98/ME, 2000/XP
Parallel-Downloads	ja	ja	ja	ja	ja	nein
Bandbreiten-Begrenzung	ja	nein	ja	ja	ja	ja
Warteschlange	ja	ja	ja	ja	ja	ja
Statistik-Funktionen	ja	ja	ja	ja	ja	ja
Eigener Tracker	ja	nein	ja	nein	nein	ja
Torrent-Maker	ja	nein	ja	nein	nein	ja
Inhalte-Filter	ja	nein	ja	nein	nein	ja



Legale Torrents: Klassiker wie der freie Film Route 66 werden via Bit Torrent an die Filesharer-Gemeinde verteilt (Punkt 4)



Das Original: Von den Erfindern des Bit-Torrent-Protokolls stammt dieser Client. Auf Extras muss man verzichten

Das Ganze kostet 6,25 Dollar pro Monat, wenn Sie sich für zwei Jahre an den Anbieter binden. Sonst werden 9,95 Dollar monatlich fällig. Allerdings ist auch diese Lösung nicht ideal, da der erzielte Datendurchsatz durch das Umleiten über spezielle Proxy-Server sinkt. Folglich brauchen Sie mehr Zeit, bis Sie eine Datei auf Ihrem Rechner haben. Im Gegensatz zu den anderen Tauschbörsen und ihren Clients kann man bei Bit Torrent übrigens keine Dateilisten browsen und sich auf Mausklick die auf der Festplatte eines

Users freigegebenen Files anzeigen lassen. Das bringt vor allem unerfahrenen Anwendern ein Plus an Sicherheit.

4. Die Rechtslage: Kein Kavaliersdelikt

Bit Torrent sollte nicht zum Download von urheberrechtlich geschützten Dateien genutzt werden. Man macht sich in dem Fall strafbar, da andere Anwender bereits während des Runterladens der Daten die ersten Fragmente weitergeleitet bekommen –

schon bevor die Datei vollständig auf Festplatte ist. Bei populären Filmen, Musikdateien und Software ist der Fall klar – hier werden Urheberrechte verletzt, und das kann im schlimmsten Fall strafrechtlich relevant sein, zumindest aber zu zivilrechtlichen Schadensersatzforderungen von Seiten des Herstellers führen. Doch auch bei Mitschnitten von beliebten Fernsehserien, die auf solchen Sites oft zu finden sind, kann man nicht davon ausgehen, dass das Tauschen legal ist. Die Begründung „das hätte

So funktionieren Torrents

Bei Bit Torrent gelangt die Datei nicht wie bei HTTP- oder FTP-Downloads nur aus einer Quelle auf den PC. Vielmehr kommt sie von verschiedenen Anwendern, die an dem individuellen Netzwerk für die jeweilige Datei teilnehmen. Dabei muss nicht einmal die gesamte Datei auf dem Rechner sein. Es reicht, wenn der Anwender ein Fragment besitzt, das er an andere Benutzer weitergibt, die möglicherweise schon über weitere Teile verfügen. Die Chance, alle Teile eines Programms zusammenzubekommen, ist dadurch größer als bei anderen Tauschsystemen, bei denen nur Besitzer der vollständigen Datei diese auch weitergeben.

Eindeutige Identität

Der Austausch von Dateien erfolgt bei Bit Torrent in einem Netzwerkverbund. Einer oder mehrere Anbieter stellen eine Datei zum Download bereit, Bit-Torrent-Clients laden die Datei dann auf Ihren PC herunter. Bei der Torrent-Technologie wird für jede bereit gestellte Datei eine Steuerdatei (.torrent) von wenigen KB Größe generiert. Diese Metadatei enthält eine eindeutige ID (Hash) mit Informationen zur Datei selbst und die Download-Adresse. Die Download-Quellen werden über einen so genannten Tracker gehostet. Er macht es überhaupt erst möglich, dass ein Client die jeweilige Datendatei findet. Im ersten Schritt wird die Torrent-Datei via Webbrowser von einer Homepage geladen und anschließend mit

einem Torrent-Client geöffnet. Erst dann startet der Download der eigentlichen Datendatei. Bei den Quellen wird zwischen „Peer“ und „Seed“ unterschieden. Ein Client ist dann ein Peer, wenn er die Datendatei noch am Laden ist. Seeds sind User, die die im Torrent angegebene Datendatei schon vollständig geladen haben und diese nur noch als Quelle für die Peers anbieten. Es ist mindestens ein Seed erforderlich, damit die Übertragung erfolgreich abgeschlossen werden kann.

Schnell wie ein Download-Manager

Nachdem man selbst Teile eines Archivs heruntergeladen hat, werden diese Teile auch an andere Bit-Torrent-Nutzer verteilt. Je mehr Peers bei der Verteilung helfen, desto schneller wird der Download sein. Das Prinzip der Übertragung ähnelt dabei einem Download-Manager. Zunächst legt der Client eine lokale Datei an, die dann aus verschiedenen einzelnen Dateisegmenten (Chunks) zusammengesetzt wird. Dadurch, dass der Tracker die aktiven Quellen kennt, muss der Bit-Torrent-Client nicht ständig nach neuen Quellen suchen und erreicht dadurch weit höhere Geschwindigkeiten, als sie etwa bei konventionellen Filesharing-Netzwerken möglich sind. Im Torrent-Netzwerk gibt es keine Suchfunktion. Der Client kennt nur die Quellen, die in der Torrent-Datei gelistet beziehungsweise den gelisteten Quellen bekannt sind.

Eigene Dateien via Torrent verteilen

Um selbst Dateien anzubieten, legt man einen Torrent an und stellt ihn über einen Tracker anderen Anwendern zur Verfügung. Benötigt wird dazu nur ein Client, der das Erstellen von Torrents unterstützt, zum Beispiel Azureus. Zunächst werden die Dateien, die mit Azureus verteilt werden sollen, in einem Ordner auf der Festplatte oder noch besser in einem komprimierten Archiv zusammengefasst. Besonders weit verbreitet sind die beiden Pack-Formate ZIP und RAR. Viele Anwender versehen ihre Torrents zusätzlich mit einem Passwort. Damit wollen sie sicherstellen, dass nur bestimmte Anwender mit den Torrents arbeiten können.

In Azureus ist über „Datei, Torrent erstellen“ der Assistent zu öffnen. Wenn man eine feste IP-Adresse besitzt, ist der „Azureus Embedded Tracker“ die richtige Wahl. Im Normalfall weist der Internet-Provider bei jeder Einwahl eine neue, dynamische IP-Adresse zu. Die Lösung für dieses

Problem: Man meldet sich zum Beispiel bei www.dyndns.com für den kostenlosen Dienst „Dynamic DNS“ an. Dadurch gibt es einen festen Domain-Namen für dynamische IP-Adressen. Diesen gibt man dann eben statt der IP-Adresse beim Anlegen der Torrent-Datei ein. Es ist darauf zu achten, dass eine Firewall die notwendigen Ports freigibt: Für die Kommunikation mit dem Tracker ist Port 6969 erforderlich, die beiden Ports 6881 bis 6889 werden für den Datentransfer mit Tauschpartnern benötigt. Danach ist anzugeben, ob es sich um eine Datei oder um ein Verzeichnis mit mehreren Dateien handelt. Es lassen sich weitere Informationen hinzufügen, etwa Versionsangaben, Bitrate oder Dateiformat. Im nächsten Fenster wählt man die Datei aus, zu der eine Torrent-Datei erzeugt werden soll. Azureus erstellt nun den Torrent, den man beispielsweise über eine Website oder per Mail verteilen kann.

ich mir doch auch gestern auf Video oder DVD mitschneiden können“ zählt nicht: Getauscht wird hier mit fremden Leuten und nicht nur mit befreundeten Einzelpersonen. Nach absolut legalen Inhalten muss man zwar etwas suchen, es gibt sie aber. Unter www.legaltorrents.com zum Beispiel finden sich eine Vielzahl von Filmen, Musikalben, Spielen, Software und anderen Inhalten, die die jeweiligen Künstler oder Hersteller kostenlos und zur freien Verwendung anbieten. Nicht alles entspricht dem Massengeschmack, vieles aber ist kreativ und interessant. Auch auf einigen Sites von Open-Source-Projekten finden sich Torrents.

Programme für Torrent-Downloads

Der Original-Bit-Torrent-Client (<http://bit.torrent.com>) beschränkt sich auf seine wesentliche Aufgabe, nämlich das Laden von Dateien. Für Download-Profis ist das Programm nicht empfehlenswert, da eine Reihe von Einstellungen fehlen, etwa das Beschränken der Bandbreite. Als Alternative gibt es eine ganze Reihe von kostenlosen Bit-Torrent-Clients. Hinsichtlich Bedienung und Ausstattung gibt es ebenso Unterschiede wie bei der Geschwindigkeit. PC-WELT stellt die populärsten Clients vor.

5. Azureus 2.5.04

Der sehr empfehlenswerte deutschsprachige Open-Source-Client Azureus benötigt eine Java-Runtime-Umgebung ab Version 1.5 und kann nicht nur unter Windows und Mac OS, sondern auch unter diversen Li-

nux-Distributionen installiert werden. Die erweiterte Version 3.0 „Zudeo“ bietet zusätzlich den Zugang zu einem eigenen Video-Portal. Für das reine Saugen von Torrents ist die Version 2.5 besser geeignet.

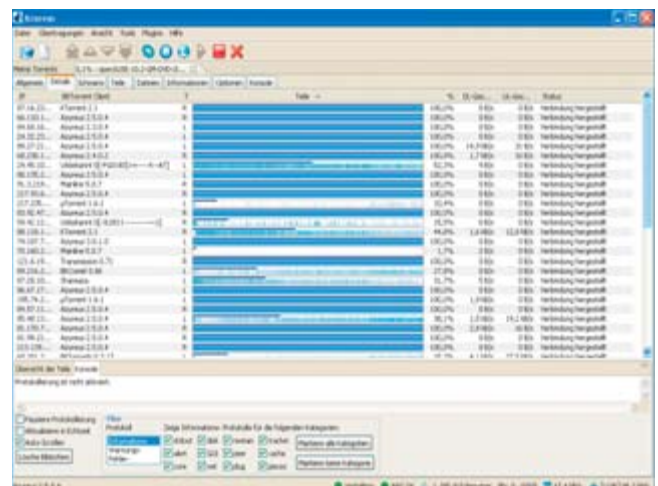
Die Installation gestaltet sich dank eines Assistenten sehr einfach: Schritt für Schritt wird man durch die allgemeinen Angaben geleitet, die Azureus für die Verbindung am Peer-to-Peer-Netzwerk benötigt. Über den Menüpunkt „Konfiguration“ im Menü „Tools“ lassen sich zahlreiche weiterführende Optionen einstellen, etwa wo Azureus die heruntergeladenen Dateien speichern soll. Das Tool bietet Zusatzfunktionen wie das Erstellen eigener Torrents.

Wird ein Torrent geladen, zeigt der Client die eigenen Up- und Download-Geschwindigkeiten, die verbleibende Restzeit, Datei- und Tracker-Informationen, die Anzahl der Seeds und Peers sowie die hochgerechnete Verfügbarkeit an. Auf einen Blick lässt sich erkennen, wie viel Prozent eines Torrents bereits übertragen wurde, sowie die Anzahl verfügbarer und noch fehlender Teilstücke davon. Mit der Peer-Exchange- und VHT-Funktion sind Downloads auch dann möglich, wenn der Original-Tracker ausfällt. Über das „Plugins“-Menü ist es sehr ein-

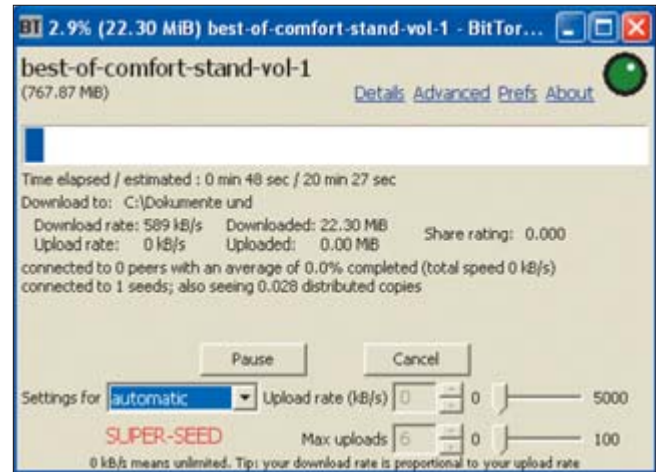
fach möglich, Erweiterungen zu installieren und damit den Funktionsumfang von Azureus zu erweitern. Mit „Safe Peer“ werden bestimmte IP-Adressen blockiert, die bewusst fehlerhafte Daten einspeisen und so versuchen, das Bit-Torrent-Netzwerk zu sabotieren. „AutoCategorizer“ organisiert Downloads und ordnet Dateien anhand von Schlagwörtern automatisch in passende Kategorien ein. Das Plug-in „Swing Web Interface“ erlaubt den Zugriff auf Azureus über den Browser. So können Anwender etwa von unterwegs die Einstellungen überwachen und Dateien veröffentlichen.

6. Bitcomet 0.86

Der übersichtliche und einfach zu bedienender Filesharing-Client stellt zahlreiche Funktionen zur Verfügung. Dazu zählt etwa die Möglichkeit, mehrere Downloads simultan



Azureus: Der derzeit wohl beste Bit-Torrent-Client sorgt mit ausgefeilter Technik für sehr hohe Transferraten (Punkt 5)



Bit Tornado: Schlicht und ohne aufwendig gestaltetes Interface präsentiert sich der einfach gehaltene Client (Punkt 7)

ware unterstützt wie Azureus das so genannte Swarming – je nach Verfügbarkeit wird ein und dieselbe Datei (Dateiteile) von mehreren Usern parallel heruntergeladen. Dadurch erhöht sich die Download-Geschwindigkeit. Um Leecher abzublocken, die nur Dateien laden, aber selbst keine Dateien anbieten, kommt ein internes Bewertungssystem zum Einsatz. Im Gegensatz zu Azureus kann Bitcomet nur einzelne Dateien herunterladen und nicht ein komplettes Verzeichnis mit darin enthaltenen Dateien . Alle wichtigen Funktionen und Bereiche des Programms sind einfach zu erreichen. Die Einstellungen sind übersichtlich angeordnet und auch für unerfahrene User leicht zu bedienen. Kompliziertere Optionen werden

Der englischsprachige Client bietet verschiedene vorgefertigte Konfigurationsprofile zur schnellen Auswahl an. Alternativ legt man Einstellungen wie die Upload-Rate sowie die Anzahl der parallelen Uploads manuell fest. Das Tool zeigt eine Reihe nützlicher Informationen über den Tracker sowie die jeweiligen Verbindungen an und ermittelt die verbleibende Download-Zeit. Weiterhin erfährt man alle Details zum aktuellen Torrent wie Adresse, Prüfsummen und Erstellungsdatum. Nach einem Klick auf den

Ab Version 8 besitzt der Webbrowser Opera standardmäßig eine Unterstützung für das Bit-Torrent-Protokoll. Nach einem Klick auf einen Torrent-Link auf einer Website blendet Opera einen Dialog ein, der zur Angabe eines Zielverzeichnisses für den Dateien-Download auffordert. Ein Klick auf „Ja“ startet den Download. Nachdem dieser beendet ist, werden die Dateien solange an andere Nutzer verteilt, bis Opera beendet oder der Transfer manuell gestoppt wird. In den Bit-Torrent-Einstellungen von Opera lassen sich die Bandbreite für Downloads und Uploads sowie der Port für eingehende Verbindungen festlegen. Zum Testen der Funktionalität genügt ein Klick auf die Schaltfläche „Testen“ neben dem Feld des Eingangs-Ports. Schlägt der Test fehl, muss in der Regel der Port in den Einstellungen einer Firewall freigeschaltet werden. Eine Desktop-Firewall gibt in der Regel bei der ersten Torrent-Verbindung einen entsprechenden Warnhinweis aus und erlaubt nach expliziter Bestätigung die dauerhafte Freigabe. Übrigens verfügt Opera über eine Bit-Torrent-Suche, die über das Suchfeld in der Adressleiste erreichbar ist.

Auch moderne Download-Manager wie die Freeware Flashget 1.82 (www.flashget.com, für Windows 95/98/ME, 2000/XP und Vista) und Getright 6 (www.getright.com, für Windows 95/98/ME, 2000/XP und Vista, 30 Dollar) unterstützen von Haus aus das BitTorrent-Protokoll. Beim Anklicken einer Torrent-Datei im Browser übernehmen die Download-Manager zuerst das Laden der Steuerdatei und führen anschließend den eigentlichen Transfer der Datendatei aus.



Opera: Ohne Zusatz-Tools übernimmt der Webbrowser das Laden von Torrents

Download-Ärger ersparen: Fakes erkennen

Nicht immer ist bei getauschten Dateien das drin, was draufsteht. Deshalb ist es sinnvoll, einen Torrent schon vor dem Download unter die Lupe zu nehmen. So erspart man es sich, eine mehrere hundert Megabyte große Datei herunterzuladen – nur um hinterher festzustellen, dass es sich nicht um die beschriebene Datei handelt. Diese Aufgabe erledigt die englischsprachige Freeware **Torrent Spy** (<http://torrentspy.sourceforge.net>, für Windows 95/98/ME, 2000/XP und Vista), ein einfaches, gut zu bedienendes Open-Source-Tool. Das Programm hat übrigens nichts mit der gleichnamigen Suchmaschine für Torrents zu tun. **Torrent Spy** muss nicht installiert werden, das Tool lässt sich einfach vom Desktop aus starten oder man zieht einen Torrent per Drag & Drop direkt auf das Icon. Binnen einiger Sekunden analysiert das Tool den Torrent und zeigt unter anderem an, welche Dateien enthalten sind, wie viele andere Anwender die Daten komplett oder unvollständig bereitstellen und wann der Torrent erstellt wurde. Diese Information hilft etwa zu erkennen, ob es sich um die richtige Version einer Software handelt. Per Klick auf „Data“ zeigt die Software weiterführende Informationen sowohl über den Torrent als auch über den dazugehörigen Tracker. Dort sieht man beispielsweise, wie viele An-

wender die Daten bereits heruntergeladen haben. Wenn man mit den Informationen zufrieden ist und den Download starten möchte, genügt ein Klick auf den „Launch“-Button auf der Registerkarte „General“ – und der Download startet über den voreingestellten Bit-Torrent-Client.

Tipp: Besonders schnell lässt sich die Analyse durch **Torrent Spy** über das Kontextmenü beim Aufruf eines Torrents starten. Um den Eintrag einzurichten, geht man auf „System“ und wählt die Option „Add the Torrent with TorrentSpy context menu options“. Hier legt man außerdem fest, ob sich das Utility auch aus dem Internet Explorer heraus anwählen lässt.



Detailinfos abrufen: Mit der Freeware Torrent Spy erkennen Sie Fake-Dateien

Button „Advance“ zeigt Bit Tornado alle IP-Adressen an, von denen heruntergeladen werden kann, inklusive der Transferrate.

8. Shareaza 2.2.5.0

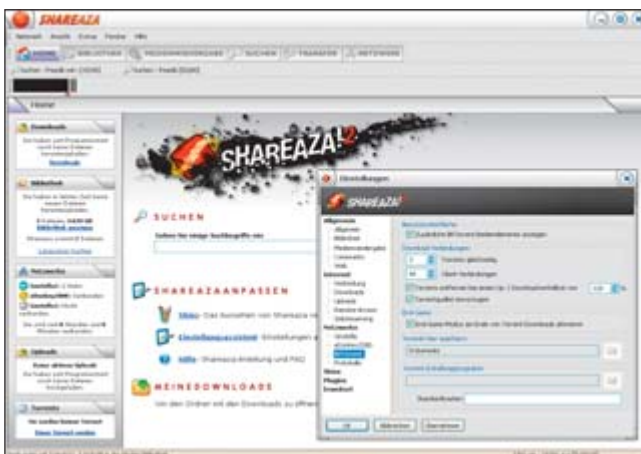
Das deutschsprachige Allround-Werkzeug zum Tauschen von Dateien unterstützt neben dem Gnutella-Netzwerk auch Dateitransfer über Emule und Bit Torrent. Die Freeware lässt sich an die Bandbreite Ihrer Internet-Anbindung anpassen. Neben einer umfangreichen Medienverwaltung und einem eingebauten Player gibt es eine Chat-Funktion. Der Client unterstützt den gleichzeitigen Transfer von mehreren Hosts und kann unterbrochene Übertragungen jeder-

zeit wieder aufnehmen. Dank der Ultrapeer- und Query-Routing-Technology wird die Bandbreite optimal ausgenutzt. Shareaza besitzt eine brauchbare Suchfunktion für Musik, Videos und Bilder, wobei sich die Ergebnisse weiter einschränken lassen. Gegenüber den Spezialisten wie Azureus bietet das Tool nur eingeschränkte Funktionen. Es eignet sich daher vorwiegend für Nutzer, die mehrere Netze abdecken möchten.

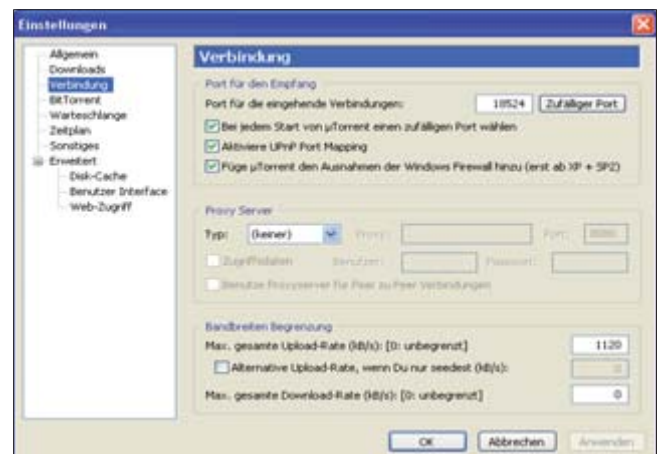
9. uTorrent 1.61

Der sehr kompakte Bit-Torrent-Client besitzt eine Fülle an Einstellungsmöglichkeiten, die Bedienung ist klar und übersichtlich strukturiert. Zu den Besonderheiten des

Clients zählen die Warteschlange, die Fähigkeit, mehrere Dateien gleichzeitig zu laden, und ein Torrent-Maker. Integriert ist das so genannte Super-Seeding. Hierbei werden alle Teile einer Datei eines Seeders nur einmal an einen anderen Peer verschickt. Das Feature wird vor allem dann eingesetzt, wenn neue Dateien möglichst bandbreitenschonend verbreitet werden sollen, um die Zahl der Seeder zu erhöhen, die die gesamte Datei anbieten. uTorrent bietet die automatische Wiederaufnahme von abgebrochenen Downloads. Mit der Funktion „WebUI“ lässt sich der PC, auf dem uTorrent installiert ist, über jeden beliebigen anderen PC im LAN oder Internet fernsteuern.



Allrounder: Neben den Filesharing-Netzen Gnutella und Edonkey kommt Shareaza auch mit Torrents zurecht (Punkt 8)



Funktional: uTorrent erlaubt das Wechseln der Ports für mehr Sicherheit und die Beschränkung der Bandbreite (Punkt 9)



Hardcore ohne Jugendschutz

Statt skurriler Filmchen wie bei Youtube gibt es bei Youporn, Pornotube und Xtube unzensurierte Hardcore-Erotikfilme ohne Alters-Check zu sehen. Jugendschützer sind bestürzt.

Von **Ramon Schwenk**

Die gesamte Pornobranche ist zu einem mächtigen Wirtschaftsfaktor im Internet geworden. Bislang waren die meisten Porno-Seiten kostenpflichtig und verlangten eine Anmeldung per Kreditkarte oder Altersverifikationssystem. Neu sind werbefinanzierte Erotik-Videoportale nach dem Vorbild von Youtube. Die Dienste setzen explizit auf Sexinhalte. Statt User Generated Content – dem Schlagwort der Web-2.0-Ära – gibt es User Generated Hardcore gespickt von Werbung der Porno-Industrie. Zu haben sind Gratis-Videoclips mit Sex in allen Varianten, die Nutzung der Youtube-Klone ist kinderleicht, und Jugendschutz gibt es nicht.

1. Gigabyte-weise kostenlose Schmuttel-Filmchen

Bei Youtube.com, dem wohl erfolgreichsten und größten Videoportal, bekommen Internet-Nutzer von Menschen aus allen Ecken der Erde schräge, komische oder schlicht langweilige Video-Eigenkreationen. Weniger Kreative laden TV- oder Filmausschnitte unabhängig vom urheberrechtlichen Status der Inhalte hoch. Erotische bis pornografische Videos und Bilder finden sich bei Youtube & Co. eher selten – zu gut wachen die Content-Sheriffs der Betreiber nebst den automatischen Filtersystemen über die eingebrachten Videoinhalte. Zwar verbieten die

Nutzungsrichtlinien der Dienste das Veröffentlichende von derartiger Filmchen. Doch eine gewisse Dunkelziffer an Clips mit pornografischem Inhalt hätte man erwartet. Abgesehen von einigen Zufallstreffern, die allerdings nie lange abrufbar sind, liefern Suchanfragen mit entsprechenden Begriffen jedoch keine entsprechenden Treffer.

Das Pendant zu Flickr nennt sich Eroshare und das zu Youtube – wen wundert es – Pornotube. Wer sich einer der hierzulande üblichen Schreibweise bedient, wird ebenfalls fündig: Pornotube versorgt das Internet mit die Amateurvideos von zweifelhafter Qualität. Spezielle Dienste decken auch besondere sexuelle Vorlieben ab, die man unter dem Begriff Fetisch zusammenfassen kann. Den Weg dazu weist beispielsweise Socialporn: Die Video-Website ist im Stil eines Weblogs aufgebaut. Der Betreiber selbst bietet keine Pornoinhalte an, sondern bringt Besucher geradewegs zu anderen Sites mit Gratisbildern von „NylonExtreme“ über „TheBlackGallery“ bis hin zu „Redheadwife“. Literotica hat sich kostenlosen Erotikgeschichten – den Free Stories – verschrieben: Nach Betreiberangaben stehen auf der Website über 75.000 Dokumente zum Gratisabruf bereit, einige davon mit kaum erträglichem Inhalt. Jeder Interessent kann auf dieser Seite seine Texte als einfache Textdatei hochladen.

2. Die Zugriffszahlen sind imposant

Wenn die auf einschlägigen Seiten bei den einzelnen Clips angezeigten Zugriffszahlen stimmen, arbeiten die Portale offensichtlich mit großem Erfolg. Augenscheinlich steckt jede Menge Potenzial hinter der Idee der von zeigefreudigen Anwendern veröffentlichten Erotik-Clips. Die Seiten der Youtube-Nachahmer sind optisch am Vorbild angelehnt und weisen die üblichen Web-2.0-Funktionen wie Bewertungen, Top-Listen, News und Kommentierungen auf. Die Videoportale werden in erster Linie für Werbung für professionelle Filmproduktionen genutzt. Zwischen selbst gedrehten Clips finden sich Trailer und Szenenfotos aus Kauf-DVDs und von anderen Websites, die eine kostenpflichtige Registrierung erfordern.

Doch auch so viel ist klar: Die Sites werden nicht zum Spaß online gestellt – damit wird Geld verdient. Und zwar jede Menge Geld von zahlreichen Beteiligten – Providern,



Hässliche Optik: Socialporn bietet selbst keine Erotikbilder an, sondern stellt Links zu geprüften Gratis-Galerien vor (Punkt 1)

Domain-Inhabern, Webmastern, Akteuren, die sich beispielsweise vor Kameras präsentieren, und Dienstleistern. Das Ganze ist ein dichtes Geflecht von Geschäftstüchtigen, die sich gegenseitig unterstützen, um die Kundschaft von einem Angebot zum nächsten zu ziehen. Eine Kundschaft, die fast ausschließlich männlich ist.

3. Rotlichtbezirk ohne jede Alterskontrolle

Eine Gemeinsamkeit der neuen Clip-Web-sites ist der Umstand, dass sich die Filmchen und Aktbilder ohne Alterskontrolle abrufen lassen. Eroshare, Youporn, Porntube und Xtube verzichten ganz auf ein Zugangskontrollsystem. Pornotube verlangt vom Besucher immerhin die Eingabe des Geburtsdatums. Dazu wählt der Gast das entsprechende Datum über Ausklappfelder aus. Die Altersabfrage hat allerdings reine Alibifunktion, denn einstellen kann man ein beliebiges Datum, und die Auswahl wird nicht weiter kontrolliert.

4. Grauzone: Fehlender Inhalte-Check

Bedenklich ist auch der Umstand, dass das von den Benutzern veröffentlichte Material kaum geprüft wird. Für eine umfassende Inhaltsverifizierung bräuchten die Anbieter jede Menge Personal. Wie bei Video-Sharing-Plattformen üblich kann von den Nutzern Filmmaterial in den gebräuchlichen Videodateiformaten hochgeladen werden. Der Server konvertiert die Dateien anschließend ins FLV-Format, damit es sich über den in den Browser eingebetteten Flash-

Player abspielen lässt. Wie bei Youtube lassen sich die auf dem Server gespeicherten Clips sogar in die eigene Homepage einbinden. Dazu genügt es, den nach dem Upload eines Film angezeigten Link in den HTML-Code der Zielseite einzubauen. Im laxen Umgang mit Inhaltskontrollen lauern zahlreiche Gefahren. Alleine die theoretische Möglichkeit, Sex- und Gewalt-

videos mit gesetzeswidrigem Inhalt veröffentlichten zu können, mag mancher Nutzer als Ansporn sehen. Zudem ist das Vertrauen der Portalbetreiber auf den Community-Gedanken absurd: Sie veröffentlichen Videos zunächst sofort in der Hoffnung darauf, dass Nutzer rechtlich bedenkliches Material melden. Die Community wird jedoch höchst selten eingreifen, denn ihr Interesse sind ja gerade möglichst ausgefallene Clips. So ist es nur eine Frage der Zeit, bis Bilder und Videos mit strafbewehrtem Inhalt zum Abruf durch jedermann bereitstehen.

Wie wenig sich die Betreiber um Recht und Gesetz kümmern, demonstriert der Infotext auf der Begrüßungsseite eines Dienstes: „Bei Stripfire.com kannst Du jetzt gratis und anonym, nachdem Du Dich anonym regis-

Überblick Gratis-Erotik

Inhalt	Seite
1. Schmuttel-Filmchen gratis	40
2. Die Zugriffszahlen sind imposant	40
3. Rotlichtbezirk ohne jede Alterskontrolle	41
4. Fehlender Inhalte-Check	41
5. Googler landen kaum Treffer	41
6. Sex-Surfen als Volkssport	42
7. Streit um den Jugendschutz	42
8. Online-Sex als Suchtproblem	43
9. Filter für Jugendliche unzuverlässig	44
10. Filtern über Rating-Systeme	45
11. Inhalte Filtern über Suchbegriffe	45
Kästen	
Expertenrat: Eltern sind gefordert	43
Sexfallen im Internet	44
Surfen mit dem Inhaltsratgeber	45

triert hast, Videos und Bilder hochladen und verwalten. Zeig uns wie Du [gelöscht]! Wenn Deine Amateursex-Videos gut sind, kannst Du bald auch Geld damit verdienen!“

5. Suchmaschinen-Nutzer landen kaum Treffer

Sex-Portale sind nicht nur Plattform für die von Anwendern eingesandten Inhalte, sondern dienen mit ihren zahlreichen Links auch als Wegweiser zu anderen Hardcore-Sites. Damit unterlaufen sie die Jugend-



Mehr Schein als sein: Die bloße Abfrage des Geburtsdatums ist kein geeigneter Schutz, um Minderjährigen den Zugang zu pornografischen Inhalten zu verweigern (Punkt 3)



Zugriff: Anders als für deutschsprachigen Sex-Seiten gibt es international kaum brauchbare Beschränkungen (Punkt 7)

schutzmaßnahmen der populären Suchmaschinen. Wer nach direkt abrufbaren Sex-Inhalten über Suchdienste wie Google oder Yahoo recherchiert, wird nur wenige Treffer landen. Zahlreiche Suchmaschinenbetreiber, darunter auch AOL, MSN und T-Online, haben im Rahmen der Freiwilligen Selbstkontrolle Multimedia-Dienstanbieter (FSM, www.fsm.de) einen entsprechenden Kodex unterzeichnet. Websites mit offensichtlich pornografischen Inhalten sollen danach nicht mehr auffindbar sein. Außer Hardcore-Inhalten betrifft die vereinbarte Selbstbeschränkung noch weitere Inhalte. So sollen beispielsweise Internet-Angebote mit kriegsverherrlichendem oder verfassungsfeindlichem Content nicht mehr im Volltextindex der Suchmaschinen landen. Auch gegen die Menschenwürde verstoßendes Material soll unberücksichtigt bleiben.

6. Sex-Surfen als Volkssport

Wie viele Anwender Online-Sex- und Erotikangebote nutzen, lässt sich nicht genau sagen. Es gibt so gut wie keine Erhebungen darüber, oder aber die Daten aus dem so bezeichneten Adult-Bereich dürfen nicht veröffentlicht werden. Laut einer älteren Studie haben die Deutschen beim Surfen auf

Sexsites die Nase vorn. Keine andere Nation soll mehr Zeit auf den einschlägigen Seiten verbringen. Jeder dritte Deutsche surft angeblich regelmäßig auf Sex-Seiten – im Schnitt 70 Minuten monatlich. Das Internet ist vor allem durch die Anonymität beim Surfen, die permanente Verfügbarkeit und zum Teil auch aufgrund kostenloser Inhalte zur Hauptverbreitungsart für Pornografie geworden.

Sex-Websites agieren in einer rechtlichen Grauzone, da der Jugendschutz nicht gewährleistet werden kann und teilweise auch verbotene Inhalte verbreitet werden. Kopfschmerzen bereiten der Internet-Erotikbranche hierzulande vor allem die nach wie sehr strengen gesetzlichen Auflagen durch die Jugendschützer.

Anbieter, die kein Altersverifikationssystem (Adult Verification System, kurz AVS) verwenden, machen sich dabei nach deutschem Recht strafbar. Pornografische Inhalte im Web sind in Deutschland aufgrund der gesetzlichen Jugendschutzbestimmungen unzulässig. Ausnahmsweise ist die öffentliche Zugänglichmachung der Sex-Inhalte im Rahmen geschlossener Benutzergruppen möglich. Dazu muss allerdings sichergestellt sein, dass die Teilnehmer nicht unter 18 Jahren alt sind. Zu diesem Zweck verlangen manche Site-Betreiber als Altersnachweis die Eingabe der Personalausweis- beziehungsweise Kreditkartennummer. Diese Form der Zugangsbeschränkung wird jedoch von der Rechtsprechung nicht als wirksam eingestuft. Erforderlich sind vielmehr effektive Maßnahmen wie das Postident-Verfahren, bei dem das Alter durch einen Postmitarbeiter überprüft wird.

7. Immer wieder Streit um den Jugendschutz

Die in Deutschland ansässigen Betreiber von Internet-Erotikseiten mühen sich seit



Bedenklich: Die Betreiber dieser Seite mit nur zum Teil kostenlosen Clips veröffentlichen Inhalte von anonym registrierten Anwendern ohne Herkunftsnachweis (Punkt 4)



Jahren um Anerkennung. Die großen Anbieter haben dazu den Verein zur Förderung des Kinder- und Jugendschutzes in Telemedien, Jusprog e.V., gegründet. Jusprog hat auf Basis des ICRA-Filtersystems das so bezeichnete Jugendschutzprogramm (www.jugendschutzprogramm.de) geschaffen. Es soll Eltern die Möglichkeit geben, ihren Nachwuchs vor dem Schlimmsten zu bewahren und sie vor „entwicklungsbeeinträchtigenden Inhalten“ schützen. Das System arbeitet mit einem Negativ-Filter. Wird die Filter-Software von Eltern auf dem heimischen Computer aktiviert, so sind die in der Negativ-Liste verzeichneten Seiten nur noch per Passwort-Eingabe zu erreichen. Um die Pflege der Schwarzen Liste mit Sex-Seiten kümmert sich der Verein. Die großen Web-Seiten wie Pornotube Xtube sind nach unseren Tests bereits in der Filterdatenbank enthalten und als „gesperrt“ eingestuft. Viele kleinere Sites fehlen dagegen.

8. Online-Sex als Suchtproblem

Exzessives Surfen auf Sex-Sites kann eine Reihe von Auswirkungen für die Betroffenen haben. Stundenlange Bilder- und Video-Downloads, nächtelange Chats und virtueller Sex mit Fremden – sogar dann, wenn der eigene Partner im Nebenzimmer anwesend ist: Von gelegentlichen Besuchen auf Erotikportalen bis hin zur Online-Sexsucht ist es für manchen nur ein kleiner Schritt. Wen es erwischt hat, der riskiert unter Umständen viel: Familien zerbrechen, Jobs sind in Gefahr, finanzielle Probleme drohen.



Online-Sucht: Zunehmend auch hierzulande ergeben sich Suchtprobleme durch den Konsum von Internet-Erotik (Punkt 8)

Pornografiesucht wird vor allem in den USA zunehmend als ernstzunehmendes gesellschaftliches Problem betrachtet. Die Thematisierung dort ist auch ein Anliegen religiöser Kreise. Hierzulande diskutieren Betrof-

Expertenrat: Eltern sind gefordert

Das Internet ist für abenteuerlustige Kinder und Jugendliche ein nicht ungefährlicher Spielplatz. Eltern fragen sich, wie man den Nachwuchs vor Sex-Portalen schützt. Erotikseiten ohne Altersverifikation werden dank Suchmaschinen und Mund-zu-Mund-Propaganda künftig immer öfter auch von Minderjährigen gefunden. Zudem wird die Masse der Angebote zunehmen. Theoretisch der einfachste Weg, ein Kind vor problematischen Web-Inhalten zu schützen: Sie lassen es nicht ins Netz. **Eigeninitiative ist gefragt**

Kinder sind neugierig, sie wollen selbst ausprobieren, was sie bei Klassenkameraden, Geschwistern und Freunden sehen oder anderswo gehört haben. Verbote, technische Sperrmaßnahmen und die Forderung nach staatlicher Reglementierung bringen in der Praxis nur wenig. Studien belegen, dass soziale Kompetenz und Bildung dank Internet-Zugangsmöglichkeit in jungen Jahren verbessert wird. Wer als Jugendlicher heute nicht surfen kann, hat somit Nachteile für die Zukunft.

Letztlich müssen die Eltern offen sein, Aufklärung betreiben und aktiv das Gespräch suchen. Finden Sie heraus, weshalb der Nachwuchs eine bestimmte Seite besucht, und zeigen Sie auf, weshalb das dort Gezeigte menschenverachtend ist. Im Idealfall kommt Ihr Kind dann selbst zu dem Schluss, dass solche Seiten Müll sind.

Das rät die Expertin

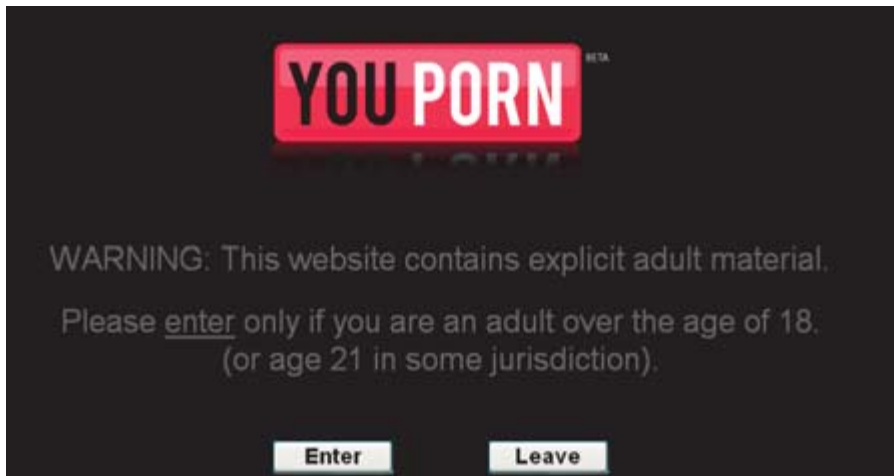
Wenn Sie schlimme Befürchtungen hinsichtlich der PC- und Internet-Nutzung Ihres Nachwuchses haben, sollten Sie nicht abwarten, sondern aktiv werden. Reicht ein klärendes Gespräch nicht aus, müssen Sie möglicherweise spezielle Knackprogramme einsetzen, um sich selbst Zugang zum Rechner verschaffen.

Renate Cöster, evangelische Theologin, Jugendpädagogin und Lerntrainerin aus Bonn, haben wir befragt, weshalb Minderjährige Verbote bezüglich der Internet-Nutzung ignorieren: „Kinder sind von Natur aus neugierig, sie wollen selbst ausprobieren, was sie bei Klassenkameraden, Geschwistern und Freunden sehen oder anderswo gehört haben. Solche Erfahrungen tragen auch dazu bei, dass sie in ihrer Clique mitreden können. Das gilt für gute wie für schlechte Web-Seiten.

Grundsätzlich haben Kinder kein Interesse daran, etwas zu tun, was ihnen schadet. Sie wollen aber ihren Spaß haben – wie die Erwachsenen im Übrigen auch. Deshalb sind sie nicht immer davon überzeugt, dass alles, was Sie als Eltern verbieten, wirklich schlecht für sie ist.“



Renate Cöster, Jugendpädagogin und Lerntrainerin



Content-Filterprogramme: Sie sollen Kinder und Jugendliche von nicht altersgerechten Web-Inhalten schützen, arbeiten aber nur unzuverlässig (Punkt 9)

fene vor allem auf Websites wie www.online-sucht.de. Suchtartiger Konsum kann reale Beziehungen in Mitleidenschaft ziehen, da die Erlebnisse in der virtuellen Welt in der wirklichen nicht nachvollziehbar beziehungsweise erlebbar sind.

Wie bei der Spielsucht führt auch die Pornografiesucht in seltenen Fällen zu erheblichen finanziellen Schäden bei den Betroffenen.

Pornografieabhängige können in ihrem persönlichen Sexualleben Schaden erleiden, vereinsamen. Psychotherapeutische Hilfe wird wegen suchtartigen Konsums von Pornografie selten in Anspruch genommen, wohl auch, da die Thematik schambesetzt ist. Diese Scham kann auch daran hindern, ein offenes Gespräch mit einer nahe stehenden Person zu suchen.

Ein Eingestehen der Sucht, gegebenenfalls das offene Gespräch mit der Partnerin zu suchen und die Inanspruchnahme psychotherapeutischer Hilfe sind der Einstieg in den Ausstieg aus der Sucht. In den USA gibt es auf süchtiges sexuelles Verhalten ausgerichtete Spezialkliniken, auch hierorts kann unter Umständen eine stationäre Behandlung in einer Suchtklinik angezeigt sein.

9. Filter für Jugendliche nicht zuverlässig

Filterprogramme versprechen, den Nachwuchs von nicht jugend geeigneten Internet-Angeboten fernzuhalten. Dadurch sollen Minderjährige auf bestimmte Seiten mit gefährdenden Inhalten wie Sex, Rassismus und Gewalt keinen Zugriff erhalten – der Browser zeigt diese URLs nicht mehr an. Solche Filter arbeiten mit Positiv- und/oder Negativlisten und versuchen außerdem, mit Context-Rating sowie Suchbegriffen die guten von den schlechten Web-Seiten zu trennen. Doch die zugrundeliegenden Techniken sind noch immer nicht ausgereift.

Negativliste: Dabei setzen Eltern Websites etwa mit pornografischem Inhalt auf die

Abzocke: Sexfallen im Internet

Manche Surfer lassen sich von Online-Sexsites bis auf die Unterhose ausplündern. Größtenteils aus Unwissenheit und aus Übereifer gehen sie beim Surfen einen Vertrag ein, ohne sich über die dadurch anfallenden Kosten im Klaren zu sein.

Bei angeblich kostenlosen Erotikangeboten im Internet schaltet mancher Zeitgenosse den Verstand aus. Meist fängt es ganz harmlos an. Auf der Suche nach Informationen surft man durch diverse Seiten im Web. Und manchmal blinken Werbebanner mit leicht bekleideten Damen und locken mit angeblich kostenlosen Bildern und Videos. Irgendwann unterliegt der Surfer seiner Neugier und klickt eines der augenfälligen Banner an. Es folgt eine Begrüßungsseite mit Links zu „Free Pics“, also kostenlosen Vorschaubildern. Mehr Gratisfotos oder Videos soll es nach einer Anmeldung mit den persönlichen Daten im Rahmen einer Probemitgliedschaft geben. Die Folge sind Kosten, die schnell mehrere hundert oder gar tausend Euro betragen können.

Vertragsfalle: Viele Sex-Seiten verlangen einen Adult-Check, bevor man die schlüpfrigen Inhalte wirklich auf den Bildschirm bekommt. Oft wird neben Name und Geburtsdatum auch noch nach der Kreditkartennummer gefragt, angeblich um das Alter zu überprüfen. Manchmal bestätigen Sie mit der Eingabe gleich eine Jahresmitgliedschaft, ohne gesondert darauf hingewiesen zu werden. Nähere Informationen liefert erst ein Blick ins Kleingedruckte der Website.

Premium-Mitgliedschaft: Einige Erotikseiten bieten Interessenten eine teure „Platinum/Gold-Membership“ an, für die es angeblich wesentlich mehr Leistung gibt. Weil die Betreiber von Sex-Seiten ihre Foto- und Videoinhalte untereinander austauschen, sind viele der Bilder und Filmchen an anderer Stelle für weniger Geld oder gar gratis zu bekommen.

Highspeed-Zugang: Lange Ladezeiten für Sex-Inhalte sollen durch die kostenpflichtige Reservierung von Bandbreite der Vergangenheit angehören. Der tatsächliche Tempozugewinn ist in der Regel aber gering.



Sperrliste und machen diese dadurch unzugänglich. Nicht aufgeführte Adressen lassen sich weiterhin problemlos ansurfen. Der Vorteil des Verfahrens: Die Bewegungsfreiheit im Netz wird nur relativ wenig behindert. Allerdings – und das ist der große Nachteil – kann eine Negativliste nie auch nur annähernd komplett sein. Hinzu kommt, dass die Pflege einer solchen Negativliste extrem umständlich ist.

Positivliste: Dabei sind nur diejenigen Web-Adressen, die in der Liste stehen, als Surfziel erlaubt. Der Nachteil liegt darin, dass damit die uneingeschränkte Recherche im Internet nicht mehr möglich ist. Wenn lediglich die Navigation auf einem eng begrenzten Site-Kontingent erwünscht ist, wie das bei jüngeren Kids oft der Fall sein dürfte, ist dieses Verfahren jedoch durchaus sinnvoll.

10. Filtern über Rating-Systeme

Ein weiteres Verfahren, welches das Ansurfen nicht jugendgeeigneter Inhalte verhindern soll, ist Content-Rating. Einige Browser, etwa der Internet Explorer, unterstützen Content-Rating von Haus aus, auch Filterprogramme verwenden das Verfahren zusätzlich zu den Listen. Rating-Systeme basieren auf freiwilliger Selbstkontrolle. Das bedeutet: Jeder Betreiber einer Website kann sein eigenes Angebot beurteilen. Ob er das tut und wenn ja, wie die Bewertung ausfällt, ist seine eigene Entscheidung.

So funktioniert das Rating: Mittels des Standards PICS (Platform for Internet Content Selection, www.w3.org/PICS/) können Website-Betreiber eine Bewertung für ihre Inhalte angeben. Diese Klassifizierung erfolgt durch Online-Formulare anhand von Kriterien wie Gewalt oder Erotik. Die Bewertungsinformationen vermerkt der Web-Anbieter dann in Form von Meta-Tags im Kopf jeder einzelnen Seite. Diese Angaben erkennt der Browser oder die Filter-Software beim Aufruf der Seite und kann so die Seite bei Bedarf sperren. Das Verfahren hat jedoch zwei Grundprobleme: Zum einen bleibt

es natürlich nicht aus, dass Anbieter ihre eigenen Inhalte anders bewerten, als Eltern dies tun würden. Zum anderen sind nur die wenigsten Sites bewertet. Wenn nun ein Filterprogramm nichtbewertete Seiten einfach zulässt, bietet Content-Rating praktisch keinen Schutz mehr. Sperrt es solche Seiten dagegen, dann funktionieren auch viele harmlose Websites nicht mehr.

11. Inhalte Filtern über Suchbegriffe

Die meisten Filterprogramme verfügen deshalb zusätzlich über eine Funktion, die Seiten nach bestimmten Begriffen durchforstet und sie sperrt, wenn einer dieser Begriffe im Seiteninhalt vorkommt.

Beispielsweise lassen sich alle Seiten sperren, die Wörter mit „Sex“ oder „Anal“ enthalten. Auch dieses Verfahren birgt jedoch Probleme, wie folgende zwei Beispiele zeigen: Wird „Sex“ ausgefiltert, kann sich der junge Anwender keine Seiten mehr zum



Erotikinhalt: Filterprogramme mit Rating-Systemen sind unvollständig (Punkt 10)

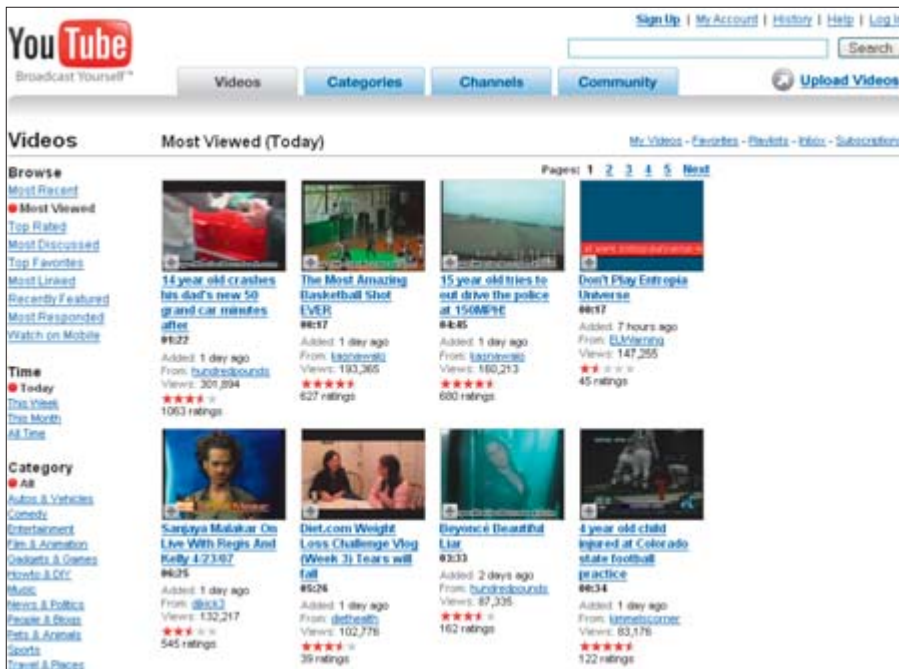
Thema Aids-Prävention oder Sexuaufklärung ansehen. Und da „Kinderkanal“ die Buchstabenfolge „anal“ enthält, könnte ein Filter auch diese Seiten sperren. ❌

IE: Surfen mit dem Inhaltsratgeber

Einen gewissen Schutz vor bedenklichen Websites bietet der Internet Explorer ab Version 6.0 mit seinem Inhaltsratgeber. Damit können Sie Kinder beim Surfen schützen, indem Sie eine Filterfunktion aktivieren oder selbst festlegen, welche Websites der Nutzer des PCs ansehen kann. Über eine Liste mit bestimmten Web-Adressen haben Sie die Möglichkeit, den Zugriff auf Sites gezielt zuzulassen und auf andere zu verhindern. Theoretisch können sich Eltern so das Geld für ein zusätzliches Filterprogramm sparen. Der Haken dabei: Das gilt nur, wenn Sie sich darauf verlassen können, dass Ihr Sprössling den Filtereinsatz zu seinem Schutze auch akzeptiert. Denn schließlich kann er den Inhaltsratgeber auch deaktivieren, etwa mit dem kostenlosen Content Advisor Password Remover (www.nirsoft.net, 6 KB).



Internet Explorer: Der Inhaltsratgeber ist mit Knack-Tools leicht auszuhebeln



Laden Sie, was Sie wünschen!

Auf immer mehr Websites sollen Schutzmechanismen das Speichern von Bildern, Filmen und Songs verhindern. Doch viele der Sperren lassen sich überlisten.

Von **Sebastian Deichsbach**, **Tim Kaufmann** und **Markus Weber**

Per Suchmaschine haben Sie eine interessante Website aufgespürt, deren Inhalte Sie gerne auf Festplatte speichern möchten. Die Seite bietet haufenweise Videos zum Anschauen, aber keine Option zum Download. Oft lassen sich die in Webseiten eingebetteten Videos, Bilder und Musikdateien nicht einfach im Browser herunterladen. Dafür sorgen spezielle Schutzverfahren, mit denen die Betreiber des Servers unerwünschte Downloads verhindern wollen. Bei Youtube, Myvideo & Co. ist die Sperre beispielsweise Standard. Wir zeigen Ihnen, wie das Laden trotzdem klappt.

1. So wandern Online-Videos auf Ihre Festplatte

Video-Inhalte im Netz nehmen stark zu. Grund dafür sind steigende Bandbreiten und nicht zuletzt Video-Portale wie Youtube & Co. Videos anzuschauen macht Spaß – viele Anwender haben aber den Wunsch, besonders gelungene Inhalte dauerhaft auf ihrer Festplatte zu archivieren. Anschließend möchten sie diese vielleicht aufs Handy oder ein anderes portables Abspielgerät kopieren. Manch einer möchte die Videos weiterbearbeiten – sie also etwa schneiden und/oder auf eine DVD brennen.

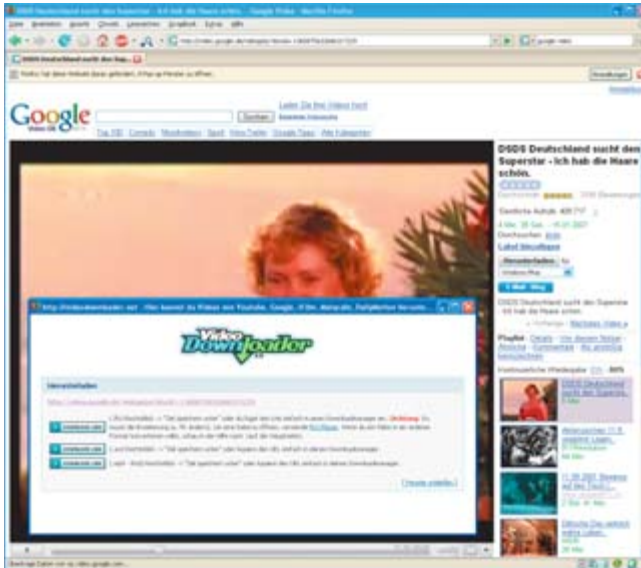
Die meisten Internet-Videodienste bieten aber keine Option, die Inhalte herunterzuladen. Da sie von Werbeeinnahmen leben, ist es ihr Ziel, die Benutzer zum erneuten Anschauen eines Videos wieder auf ihre Webseite zu locken. Mit einigen Tricks ist es dennoch möglich, die Videos auf die Festplatte zu bannen. Verboten ist das nach Ansicht einiger Experten nicht, denn es wird dabei kein technisch wirksamer Kopierschutz im Sinne des Urheberrechtsgesetzes umgangen. Sie dürfen die Videos allerdings ohne Zustimmung des Autors nicht selber öffentlich weiterverbreiten.

Tipp: Um die Filme nach dem Download in ein Format zu konvertieren, das Ihr mobiles Abspielgerät oder Ihr Schnittprogramm unterstützt, verwenden Sie den kostenlosen Dienst **Media-Convert** <http://media-convert.com/konvertieren/>.

2. So klappt es mit dem Internet Explorer

Im Web kursieren haufenweise kostenpflichtige Spezial-Tools, mit denen sich Inhalte von Videoportalen wie Youtube.com, Metacafe.com, Clipfish.de und Myvideo.de herunterladen lassen. Doch keines deckt wirklich alle Dienste ab. Außerdem müssen Sie bei diesen Tools die Videos, die Sie ja bereits komplett angeschaut haben, zum Archivieren erneut herunterladen. Dazu besteht aber gar keine Notwendigkeit, denn bei fast jedem Dienst haben Sie die Videodateien nach dem Anschauen schon auf Ihrer Festplatte liegen, wenn auch an einer schlecht zugänglichen Stelle – nämlich im Zwischenspeicher („Cache“) des Browsers. Im Internet Explorer (IE) ist es ohne weiteres möglich, die Daten aus dem Cache-Speicher herauszuholen. Dazu klicken Sie im Browser auf „Extras, Internetoptionen“, dann auf der Registerkarte „Allgemein“ unter „Temporäre Internetdateien“ (IE 6) beziehungsweise „Browserverlauf“ (IE 7) auf „Einstellungen“.

Überprüfen Sie hier zunächst, ob dem Cache genügend Speicherplatz zugewiesen sind. 100 bis 200 MB sollten es schon sein, damit auch mehrere längere Videos darin Platz finden, ohne gleich wieder automatisch gelöscht zu werden. Viel mehr Speicherplatz ist aber nicht zweckmäßig, da dadurch die Übersichtlichkeit verloren geht. Klicken Sie auf „Dateien anzeigen“, um zum Zwischenspeicher-Verzeichnis zu gelangen.



Video-Downloads: Mit der kostenlosen Erweiterung für Firefox decken Sie den echten Download-Link zur Datei auf (Punkt 4)

Am besten, Sie legen sich ein Lesezeichen für den Ordner an, um sich in Zukunft die Klickorgie zu sparen.

Nun gilt es, die Videos in dem Wust an zwischengespeicherten Web-Seiten und Bildern zu finden. Klicken Sie dazu auf „Ansicht, Details“, um eine sortierbare Listenansicht des Verzeichnisses zu erhalten. Sortieren Sie nun die Liste nach Größe, denn Videos sind typischerweise mehrere MB, Web-Seiten und Internet-Bilder hingegen nur wenige KB groß. Dazu klicken Sie auf die Spaltenüberschrift „Größe“. Wenn daraufhin die kleinsten Dateien oben erscheinen, klicken Sie erneut auf „Größe“, um die Sortierung umzukehren. Der Spalte „Internetadresse“ können Sie entnehmen, von welcher Quelle die Dateien stammen. Haben Sie ein oder mehrere Videos gefunden, markieren Sie diese und klicken auf „Bearbeiten, Kopieren“. Wechseln Sie im Windows Explorer zu einem Ordner, in dem Sie die Dateien ablegen möchten, und wählen Sie „Bearbeiten, Einfügen“.

3. Firefox mit Download-Erweiterung nutzen

Für Firefox stehen gleich mehrere kostenlose Erweiterungen bereit, die den Download von Videos erleichtern. Um in Firefox komfortabel an die zwischengespeicherten Dateien zu kommen, installieren Sie die kostenlose englischsprachige Firefox-Erweiterung **Cacheviewer** (<https://addons.mozilla.org/de/firefox/addon/2489>).

Über „Extras, Cache-Viewer“ starten Sie das Tool, das Ihnen ähnlich wie beim IE die Dateien im Zwischenspeicher in einer Listenansicht anzeigt. Per Klick auf die Spaltenüberschrift „Size“ sortieren Sie nach Größe. Ein Rechtsklick auf einen Eintrag und der Kontextmenü-Befehl „Save as“ kopiert die Datei an einen beliebigen Ort. Der Firefox-Cache ist mit 50 MB etwas knapp bemessen. Über „Extras, Einstellungen, Erweitert, Netzwerk“ lässt sich

die Größe aber ganz individuell anpassen.

4. Weitere Download-Zusätze für Firefox

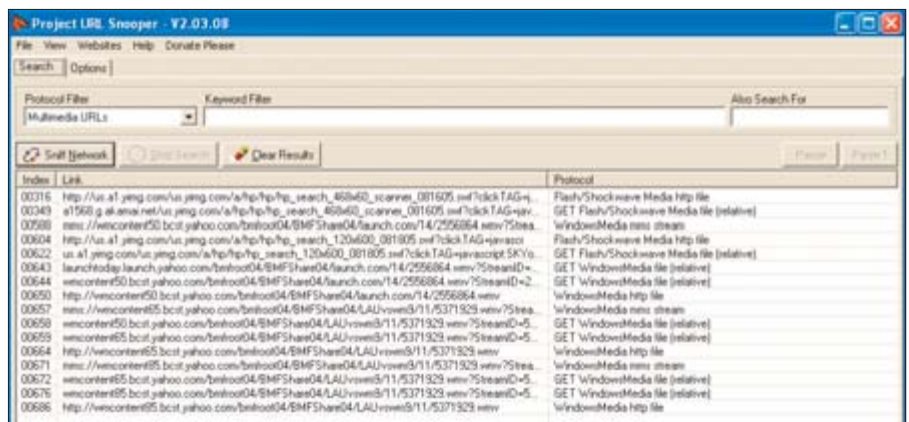
Die Gratis-Erweiterung **Video Downloader** (auf CD und unter www.erweiterungen.de) macht sich nach der Installation über ein kleines Symbol in der rechten unteren Ecke des Firefox-Fensters bemerkbar. Wenn Sie ein Video ansehen und auf dieses Symbol klicken, dann öffnet sich ein Fenster, das Ihnen den Download des Videos ermöglicht. Nachteil von Video Downloader: Das Tool funktioniert nicht mit jeder Video-Website zuverlässig.

Auch den Online-Dienst **Keepvid** können Sie auf Multimedia-Streams ansetzen. Die gleichnamige Erweiterung für Firefox läuft aber nicht mit Version 2.0 des Open-Source-

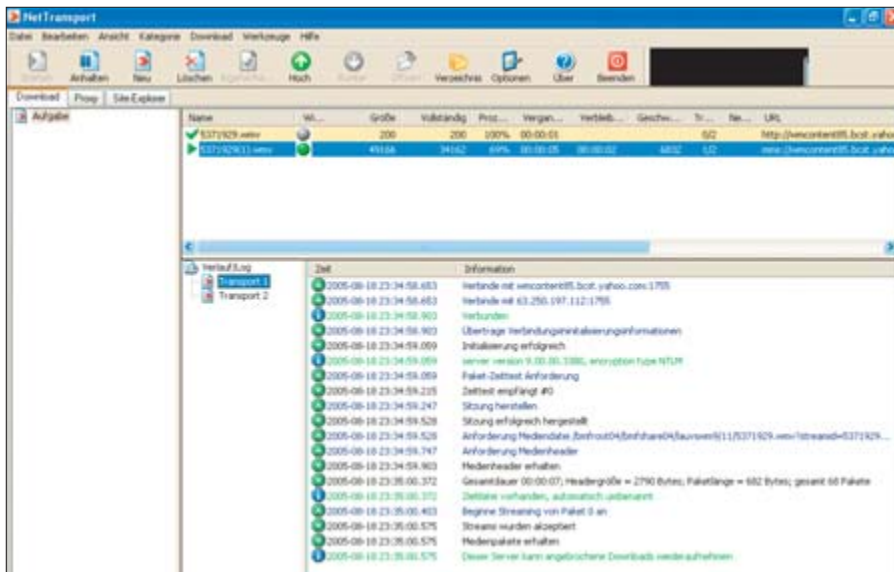
Überblick Download-Sperre

Inhalt	Seite
1. Online-Videos auf Festplatte laden	46
2. Im Internet Explorer	46
3. In Firefox mit Download-Erweiterung	47
4. Weitere Download-Zusätze für Firefox	47
5. FLV-Dateien abspielen	48
6. Nutzen Sie einen URL-Schnüffler	48
7. Adressen abgreifen: So klappt es	49
8. Herunterladen mit Net Transport	49
9. Videos von anderen Quellen laden	49
10. Vom Bildschirm mitschneiden	50
11. Online-Bilder grabben	50
12. So laden Sie die Bilder	51
13. Download beschränken	51
14. Bilder abfotografieren	51
Kästen	
Flashget: Mächtiger Gratis-Downloader	48
Jede Datei abspielen	49
Saugen bis die Leitung platzt	50
Fotos per Offline-Reader	51

Browsers zusammen. Es geht aber auch manuell: Öffnen Sie die Website <http://keepvid.com> in einem zweiten Browser-Fenster. Geben Sie die URL zum Videoclip bei „Download videos...“ ein, und wählen Sie Ihren Videodienst in der Ausklappliste dahinter aus. Sobald Sie auf den Button „Download“ klicken, zeigt der Dienst darunter den direkten Link zum Video an. Klicken Sie ihn mit der rechten Maustaste an und speichern Sie die Datei. Wenn der Download in Firefox



Schnüffelnase: URL Snooper protokolliert, welche Dateien Ihre Abspiel-Software online aufruft, und legt damit die Grundlage für den Download (Punkt 6)



Saugen mit Net Transport: Der Download-Manager eignet sich für das Herunterladen von Videos und Musik im Quicktime-, Real-Media- und Windows-Media-Format (Punkt 8)

nicht funktioniert, kopieren Sie die URL, und fügen Sie sie in den Download-Manager Flashget ein (siehe Kasten unten).

5. FLV-Dateien abspielen

Sowohl für Firefox als auch für den Internet Explorer gilt: Sollte die Dateiendung nicht korrekt sein – speziell bei Youtube kommt

das vor – ergänzen Sie diese in Form von „.flv“. FLV steht für Flash Video und ist das Standardformat der meisten Videoportale. Um FLV-Dateien abspielen zu können, installieren Sie den englischsprachigen **FLV Player 1.3.3** (für Windows 98/ME, 2000 und XP, auf CD und unter www.martijn.de/visser.com, 981 KB) .

Wenn Sie die Videodateien zwischen all den anderen Cache-Dateien nicht finden können, löschen Sie den Zwischenspeicher, bevor Sie das gewünschte Video aufrufen. Das erledigen Sie über „Extras, Internetoptionen, Dateien löschen“ (IE 6) beziehungsweise den Befehl „Extras, Browserverlauf löschen“ (IE 7). In Firefox klicken Sie auf „Extras, Private Daten löschen“.

Die Freeware **Video Lan Client**, kurz VLC (für Windows 98/ME, NT 4, 2000 und XP, Download unter www.videolan.org, 6,21 MB), spielt mit Ausnahme von Realmedia-Dateien so gut wie alle Formate einschließlich FLV und DVD ab, ohne dass Sie zuvor Codecs installieren müssen. Das ist praktisch, wenn Sie keine Codecs installieren wollen oder können.

6. Spionieren: Nutzen Sie einen URL-Schnüffler

Auch wenn Sie statt Streaming-Video eine konventionelle Web-Videodatei herunterladen möchten, beginnt der Vorgang mit dem Aufruf einer URL, also einer Internet-Adresse, etwa `rtsp://videos.<meine-domain>.de/2342333.rm?streamid=1;seq=0;rtptime=0`. Wenn Sie die URL einer auf einer Website verlinkten Videodatei kennen, dann können

Flashget: Mächtiger Gratis-Downloader

Flashget 1.82 beschleunigt Ihre Downloads. Der Download-Manager (auf CD und unter www.flashget.com, 3,07 MB) macht die Übertragung von Dateien aus dem Internet schneller, indem er verschiedene Teile einer Datei parallel herunterlädt, um sie anschließend wieder zum Original zusammenzusetzen. Das Tool für Windows 95/98/ME, NT 4, 2000 sowie XP findet sogar Mirror-Server, die eine Kopie der Datei vorhalten, und kann Daten so aus mehreren Quellen gleichzeitig ziehen.

Flashget sticht deutlich aus der Masse hervor – das Tool beherrscht nämlich auch Streaming-Formate und bietet einen Site-Explorer: Nach Eingabe einer FTP- oder HTTP-Adresse zeigt die Freeware den Inhalt der Homepage oder des Servers an. Wie in einem FTP-Client sehen Sie die Inhalte des Servers auf Link- und Dateiebene. Dabei legt das Tool vieles offen, was die Betreiber von Servern eigentlich verstecken müssten.

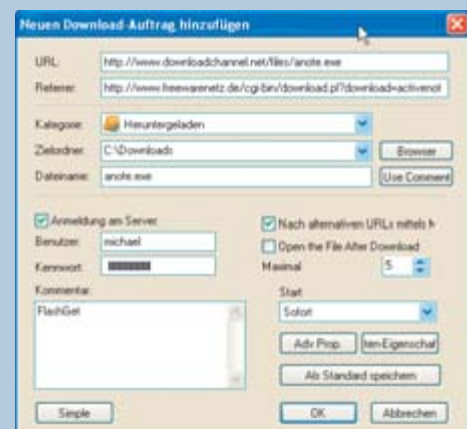
Downloads durchführen: Flashget integriert sich in den Internet Explorer und springt an, sobald Sie auf einen Link klicken, der zu einem Download führt. Neben Dateien von Web- und FTP-Servern lädt das Tool BitTorrent-URLs. Geben Sie das gewünschte Zielverzeichnis an und bestätigen mit „OK“. Nun beginnt Flashget mit dem Herunterladen der Datei. Um eine Datei später zu laden oder Anmeldedaten wie Benutzername und Passwort für eine Website einzugeben, klicken Sie auf „Advanced“.

Seiten durchsuchen: Geben Sie in die Adresszeile die URL des Servers ein, den Sie durchsuchen möchten. Daraufhin zeigt Flashget eine Übersicht

aller Musikstücke, Fotos und Videoobjekte an. Markieren Sie die Inhalte, die Sie auf Ihrer Platte speichern möchten. Flashget sichert die gewählten Dateien dann automatisch in den Download-Ordner. Praktisch: Für den Transfer startet das Utility mehrere gleichzeitige Dateianfragen

an den Download-Server und erzielt durch die Bündelung fast immer die Höchststraten, die Ihre Internet-Verbindung zulässt.

Tricks: Die Streaming-Formate MMS (Microsoft Media Services) und RTSP (Real Time Streaming Protocol) werden von Flashget wie herkömmliche Datei-Links verarbeitet. Damit ist die Freeware in der Lage, auch Video-Streams zu saugen und zur Archivierung auf der Festplatte zu speichern.



Dateien saugen: Flashget kommt auch mit eingebetteten Dateien zurecht

Sie diese auch fast immer herunterladen. Auf der Jagd nach Video-URLs studieren Anwender oftmals sogar den Quelltext von Video-Webseiten, quasi den Programmcode, aus dem die einzelnen Seiten bestehen. Das ist mühsam, zeitraubend und führt bei vielen Sites nicht einmal Profis mit vertretbarem Aufwand zum Ziel.

Eleganter ist deshalb der Ansatz der Freeware **URL-Snooper** (Version 2.18 für Windows 95/98/ME, 2000 und XP, auf CD und unter www.donationcoder.com/Software/Mouser, 1,8 MB). Sie nimmt sämtlichen Datenverkehr unter die Lupe, der über die Internet-Leitung fließt, und filtert alle Multimedia-URLs heraus, die eines der auf Ihrem PC installierten Programme aufruft. Diese Adressen können Sie auf einfachem Weg in einen Download-Manager kopieren und die Dateien so herunterladen.

7. Adressen abgreifen: So klappt es

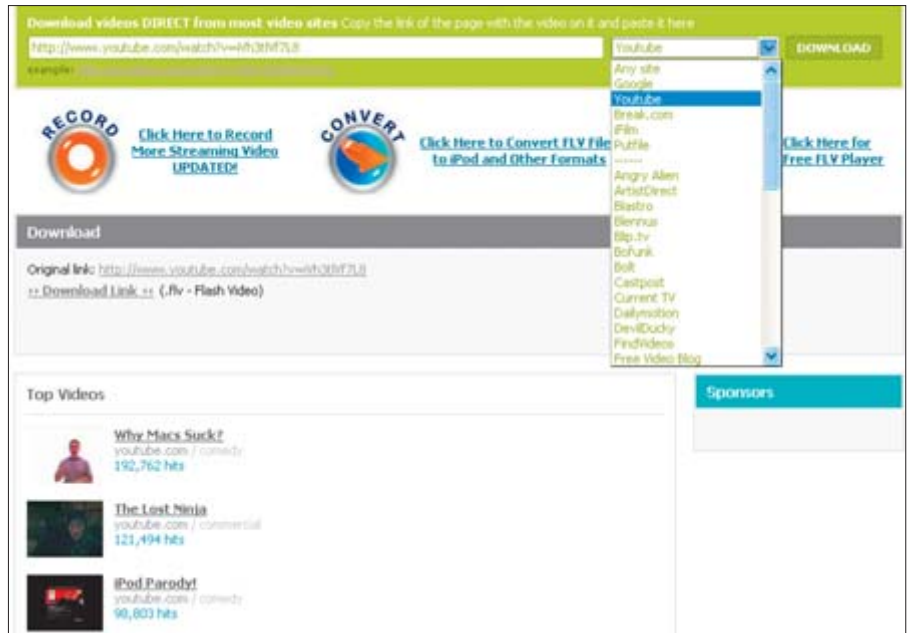
Starten Sie URL-Snooper, und wählen Sie unter „Options, Network Adapter“ die Netzwerkkarte aus, über die Sie mit dem Internet verbunden sind. Wenn Sie über eine Einwahl-Verbindung online gehen, stellen Sie „Generic NdisWan adapter“ ein. Wechseln Sie zurück auf den Reiter „Search“, und klicken Sie auf „Sniff Network“, um das Tool auf Ihre Daten anzusetzen.

Zurück im Browser laden Sie die Website, die das gewünschte Video enthält, und klicken auf den zugehörigen Link. Behalten Sie dabei URL-Snooper im Auge. Wenn alles funktioniert, tauchen bald die ersten URLs im Programmfenster auf. Es ist nicht ungewöhnlich, dass das Tool auch bei nur einem Video gleich mehrere Adressen auswirft. Meistens führt die erste oder die letzte vor dem Abspielen aufgerufene URL zum Ziel. Sobald das Video läuft, können Sie URL-Snooper mit „Stop Search“ anhalten.

Tipp: Stellen Sie „Protocol Filter“ auf „Show All“, und geben Sie in das „Keyword Filter“-Feld etwa „JPG“ an, dann zeigt URL-Snooper sämtliche URLs heruntergeladener Bilder im JPG-Format an – auch eine Möglichkeit, an Fotos zu gelangen.

8. Filme: Herunterladen mit Net Transport

Die Shareware **Net Transport** eignet sich perfekt für Multimedia-Downloads, denn sie versteht nicht nur das HTTP-Protokoll, son-



Videos laden: Geben Sie die URL in das Eingabefeld ein, und wählen Sie die Quell-Website aus, dann zeigt der Dienst den Download-Link an (Punkt 4)

dern auch das von Real und Microsoft verwendete RTSP (Real Time Streaming Protokoll) und MMS (Microsoft Media Services). Die kostenlose Demoversion arbeitet mit unbegrenzter Laufzeit, so dass Sie sie in Ruhe ausprobieren können (Version 2,30 für Windows 95/98/ME, 2000, XP und Vista, auf CD und unter www.xi-soft.com, 1,6 MB, 25 US-Dollar).

Nach dem Start des Tools klicken Sie auf „Neu“ und fügen die URL aus URL-Snooper in das „URL“-Feld ein. Unter „Ziel“ wählen Sie einen Speicherort für Ihre Datei aus, tragen ein eventuell notwendiges Login rechts oben bei „Authentifizierung“ ein und klicken

auf „OK“. Daraufhin macht sich Net Transport an die Arbeit, und kurz darauf finden Sie die fertige Datei auf Ihrer Festplatte.

9. Videos von anderen Quellen herunterladen

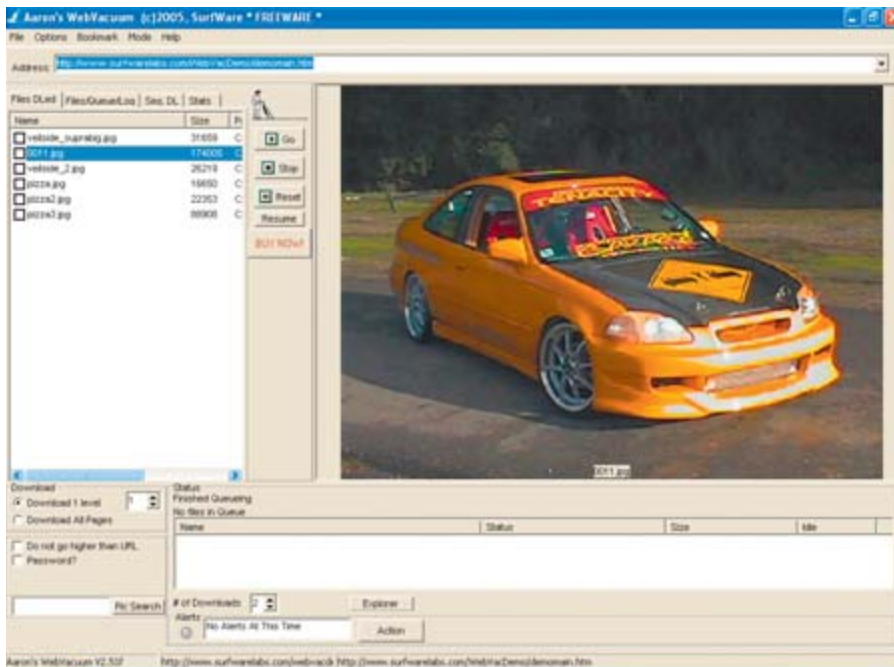
Die großen Videoportale verwenden nahezu alle das Flash-Video-Format als „progressive Download“. Ein Video wird dabei immer als ganze Datei übertragen, die sich schon während des Ladens abspielen lässt. Im Gegensatz dazu verwenden viele konventionelle Websites die Streaming-Technologie. Dabei überträgt der Server nicht die komplette Videodatei, sondern immer nur

So klappt's: Jede Datei abspielen

Im Idealfall sollte ein Doppelklick auf eine Video- oder Audiodatei dazu führen, dass eine Anwendung das Video oder den Sound wiedergibt. Damit die Wiedergabe funktioniert, brauchen Sie für jede Video- und Audiodatei den richtigen Codec. Wer im Web nicht nach einzelnen Codecs suchen, sondern lieber auf einen Schlag alle wichtigen Codecs einrichten möchte, greift zu einem Codec-Pack, etwa von www.xpcodecpack.com (5,83 MB). Damit installieren Sie gleichzeitig viele verschiedene Codecs, ohne sich selbst um die Details kümmern zu müssen. Egal welches Audio- oder Videoformat – gute Codec-Packs kennen sie fast alle.

Vorsicht Falle: Oft ist der Inhalt eines Codec-Packs zumindest teilweise veraltet, und Windows wird häufig mit unnützen Codecs zugemüllt, die Sie gar nicht benötigen. Außerdem überschreiben manche Pakete ohne Rückfrage bereits vorhandene Codecs.

Raubkopieralarm: Manche Ersteller von Codec-Paketen halten sich nicht an das Urheberrecht und nehmen auch lizenzpflichtige Codecs in ihre Archive auf. Sie als Anwender können nicht erkennen, ob raubkodierte Codecs enthalten sind.



Bilder systematisch absaugen: Die Shareware Web Vacuum durchsucht Server und lädt Grafikdateien aus dem Web automatisch auf die Festplatte (Punkt 11)

den Teil, der gerade abgespielt wird. Ein komplettes Zwischenspeichern findet dabei nicht statt, daher greift der Cache-Trick hier ins Leere.

Sofern die Website das Windows-Media-Format einsetzt, können Sie sich mit dem englischsprachigen Tool **WM Recorder** behelfen, um die Inhalte aufzuzeichnen. In der Regel ist auf den Websites angegeben, welches Videoformat eingesetzt wird.

WM Recorder ist seit Version 9.0 kostenpflichtig (Version 11.3 auf CD und unter www.wmrecorder.com). Für unsere Zwecke ist die kostenlose Version 8.0 ausreichend, die weiterhin im Web kursiert.

10. Videoausgabe vom Bildschirm mitschneiden

In hartnäckigen Fällen kommen Sie durch das Mitschneiden des Videos mit **Hypercam**

2.14 (für Win 95/98/ME, NT 4, 2000 und XP, auf CD und unter www.hyperionics.com) ans Ziel: Installieren Sie das Tool, und starten Sie das Video. In Hypercam klicken Sie in auf „Start Rec.“, um den Mitschnitt zu beginnen. Am Ende der Wiedergabe drücken Sie die <F2>-Taste, um die Aufnahme zu beenden. Behalten Sie die Angaben bei „Total frames“ (Einzelbilder gesamt) und „Skipped“ (Verlorene Bilder) im Blick. Gingen Bilder verloren, reduzieren Sie den Wert bei „Rate in Frames“ und probieren die Aufnahme erneut. Hypercam-Aufnahmen können Sie beispielsweise mit dem Windows Media Player abspielen. Erscheint dabei nur ein blaues, grünes oder schwarzes Bild, deaktivieren Sie die Windows-Hardware-Beschleunigung. Dazu verschieben Sie den Regler unter „Start, Systemsteuerung, Anzeige, Einstellungen, Erweitert, Problembehandlung“ auf die zweite Position von links. Starten Sie Hypercam und den Browser neu, und wiederholen Sie die Aufnahme. Vergessen Sie nicht, die Hardware-Beschleunigung später wieder zurückzustellen.

11. Online-Bilder mit Web Vacuum grabben

Die Freeware-Variante von **Web Vacuum** eignet sich für Bilder-Sammler, die es nicht allzu eilig haben (Version 2.72 für Win 98/ME, NT 4, 2000, XP, auf CD und unter www.surfwarelabs.com, 1,41 MB). Gegenüber der knapp 30 US-Dollar teuren Profi-

Down Them All: Saugen bis die Leitung platzt

Die Gratis-Erweiterung Down Them All für Firefox sorgt für eine optimale Auslastung der Internet-Bandbreite und flotte Downloads. Die Extension (auf CD) erweitert den Browser um viele neue Funktionen, inklusive Beschleuniger für Downloads. Das kostenlose Modul installieren Sie von CD oder über die Website www.downthemall.net. Down Them All besteht aus drei Teilen: Den eigentlichen Download-Manager finden Sie unter „Extras, dTa!-Manager“, die Link-Anzeige mit den Download-Verweisen der aktuellen Web-Seite öffnen Sie mit „Extras, DownThemAll!“ und die 1-Klick-Ladefunktion mit „Extras, dTaOneClick“. Zusätzlich integriert sich die Erweiterung in das Download-Fenster des Browsers und in das Kontextmenü von Datei-Links.

So laden Sie Dateien: Sobald Sie einen Download-Link anklicken und bei „Wie soll Firefox mit dieser Datei verfahren?“ die Option „DownThemAll!“ wählen, wird das Download-Tool aktiv. Es erscheint ein Fenster, in dem Sie den gewünschten Zielpfad auswählen und den Dateinamen bestätigen. Praktisch: Ist die Datei schon vorhanden, meldet sich die Software und bietet eine automatische Umbenennung an.

Eingebettete Datei laden: Eine Übersicht aller Download-Links einer Seite rufen Sie mit „Extras, DownThemAll!“ auf. Firefox öffnet ein Fenster, das Objekte wie Videos, Bilder und Dateiverweise zeigt. Mit einem Klick nehmen Sie die gewünschten Dateien in die Transferliste auf.

Download-Management: Das Statusfenster („dTa!-Manager“) listet alle laufenden oder geplanten Downloads zusammen mit dem Datendurchsatz auf. Die Einträge lassen sich sortieren, bearbeiten und löschen.

Extra: Praktisch ist die Booster-Funktion: Damit fordert die Software eine Datei simultan von mehreren Download-Servern an.



Down Them All: Die Firefox-Extension erkennt Dateinamenskonflikte bei Laden

Version ist sie nämlich insofern eingeschränkt, als sie nach den ersten 30 Bildern vor dem Download jeder weiteren Datei eine Pause von fünf Sekunden einlegt. So bringt Web Vacuum es kaum auf mehr als 300 oder 400 Bilder pro Stunde. Von dieser Einschränkung abgesehen gefällt Web Vacuum durch sein gradliniges Bedienkonzept. Nach dem Programmstart geben Sie die Start-Adresse in das Feld hinter „Address“ ein und drücken auf „Go“. Prompt macht sich das Programm an die Arbeit und speichert die verlinkten Bilder auf die Festplatte. Längere Download-Vorgänge können Sie mit „Stop“ unterbrechen und mit „Resume“ fortsetzen.

In der Grundeinstellung durchsucht Web Vacuum nur eine Ebene (englisch „level“), also nur die unter der Startadresse abgelegte Seite selbst. Möchten Sie auch die mit dieser Seite verlinkten Seiten durchforschen, verändern Sie den Wert hinter „Download 1 level“ links unten im Programmfenster auf „2“. Tragen Sie eine „3“ ein, dann durchforstet Web Vacuum auch mit den Unterseiten verlinkte Seiten und so weiter.

Setzt der Zugriff auf die Bilder-Website einen Benutzernamen und ein Passwort voraus, dann aktivieren Sie auch „Password“ und geben die zugehörigen Daten in den daraufhin erscheinenden Feldern ein.

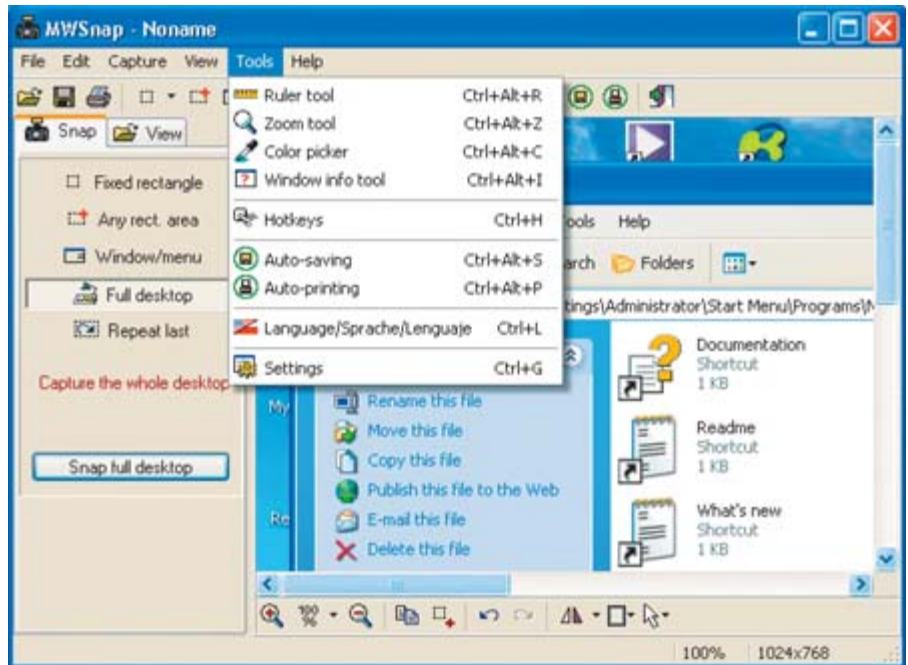
12. So laden Sie die Bilder

Unter „Options, Show Options Window, Extensions“ führt Web Vacuum die Endungen der Dateien auf, die es lädt. Vorgegeben sind hier neben Bildformaten wie JPG und GIF auch verschiedene Audio- und Videodateitypen, ZIP-Archive und ausführbare EXE-Dateien. Bilderfreunde halten diese zuweilen sehr umfangreichen Downloads nur auf. Sie sollten diese Dateitypen deshalb entfernen, in dem Sie sie einzeln markieren und jeweils auf „Remove Ext.“ klicken.

13. Download beschränken

Wichtig ist das Häkchen vor „Don't download files smaller than 10K“. Ist es gesetzt, lädt Web Vacuum nur Dateien mit einer Mindestgröße von 10 KB herunter.

Das ist praktisch, wenn Sie den Download auf hochqualitative Fotos beschränken und kleine Vorschaugrafiken ausschließen möchten. Schieben Sie den Regler unterhalb von „Don't download“ nach rechts, um die



Hintertür für Fotojäger: Mit dem kostenlosen Tool MW-Snap fotografieren Sie Fotos auf Websites vom Desktop ab. So wird jedes Foto zum Download (Punkt 14)

Vorgabe für die Mindestgröße zu erhöhen. An fortgeschrittene Anwender richten sich die Filter-Funktionen, die Sie über drei Registerkarten rechts oben im „Options“-Fenster erreichen. Mit Filtern können Sie Dateien gezielt vom Download ausnehmen („- File Filter“) oder hinzufügen („+ File Filter“). Dabei ersetzt der das „?“-Zeichen ein einzelnes und „*“ mehrere Zeichen.

14. Bilder abfotografieren

Eine ganz einfache Möglichkeit, Fotos von Websites lokal auf Festplatte zu speichern ist, die betreffende Seite mit einem Tool wie der Freeware **MW-Snap** zu fotografieren (Version 3.0 für Windows 95/98/ME, NT 4, 2000 und XP, auf CD und unter www.mirekw.com, 0,7 MB). Nach dem Programmstart macht sich das Tool mit einem Kamera-Symbol im Systray bemerkbar.

Klicken Sie das Icon mit der rechten Maustaste an, um einen Blick auf die verschiedenen Screenshot-Funktionen und die zugehörigen Tastenkombinationen zu erhalten. Das Programm kann Fotos vom ganzen Bildschirm, einem einzelnen Programmfenster, einem beliebigen Bereich oder einem Rechteck fester Größe erzeugen.

Um gezielt ein Bild aus einer Website abzufotografieren, drücken Sie die Tastenkombination <Shift>-<Strg>-<A>. Um den Bildausschnitt festzulegen, klicken Sie an der oberen linken und anschließend an der unteren rechten Ecke des zu fotografierenden Bildes. Eine Bildschirmlupe hilft Ihnen bei jedem dieser Schritte beim genauen Positionieren des Cursors. Bestätigen Sie abschließend <Return>. Dann öffnet sich das Tool mit dem Screenshot, und Sie können ihn speichern. 

HT-Track: Fotos per Offline-Reader

Wenn Sie mehr als nur ein paar Fotos auf die Platte ziehen möchten, ist der manuelle Download zu umständlich. Ambitionierte Fotosammler automatisieren ihre Arbeit mit einem Offline-Grabber. In ein solches Programm geben Sie lediglich eine Web-Adresse als Ausgangspunkt ein. Die Software übernimmt dann den vollautomatischen Download dieser Startseite und der damit verlinkten anderen Seiten – inklusive der zugehörigen Grafiken, Sound- und Videodateien. Empfehlenswert ist die Freeware **HT-Track 3.41-2** (für Windows 98/98/ME, 2000, XP und Vista, auf CD und unter www.httrack.com, 3,4 MB).



Alles knacken

Einen Kopierschutz zu umgehen ist hierzulande verboten. Trotzdem finden sich im Internet ständig neue Tools und Anleitungen, um den Schutz für Musik, DVDs oder Spiele auszuhebeln. Wir zeigen, wie es ganz legal geht.

Von **Margrit Kuther** und **Claudius Wirt**

Sie schmökern gemütlich in einer Buchhandlung und finden einen interessanten Roman. Beim Bezahlen an der Kasse weist Sie der Verkäufer darauf hin, dass Sie dieses Buch erst nach 22 Uhr lesen dürfen, und zwar nur mit einer Leselampe, die der Verlag empfiehlt.

Unverschämt, finden Sie? Kaum anders gehen Online-Anbieter von Musik und Videos vor: Sie schützen Songs und Filme per DRM (Digital Rights Management) gegen unerlaubte Kopien. Und schreiben Ihnen dabei vor, was Sie mit den gekauften Dateien machen und mit welchen Geräten Sie sie abspielen dürfen. Diese Einschränkungen sind

nicht nur Crackern ein Dorn im Auge. Im Internet kursieren Tools, mit denen sich der DRM-Schutz entfernen lässt – wenn man den entsprechenden Song oder Film zuerst legal erworben hat. Dennoch ist der Einsatz dieser Knack-Tools verboten – folglich verschwinden sie auch rasch wieder von den entsprechenden Sites. Außerdem feilen die Anbieter ständig am DRM-Schutz: Tool-Entwickler und Cracker befinden sich in einem ständigen Wettlauf.

Die DRM-Einschränkungen stören Sie, aber Sie wollen sich deshalb nicht auf rechtlich unsicheres Terrain begeben? Wir stellen Ihnen legale Methoden vor, mit denen Sie

Musik- und Videodateien problemlos von der Kopierschutzbeschränkung befreien: Das funktioniert meist sehr bequem mit kostenlosen Tools oder Shareware.

Ein Qualitätsunterschied zum Original lässt sich oft kaum feststellen. Auch Video-DVDs können Sie auf legale Weise kopieren – wie es geht, verraten wir Ihnen ebenfalls.

Weit entwickelt ist der Kopierschutz von Spielen: Schutzmechanismen lassen sich kaum mehr umgehen. Aber die Cracker-Community, die sich in einschlägigen Web-Foren versammelt, lässt nichts unversucht, auch einen scheinbar unverletzlichen Kopierschutz aufzuweichen.



Überblick Kopierschutzpraxis

Inhalt	Seite
1. Hacker-Tools knacken DRM	53
2. Digitaler Kopierschutz am Ende	53
3. Cracker gegen DRM-Schutz	54
4. DRM-Sperre legal löschen	54
5. WMA-Schutz legal entfernen	55
6. WMA-Entdongelung ohne Rohling	55
7. Blitzkopie mit Tunebite	56
8. Jeden Film legal kopieren	56
9. Filme mitschneiden	57
10. Qualitätsunterschiede beim Grabben	57
Kästen	
DRM im Überblick	54
Direktaufnahme per Soundkarte	55
Brennlücke nutzen	56
High-End-Analog-Kopie	57

1. Schwacher Schutz: Hacker-Tools knacken DRM

Musikportale im Internet bieten perfektes Home-Shopping für einzelne Songs und ganze Alben. Das Runterladen von Lieblings-Hits ist bequem, schnell und gar nicht so teuer. Die Theorie klingt wunderbar: Diverse Musikstücke im Internet kaufen, überall abspielen und auf CDs brennen. In der Realität ist es hingegen so, dass der Käufer mit seinen Liedern nicht zwangsläufig machen kann, was er möchte. Der wachsenden Popularität zum Trotz haftet Musikportalen dadurch der Ruf der Anwender-Gängelung an. Was für die Musik-CD der Kopierschutz, ist beim online gekauften Song das Digital Rights Management (DRM): Beide sollen die Inhalte sichern – nerven aber vor allem den Anwender.

Bei DRM wird jeder heruntergeladene Song mit einem anwenderspezifischen Schlüssel gesichert. Wichtigster Kritikpunkt sind unterschiedliche Methoden beim digitalen Rechtemanagement, die jedem Song anhaftet. Sie regeln, wie der Käufer mit der Datei weiterverfahre kann. Oft merkt der Nutzer

erst nach dem Laden, dass er die bezahlten Titel gar nicht auf seinem MP3-Player anhören kann.

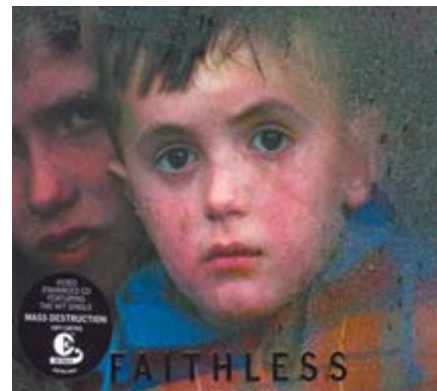
2. Digitaler Kopierschutz für Musik am Ende

Im Internet gibt es Tools, mit denen sich der DRM-Schutz von Musikdateien nachträglich entfernen lässt. Bereits kurz nach dem Start von Apples iTunes Music Store war ein Programm im Web und in Newsgroups zu haben, das den DRM-Schutz aushebelte. Es nutzte den Benutzernamen und das Passwort vom Music-Store-Server, decodierte mit Hilfe des persönlichen Nutzerschlüssels die auf Festplatte gespeicherten Songdateien und entfernte den DRM-Schutz. Die meisten der Programme funktionieren nur, wenn der Anwender auf die passenden Nutzerschlüssel zugreifen kann: Den DRM-Schutz können Sie also nur entfernen, wenn Sie vorher die entsprechenden Titel im Online-Shop gekauft haben. Anders als beim Kopieren auf CD und dem anschließenden Umwandeln (siehe Punkt 4) geht das Entfernen des DRM-Schutzes mit diesen Tools

nicht auf Kosten der Tonqualität: Sie spalten die DRM-Infos praktisch von den Audio-dateien ab – zurück bleibt das ursprünglich codierte Audiomaterial.

3. Wettlauf: Cracker gegen DRM-Schutz

Mit jeder neuen Version von iTunes kann Apple den DRM-Schutz der Kaufmusik verändern. Dadurch funktionieren Anti-DRM-Tools nicht mit der jeweils neuesten Version



Nerven: DRM samt Kopierschutz von Audio-CDs gängeln den Käufer (Punkt 2)



Entdangeln: Kopiergeschützte Songs im WMA-Format lassen sich ohne Kopierschutz im MP3-Format speichern (Punkt 5)

der Abspiel-Software von Apple. Zwar müssen Sie iTunes nicht automatisch aktualisieren. Allerdings bringen neue Versionen nicht nur veränderte DRM-Funktionen, sondern auch neue Angebote, die sich mit älteren Versionen nicht nutzen lassen. Wer iTunes nicht aktualisiert, um Anti-DRM-Tools weiter nutzen zu können, verzichtet eventuell auf nützliche Zusatzfunktionen der Apple-Software. Auch Microsoft verändert mit jeder neuen Version des Abspielpro-

gramms Windows Media Player die DRM-Bibliotheken. Bei Windows Vista hat Microsoft das digitale Rechte-Management sogar direkt ins Betriebssystem integriert. Die Entwickler der Anti-DRM-Tools liefern sich also einen ständigen Wettlauf mit den DRM-Machern: Die einen nehmen die jeweils aktuelle DRM-Version auseinander, um nachzuvollziehen, was der Hersteller beim Schutz verändert hat. Die anderen ergänzen ihre Kopiersperren um zusätzliche Funktionen.

4. DRM-Sperre legal löschen

Online gekaufte Musik lässt sich ganz legal vom DRM-Kopierschutz trennen: Brennen Sie die heruntergeladenen Songs in der gewünschten Reihenfolge einfach als Audio-CD und wandeln sie dann ins MP3-Format um. Durchs Konvertieren geht der DRM-Schutz verloren. Allerdings leidet auch die Tonqualität unter dem zweimaligen Umwandeln – vom geschützten M4P- oder WMA-Format zu WAV-Dateien und dann ins kom-

primierte MP3-Format. Lieder aus dem iTunes-Store (Datei-Endung: M4P) müssen Sie mit iTunes brennen – übliche Brennprogramme wie Nero Burning ROM unterstützen das M4P-Format mit DRM nicht. Zum Brennen erstellen Sie in iTunes zunächst eine Wiedergabeliste („Datei, Neue Wiedergabeliste“) mit den geschützten Songs – diese Liste kann auch ungeschützte Lieder enthalten. Gehen Sie dann zu „Bearbeiten, Einstellungen, Erweitert, Brennen“ und wählen „Audio-CD“ als Format. Zwar bietet iTunes auch „MP3-CD“ als Zielformat an, doch das Brennen DRM-geschützter Songs in diesem Format verweigert das Programm mit einer Fehlermeldung.

Tipp: Um Rohlinge zu sparen, wählen Sie zum Brennen eine CD-RW, die sich wieder löschen lässt – etwa in Nero Burning ROM über „Rekorder, Re-Writable Disk löschen“. Nach dem Ende des Brennvorgangs zeigt iTunes die Audio-CD links im Auswahl-Menü mit einem CD-Icon an. Stellen Sie nun unter „Bearbeiten, Einstellungen, Erweitert, Importieren, Importieren mit“ den „MP3-Codierer“ ein. In der Option darunter wählen Sie die Bit-Rate, mit der das Codieren erfolgen soll. Anschließend importieren Sie mit einem Klick auf die entsprechende Schaltfläche rechts oben die Lieder in Ihre Musikbibliothek. Nach dem Umwandeln sind die Songs DRM-frei.

Überzeugen Sie sich: Wenn Sie einen Rechtsklick auf einen der importierten Songs ausführen, weist sich dieser unter

Hemmschuh: DRM-Verfahren im Überblick

Der Begriff Digital Rights Management (DRM) fasst verschiedene Methoden zusammen, die digitale Inhalte vor unerlaubtem Kopieren schützen sollen. Vor allem im Zusammenhang mit Musikdateien ist DRM verbreitet.

Funktionsweise: DRM-Systeme stellen sicher, dass Sie den digitalen Inhalt nicht entschlüsseln und nur mit der entsprechenden Lizenz darauf zugreifen können. Wenn die Lizenz an den PC gebunden ist, verhindert DRM, dass Sie geschützte Inhalte auf einem anderen PC ohne Lizenz abspielen können. Im Vergleich zu herkömmlichen Seriennummern oder Registriercodes verwenden DRM-Systeme eine komplizierte Technik.

DRM besteht aus zwei Komponenten: Der eigentlichen Audiodatei in verschlüsselter Form und der Lizenz. Die Lizenz wird beim Kauf überspielt und enthält den Schlüssel, der den Titel temporär fürs Abspielen oder Brennen freischaltet. Damit das funktioniert, muss die Abspiel-Software das jeweilige DRM-Verfahren unterstützen. Die meisten Online-Musikkläden setzen auf Microsoft-DRM, das der Windows Media Player unterstützt. Der Player sorgt dafür, dass die Vorgaben in der Lizenz eingehalten wer-

den, indem er die Anzahl der Brenn- und Kopiervorgänge für den Titel zählt. Ist das Limit überschritten, verweigert er weitere Kopien. Wenn Sie bei einem Download-Shop einen Titel zum Kauf auswählen, zeigt Ihnen der Dienst an, wie oft sie den Song brennen und auf DRM-konforme Musik-Player übertragen dürfen. Häufig gilt: zehnmal brennen und bis zu 25-mal übertragen.

Mehrere Standards: Es gibt kein einheitliches DRM-Verfahren, sondern mehrere Systeme, die zueinander nicht kompatibel und die mit einem bestimmten Dateiformat verknüpft sind, beispielsweise AAC und WMA. Von Microsoft stammt das WMA-Format. Der Software-Riese bietet sowohl DRM-Server wie auch den DRM-fähigen Windows Media Player für dieses Format an.

Auch Apple und Real Networks kämpfen mit dem AAC-Format (Advanced Audio Coding) um die Vorherrschaft. Darüber hinaus bietet die Fraunhofer-Gesellschaft ein DRM-Verfahren für spezielle MP3-Dateien mit eingebautem DRM an. Die Wiedergabe erfordert aber einen speziellen Player.

„Informationen, Zusammenfassung, Art“ als „MPEG-Audiodatei“ aus. Bei den mittels DRM geschützten Titeln steht dagegen „Geschützte AAC-Datei“.

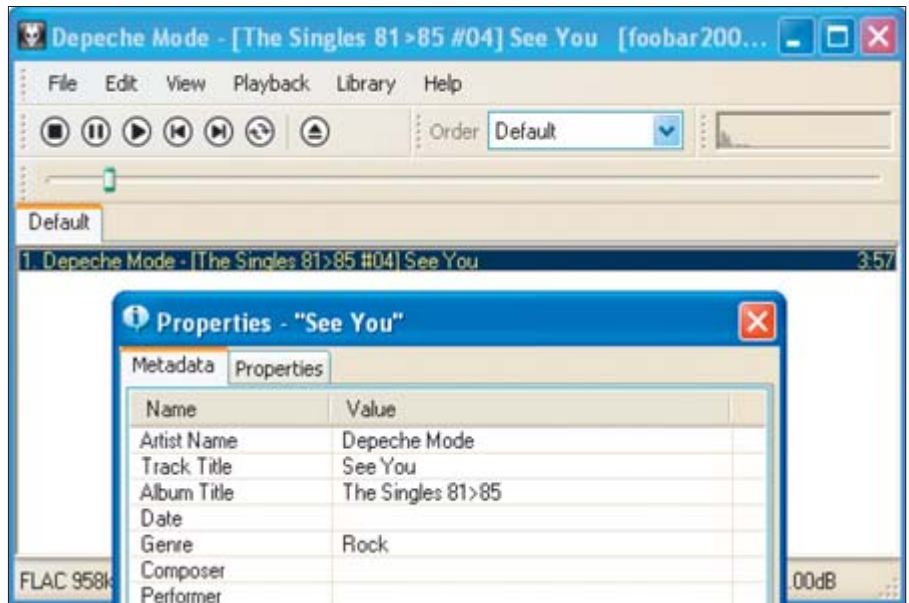
5. Schutz von WMA-Dateien legal entfernen

Auf ähnliche Weise wie iTunes-Songs lassen sich auch Musikstücke umwandeln, die per Microsoft-DRM geschützt sind (Datei-Endung: WMA): Unter anderem bei www.musicload.de kaufen Sie Songs im Windows-Media-Audio-Format, die mit DRM-Kopierschutz versehen sind.

Im Windows Media Player 9 gehen Sie zu „Datei, Kopieren, Auf Audio-CD kopieren“, im Media Player 10 zu „Datei, CDs und Geräte, Audio-CD brennen“. Im Media Player 11 verwenden Sie den „Brennen“-Button.

Dann erstellen Sie jeweils eine Wiedergabeliste mit den gewünschten Songs, die Sie anschließend per „Brennen starten“ auf CD bannen. Eventuell müssen Sie fürs Brennen mit dem Windows Media Player 9 oder 10 noch das Nero-Plug-in Fast CD-Burning nachinstallieren. Zum Brennen einer Audio-CD mit WMA-Liedern eignen sich neben dem Windows Media Player auch die Standard-Brennprogramme Nero 7 Premium Reloaded und Win on CD.

Nachdem Sie die CD gebrannt haben, wandeln Sie die Songs ins MP3-Format um. Falls Sie iTunes verwenden, geht das über „CD importieren“, in anderen Programmen funktioniert es ähnlich. Wenn Sie die Originaldatei im Windows Media Player öffnen, kön-



Verlustfrei aufnehmen: Abhängig vom gewählten Dateiformat und den Aufnahme-Einstellungen kommt es beim Encoden nicht zum Verlust von Toninformationen (Punkt 6)

nen Sie unter dem Punkt „Datei, Eigenschaften, Lizenz“ sehen, wie oft die Datei noch gebrannt werden kann.

6. Schnelle WMA-Entdongelung ohne Rohling

Mit Zusatz-Tools können Sie bei geschützter WMA-Musik ganz auf einen Rohling verzichten. Dazu wählen Sie im Brenn-Menü des Windows Media Player im Drop-down-Menü auf der rechten Seite das „Nero Fast CD-Burning“-Plug-in aus. Nach einem Klick auf „Kopieren“ wechseln Sie im folgenden Menü von Ihrem Standard-Brenner auf den

Image Recorder von Nero. Der erstellt eine Audio-CD der ausgewählten Wiedergabeliste in einer Image-Datei mit der Dateiendung NRG. Diese Image-Datei laden Sie anschließend in ein virtuelles Laufwerk – zum Beispiel den Nero Imagedrive. Nun kommt **Isobuster** (für Win 98/ME, 2000, XP und Vista, Download unter www.isobuster.com, 2,6 MB) ins Spiel: Wählen Sie im Menü der Shareware das virtuelle Laufwerk mit der Image-Datei aus. Im Fenster auf der rechten Seite sehen Sie nun die Lieder, die auf der virtuellen Audio-CD enthalten sind. Per Rechtsklick und der Option „Extrahieren

DRM löschen: Direktaufnahme per Soundkarte

Bei einer Direktaufnahme über die Soundkarte spielen Sie die mit DRM geschützten Audiodateien im zugehörigen Player-Programm ab. Gleichzeitig läuft auf dem PC ein Tool, das das Tonsignal direkt vom Eingang der Soundkarte mitschneidet. Durch den analogen Umweg gibt es bei optimaler Aussteuerung des Pegels kaum hörbare Qualitätseinbußen.

Empfehlenswert ist Freeware No. 23 Recorder. Nach dem Start (für Win 2000 und XP, auf CD und unter www.no23.de, 1,1 MB) tragen Sie Titel, Künstler und Albumname des umzuwandelnden Songs in die linke Fensterseite ein. Bei „Zielverzeichnis“ geben Sie an, wohin das Programm die fertigen Lieder speichern soll. Unter „MP3“ legen Sie die Bit-Rate und damit die Aufnahmequalität fest – eine gute Wahl ist 192 KBit/s. Rechts wählen Sie Ihre Soundkarte aus. Das Feld darunter ist wichtig, denn damit stellen Sie die Signalquelle ein – im Zweifel hilft ausprobieren weiter. Klicken Sie auf „Record“, und starten Sie die Wiedergabe des Songs in der entsprechenden Abspiel-Software. Achten Sie auf die Pegelanzeige rechts

oben im Programmfenster: Schlägt sie in den roten Bereich, steuern Sie den Titel mit den beiden Reglern „Master“ oder „Volume“ in der Wiedergabe-Software aus.



Musik-CD analog kopieren: Die Freeware No. 23 Recorder nimmt dazu das Signal der Soundkarte analog auf



Allzweckkopierer: Die Software erstellt legal Kopien von geschützten als auch von ungesicherten DVD-Filmen (Punkt 8)

Track, Extrahiere Audio zu Wavedatei“ wandelt Isobuster die Songs in WAV-Dateien

Aufnahme DRM-frei in den Formaten MP3, OGG und WMA. Der Clou: Tunebite wandelt

um. Damit sind die Lieder DRM-frei und lassen sich beliebig weiterverarbeiten. Zum Beispiel können Sie sie nun mit einem Konverter wie **Dbpoweramp Music Converter** (auch auf CD) ins MP3-Format umwandeln.

7. Blitzkopie mit Tunebite

Es gibt Programme, die DRM-geschützte Songs in doppelter oder vierfacher Geschwindigkeit abspielen und aufnehmen, zum Beispiel **Tunebite**. Mit dem in der Premiumversion rund 20 Euro teuren Tool (für Win 2000 und XP, Download unter www.tunebite.de, 12 MB) schneiden Sie über einen Spezialtreiber das über die Soundkarte ausgegebene Signal mit und sichern die

beliebig viele Dateien hintereinander automatisch im Stapelbetrieb um. Außerdem übernimmt die Software Angaben zu Titel und Interpreten in die Zieldateien.

Im Anschluss an die Installation richtet ein Assistent die Audio-Einstellungen automatisch ein. Zum Sichern im MP3-Format benötigt das Programm einen zusätzlichen Gratis-Encoder, den Sie mit Hilfe des Assistenten aus dem Web laden.

Die Handhabung ist einfach: Das Hauptfenster von Tunebite besteht aus zwei Bereichen: In die linke Fensterhälfte ziehen Sie die Dateien, von denen Sie eine ungeschützte Kopie wünschen. Dann legen Sie den Zielpfad und die Audiodatei-Formateinstellungen fest. Mit „Go!“ starten Sie die Konvertierung.

8. Video-DVDs – jeden Film legal kopieren

Fast alle Film-DVDs sind per Kopierschutz CSS (Content Scrambling System) gesichert. Doch diese Barriere können Sie legal überwinden, wenn Sie eine analoge Kopie erstellen. Denn verboten sind nur digitale Sicherungen geschützter Filme.

Grafikkarte anzapfen: Haben Sie eine Grafikkarte mit Video-Eingang? Dann findet sich auf Ihrem PC zumeist auch ein Video-Aufzeichnungsprogramm. In diesem Fall kommen Sie kostenlos zur analogen Kopie. Zunächst müssen Sie den Video-Ausgang des DVD-Players mit dem Video-Eingang der Grafikkarte und den Soundausgang des Players mit dem Eingang der Soundkarte verbinden. Je nach verwendetem Kabel wählen Sie im Aufzeichnungsprogramm die Art der Videoverbindung, also etwa „Composite“ oder „S-Video“. Meist müssen Sie noch den Sendestandard angeben – für Deutschland ist das „PAL B“. Schließlich definieren Sie die Aufnahmequalität. Suchen Sie nach einem Menü wie „Video“ und hier nach Optionen wie „DVD“ oder „Video-CD“. Legen Sie den Ordner fest, in dem die Ergebnisdatei landen soll. Starten Sie die DVD im Player, und aktivieren Sie im Aufzeichnungsprogramm die Funktion zum Starten der Aufnahme. Die Kopie brennen Sie dann etwa mit Nero.

Kopierprogramm: Das Backup per Grafikkarte ist zwar kostenlos, es erfordert jedoch einigen Aufwand: Sie müssen die passenden Kabel suchen und sich in Eigenregie durch die Menüs der Aufzeichnungs-Software und

Gute Tonqualität: Brennücke nutzen

Definitiv legal und ohne Qualitätsverlust wandeln Sie Musik mit einem anderen Verfahren um, das etwas umständlicher ist als die Aufzeichnung mit Tunebite. Bei dieser Methode nutzen Sie eine Option, die fast jedes gekaufte Musikstück bietet: Sie brennen die Musik auf CD und lesen sie anschließend mit einem Gratis-Tool wie **Cdex 1.70 Beta 2** (auf CD) aus.

Da die gebrannte CD nicht kopierschutz ist, verstoßen Sie gegen kein Gesetz. Die meisten CD-Ripper legen die Stücke gleich als MP3s auf der Festplatte ab. Allerdings müssen Sie sie – und das ist der Pferdefuß – anschließend noch richtig benennen. Denn die Titelinformationen gehen beim Brennen und anschließenden Rippen verloren. **Einzige Ausnahme:** Alle Beteiligten – also Abspiel-Software, Brenner und Ripper – unterstützen die Funktion „CD-Text“. Dann können Sie zumindest Interpret und Titelangabe retten. Wenn Sie die selbst gebrannten CDs nach dem Rippen nicht mehr brauchen, nutzen Sie besser ein wiederbeschreibbares Medium (CD-RW). Noch einfacher und schneller geht's, wenn Sie das Brennprogramm keine echte CD brennen, sondern ein CD-Image erstellen lassen. Die Image-Datei binden Sie anschließend als virtuelles CD-Laufwerk ein. Der Auslesevorgang läuft dadurch schneller ab.

Das ideale Werkzeug für diese Aufgabe wäre ein virtueller CD-Brenner – ein Treiber, der dem Betriebssystem sowie allen Anwendungen vorgaukelt, er wäre ein echter Brenner, und statt einer CD eine Image-Datei ausspuckt. Anschließend sollte er das Image gleich als Laufwerk in Windows einbinden. Original CD Emulator Personal Edition 2.30 soll genau das können. Allerdings wird das Programm mittlerweile nicht mehr weiterentwickelt.

des Brennprogramms arbeiten. Wem dieser Weg zu anstrengend ist oder wer keine passende Hardware hat, der kann auf kommerzielle Kopierprogramme zurückgreifen, beispielsweise zu **Davideo DVD Kopierer 2006** (www.gdata.de, rund 35 Euro).

9. Filme per Mitschneiden von DRM befreien

Von kopiergeschützten Video-DVDs können Sie auch mittels eines Grabber-Tools eine Kopie des Films auf Festplatte erstellen. Dazu spielen Sie den Film ab und zeichnen ihn gleichzeitig auf. Sie benötigen dafür einen Rechner mit leistungsfähiger CPU, da diese die Hauptlast trägt. Den Film spielen Sie mit einer beliebigen Player-Software ab, etwa dem Windows Media Player. Zum Aufzeichnen verwenden Sie die englischsprachige Shareware **Hypercam** (auch auf CD).

Auswahl erstellen: Zunächst definieren Sie den Fensterbereich, in dem der Film läuft. Dazu starten Sie ihn in Ihrer Player-Software und aktivieren Hypercam. Dort klicken Sie auf „Screen Area, Select Region“ und markieren die gewünschte Fensterfläche auf dem Bildschirm mittels Fadenkreuz.

Videoqualität vorgeben: Definieren Sie anschließend auf der Registerkarte „AVI File“ die Aufnahmequalität. Wenn Ihre CPU mitspielt, wählen Sie für „Rate in Frames per Second, Record:“ einen Wert zwischen 20 und 25. Die „Frame compression quality“ sollte bei etwa 75 Prozent liegen. Wenn Ihr System mit der gewählten Einstellung völlig überfordert ist, bricht die Aufnahme ab. Au-

ßerdem können bei zu hohen Werten Fehler auftreten. In solchen Fällen setzen Sie dann niedrigere Werte. Für eine akzeptable Aufnahmequalität sollten Sie 15 Bilder pro Sekunde nicht unterschreiten. Die Standardeinstellung gibt allerdings sogar zehn Bilder vor. Für die Komprimierung liegt eine vernünftige Untergrenze bei 60 Prozent. Pfad und Dateinamen der Aufzeichnung legen Sie unter „AVI File Name“ fest.

Tonaufnahme: Aktivieren Sie noch „Record Sound“, damit auch der Ton aufgezeichnet wird. Für die Klangqualität können Sie auf der Registerkarte „Sound“ die Standardwerte beibehalten. Wenn Sie alle Einstellungen vorgenommen haben, starten und stoppen Sie die Aufzeichnung über <F2>. Lassen Sie das Video wie gewohnt durchlaufen, Hypercam hält es im Hintergrund fest. Den aufgezeichneten Film können Sie dann direkt mit dem Media Player abspielen.

10. Qualitätsunterschiede beim Video-Grabben

Die unregistrierte Version von Hypercam zeigt im Abspielfenster den Hinweis „Unregistered HyperCam“. Wenn Sie die Kopie mit dem Original vergleichen, werden Sie Qualitätsunterschiede bemerken: Je nach CPU-Leistung sehen Sie mehr oder weniger störende Pixelfehler. Bei einigen kopiergeschützten Filmen stellten wir fest, dass in der Aufzeichnung regelmäßig kurze Sequenzen fehlten. Die Bildqualität ist aber allemal besser als die von in Kinos abgefilmten Screener-Kopien aus dem Internet.



Mitschneiden: Das klappt bei Video-DVDs und Internet-Videos mit Aufwand (Punkt 9)

Die Aufnahmequalität mit Hypercam lässt sich in gewissen Grenzen verbessern, wenn Sie die Arbeit auf zwei Rechner verteilen. Der Rechner, der den Film abspielt, benötigt einen Video-Ausgang, der PC, der den Film zeitgleich aufzeichnet, einen Video-Eingang. Beide Videobuchsen verbinden Sie mit einem entsprechenden Anschlusskabel. Damit das Signal am Video-Ausgang ankommt, müssen Sie im Grafikkartentreiber das entsprechende Ausgabegerät wählen. Sie finden es meist unter einem Menüpunkt wie „Anzeige“.

High-End: Echte Analog-Kopie

Die bereits beschriebenen **Entsperrverfahren** nutzen den PC zur Wiedergabe der geschützten Dateien. Deutlich zeitaufwendiger ist eine echte analoge Kopie von einem CD- oder DVD-Player. Diese Methode eignet sich vor allem für Musikliebhaber, die über eine hochwertige Hi-Fi-Ausstattung samt korrespondierender Soundkarte verfügen und die qualitativen Vorteile im Hinblick auf Klangwärme und Rauschfreiheit ausnutzen möchten. Ob der Aufwand für heruntergeladene Songs lohnt, hängt von der Güte der Dateien ab. Das Verfahren eignet sich auch zum Überspielen von Vinylplatten und für Super-Audio-CDs (SACDs).

Zunächst brennen Sie die geschützten Songs als Audio-CD. Verbinden Sie den Analogausgang des CD-Players mit dem Line-in-Eingang der Soundkarte. Für analoge Kopien von SACDs benötigen Sie eine für Surround-Aufnahmen ausgestattete Profi-Soundkarte wie die Terratec Aureon 7.1 (www.terratec.de) oder E-MU 1820 (www.emu.com) und sechs Anschlusskabel. Zum Aufnehmen analog eingespielter CDs eignet sich bei-

spielsweise das kostenlose **Audacity** (für Windows 95/98/ME, NT 4, 2000 und XP, auf CD und unter <http://audacity.sourceforge.net>, 4,31 MB). Bei SACDs kommen Sie mit Audacity nicht weiter, denn Sie benötigen eine mehrkanalfähige Spezial-Software wie Wavelab 6 oder Samplitude 8 Classic. Für das analoge Kopieren von DVD-Audios eignet sich dieses Verfahren übrigens normalerweise nicht. Hat der Hersteller der Scheibe die DVD nämlich als geschützt gekennzeichnet („Watermarking“), bricht ein DVD-Player die Wiedergabe der analogen Kopie nach 30 Sekunden Spieldauer ab.



Super-Audio-CDs kopiert: Klanglich exzellent mit einer mehrkanalfähigen Soundkarte



Tools aus dem Giftschränk

Manche Programme sind wie Medikamente: Sie sind wirksam, aber in den falschen Händen können sie Schaden anrichten. Wir stellen Werkzeuge mit Risiken und Nebenwirkungen vor.

Von Tobias Weidemann

Nicht jedes Tool ist nur gut oder nur böse. Zahlreiche Anwendungen sind sehr nützlich, lassen sich aber auch missbrauchen. Wir stellen Ihnen solche Programme vor. Denn nur wer die Gefahren kennt, kann sich wirksam davor schützen.

Beispiel WLAN: Knack- und Einbruch-Tools für WLANs und andere Netzwerke sind illegal. Gleichzeitig machen sie deutlich, wie einfach es ist, bespitzelt zu werden. Und sie helfen Ihnen dabei, Schwachstellen im eigenen Netz ausfindig zu machen.

Beispiel Keylogger: Den Datenverkehr anderer Anwender mitzuschneiden oder zu belauschen ist nicht erlaubt. Es kann aber

auch sinnvoll sein, etwa als Eltern die Internet-Aktivitäten des Nachwuchses zu protokollieren. Sie müssen wissen, ob der Sohn beispielsweise heimlich Filme aus dem Netz herunterlädt oder mit wem sich die Tochter im Chat-Room unterhält und um was für Themen es da geht.

Achtung: Wenn Sie die hier vorgestellte Software ausprobieren, müssen Sie unbedingt die geltenden Gesetze beachten. Auch nicht für Testzwecke ist es erlaubt, das Funknetzwerk des Nachbarn zu hacken und sich Zugriff auf seine Daten zu verschaffen, sich als jemand anders auszugeben oder Kopierschutzverfahren auszuhebeln.

Sicherheit & Verschlüsselung

Free KGB Keylogger: Daten mitschneiden

Nützlich: Es gibt Tools, die jeden Tastaturanschlag protokollieren, etwa jede aufgerufene Website und jeden getippten Satz in einem Chat. Solche Keylogger können Eltern helfen, ihre Erziehungsverantwortung wahrzunehmen. So können sie nachvollziehen, was ihre Kinder am PC getan haben. Das erweist sich etwa als vorteilhaft, wenn eine Rechnung eines teuren Bezahlendienstes ins Haus flattert, mit dem der Nachwuchs ein Abonnement abgeschlossen haben soll. Ein guter Vertreter dieser Programmkategorie ist **Free KGB Keylogger**. Es protokolliert alle Tastaturanschläge und ordnet sie den aufgerufenen Fenstern zu. Das Tool zeigt, welche Anwendungen wann geöffnet wurden, und überwacht die Zwischenablage sowie die Eingabe von Passwörtern.

Die Gratis-Version erscheint zwar nach <Strg>-<Alt>-<Entf> nicht als Task, und die Verknüpfungen im Startmenü, in den Programmlisten sowie auf dem Desktop lassen sich über die Registerkarte „Unsichtbarkeit“ ausblenden. Ab einem gewissen Alter und Kenntnisstand der Kinder sollten Sie dennoch auf eine der Bezahlversionen setzen (ab 29,95 Euro). Denn nur diese lassen sich vollständig im Hintergrund betreiben, und sie verschicken die Log-Dateien auf Wunsch geheim per Mail oder FTP.

Gefährlich: Anders sieht die Situation aus, wenn beispielsweise der Betreiber eines Internet-Cafés mit einem derartigen Tool überwacht, was seine Kunden am Rechner tun. Das verletzt nicht nur die persönlichen Rechte, sondern ist auch im Rahmen der deutschen Datenschutzgesetze verboten.

Tipp: Gegen Keylogger können Sie sich mit virtuellen Keyboards wehren. Hier erscheinen in einem Fenster sämtliche Zeichen in alphabetischer Reihenfolge oder im Layout einer Tastatur. Der Anwender tippt gewissermaßen mit der Maus und platziert die Zeichenkette per Copy & Paste an die gewünschte Stelle. Um längere Texte zu schreiben, ist das Verfahren zu umständlich. Es ist aber sinnvoll, wenn Sie beim Online-Banking Zugangsdaten eingeben müssen.

Mouse-only-Keyboard (auf CD) stellt Klein- und Großbuchstaben, Zahlen und

Sonderzeichen in einer Tabelle dar – Sie tippen einfach mit der Maus. Das englischsprachige Tool müssen Sie nicht extra installieren, Sie können es einfach von einem USB-Stick oder einer virtuellen Festplatte starten, etwa aus Ihrem Webmailer heraus.

Aircrack: Netzwerk auf Sicherheit checken

Nützlich: Sind Sie sicher, dass Ihr Nachbar nur seinen eigenen Router nutzt? Wer auf seinem PC die verfügbaren WLAN-Zugänge prüft, sieht oft nicht nur seinen Zugang. Dass es mit etwas technischem Geschick möglich ist, in ein WPA- oder WEP-geschütztes WLAN einzudringen, zeigen Tools wie **Aircrack** (auf , gratis). Mit dem englischsprachigen WLAN-Hacker prüfen Sie, wie sicher Ihr eigenes Netzwerk ist. Um das Programmpaket einzusetzen, benötigen Sie noch die Dateien Peek.DLL und Peek5.SYS, die Sie aus urheberrechtlichen Gründen nicht auf unserer CD finden, sondern über www.pcwelt.de/cda bekommen. Kopieren Sie die beiden Dateien ins Verzeichnis Aircrack-ng-0.6.2-win\bin. Aircrack können Sie auf zwei Arten steuern: über die Kommandozeile oder über eine einfache grafische Oberfläche, die Sie mit Aircrack-ng gui.EXE aufrufen. Hier finden Sie vier Module, unter anderem Airodump. Dieses Tool schneidet gesendete Datenpakete mit und analysiert die 24-stelligen Initialisierungsvektoren. Je mehr solcher Vektoren das Tool mitschneidet, desto leichter kann es auf einen WEP-Schlüssel schließen. Im Durch-

schnitt sind rund 150.000 bis 200.000 Datenpakete nötig, um einen 64-Bit-Schlüssel zu ermitteln; beim 128-Bit-Schlüssel müssen es bereits rund 800.000 Pakete sein. Auch den WPA-Schlüssel kann Aircrack ermitteln. Dazu schneidet das Tool nur den Verbindungsaufbau mit und greift danach per Brute-Force-Methode an, probiert also sämtliche Möglichkeiten durch. Sie sollten deshalb als Kennwort unbedingt eine scheinbar unsinnige Zeichenfolge wählen. **Gefährlich:** Mit Aircrack können nicht nur Sie herausfinden, wie sicher Ihr eigenes Netzwerk ist. Genauso gut können Hacker ein fremdes WLAN ausspionieren, das sich in ihrer unmittelbaren Umgebung befindet.

Torpark: Surfen mit Tarnkappe

Nützlich: Anonymisierer sind Tools, die den Datenverkehr in einem komplizierten Geflecht über mehrere Server umleiten. Im Nachhinein kann nicht einmal das System selbst nachvollziehen, von welchem Rechner oder über welche IP-Adresse eine Anfrage kam und welche Datenpakete dorthin geflossen sind. Jeder Benutzer ist nur ein Teil des Netzwerks und stellt mit sicher, dass niemand Zugriff auf das komplette Netzwerk hat. Je mehr Teilnehmer, desto sicherer ist die Anonymisierung. Nachteil dabei: Sie surfen etwas langsamer.

Leistungsfähig und einfach zu handhaben ist **Torpark** (auf , eine Kombination aus der Anonymisierungs-Software Tor und dem Browser Firefox. Vorteil: Weil der Quellcode jeweils offen liegt, kann der An-

Überblick Spezial-Werkzeuge

Inhalt	Seite
Sicherheit & Verschlüsselung	58
Codes & Passwörter	60
Kasten	
Tools aus dem Giftschränk	59

wender sicherstellen, dass die Software keine Spionagefunktionen enthält. Das Open-Source-Tool lässt sich sogar ohne Installation ausführen. Extrahieren Sie einfach die gepackte Datei in ein beliebiges Verzeichnis, etwa auf Ihrem USB-Stick. Die deutschsprachige Bedienerführung erreichen Sie über „Tools, Switch Language“.

Gefährlich: Torpark sorgt dafür, dass der Anwender beim Surfen nicht identifiziert werden kann. Aus diesem Grund haben US-amerikanische Politiker nach den Anschlägen des 11. September ein Verbot von derartigen Verschleierungs-Tools gefordert. Denn auch das Tun von Kriminellen lässt sich nur sehr eingeschränkt nachvollziehen. Allerdings hätte ein Verbot bei Torpark kaum eine Wirkung: Es gibt keinen zentralen Dienst, den man abschalten könnte.

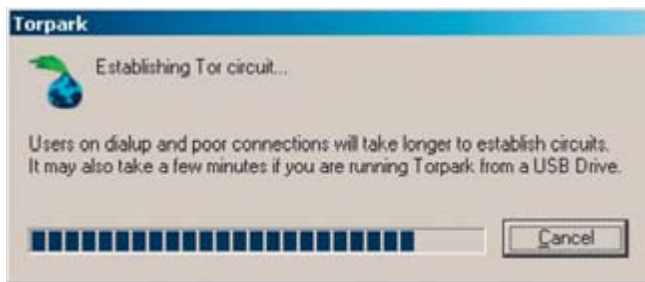
Truecrypt: Daten sicher verwahren

Nützlich: Um Teile Ihrer (externen) Festplatte oder Ihren USB-Stick vor Unbefugten zu schützen, brauchen Sie ein Verschlüsselungs-Utility. Wenn etwa Ihr Notebook ge-

Fast alle gratis: Tools aus dem Giftschränk

Produkt	Funktion	Win-Betriebssysteme	Internet (Download)	Sprache	Seite
 Aircrack 0.6.2	WLAN-Sicherheit checken	2000, XP	www.aircrack-ng.org (1,22 MB)	Englisch	59
 Belarc Advisor 7.2k ¹⁾	Seriennummern auslesen	95/98/ME, NT 4, 2000, XP	www.belarc.com (1,01 MB)	Englisch	60
 DVD Next Copy 2.5.8.2²⁾	Film-DVDs kopieren	2000, XP, Vista	www.dvdnextcopy.com (4,95 MB)	Deutsch	61
Elcomsoft-Tools ³⁾	Dateipasswörter auslesen	95/98/ME, NT 4, 2000, XP	www.elcomsoft.com		59
Free KGB Keylogger 1.94	Tastaturanschläge protokollieren	95/98/ME, NT 4, 2000, XP	www.refog.de/keylogger (1,45 MB)	Deutsch	58
Machinist2.DLL 2.0	Kopierschutz umgehen	2000, XP, Vista	keine Angabe aus juristischen Gründen	Englisch	61
Magical Jelly Bean Keyfinder 2.0 Beta 2.5	Windows-CD-Key auslesen	95/98/ME, 2000, XP	www.magicaljellybean.com (318 KB)	Englisch	60
 Mouse-only-Keylogger 1.4	zahlreiche Keylogger umgehen	95/98/ME, NT 4, 2000, XP	www.myplanetsoft.com (93 KB)	Englisch	58
 Mozilla Password Recovery 2.1 ⁴⁾	Mozilla-Passwörter auslesen	95/98/ME, NT 4, 2000, XP	www.passcape.com (1,60 MB)	Deutsch	61
 Torpark 2.0.0.3a	Anonym surfen	98/ME, 2000, XP	http://torpark.nfshost.com (10,6 MB)	Deutsch	59
 Truecrypt 4.3	Daten verschlüsseln	2000, XP	http://truecrypt.sourceforge.net (1,35 MB)	Deutsch	60

¹⁾ auf CD und unter www.pcwelt.de ²⁾ für private Nutzung gratis ³⁾ Shareware, 69,99 Dollar, Einschränkungen siehe Text ⁴⁾ je Tool 30 Euro für private, 60 Euro für gewerbliche Nutzer ⁵⁾ Shareware, 27 Dollar, Einschränkungen siehe Text



Kein Firefox wie jeder andere: Mit Torpark bleiben Sie unerkannt im Web, surfen allerdings etwas langsamer als gewohnt

stohlen wird oder verloren geht, stellen Sie sicher, dass niemand auf Ihre persönlichen oder geschäftlichen Daten zugreifen kann. Hier empfehlen wir, auf ein Open-Source-Tool zu setzen. Damit kann man sicherstellen, dass es keine Hintertüren- oder Spionagefunktionen gibt. **Truecrypt** (auf CD) ist leistungsfähig und lässt sich einfach handhaben. Mit der Freeware können Sie Datei-Archive oder ganze Partitionen chiffrieren. Das Utility arbeitet mit einer Echtzeitverschlüsselung, ohne Daten auf der Platte zwischenspeichern.

Ein als Truecrypt-Volume bezeichneter Container kann entweder sichtbar oder versteckt in einem anderen Container liegen. Die zweite Methode ist besonders sicher, da man auf den ersten Blick nicht erkennt, dass

können die Größe der Container frei wählen (bei FAT maximal 4 GB). Wir raten dringend davon ab, dynamische Container zu erstellen, die ihre Größe je nach Bedarf automatisch anpassen. Im schlimmsten Fall droht hierbei nämlich Datenverlust!

Als Verschlüsselungsalgorithmus empfehlen wir eine Kombination aus AES und Twofish, da dies den optimalen Kompromiss aus hinreichend hoher Sicherheit und gutem Tempo darstellt. Bei einem langsamen PC (weniger als 1 GHz CPU-Takt) sollten Sie auf Blowfish oder AES allein setzen.

Im Hauptmenü bestimmen Sie den Buchstaben für das verschlüsselte Laufwerk. Nach dem Klick auf „Verbinden“ können Sie auf das Laufwerk wie auf ein gewöhnliches Festplatten- oder DVD-Laufwerk zugreifen.

hier weitere Daten verborgen sind. Sie können wahlweise ein gesamtes Laufwerk verschlüsseln oder einen Container auf einem Laufwerk erstellen. Wichtig: Verschlüsseln Sie nur leere Datenträger, da ansonsten die darauf befindlichen Daten verloren sind. Sie

Gefährlich: Verschlüsselungs-Tools sind seit dem 11. September 2001 in Verruf geraten. Terroristen haben nachweislich auf diesem Weg Daten ausgetauscht. Nicht einmal den Ermittlungsbehörden und Geheimdiensten ist es im Nachhinein gelungen, gut verschlüsselte Festplatten zu decodieren. Allerdings: Verschlüsselte Daten sind nicht für alle Zeiten sicher. Die Algorithmen werden zwar immer komplizierter, spiegeln aber nur den Stand der Technik wider. Eine heute verschlüsselte Festplatte dürfte somit in einigen Jahren dechiffrierbar sein – sofern die Daten dann noch lesbar sind.

Codes & Passwörter

Belarc Advisor: Alle Seriennummern im Griff

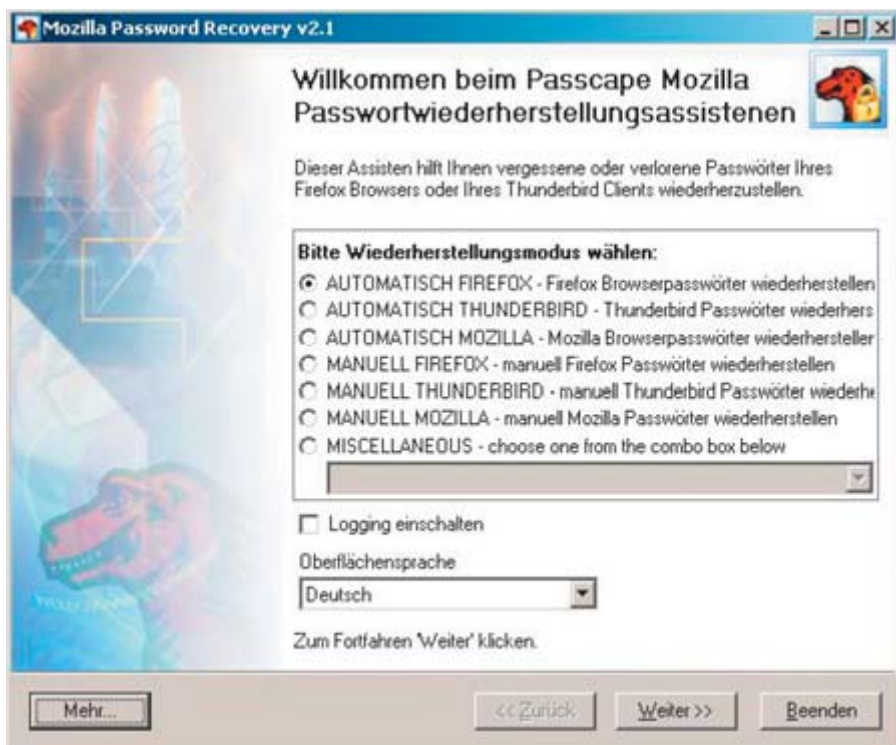
Nützlich: Jeder PC-Besitzer musste wohl schon seinen PC neu aufsetzen und stand vor dem bekannten Problem: Die Seriennummern für alle Anwendungen sind nie sofort greifbar. Mit Belarc Advisor (auf CD, für private Nutzung kostenlos) bekommen Sie Informationen über die auf Ihrem PC installierte Software. Das Tool liest die Seriennummern über die entsprechenden Registry-Einträge aus. Speichern Sie einfach die HTML-Seite, die Sie als Ergebnis erhalten, zum Beispiel auf Ihrem USB-Stick.

Außerdem erfahren Sie, welche Versionen auf Ihrem Rechner installiert waren. Das ist hilfreich, wenn ein Tool nach der Neu-Installation nicht mehr wie gewohnt arbeitet. Sie können dann sehen, ob Sie vorher eine andere Fassung eingesetzt haben.

Gefährlich: Mit Belarc Advisor können auch andere Anwender sehen, welche Software mit welchen Lizenzschlüsseln auf Ihrem System installiert ist. Deswegen verhindern Betreiber von Uni-Rechnern oder Internet-Cafés in der Regel, dass sich solche Tools auf den Gastrechnern installieren lassen.

Keyfinder: Windows-Keys auslesen und ändern

Nützlich: Nicht selten kommt es vor, dass Anwender bei einer Neu-Installation den Windows-CD-Key nicht mehr greifbar haben. Wer ihn nicht umständlich bei der Microsoft-Hotline erfragen kann oder will, kann **Magical Jelly Bean Keyfinder** nutzen. Die englischsprachige Freeware liest den Installationsschlüssel aus der Registry aus. Sie können ihn dann in die Zwischenablage



Alles sehen: Das Passcape-Tool zeigt selbst dann die abgelegten Firefox-Passwörter, wenn Sie ein Master-Passwort gesetzt haben

kopieren und ausdrucken. Überaus praktisch ist auch die Möglichkeit, unter Windows 95/98/ME, 2000 und XP den Key zu ändern (über „Tools, Change Windows Reg Info“). Wer seinen PC verkauft, kann die Windows-Lizenz ummelden, wenn er die eigene Lizenz behalten will. Voraussetzung ist, dass der Käufer eine Lizenz derselben Windows-Version besitzt. Auch der Name des PC-Nutzers lässt sich ändern.

Gefährlich: Mit Magical Jelly Bean Keyfinder könnte jeder Windows-Seriennummern auslesen, sobald er Zugriff auf ein fremdes System hat. Wenn eine Nummer doppelt verwendet wird, drohen Scherereien mit Microsoft, etwa Probleme bei der Neu-Installation oder bei Updates.

Password Recovery: Kennwörter auslesen

Nützlich: Browser wollen es dem Anwender einfach machen. Sie bieten an, Passwörter automatisch einzufügen oder zu vervollständigen. Was aber tun, wenn der Rechner nicht mehr hochfährt oder der Browser den Dienst verweigert? Hier hilft **Mozilla Password Recovery** (auf CD). Wenn Sie Ihre Festplatte an einem anderen PC anschließen, liest die Shareware Passwörter und Zugangsdaten aus, die in Mozilla, Firefox und Thunderbird abgelegt wurden. Die Software unterscheidet zwischen der automatischen und der manuellen Wiederherstellung. Anders als vergleichbare Programme kann Mozilla Password Recovery die Kennwörter auch sichtbar machen, wenn sie mit einem Master-Passwort geschützt sind. In der unregistrierten Version zeigt das Tool maximal dreistellige Passwörter an. Die Herstellerfirma Passcape (www.passcape.com) bietet vergleichbare kostenpflichtige Tools auch für Internet Explorer, Opera, Outlook und einige weitere Mail-Clients an.

Gefährlich: Mit Mozilla Password Recovery kann jeder Unbefugte Kennwörter aus Ihrem System auslesen, auch wenn diese per Master-Passwort geschützt sind. Da viele Nutzer ähnliche oder gar identische Passwörter verwenden, lassen sich die Login-Daten zu anderen Zugängen erschließen.

Elcomsoft-Tools: Mit Passwort geschützte Dateien retten

Nützlich: Sie haben wichtige Dateien mit einem Passwort geschützt – und es vergessen. Hier brauchen Sie ein Knack-Tool. Es

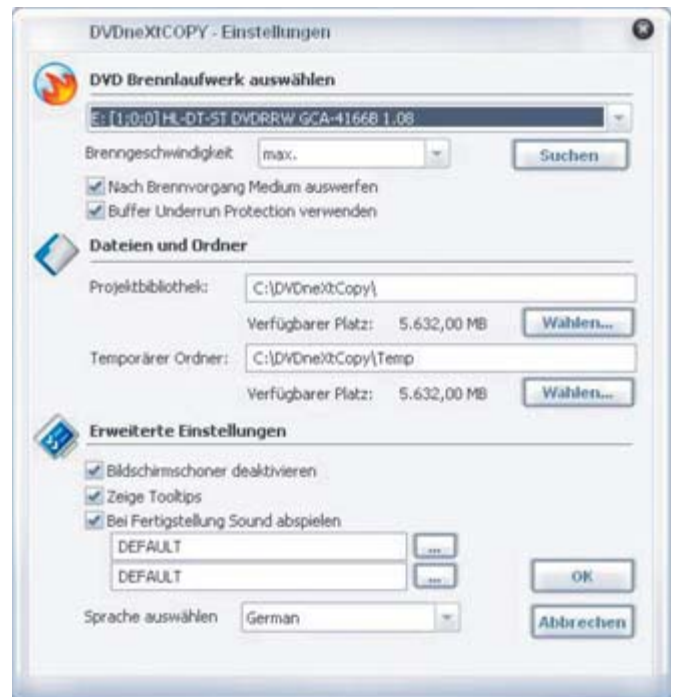
gibt sie inzwischen für alle Dokumentarten, ob Office-, Grafik- oder PDF-Dateien. In den meisten Fällen kommen die Tools nicht mit allen Versionen dieser Dokumente klar. Bevor Sie also ein kostenpflichtiges Tool freischalten, sollten sie auf jeden Fall sicherstellen, dass es das betreffende Dokument wirklich öffnen kann. Seriöse Programme beweisen das, indem sie zumindest die ersten Zeichen kostenfrei entschlüsseln. Oft reicht das auch schon aus, um sich wieder an das eigene Passwort zu erinnern. Eine breite

Palette recht leistungsfähiger Passwort-Knacker liefert Elcomsoft (www.elcomsoft.com) – insgesamt 24 **Elcomsoft-Tools** stehen zur Verfügung. Die Kehrseite der Medaille: Der Anwender zahlt für jedes Dateiformat extra (30 Euro für Privatanwender, 60 Euro für gewerbliche Kunden).

Gefährlich: Mit Passwort-Knackern öffnen nicht nur Sie Ihre Dateien, sondern im schlimmsten Fall auch die anderer Anwender. Allerdings haben Fremde es schwerer: Der Kennwortschutz lässt sich nämlich nur mit der richtigen Programmversion und den passenden Einstellungen knacken – und die muss man erst einmal kennen.

DVD Next Copy: Filme legal kopieren und umcodieren

Nützlich: Multimedia-Tools aus dem Giftschrank haben meist mit dem Umgehen von Kopierschutzmechanismen zu tun, was – insbesondere bei Filmen und Musik – in Deutschland per Gesetz verboten ist. Ein Programm, das Sie in der vom Hersteller angebotenen Form bedenkenlos einsetzen dürfen, ist **DVD Next Copy** (auf CD). Das Tool fertigt nicht nur 1:1-Kopien an, sondern codiert das Video- und Audiomaterial auf Wunsch auch platzsparend um. Praktisch: Sie können Images von Filmen auf der Festplatte speichern und entweder dort darauf



Filmarchiv: DVD Next Copy kopiert DVDs auf die Festplatte. Mit geschützten Scheiben geht das in der Standardausstattung nicht

zugreifen oder sie von hier aus brennen. So schützen Sie Ihre Originalmedien und haben Ihre komplette Filmesammlung bei Bedarf immer dabei. Die Qualität lässt sich in mehreren Stufen regeln, immer abhängig davon, wie lange die Komprimierung dauern darf. Mit DVD Next Copy können Sie übrigens auch Kopien von Filmen anfertigen, die keinen Ländercode mehr enthalten. Das ist legal, da diese Beschränkung mit einem eventuell vorhandenen Kopierschutz nichts zu tun hat. Technisch gesehen werden dabei nämlich nur Abweichungen von den DVD-Standards ignoriert.

Achtung: Der Hersteller bietet zwar eine Zufriedenheitsgarantie. Das heißt, er verspricht „Geld zurück wenn nicht zufrieden“ und Mailsupport innerhalb von 24 Stunden, wenn mal etwas mit der Software nicht klappt. Eine Postanschrift oder Telefonnummer findet man auf der Website jedoch nicht, nur eine Mailadresse.

Gefährlich: Das Programm verarbeitet in der hier angebotenen Version den deutschen und amerikanischen Gesetzen entsprechend nur Film-DVDs, die nicht mit kopiergeschützt sind. Das ändert sich jedoch mit dem Plug-in Machinist2.DLL. Es darf allerdings nur in Staaten genutzt werden, in denen das Umgehen von Kopierschutzmechanismen nicht unter Strafe steht. ❌



Jede Software gratis nutzen

Ob Shareware, eingeschränkte Demo – so gut wie jede Testversion lässt sich recht einfach als uneingeschränkt laufende Vollversion freischalten. In einigen Fällen ist das sogar legal.

Von **Ramon Schwenk**

Mit kostenlosen Shareware- und Demoversionen wollen immer mehr Software-Hersteller Anwender von der Qualität ihrer Produkte überzeugen und sie zum Kauf bewegen. Solche Test-Software ist entweder zeitlich oder funktional eingeschränkt. Adobe beispielsweise stellt 30-Tage-Testversionen für fast alle seine Produkte zum kostenlosen Herunterladen bereit, von Premiere Pro 2.0 über Photoshop CS 3 bis hin zu Acrobat 8.0 Professionell. Auch die Hersteller Corel, Symantec, Ulead & Co. locken potenzielle Kunden mit Testversionen ihrer Anwendungen. Es handelt sich in der Regel um technisch voll funktionsfähige Software,

die sich teilweise durch die Eingabe einer gültigen Seriennummer in eine reguläre Version umwandeln lässt.

Eine zeitliche Begrenzung – meistens 30 Tage ab Installation – kann man in den meisten Fällen mit geeigneten Tools umgehen. Dadurch sind die Programme auch nach Ablauf der Testphase voll funktionsfähig. Viele Hersteller verbieten das nicht ausdrücklich.

Funktionseingeschränkte Versionen kann der Anwender meist zur Vollversion upgraden, indem er den kompletten Umfang mit einer Seriennummer freischaltet. Das ist freilich nur dann erlaubt, wenn er Nutzer eine Lizenz käuflich erworben hat.

Software mit zeitlicher Einschränkung

Wenn Sie eine Testversion installieren, können Sie sie normalerweise ab diesem Tag über einen festen Zeitraum nutzen. Danach teilt Ihnen die Software mit, dass die Testphase abgelaufen ist. Das ist ärgerlich, wenn Sie in den 30 Kalendertagen nur ein- bis zweimal dazu kommen, sich die Software näher anzuschauen.

Viele Hersteller bauen in ihre Demoversionen so wenig Schutz ein, dass sie sich kindeleicht durch Zurückstellen der Rechnungslänge länger nutzen lassen, und untersagen eine Nutzung nach Ablauf des Testzeitraums auch nicht. Man muss davon ausgehen, dass diese Hersteller nichts dagegen haben, wenn ein Anwender den Testzeitraum etwas verlängert. Zumindest dann nicht, wenn er noch nicht genügend Gelegenheit hatte, die Software auszuprobieren, und das Programm nun noch ein- bis zweimal testen möchte. Dauerhaft nutzen darf man die Software freilich nur dann, wenn man eine gültige Lizenz besitzt.

Testzeitraum manuell verlängern

Eine Lösungsmöglichkeit besteht darin, das Systemdatum mit Bordmitteln zurückzustellen, um der Software vorzugaukeln, dass die Frist noch nicht abgelaufen ist. Das geht nach einem Doppelklick auf die Uhrzeit im Systray. In der Praxis ist dieser Weg unkomfortabel: Der Nutzer muss vor dem Start der Software daran denken, das Datum umzustellen. Wenn die Software das Datum geprüft hat, muss er die Änderung zurücknehmen.

Darum geht's: Software freischalten

Die meisten zeitbeschränkten Demos sind ungenügend geschützt. Schon mit einfachen Tricks kann man den Testzeitraum verlängern. Oft untersagen die Lizenzbedingungen eine Nutzung nach dem vorgesehenen Testzeitraum nicht ausdrücklich. Inwieweit es dann legal ist, das Programm etwas länger auszuprobieren, ist rechtlich ungeklärt. Seriennummern aus dem Web darf man hingegen nur einsetzen, wenn man seinen legal erworbenen Schlüssel verlegt hat.

Programm	Parameter	Inst. Datum	Wartezeit	Endung	Warten	Meldung
H:\Programme\Ado...	keine	4.8.2006	3000 ms	keine	Nein	Nein
H:\Programme\Ule...	keine	25.7.2006	3000 ms	keine	Ja	Nein
H:\Programme\Ado...	keine	7.4.2006	3000 ms	keine	Nein	Nein
H:\Programme\Col...	keine	5.10.2004	3000 ms	keine	Nein	Nein
H:\Programme\Cor...	keine	20.7.2006	2000 ms	keine	Nein	Nein
H:\Programme\Ado...	keine	25.8.2005	3000 ms	keine	Nein	Nein
H:\Programme\Un...	keine	19.7.2006	3000 ms	keine	Nein	Nein
H:\Programme\Win...	keine	5.10.2004	4000 ms	keine	Nein	Nein

Zeitwechsel: Mit Dkill legt man für jede Anwendung ein Datum fest, auf das der PC vor dem Start der Software springen soll

men, um systemnahe Programme nicht durcheinanderzubringen. So meldet beispielsweise der Kaspersky-Virenwächter beim Zurückstellen des Systemdatums, dass die Lizenz abgelaufen sei. Auch Backup-Tools, die nach einem festen Zeitplan automatisch Sicherungskopien anlegen, vertragen keine Änderung der Systemzeit. Das bedeutet übrigens auch, dass sich Testversionen von systemnahen Programmen nicht durch simples Umstellen des Datums zu einer längeren Zusammenarbeit bewegen lassen.

Testphase mit Zusatz-Tools verlängern

Manche versierte Anwender greifen zu Spezial-Tools, mit denen sich die Systemuhr bequemer umstellen lässt. Einige ändern das Datum automatisch vor dem Start einer Software und stellen es direkt anschließend wieder her. Solche Tools sollten bereits vor Ablauf der Testperiode installiert und aktiviert werden. Wenn der Benutzer die betreffende Anwendung bereits einmal danach zu starten versucht hat, hat sie möglicherweise in den Tiefen der Windows-Registry ver-

Systray ein. Ein Rechtsklick darauf öffnet einen Dialog, in dem vier Optionen zur Auswahl stehen: „15 Tage“, „1 Monat“, „6 Monate“ und „1 Jahr“. Um diese Zeiten lässt sich die Systemuhr sowohl vor- als auch zurückstellen. Um ein benutzerdefiniertes Datum zu wählen, geht der Anwender im Menü von Date Wizard auf „Datum eingeben“. Soll die Systemzeit etwa um 30 Tage zurückgestellt werden, wechselt man zur Registerkarte „Relatives Datum“, klickt auf den Pfeil neben „Tage“ und wählt im Untermenü „30“ aus. Bei „Richtung“ markiert der Nutzer die Option „Zurückstellen“ und bestätigt die Änderungen mit „OK“. Nachdem der Anwender das Datum zurückgestellt und die betreffende Anwendung gestartet hat, muss er entweder das Datums-Tool beenden oder aus dem Kontextmenü „Datum wiederherstellen“ wählen. Hierbei wird die Systemuhr wieder auf das korrekte Datum gesetzt.

Dkill verwaltet mehrere Testversionen

Die vielseitige Freeware **Dkill 95** erlaubt es, jeder Anwendung ein bestimmtes Startdatum zuzuordnen. Das Tool ist interessant für

merkt, dass die Testphase vorüber ist. Dann bringt auch das Zurückstellen des Datums nichts mehr.

Systemuhr zurücksetzen

Die populäre Freeware **Amok Date Wizard** verlängert die Laufzeit eines einzigen Programms. Nach der Installation richtet das Programm ein Icon im

Überblick Alles freischalten

Inhalt	Seite
Zeitlich eingeschränkte Software	
Testzeitraum manuell verlängern	62
Testphase mit Zusatz-Tools verlängern	63
Systemuhr zurücksetzen mit Date Wizard	63
Dkill verwaltet mehrere Testversionen	63
Freischalten mit Seriennummern	
Im Web nach Seriennummern suchen	64
Seriennummern per Gratis-Tool suchen	64
Seriennummern aus Schlüsselgeneratoren	64
Verboten: Raubkopien tauschen	65
Kästen	
Darum geht's: Software freischalten	62
Software freischalten: Kostenlose Tools	63
Eula: Was verbietet der Hersteller, was nicht?	65

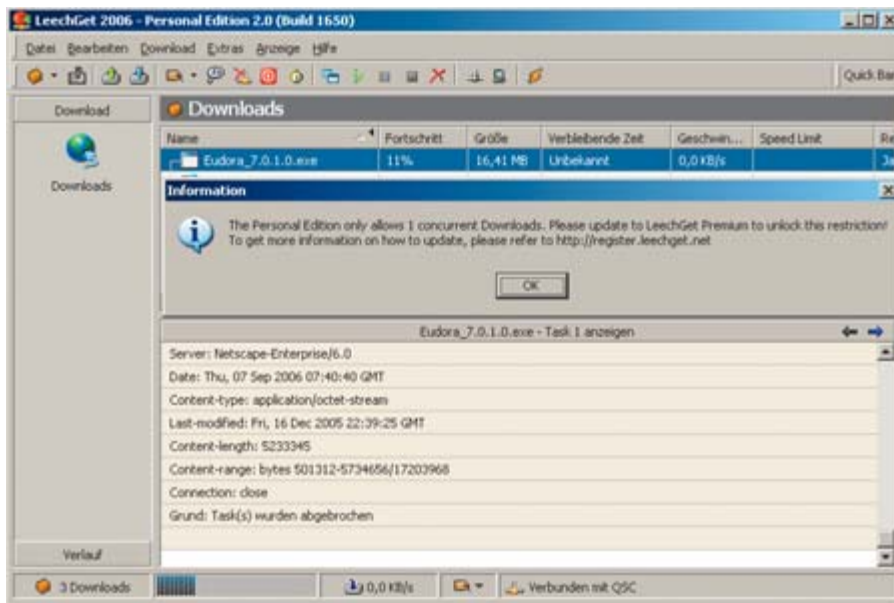
Anwender, die mehrere Programme über einen längeren Zeitraum ausprobieren möchten. Es legt für jedes eine Verknüpfung ins Startmenü oder auf den Desktop. Beim Start von Dkill 95 erscheint ein Einrichtungsassistent. Zunächst wählt der Anwender hier die EXE-Datei der Software, deren Testphase verlängert werden soll. Im nächsten Schritt muss er angeben, wo das Tool die Verknüpfung zur Datei ablegen soll. Anschließend vergibt der Nutzer eine aussagekräftige Bezeichnung für die neue Verknüpfung. Die Freeware erkennt, an welchem Tag das Programm installiert wurde, und schlägt diesen Tag automatisch als Standard-Startdatum vor.

Schließlich ist noch zu entscheiden, wie viele Millisekunden nach dem Start der betreffenden Testversion das Tool die Systemzeit wieder auf das aktuelle Datum umstellen soll. Vorgegeben sind 3000 Millisekunden – also drei Sekunden. Diese Einstellung muss der Benutzer nur dann ändern, wenn es nach dem Start der Anwendung Probleme mit systemnahen Programmen gibt. Meckert beispielsweise das Windows-Sicherheitscenter, dass der Virenschanner nicht über die neuesten Signaturen verfügt, kann der Anwender die Wartezeit verkürzen, etwa auf „2000 Millisekunden“. Dann besteht allerdings die Gefahr, dass das Datum wieder auf den aktuellen Stand zurückgesetzt wird,

Software freischalten: Kostenlose Tools

Programm ¹⁾	Kategorie	Internet (Download)	Seite
Amok Date Wizard 1.1b	Datums-Tool	www.amok.am (367 KB)	63
Dkill 95 2.1b	Datums-Tool	www.freewarepage.de/download/327.shtml (927 KB)	63
Craagle 1.91 ²⁾	sucht Seriennummern	www.hrtsea.com/soft/Craagle.exe (377 KB)	64
Antivir PE Classic 7	Virenschanner	www.free-av.de (11 MB)	64
Firefox 1.5.0.7 PC-WELT-Edition	Web-Browser	www.pcwelt.de/afxp (6 MB)	64

1) Alle Tools laufen unter Windows 98/ME, 2000 und XP. 2) englischsprachig



Stärkerer Schutz: Bei Testversionen, die über einen eingeschränkten Funktionsumfang verfügen, hilft kein einfacher Trick am System

noch bevor die betreffende Testversion ihre Datumsüberprüfung durchgeführt hat. Nach einem Klick auf die Schaltfläche „Fertigstellen“ legt Dkill 95 die Verknüpfung an. Über den „Dkill95 2.1b Manager“ lassen sich die Einstellungen ändern. In hartnäckigen Fällen, also bei Programmen, die sich mit den Standardeinstellungen nicht täuschen lassen, muss der Nutzer ein wenig tricksen. Im Register „Erweitert“ gibt es dafür die beiden Optionen „Alle Programme über die Datumsänderung informieren“ und „Datum erst nach Programmende zurücksetzen“.

Freischalten mit Seriennummern

Von vielen Anwendungen gibt es Demoverversionen, die nicht zeitlich, sondern in den Funktionen eingeschränkt sind. Diese lassen sich nur mit einem Lizenzschlüssel in Vollversionen verwandeln. Davon kursieren zwar viele im Web. Da der Hersteller aber bewusst nicht den kompletten Funktionsumfang zum Testen bereitstellt, darf man sich nicht einfach eine Seriennummer besorgen und sich dann darauf berufen, man wolle die Software lediglich ausprobieren. Etwas anderes ist es, wenn Sie ein Programm offiziell erworben, aber die Seriennummer verloren haben und Sie den Software-Hersteller nicht rechtzeitig erreichen können oder er möglicherweise gar nicht mehr existiert.

Sollte ein Festplattencrash eine Neuinstallation nötig machen, wäre eine Option, sich fürs Erste eine Nummer aus dem Web zu besorgen. Sie sollten anschließend aber den Hersteller kontaktieren und nach einem Ersatz für die verlorene Nummer fragen.

Im Web nach gültigen Seriennummern suchen

Die Suche nach Seriennummern im Internet ist nicht schwierig: Selbst wenig versierte Nutzer finden binnen weniger Minuten funktionierende Lizenzschlüssel. Bekannteste, aber beileibe nicht einzige Anlaufstelle ist die seit mehr als zehn Jahren im Web vertretene Seite Astalavista (<http://astalavista.box.sk>). Der Nutzer muss lediglich den Programmnamen in das oberste Eingabefeld „astalavista.box.sk“ tippen und die Suche mit einem Klick auf „search“ starten. Daraufhin durchforstet die Suchmaschine mehrere einschlägig bekannte Server, darunter Cracks.am, Keygen.ms und Superserials.com, und gibt die entsprechenden Fundstellen aus.

Der Besuch dieser Seiten sollte aber nur mit einem installiertem Virensch scanner wie **Anti-vir Personal Edition Classic** (auf CD) und mit einem sicheren Browser wie **Firefox** erfolgen. Denn auf den Websites lauern Viren, Trojaner und Spyware, die oftmals per Script aktiv werden.

Bei der Suche nach Seriennummern kann auch Google hilfreich sein. So liefert bei-

spielsweise die Suche nach „serial <Programmname>“ zu vielen Programmen ebenfalls Fundstellen, die Anwender mit passenden Freischaltcodes versorgen.

Seriennummern per Gratis-Tool suchen

Eine schnellere Möglichkeit, an Seriennummern zu gelangen, ist die Nutzung eines speziellen Such-Tools, das die Adressen mehrerer einschlägiger Suchmaschinen kennt und sie parallel abfragt. In der Szene derzeit am beliebtesten ist die englischsprachige Freeware **Craagle**.

Das Tool ist einfach zu handhaben. Es startet ohne Installation. Der Anwender wählt im Bereich „What“ aus, was er sucht, etwa „Serials“. Im Feld „Where“ ist standardmäßig „- Search all -“ eingetragen, so dass das Tool alle in der Datenbank enthaltenen Server in die Suche einbezieht. In Sachen Seriennummern sind das 16 Anlaufstellen, darunter die bekannten Anbieter Seriall.com, SerialSite.com und FreeSerials.ws.

In das Feld „Search“ kommt der Programmname mit oder ohne Versionsnummer. Ein Klick auf „Search“ startet die Suche. Die Ergebnisse präsentiert Craagle als übersichtliche Liste. Nach einem Doppelklick auf einen der Einträge lädt das Tool die Seriennummer herunter und zeigt sie im unteren Fensterbereich an. Da die Betreiber mancher Seriennummer-Seiten es nicht gerne sehen, wenn die Nutzer an das Gesuchte gelangen, ohne vorher einen Blick auf Werbung auf ihrer Website geworfen zu haben, kann es vorkommen, dass Craagle nach einem Doppelklick auf eine Fundstelle keine weiterführenden Infos anzeigt.

Seriennummern aus Schlüsselgeneratoren

Auch viele Software-Hersteller besuchen einschlägige Seriennummern-Websites, um Seriennummern für ihre eigenen Produkte zu finden. Aber nicht, um sie weiterzuverkaufen, sondern um sie in einer nächsten Programmversion auf eine Schwarze Liste zu setzen. Ein Update der Software würde dann die Seriennummer nicht mehr akzeptieren. Daher gibt es für viele Programme Schlüsselgeneratoren („Key Generator“ oder auch „Keygen“). Um hiergegen vorzugehen, müsste der Hersteller sein Verfahren zur Schlüsselerzeugung ändern und allen registrierten Anwendern neue Lizenzschlüssel

sel zusenden. Diesen Aufwand scheuen die meisten – und so sind von Keygens erzeugte Seriennummern langlebiger als fertige.

Cracks: Bei Programmen, die eine Online-Aktivierung erfordern, laufen Keygens ins Leere. Für solche Fälle und für Anwendungen, die sich nicht durch einen Lizenzschlüssel in eine Vollversion verwandeln lassen, stellen Hacker Cracks bereit. Dabei handelt es sich um Tools, die die ausführbare Programmdatei der jeweiligen Demoversion oder DLL-Dateien derart verändern, dass sie die automatische Datumsüberprüfung nicht mehr durchführt oder die Seriennummer nicht mehr überprüft.

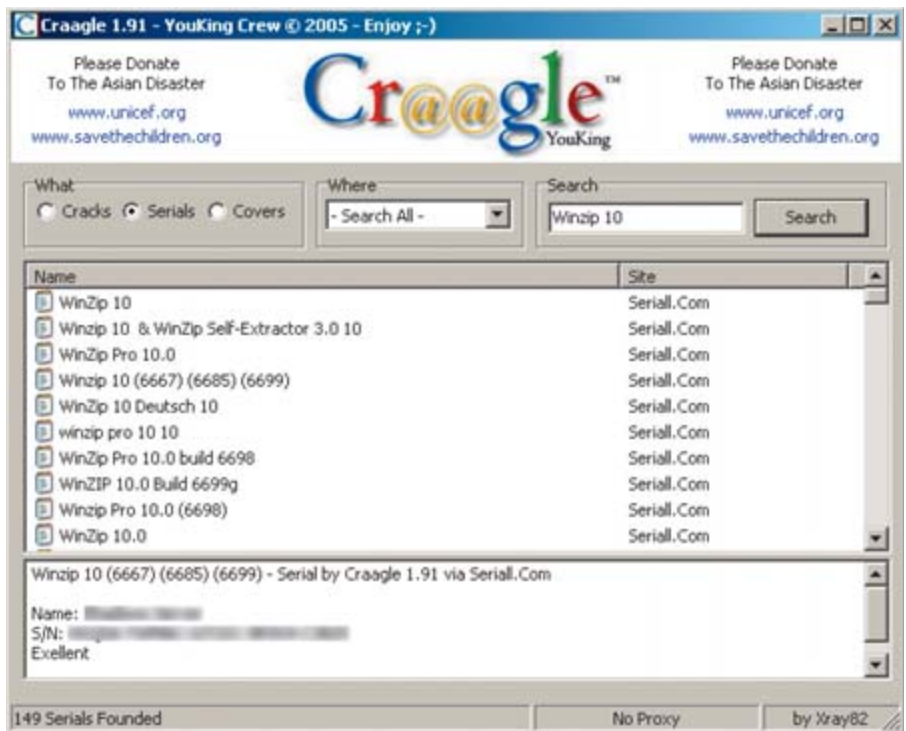
Solche Software-Veränderungen stellen eine Urheberrechtsverletzung dar. Im Extremfall wird man Cracks aber wohl anwenden dürfen, etwa wenn der Hersteller nicht zu erreichen ist und die rechtmäßig erworbene Software für eine unaufschiebbare Aufgabe dringend gebraucht wird. Existiert der Hersteller nicht mehr, hat er auch keine Rechte mehr an der Software, so dass ein Crack in diesem Fall rechtlich unbedenklich wäre.

Da es sich bei Schlüsselgeneratoren und Cracks um ausführbare Dateien handelt, gilt: Prüfen Sie sie vor der Benutzung mit einem Virens Scanner.

In jedem Fall verboten: Raubkopien tauschen

Statt eine eingeschränkte Version eines Programms zu testen, versuchen manche Anwender, kostenlos an eine Vollversion zu kommen. Das ist in jedem Fall verboten.

Tauschbörsen: Wer an illegale Kopien kommen wollte, hat früher oft Tauschbörsen dafür genutzt. Dieser Weg bietet sich jetzt nicht mehr an: Zum einen sind dort Fakes sehr verbreitet – also Dateien, die etwas anderes enthalten, als der Dateiname ver-



In einem Aufwasch: Das Tool Craagle fragt mehrere einschlägige Suchmaschinen im Internet parallel nach einer gewünschten Seriennummern für eine Software ab

spricht. Zum anderen spielt die rechtliche Lage eine Rolle. Wie die in den letzten Monaten durchgeführten Schläge gegen deutsche Tauschbörsen-Nutzer zeigen, greifen die Hersteller zu härteren Mitteln, um die Verbreitung unrechtmäßig kopierter Inhalte zu stoppen. Und auch wenn die eingeleiteten Verfahren derzeit nur Anwender betreffen, die Musikdateien zum Tausch angeboten haben, ist nicht auszuschließen, dass als Nächstes die Software-Hersteller in die Offensive gehen und Nutzer von Tauschbörsen gerichtlich verfolgen lassen.

Profis meiden Tauschbörsen inzwischen und ziehen sich etwa in den IRC (Internet Relay Chat) und in Newsgroups zurück.

Web-Speicher: Gern genutzt werden auch Anbieter von kostenlosem Speicherplatz im Web wie www.yourfilehost.com oder www.rapidshare.com, von denen es immer mehr gibt. Herunterladen kann man die Dateien von dort nur, wenn man den genauen Link kennt. Nach dem Upload der Dateien veröffentlichen die Verbreiter der Raubkopien die Links auf einschlägigen Websites. Mit speziellen Suchparametern ist es möglich, diese Links mit Google zu finden. Manche Anwender nutzen das bekannte Tool Free File Host Search (FFHS, www.pcwelt.de/691), das solche Suchparameter enthält. Es handelt sich dabei um ein Bookmarklet – also ein Mini-Javascript, das als Lesezeichen abgelegt wird. Beim Klick darauf öffnet sich eine Eingabebox, in die man einen Suchbegriff eingibt, zum Beispiel den Namen eines Programms. Das Javascript fügt dem Begriff die speziellen Parameter an und übergibt die Suchanfrage an Google. Um das Bookmarklet in den Internet Explorer einzufügen, klickt der Anwender mit der rechten Maustaste auf „FFHS – IE version“ und wählt „Zu Favoriten hinzufügen“. In Firefox funktioniert das per Rechtsklick auf „FFHS – Firefox version“ und „Lesezeichen für diesen Link hinzufügen“. Mit dem Tool Raubkopien zu suchen ist unzulässig. ❌

Eula: Was verbieten Hersteller, was nicht?

Wenn Sie eine Software installieren, erscheint auf dem Bildschirm zuallererst das „End Users License Agreement“ – kurz: Eula. Es lohnt sich, diese Lizenzbestimmungen durchzulesen.

Testversionen länger nutzen: Manche Hersteller beschränken die zulässige Nutzung nicht auf die Testphase. Bei unseren Stichproben konnten wir in den meisten Fällen keinen Passus finden, der die Nutzung über den Testzeitraum hinaus verbietet. Es gibt aber Ausnahmen: Beispielsweise weist Adobe in Punkt 14.5 des Software-Lizenzvertrags von Photoshop Elements darauf hin, dass die bestehende Lizenz nach Ablauf der Testphase endet. Ob allein aus einer leicht zu umgehenden, in die Software integrierten Zeitsperre ein Verbot abgeleitet werden kann, die Software auch darüber hinaus zu nutzen, ist fraglich.



Die besten Rootkit-Finder

Rootkits sind schädliche Programme der ganz fiesen Art. Für den Anwender unsichtbar, können sie den kompletten PC ausspionieren. Wir verraten, wie Sie sich wirksam schützen.

Von **Arne Arnold**

Rootkits sind hinterhältig. Denn sie manipulieren Ihr System so, dass Sie den schädlichen Code der Kits nicht sehen und damit auch nicht beseitigen können. Wir erklären in diesem Beitrag, wie Rootkits genau funktionieren, wer sie verbreitet – und vor allem, wie Sie sich vor den gefährlichen Biestern schützen. Dafür haben wir insgesamt 12 Sicherheits-Tools getestet.

Technik & Angriffe

So funktionieren Rootkits

In der Windows-Welt bezeichnet der Begriff Rootkit ein Programm, das Dateien auf

einem Rechner so versteckt, dass der Anwender diese nicht mehr entdecken kann. Bei den Dateien handelt es sich meist um schädlichen Code wie Spyware oder Trojaner – oder etwa um einen heimlich installierten Kopierschutz. Das Rootkit manipuliert die Kommunikation zwischen Anwendungen und dem Betriebssystem. Es filtert dabei Informationen, die eine Anwendung vom System angefordert hat.

Zwei Arten: Rootkits lassen sich in zwei Gruppen einteilen – und zwar danach, wie sie vorgehen. Die erste Gruppe bilden Rootkits, die sich tief in das System eingraben. Sie installieren sich zwischen zwei Schich-

ten der Systemfunktionen und filtern dann Informationen. Da sich diese Rootkits dabei im Kern des Betriebssystems (englisch: Kernel) verankern, werden sie auch als Kernel-Rootkits bezeichnet.

Ein Beispiel: Das Rootkit kopiert die Dateien Schädling.EXE und Spionage.DLL sowie Teile von sich selbst in ein Verzeichnis. Dann manipuliert es den Kernel so, dass diese Dateien nicht mehr angezeigt werden. Sie sind unsichtbar und können aus der Tarnung heraus beliebigen Schaden anrichten.

Die zweite Gruppe agiert auf der Ebene der Anwendungen. Diese Rootkits manipulieren laufende Prozesse im Speicher und enthalten auf diese Weise den Anwendungen einen Teil der angeforderten Infos vor.

So schleichen sich Rootkits ein

Die Technik der Rootkits beschränkt sich darauf, Schad-Software zu verstecken. Sie umfasst keinen speziellen Code, um sich selbst zu verbreiten. Tatsächlich streuen Gauner Schädlinge mit Rootkit-Technik wie gewöhnliche Trojaner – also über Sicherheitslücken in Windows und Anwenderprogrammen. Beliebt ist nach wie vor auch der alte Trick mit dem Mailanhang, der eine Rechnung, Mahnung oder Ähnliches sein soll, in Wirklichkeit aber der Schädling ist. Einige Rootkits kursieren als Sourcecode frei im Internet, andere werden verkauft. Vor allem die Verbreiter von Spyware haben sich schnell auf die Rootkit-Technik gestürzt. Sie kommt ihnen gerade recht, weil ihre Spionageprogramme auf diese Weise unentdeckt auf den PCs der Anwender arbeiten.

Per Rootkit-Technik werden auch Trojaner verbreitet. Sie machen einen Rechner fernsteuerbar, so dass der Programmierer des Schadcodes diesen missbrauchen kann.

Für technisch Interessierte

Rootkits können sich an vielen Stellen in Windows einklinken. Wenn Sie sich für die technischen Hintergründe interessieren – eine Methode erklären wir hier:

Subsystem: Die Sicherheitsarchitektur von Windows NT 4, 2000 und XP sieht vor, dass der Kern des Betriebssystems geschützt wird. Er selbst und einige Treiber laufen im Kernel-Modus und haben Zugriff auf alle Funktionen des Systems ebenso wie auf die Hardware. Anwendungen dagegen arbeiten im User-Modus, der nur minimale Zugriffsrechte besitzt. Trotzdem brauchen Anwen-

dungen auch Informationen über das System. Etwa muss ein Dateimanager wissen, welche Dateien auf der Festplatte gespeichert sind. Windows arbeitet deshalb mit einem Subsystem, über das eine Anwendung Infos vom Systemkern anfordern kann – die API (Application Programming Interface). Dieses Subsystem bietet Dynamic Link Libraries (DLLs), etwa die Kernel32.DLL, User32.DLL und Advapi32.DLL.

Die IAT-Manipulation: Startet man ein Programm, wird es in den Arbeitsspeicher geladen. Der Loader des Subsystems wertet dabei auch die Import Address Table (IAT) der Programmdatei aus. Darin stehen unter anderem die benötigten DLLs und ihre Funktionen. Ein Beispiel ist „FindFirstFile“ aus

der Kernel32.DLL, die am Ende auch die Funktion „FindNextFile“ zurückgibt. Zusammen mit dem Aufruf der Funktion „NtQueryDirectoryFile“ aus dem EAX-Register lassen sich so alle Dateien eines Verzeichnisses lesen. Ein Rootkit kann sich nun zwischen eine Anwendung und das System – die Kernel32.DLL – schieben, indem es Funktionen in der IAT der Anwendung auf sich selbst umleitet.

Abwehr & Tests

So schützen Sie sich

Die gute Nachricht: Eine Abwehr ist möglich und gar nicht so schwer. Denn alle bekannten Kernel-Rootkits können sich nur

Überblick Achtung: Rootkits

Inhalt	Seite
Technik & Angriffe	66
Abwehr & Tests	67
Anti-Rootkit-Tools: Wie wir testen	69
Kästen	
Achtung: Windows ist ein Rootkit	67
Tests: Rootkit-Finder	68

ins System einklinken, wenn sich der Anwender mit Admin-Rechten angemeldet hat. Arbeiten Sie aber mit Benutzerrechten, dann haben die Rootkits keine Chance. Ein Konto mit eingeschränkten Rechten erstellen Sie unter Windows XP und Vista über „Systemsteuerung, Benutzerkonten“.

Achtung: Sie müssen immer auch ein Konto mit Administratorrechten behalten, damit Sie etwa noch neue Programme unter Windows installieren können.

Als zweite Schutzmaßnahme setzen Sie eine gute Sicherheits-Software ein. Unser Test hat gezeigt, dass leistungsfähige Antiviren-Tools Rootkit-Schädlinge schon vor der Installation stoppen können.

Test: Die besten Rootkit-Finder

Wir wollten wissen, mit welchen Tools Sie sich am besten gegen Rootkits schützen können. Darum haben wir 12 Programme nach Rootkits suchen lassen. Die Tools stammen zum einen aus der Gruppe der klassischen Antiviren-Programme, zum anderen handelt es sich um spezielle Rootkit-Finder. Im Test sind auch zwei Sicherheits-Utilities von Microsoft, **Windows Defender** und das **Windows-Tool zum Entfernen bössartiger Software**. Beide stehen zwischen klassischem Virenschanner und Spezial-Tool.

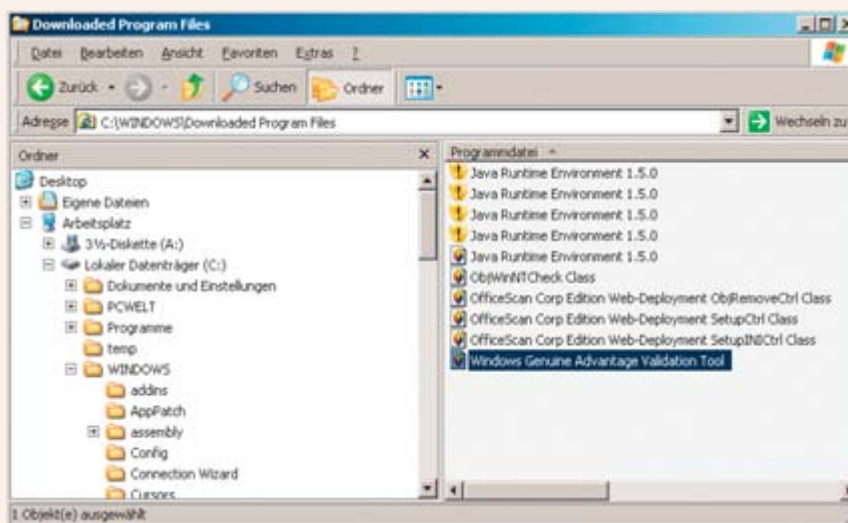
Das Ergebnis: Antiviren-Programme, die sich in der Vergangenheit einen guten Ruf bei der Suche nach Viren erworben haben, schneiden mittlerweile auch bei der Jagd auf Rootkits gut ab. So teilen sich gleich zwei klassische Antiviren-Tools den ersten Platz: **Norton Antivirus** und **Kaspersky Anti-Virus** zeigten eine beinahe identisch gute Leistung und schafften beide 29 von den möglichen 31 Punkten. Mit deutlichem Abstand, aber mit noch guten Ergebnissen kommt das kostenlose **Antivir PE Classic** (auf CD) auf den dritten Rang, gefolgt vom **Antiviren-Kit**.

Achtung: Windows ist ein Rootkit

Betrachtet man bestimmte Verhaltensweisen, muss man feststellen: Windows ist selbst ein Rootkit. Denn das System filtert und manipuliert die Infos darüber, welche Dateien vorhanden sind und welche nicht, fast wie die fiesen Kits. Microsoft nennt das etwa Namespace und verkauft es als Funktion für mehr Komfort.

Windows-Explorer: Machen Sie sich selbst ein Bild von der Manipulation. Werfen Sie mit dem Explorer einen Blick in den Ordner „Windows\Downloaded Program Files“. Darin sollen sich die vom Internet Explorer heruntergeladenen Active-X-Komponenten befinden. Doch die meisten Dateien, die Windows dort anzeigt, gibt es so gar nicht. Das WGA-Tool etwa besteht aus mehreren Programmen, die Sie hier nicht zu sehen bekommen. Das lässt sich zum Beispiel über die Befehlszeile prüfen. Wer sich den Inhalt des Ordners mit „dir“ anzeigen lässt, bekommt andere, aber meist bei weitem nicht alle Dateien der Active-X-Komponenten aufgelistet.

Registry: Wo sich tatsächlich alle Dateien der Active-X-Komponenten befinden, lässt sich nur mit Aufwand ermitteln: Öffnen Sie im Windows-Explorer jeweils das Kontextmenü der vorgeblichen Dateien. Unter „Eigenschaften, Allgemein“ kopieren Sie die jeweilige ID und suchen diese nun in der Registry. Dort finden Sie dann den Pfad zu den Dateien.



Getäuscht: Der Windows-Explorer zeigt Dateien, die keine sind. Es handelt sich hier um Active-X-Komponenten, die Windows zusammenfasst und als eine Datei darstellt

Knacken Achtung: Rootkits

Auf Platz 5 landet das erste speziell auf Rootkits optimierte Programm: **Blacklight** bietet keinen klassischen Dateiscanner oder Wächter, denn es ist nur für die Suche nach bereits aktiven Rootkits ausgelegt. Entsprechend kann es keine Installationsdateien finden und nicht punkten. Bei weiteren Tests erlaubte es sich keinen einzigen Fehler. Fast ebenso gut schnitt das Spezial-Tool **Rootkit Unhooker** ab.

Die übrigen Testkandidaten empfehlen sich nicht für den Einsatz gegen Rootkits. Sie kommen nur in Betracht, wenn die anderen Tools doch mal versagt haben.

Übrigens: Das Microsoft-Tool **Windows Defender** meldete die Installationsversuche der Rootkits mit der allgemeinen Warnung, dass ein Programm versuche, Änderungen am System vorzunehmen. Wachsam, fortgeschrittenen Anwendern genügt diese Information, um ihren PC abzuschotten.

So setzen Sie die Tools ein

Damit sich erst gar kein Rootkit auf Ihren PC einschleichen kann, arbeiten Sie nur mit Benutzerrechten und setzen ein Antiviren-Programm ein. Empfehlenswert sind die ersten vier Tools aus der Tabelle. Denn

jedes Programm spürte bereits die Installationsdateien der Rootkits auf. Die Wächter blocken somit die Schädlinge ab, noch bevor sie das System verändern.

Der Schutz lässt sich weiter optimieren, indem Sie ab und an das kostenlose Programm **Blacklight** von F-Secure einsetzen. Es fand sowohl Schädlinge, die Dateien, als auch solche, die Prozesse verstecken. Es ergänzt somit die anderen Tools optimal. Blacklight läuft immer nur ein paar Wochen. Danach laden Sie das Tool in einer neuen, rund 1 MB großen aktuellen Version von der Hersteller-Site herunter.

Im Überblick: 12 Antirootkit-Tools

Hersteller/Produkt	Norton Antivirus 2007	Kaspersky Anti-Virus 6.0	Avira Antivir PE Classic 7	G-Data Antiviren-Kit 2007	Blacklight 1.0 Beta	Rootkit Unhooker 3.01
Anbieter	Symantec	Kaspersky	Avira	G-Data	F-Secure	— 1)
Internet (Download)	www.symantec.de	www.kaspersky.de	www.fee-av.de (15 MB)	www.gdata.de	www.f-secure.com/blacklight (900 KB)	www.pcwelt.de/7b2) (154 KB)
Preis	40 Euro	30 Euro	gratis	30 Euro	gratis	gratis
Windows-Betriebssysteme	XP, Vista	98/ME, NT 4, 2000, XP, Vista	98/ME, 2000, XP	2000, XP, Vista	2000, XP, 2003 Server, Vista 32 Bit	2000, XP, 2003 Server
Sprache	Deutsch	Deutsch	Deutsch	Deutsch	Englisch	Englisch
Platz	1 PC WELT	1 PC WELT	3	4	5	6
Note	1,5 Testsieger	1,5 Testsieger	2	2,5	2,5	2,5
TESTERGEBNISSE						
Datei-versteckende Rootkits (inaktiv/aktiv/Entfernung)						
AFX	ja/ja/ja	ja/ja/ja	ja/ja/ja	ja/ja/ja	-/ja/ja	-/ja/ja
Hacker Defender 1.00	ja/ja/ja	ja/ja/ja	ja/nein/nein	ja/nein/nein	-/ja/ja	-/ja/ja
Hacker Defender 1.00r	ja/ja/ja	ja/ja/ja	ja/nein/nein	ja/nein/nein	-/ja/ja	-/ja/ja
NT Illusion	ja/ja/ja	ja/ja/ja	ja/nein/nein	ja/ja/nein 2)	-/ja/ja	-/ja/ja
NT Rootkit	ja/ja/ja	ja/ja/ja	ja/ja/nein	ja/ja/nein 2)	-/ja/ja	-/ja/ja
Vanquish	ja/ja/ja	ja/ja/ja	ja/ja/ja	ja/ja/ja	-/ja/ja	-/ja/ja
Winrootkit	ja/ja/ja	ja/ja/ja	ja/ja/ja	ja/ja/nein 2)	-/ja/ja	-/ja/ja
Rootkits gefunden	alle 21	alle 21	14 von 21	14 von 21	14 von 21	14 von 21
Malware mit Rootkit-Techniken 3) (inaktiv/aktiv/Entfernung)						
Feebs!ITW#25	ja/ja/ja	ja/ja/ja	ja/ja/nein	ja/ja/nein 2)	-/ja/ja	-/ja/ja
Maslan.C	ja/ja/ja	ja/ja/ja	ja/ja/ja	ja/ja/nein 2)	-/ja/ja	-/ja/nein
Malware gefunden	alle 6	alle 6	5 von 6	4 von 6	4 von 6	3
Prozess-versteckende Rootkits (inaktiv/aktiv)						
FU	ja/nein	ja/nein	ja/nein	ja/nein	-/ja	-/ja
FU2	ja/nein	ja/nein 1)	ja/nein 1)	ja/nein	-/ja	-/ja
Rootkits gefunden	2 von 4	2 von 4	2 von 4	2 von 4	2 von 4	2 von 4
GESAMTSUMME (31)	29 von 31	29 von 31	21 von 31	20 von 31	20 von 31	19 von 31

1) Unbekannter Programmierer 2) Das System stürzte ab 3) In the Wild (verbreitet), versteckt Dateien

Gratis-Schutz: Wer als Antiviren-Programm Antivir PE Classic einsetzt und es durch Blacklight ergänzt, macht seinen PC sicher. Allerdings sollten Sie häufig mit Blacklight prüfen, ob sich nicht doch ein Rootkit eingeschlichen hat. Denn Antivir war bei der Suche nach bereits versteckten Rootkits nicht so zuverlässig wie die beiden Testsieger.

Gestoppt: Ihr Antiviren-Programm meldet, dass sich ein Rootkit auf Ihrem Rechner installieren will? Dann hat es die Installation verhindert, und Sie müssen nur noch das Löschen der gefährlichen EXE-Datei bestätigen. Ihrem System ist nichts passiert.

Neu-Installation: Anders sieht es aus, wenn bei einem Scan ein aktives Rootkit gemeldet wird. Zwar waren im Test die guten Tools in der Lage, den Code zu entfernen. Doch es tauchen immer wieder Schädlinge auf, die automatisch neuen Code aus dem Internet nachladen. Dass das Antiviren-Programm auch diesen erkennt, ist nicht garantiert. Somit sollten Sie Ihr System neu aufsetzen, wenn auf Ihrem PC ein Rootkit aktiv war.

Wie wir testen

Die Spezialisten Andreas Marx und Guido Habicht vom Sicherheitslabor AV-Test

(www.av-test.org) haben die 12 Programme auf die Suche nach Rootkits geschickt. Die einzelnen Tools mussten im Software-Testlabor zeigen, ob sie die Installationsdateien auf Festplatte finden, aktive Rootkits aufspüren und diese entfernen können. Für jede erfolgreiche Aktion gab es einen Punkt. Insgesamt waren 31 Punkte zu erreichen. Programme ohne klassischen Dateiscanner haben keine Möglichkeit, Installationsdateien aufzuspüren – deshalb können sie die entsprechenden Punkte nicht einheimsen. In diesen Fällen steht in der Tabelle ein Strich („–“) für „nicht verfügbar“.

Windows-Tool zum Entfernen bössartiger Software 0107	AVG 7.5	Anti-Rootkit 1.2	auf CD Rootkit Revealer 1.7	Windows Defender 1.1	auf CD Rootkit Hook Analyzer 2.0
Microsoft	Grisoft	Sophos	Microsoft	Microsoft	Resplendence Software Projects
www.pcwelt.de/mal (5,4 MB)	http://free.grisoft.com (18,8 MB)	www.pcwelt.de/70a (1,1 MB)	www.pcwelt.de/37a (230 KB)	www.pcwelt.de/3d8 (5 MB)	www.pcwelt.de/444 (770 KB)
gratis	gratis	gratis	gratis	gratis	gratis
2000, XP, 2003 Server, Vista	98/ME, NT4, 2000, XP, Vista	NT 4, 2000, XP, 2003 Server	NT 4, 2000, XP	XP, 2003 Server	2000, XP, 2003 Server
Deutsch	Englisch	Englisch	Englisch	Deutsch	Englisch
7	8	9	10	11	12
3	3	3	5	5	5,5
nein/nein/nein	ja/nein/nein	–/nein/nein	–/ja/nein	–/nein/nein	–/nein/nein
ja/ja/ja	ja/nein/nein	–/ja/ja	–/ja/nein	–/nein/nein	–/ja/nein
ja/ja/ja	ja/nein/nein	–/ja/ja	–/ja/nein	–/nein/nein	–/ja/nein
nein/nein/nein	nein/nein/nein	–/ja/ja	–/nein/nein	–/nein/nein	–/nein/nein
ja/ja/ja	ja/nein/nein	–/ja/ja	–/ja/nein	–/nein/nein	–/nein/nein
nein/nein/nein	ja/nein/nein	–/ja/ja	–/nein/nein	–/nein/nein	–/nein/nein
ja/ja/ja	ja/ja/ja	–/nein/nein	–/ja/nein	–/nein/nein	–/nein/nein
12 von 21	8 von 21	10 von 21	5 von 21	0 von 21	2 von 21
nein/nein/nein	ja/ja/nein	–/nein/nein	–/nein/nein	–/nein/nein	–/nein/nein
ja/ja/ja	ja/ja/ja	–/ja/ja	–/ja/nein	–/nein/nein	–/nein/nein
3 von 6	5 von 6	2 von 6	1 von 6	0 von 6	0 von 6
ja/nein	ja/nein	–/ja	–/nein	–/nein	–/ja
ja/nein	ja/nein	–/ja	–/nein	–/nein	–/ja
2 von 4	2 von 4	2 von 4	0 von 4	0 von 4	2 von 4
17 von 31	15 von 31	14 von 31	6 von 31	0 von 31	4 von 31



HD geknackt

Der Kopierschutz von HD-DVD und Blu-Ray schien unüberwindlich, die Verschlüsselung von Premiere HD galt als sicher. Doch jetzt haben Hacker tiefe Löcher in die Systeme gerissen.

Von Lukas Merten

Erst mit hochauflösendem Video, wie es HDTV, HD-DVD und Blu-Ray ins Haus bringen, lässt sich die Bildqualität schicker Flachbildschirme und Projektoren so richtig genießen. Doch die Fan-Gemeinde des neuen Bildformats teilt sich in zwei Lager. Denen, die ihr Premiere-Abo ehrlich bezahlen, stehen immer mehr Schwarzseher gegenüber. Sie knacken die Kopierschutzverfahren mit illegaler Software und gucken, ohne zu zahlen. Wir haben uns in den einschlägigen Web-Foren umgesehen, um herauszufinden, was derzeit möglich ist.

1. Angriffsziel 1: Premiere HDTV

Seit Mitte 2006 strahlt Pay-TV-Anbieter Premiere die beiden Sender Premiere HD und Discovery Channel HD aus. Bei ersterem bestimmen noch recht junge Spielfilme wie Sin City und King Kong sowie Sport-Veranstaltungen wie die UEFA Champions League

das Programm. Discovery Channel HD sendet Dokumentationen aus Wissenschaft, Natur und Technik. Beide Sender liefern ein mit 1920 mal 1080 Punkten aufgelöstes Bild und damit gut fünfmal mehr Bildinformationen als das herkömmliche PAL-Signal. Der Empfang ist über Satellit (Astra 19,2°) und in Kabelnetzen möglich.

2. Gründe: Warum Premiere gehackt wird

Dass gehacktes Pay-TV monatlich einige Euro spart – im Fall von Premiere sind es 10 Euro pro Sender – liegt auf der Hand. Aber die Hacker lockt auch die Möglichkeit, Hürden einzureißen, die Premiere selbst

Kunden in den Weg legt. Nach den allgemeinen Geschäftsbedingungen von Premiere dürfen auch ehrlich bezahlte Smartcards nur in einem offiziell von Premiere zertifizierten Receiver (Empfänger) betrieben werden. Das bringt nicht nur wegen des begrenzten Angebots an solchen Receivern Einschränkungen mit sich.

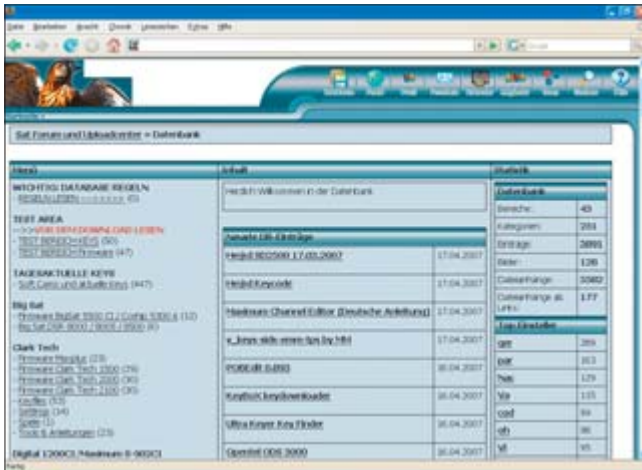
Voraussetzung für die Zertifizierung ist unter anderem die Unterstützung für das Kopierschutzsystem HDCP (High-bandwidth Digital Content Protection). In Verbindung mit HDCP und einem mit den Sendungen ausgestrahlten Zusatzsignal, dem Broadcast Flag, kann Premiere bestimmen, auf welchen Ausgängen des Receivers das Bild in welcher Qualität zur Verfügung steht. Während man bei Discovery Channel HD derzeit noch keine Einschränkungen hinnehmen muss, gibt es Premiere HD in voller Qualität ausschließlich am HDMI-Ausgang, und dort auch nur für ebenfalls HDCP-fähige Geräte. Ältere Beamer und Bildschirme ohne HDCP bleiben deshalb genauso außen vor wie HDCP-fähige Geräte, bei denen der Verbindungsaufbau mit dem TV-Empfänger – HDCP-Handshake genannt – nicht klappt. Und das kommt bei der noch recht jungen Technik gar nicht selten vor. Außerdem macht HDCP die Aufzeichnung von Premiere HD unmöglich. Wer nicht zur richtigen Sendezeit vor dem Fernseher sitzt, verpasst den Anfang des Films, von der fehlenden Möglichkeit, Lieblingsfilme in Top-Qualität auf DVD zu brennen, ganz zu schweigen.

3. Illegal: Spezialsoftware ersetzt die Premiere-Smartcard

Anfang des Jahres 2007 tauchten in Online-Foren erste Hinweise darauf auf, dass Hacker die Premiere-Verschlüsselung geknackt haben. Dabei überwandern sie sowohl das zur Verschlüsselung der HDTV-Kanäle eingesetzte Verfahren namens Nagravision wie auch den zur Sicherung der im PAL-Verfah-



Freigeschaltet: Hacker verwandeln HDTV-Empfänger wie den Topfield TF 7700 HSCI in Premiere-Empfänger (Punkt 2)



Heiße Ware: Hacker stellen ihre illegalen Programme in Foren zum Download für die Masse der Schwarzseher bereit (Punkt 3)

ren übertragenen Kanäle eingesetzten Nagravision-Dialekt namens Aladin. Seither kursiert Software als Download im Netz, die den Premiere-zertifizierten Receiver genauso überflüssig macht wie die Smartcard. Diese Software wird von Schwarzsehern auf verschiedene Weise eingesetzt.

4. Methode 1: CA-Module mit manipulierter Firmware

Neben Nagravision existieren beispielsweise mit Conax, Seca und Viaccess zahlreiche weitere Verschlüsselungsverfahren – zu viele, als dass jeder Empfänger alle beherrschen könnte. Viele Receiver bieten deshalb ein Common Interface (CI), zu Deutsch: eine

und Dragon CAM sind so konstruiert, dass sich die darin enthaltene Software (Firmware) austauschen lässt. So kann der Hersteller auch noch nach Auslieferung seines CAM Fehler bereinigen oder modernere Verschlüsselungsverfahren nachrüsten – wichtig, wenn ein Pay-TV-Sender auf ein neues Verfahren umstellt. Allerdings wird diese Patch-Funktion auch von Hackern genutzt, um dem CAM illegale Software unterzuschieben, die Verschlüsselungsverfahren und das Vorhandensein einer Smartcard simuliert. Steckt man ein derart manipuliertes CAM in einen nicht von Premiere zertifizierten, das Broadcast Flag ignorierenden Receiver, steht Premieres HDTV auf allen

gemeinsame Schnittstelle. Über diese lassen sich dem Empfänger verschiedene Verschlüsselungsverfahren durch Einlegen eines Conditional Access Module (CAM) beibringen. Tatsächlich entschlüsseln kann das CAM erst mit eingelegter Smartcard, die der Pay-TV-Sender nur gegen Bezahlung herausruckt.

Bei Hackern besonders beliebte CAM wie T-Rex, Diablo CAM

Überblick HD-TV gratis

Inhalt	Seite
1. Angriffsziel 1: Premiere HDTV	70
2. Gründe: Warum Premiere gehackt wird	70
3. Illegal: Spezialsoftware ersetzt die Premiere-Smartcard	70
4. Methode 1: CA-Module mit manipulierter Firmware	71
5. Schwarzseher-Leid	71
6. Methode 2: Manipulierte TV-Software	71
7. Beliebte Ziele: Prog DVB und DVB Viewer	72
8. Methode 3: HDTV-Receiver mit manipulierter Firmware	72
9. Angriffsziel 2: HD-DVD und Blu-Ray	72
10. HDCP, COPP und AAC	73
11. Einfallstore: Player-Software und Xbox-Laufwerk	73
12. Raubkopier-Sperre per Zwangsupdate	73
Kästen	
AACS auf einen Blick	71
Premiere-Smartcard: Mehrfachnutzung	72

Ausgängen und ohne HDCP-Schutz bereit. Übrigens belassen es modifizierte CAM selten bei der Entschlüsselung von Premiere, sondern machen gleich mehrere Pay-TVs „hell“, etwa auch Arena, Digital+ und die Grundverschlüsselung in Kabelnetzen. Zum Patchen genügt Hackern ein Schreibgerät wie das Cas3+ , das inklusive der notwendigen Software bei Ebay legal erhältlich ist.

5. Schwarzseher-Leid

Forumsberichten zufolge ist das Schwarzsehen für Hacker kein ungetrübter Genuss. Nicht jeder Receiver arbeitet mit jedem modifizierten CAM zusammen, manche stürzen beim Einlegen sogar ab. Andere Receiver erkennen das Modul zwar, zeigen aber nur ruckelnde Bilder an. Solche Probleme sind ehrlichen Abonnenten mit zertifiziertem Empfänger natürlich fremd. Hacker begehen diesen Hürden mit im Netz kursierenden Kompatibilitätslisten, die aber weder aktuell noch zuverlässig zu sein scheinen.

6. Methode 2: Manipulierte TV-Software

Mit Methode 1 gelingt den Hackern zwar der illegale Empfang von Premiere HD, aber weil es an entsprechenden Empfängern

AACS auf einen Blick

Der folgende schematische Überblick über die Funktionsweise von AACS ergibt sich aus der AACS-Spezifikation, die öffentlich auf der Website des AACS Lizenz-Administrators (www.aacsla.com) einsehbar ist.

1. Der Player verfügt über 253 vom AACS LA zugeteilte Geräteschlüssel (Device Keys), aus denen mehrere Processing Keys abgeleitet werden.
2. Beim Start der Wiedergabe werden die Processing Keys der Reihe nach am auf der DVD gespeicherten Media Key Block ausprobiert, bis dieser den Media Key freigibt.
3. Der Player fragt die auf der DVD gespeicherte Volume ID ab, die das Laufwerk nur an AACS-fähige Player herausgibt. Aus der Kombination von Media Key und Volume ID entsteht dann der so genannte Volume Unique Key.
4. Mit Hilfe des Volume Unique Key werden die verschlüsselt auf der DVD gespeicherten Title Keys entschlüsselt. Mit den Title Keys lässt sich der DVD-Inhalt entschlüsseln.
5. Die Entschlüsselung geschützter DVDs durch kompromittierte Player verhindert die AACS LA dadurch, dass sie nur noch solche Media-Key-Blöcke an DVD-Hersteller ausgibt, die sich mit keinem der in diesen Playern hinterlegten Geräteschlüssel beziehungsweise den daraus abgeleiteten Processing Keys öffnen lassen. Trifft ein Player auf eine solche DVD, sperrt er sich selbst für die Wiedergabe aller geschützten, das heißt alter wie neu erscheinender DVDs.



Neuem aufgeschlossen: DVB Viewer ist wegen seiner Plug-in-Schnittstelle bei Hackern besonders beliebt (Punkt 7)

mangelt, fällt die Aufnahme schwer. Außerdem sind Anschaffungskosten von rund 160 Euro für CAM und Schreibgerät kein Pappenstiel. Da liegt der Gedanke nah, einen bereits vorhandenen PC zum HDTV-Empfänger aufzurüsten und ihm die bereits vorhandene Entschlüsselungs-Software unterzubeln. Und genau auf dieser Vorgehensweise basiert die zweite Methode der Angreifer. Der Hacker-PC, typischerweise mit Windows XP SP 2, benötigt äußerst viel Rechenkraft für die illegale Entschlüsselungsfunktion. Ein Prozessor wie Intels Core 2 Duo E6400 oder dessen Pendant von AMD

Statt die mit den TV-Karten mitgelieferte Empfangssoftware zu verwenden, greifen Schwarzseher üblicherweise auf die legalen Programme Prog DVB (für Win 98/ME, 2000, XP, gratis auf CD und unter www.progdvb.com, 2,7 MB) und DVB Viewer (für Win 98/ME, 2000, XP und Vista, 15 Euro, www.dvbviewer.com) zurück. Sie arbeiten nicht nur mit vielen verschiedenen TV-Karten zusammen. Aus Hacker-Sicht sind sie vor allem deshalb attraktive Angriffsziele, weil sie über Plug-in-Schnittstellen verfügen und damit von Haus aus für das Nachrüsten

ist genauso Pflicht wie eine Hochleistungs-Grafikkarte von ATI oder Nvidia mit HDMI-Ausgang und Beschleunigungsfunktion für das zur Übermittlung des HDTV-Bildes verwendete H.264-Verfahren. Den Empfang des TV-Signals übernimmt eine HDTV-fähige Fernsehkarte. Hacker mit Sat-Schlüssel greifen beispielsweise auf die DVB-S2-fähige S2-3200 des Herstellers Technotrend zurück.

7. Beliebte Ziele: Prog DVB und DVB Viewer

neuer Funktionen vorbereitet sind. Die von den Programmierern der TV-Anwendungen für legale Plug-ins vorgesehene Funktion missbrauchen Hacker für ihre Zwecke. Sie docken hier das rechtlich zumindest bedenkliche Plug-in SoftCSA an, das den von der TV-Karte gelieferten, verschlüsselten Datenstrom in Zusammenarbeit mit einem illegalen Programm wie vPlug oder s2emu decodiert. Weil diese Programme ein manipuliertes CAM ersetzen, heißen sie im Hacker-Jargon „Softcam“.

8. Methode 3: HDTV-Receiver mit manipulierter Firmware

Als ob es nicht schon genügend Einfallstore gäbe, wird sich Premiere hinsichtlich seiner HDTV-Programme bald noch mit einem dritten Einbruchverfahren auseinandersetzen müssen. Dass viele Receiver ihre volle Leistungsfähigkeit erst dann ausspielen, wenn man die vom Hersteller programmierte Firmware mit einer aus dem Internet heruntergeladenen Alternative ersetzt, ist hinlänglich bekannt. Bestes Beispiel dafür ist die D-Box 2, die dank nachträglich installiertem Linux auch TV-Sendungen aufzeichnet und Filmdateien, DVDs und MP3s abspielt. Aber genauso wie Hacker CAM und TV-Anwendungen für das Schwarzsehen manipulieren, vergreifen sie sich auch an den an und für sich legalen alternativen Betriebssystemen. Sie schieben ihnen die Entschlüsselungs-Funktionen per Software-Paket unter. Letztere funktionieren zwar genauso wie Soft-CAMs, werden im Bereich der Receiver aber „Emu“ (von Emulator) genannt. Die Hacker gehen äußerst produktiv zu Werke. Auf einschlägigen Websites fanden wir so gut wie für jeden Receiver, auf den man eine alternative Betriebssoftware aufspielen kann, auch eine Software mit Emu-Funktion. Dass sich Premieres HDTV noch nicht auf diese Weise entschlüsseln lässt, dürfte schlicht daran liegen, dass noch für keinen der durch die Bank sehr neuen HDTV-fähigen Receiver ein Ersatz-Betriebssystem zur Verfügung steht, das sich um einen Emu „bereichern“ ließe.

9. Angriffsziel 2: HD-DVD und Blu-Ray

Das Kopieren von Video-DVDs hat sich wegen des schwachen Kopierschutz-Verfahrens CSS (Content Scrambling System) beinahe zum Volkssport entwickelt. Um zu

Premiere-Smartcard: Mehrfachnutzung

Neben dem legalen Betrieb der Smartcard im Premiere-zertifizierten Receiver und dem illegalen Entschlüsseln ohne Smartcard wird in Hacker-Foren noch eine dritte Lösung diskutiert. Dabei wird die ordentlich bezahlte Abokarte in einem nicht zertifizierten Receiver betrieben. Grundlage dafür können ebenfalls die manipulierten CAM wie T-Rex, Dragon CAM oder Diablo CAM sein, aus denen die zur kartenlosen Entschlüsselung notwendigen Keys (Zahlenkombinationen) gelöscht wurden. Doch auch diese Betriebsform dürfte zumindest gegen geltendes Urheberrecht verstoßen, denn die Verschlüsselungsverfahren wie NagraVision dürfen nicht ohne korrekte Lizenz verwendet werden – und über eine solche werden die unbekannten Programmierer der alternativen CAM-Firmwares wohl kaum verfügen.

Anders sieht es bei CAM aus, deren Original-Software Premieres HDTV (mit Originalkarte) entschlüsselt, beispielsweise das ältere Alphacrypt mit Firmware 3.11 oder das ganz neue Omegacrypt TC. Der Hersteller des letzteren wirbt sogar ausdrücklich damit, dass die in diesem CAM eingesetzte Entschlüsselungstechnik eine von Rechten Dritter freie Eigenentwicklung sei. Dennoch verstößt der Betrieb gegen Premieres Geschäftsbedingungen. Dem Pay-TV-Sender fehlt allerdings eine Möglichkeit zu kontrollieren, in welchen Geräten seine Smartcards eingesetzt werden.



Kommunikativ: Dem HD-DVD-Laufwerk für Microsofts Xbox 360 entlockten die Hacker besonders viele Geheimnisse (Punkt 11)

verhindern, dass sich dieses Debakel bei den Nachfolge-Formaten HD-DVD (High Density Digital Versatile Disc) und Blu-Ray wiederholt, hat die Filmindustrie hohen Aufwand betrieben. Zahlreiche Kopierschutz-techniken schützen das auf den High-End-DVDs gespeicherte, hochauflösende Bildmaterial auf dem Weg durch die Wiedergabekette. Mit den Stationen DVD-Laufwerk, Player-Software, Grafikkarte und Bildschirm/Beamer ist letztere vor allem beim Abspielen auf dem PC besonders lang und damit potenziell anfällig für Angriffe.

10. HDCP, COPP und AACS

Wie bei Premieres HDTV sorgt auch bei HD-DVD und Blu-Ray der Kopierschutz HDCP dafür, dass das Bildsignal nicht am HDMI-Ausgang der Grafikkarte abgezapft und aufgezeichnet werden kann. Dass die Grafikkarte auch wirklich HDCP-fähig ist, überprüft die Player-Software mit Microsofts COPP-Verfahren (Certified Output Protection Protocol). COPP verschlüsselt außerdem die Bilddaten auf dem Weg von der Player-Software zur Grafikkarte, so dass sie sich nicht mit einer Drittsoftware abgreifen lassen. Ohnehin ist der direkte Angriff auf die durch AACS (Advanced Access Content System) geschützten Daten auf der HD-DVD oder Blu-Ray-Disc die für Hacker interessantere Methode, denn wenn er gelingt, lässt sich der gesamte DVD-Inhalt kopieren.

AACS besteht aus mehreren Verschlüsselungsstufen (siehe Kasten „AACS auf einen Blick“ auf Seite 71), die unter anderem dafür sorgen, dass sich geschützte Medien nur mit einem den Kopierschutz beachtenden Player abspielen und auch nicht einfach 1:1 kopieren lassen. Alle Vorgänge rund um

AACS werden vom Lizenzierungs-Administrator (AACS LA) organisiert. Diese Firma verteilt digitale Schlösser und gibt die passenden Schlüssel an die Player-Hersteller.

11. Einfallstore: Player-Software und Xbox-Laufwerk

Mit AES (Advanced Encryption Standard) basiert AACS auf einem derzeit nicht zu knackenden Verschlüsselungsverfahren. Statt sich direkt an die Scheibe heranzuwagen, beobachteten Hacker in den letzten Wochen deshalb, was die Player-Software während der Wiedergabe auf ihrem PC treibt. Insbesondere behielten sie dabei die von den Programmen im Arbeitsspeicher des PCs hinterlegten Daten im Auge. Außerdem belauschten sie die Kommunikation eines per USB mit dem Rechner verbundenen HD-DVD-Laufwerks, das eigentlich als Zubehör für Microsofts Xbox 360 verkauft wird.

Dabei entdeckten die Angreifer, dass die Player Win DVD und Power DVD die für die Entschlüsselung des DVD-Inhalts notwendigen Schlüssel, die auf der DVD noch gut gesichert sind, zu ver-

schiedenen Zeitpunkten ungesichert im Arbeitsspeicher des Rechners ablegen. Mit dem Kommandozeilen-Programm Aacskeys entwickelten sie sogar eine Software, die diese Abhöraktion automatisiert und alle relevanten Schlüssel auf den Bildschirm bringt. Damit ausgerüstet kopieren gleichfalls in der Szene entstandene Tools wie Backup HDDVD und Backup Blu-Ray den entschlüsselten Inhalt der DVD auf die Festplatte, von wo aus er sich abspielen und weiterverarbeiten lässt. Der Einsatz dieser Programme ist in Deutschland illegal.

12. Raubkopier-Sperre per Zwangsupdate

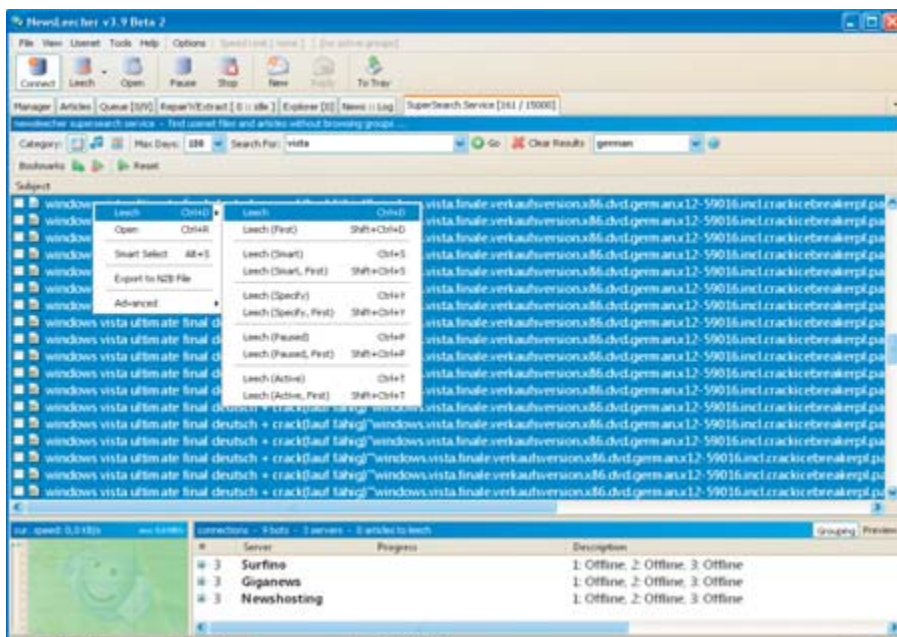
Wird bekannt, dass ein Player kompromittiert wurde, nimmt der AACS LA in für neu erscheinende DVDs erzeugte digitale Schlösser ein Signal auf, das diesen Player zur Selbstdeaktivierung zwingt. Nach dem Einlegen einer DVD, die ein solches Schloss enthält, gibt er nicht einmal mehr ältere geschützte Titel wieder. Es ist dann am Hersteller, eine aktualisierte Software zu veröffentlichen und die erneute Freigabe seines Players beim AACS LA zu beantragen. ❌

```

C:\Windows\system32\cmd.exe
C:\>aacskeys 1.0
Processing key:
Encrypted C-value:
Corresponding unit:
Decrypted C-value:
Media key:
Decrypted verification data:
Decrypted verification data should be:
Decrypted verification data:
RGID:
Host certificate from:
Host certificate (Owner):
Host Private Key (Owner):
Host nonce (Owner):
Drive certificate (Owner):
Drive nonce (Owner):
Drive key point (Owner):
Drive key signature (Owner):
Host key (Owner):
Host key point (Owner):
Host key signature (Owner):
Host key (Owner):
Volume ID:
Volume ID (Owner):
Volume Unique Key:
Title Key File (Owner):
Encrypted Title Key 1:
Encrypted Title Key 2:
Encrypted Title Key 3:
Encrypted Title Key 4:
Encrypted Title Key 5:
Encrypted Title Key 6:
Encrypted Title Key 7:
Encrypted Title Key 8:
Decrypted Title Key 1:
Decrypted Title Key 2:
Decrypted Title Key 3:
Decrypted Title Key 4:
Decrypted Title Key 5:
Decrypted Title Key 6:
Decrypted Title Key 7:
Decrypted Title Key 8:
C:\>

```

Schwarz auf Weiß: Aacskeys findet HD-DVD- und Blu-Ray-Schlüssel durch Abhören der Player-Software (Punkt 11)



Wie Katz und Maus

Mit Windows Vista wollte Microsoft endlich ein System schaffen, das Raubkopierern trotz und nur gegen Bezahlung dauerhaft funktioniert. Die Technik scheint ein Flop zu sein.

Von **Peter-Uwe Lechner**

Für das fast sechs Jahre alte Windows XP kommt der Aufwand, Raubkopierer auszusperrern, eigentlich zu spät. Trotzdem forciert Microsoft mit Windows Genuine Advantage konsequent den Kampf gegen die Software-Piraterie. Mit mäßigem Erfolg, denn mit entsprechenden Tools aus dem Internet lässt sich die Echtheitsprüfung leicht abschalten. Zudem gibt es im Internet fertige XP-Setup-CDs, die von allen Schutzmaßnahmen befreit sind.

Etwas schwerer hat es die Raubkopierer-Szene mit Windows Vista. Doch eine Hürde scheint das neue Betriebssystem ebenfalls nicht zu sein. Mit Patches aus dem Web lässt

sich auch Vista ohne gültigen Lizenzschlüssel freischalten. Und wenn Microsoft eine der verbreiteten Knackmöglichkeiten per Online-Update schließt, ist der nächste Patch der Raubkopierer nicht mehr als wenige Tage entfernt.

1. Windows-Raubkopien frei Haus

Eine illegale Windows-XP-Version im Internet zu beschaffen, ist selbst für Laien kein ernsthaftes Problem. Fertige ISO-Dateien als 1:1-Abbilder der Original-CDs finden sich ohne lange Suche in Tauschbörsen oder in Newsgroups. Oftmals sind entsprechende

Corporate Keys (Firmenlizenzschlüssel) oder Key-Generatoren mit dabei, so dass nach der Installation mit einer illegalen Seriennummer die Zwangsaktivierung von Windows XP umgangen werden kann. Besonders komfortabel sind DVD-Zusammenstellungen mit mehreren XP-Varianten zur Auswahl. So sind zum Beispiel oftmals schon Hotfixes und Updates integriert, und eine unbeaufsichtigte Installation (Full unattended) richtet Windows ohne Nachfragen in einem Schwung samt Seriennummer ein.

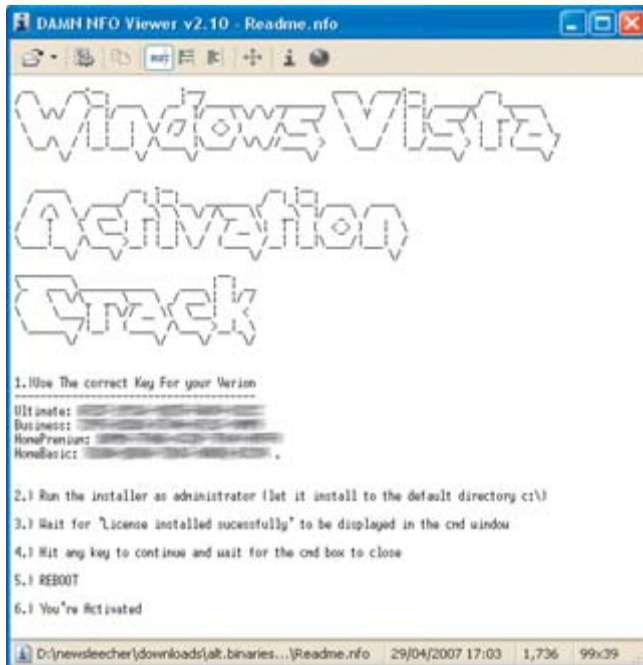
Ähnlich verhält es sich bei Vista. Auch hier haben wir verschiedene DVDs gesichtet, die mit mitgelieferten Cracks installiert und dauerhaft aktiviert werden sollen. Ein Test mit einem solchen aus einer Newsgroup geladenen ISO-Image zeigt: Ja, es klappt. Vista lässt sich installieren und mit einem Patch freischalten. Dazu ist noch nicht einmal eine Seriennummer erforderlich. Auch ein Online-Update ist möglich. Die Verbindung zum Update-Server und das Laden der zur Verfügung stehenden Aktualisierungen funktioniert wie mit einem legalen System.

2. Windows-Echtheitsprüfung

Mit den aus Windows XP bekannten Kopierschutz-Mechanismen WPA (Windows-Produkt-Aktivierung) und WGA (Windows Genuine Advantage) sowie neuen Funktionen wie Protection Platform (SPP) kombiniert Microsoft für Vista verschiedene Aktivierungs- und Prüftechniken. Damit sollen illegal verbreitete Vista-Versionen erkannt und abgeschaltet werden können. WGA soll sicherstellen, dass ausschließlich Käufer von Windows-Originalversionen mit kostenlosen Downloads und Add-ons belohnt werden. Beispielsweise lassen sich der Windows Media Player oder der Windows Defender nur

MS-Kopierschutz umgehen

Kaum hat Microsoft eine neues und nach eigenem Bekunden sicheres Kopierschutzverfahren für Windows, Office & Co. entwickelt, macht sich die weltweite Hackergemeinde auf, dieses Schutzschild innerhalb kürzester Zeit auszuhebeln. Resultat: Windows XP gibt als fertiges ISO-Image, für Vista sind verschiedene Hacks verfügbar.



Ausgehebelt: In vier einfachen Schritten lässt sich Vista mit dem passenden Crack aus dem Internet aktivieren (Punkt 1)

noch auf Systemen heruntergeladen, die eine Gültigkeitsprüfung bestanden haben (siehe Kasten „Ausgesperrt: Nur nach Überprüfung“). Die Echtheitsprüfung ist inzwischen um eine zusätzliche Funktion erweitert: Benutzer von Raubkopien werden beim Systemstart und immer wieder daran erinnert, dass sie ein illegales System verwenden. Regelmäßig wird das System überprüft. Bestimmte Daten, etwa den CD-Key, gleicht WGA mit Microsoft-Servern ab. Wenn das Programm das Windows-System als illegal erkennt oder die Prüfung nicht abschließen kann, poppt eine Meldung auf, die den Benutzer eines als illegal eingestuften Systems ermahnt, sein System zu legalisieren.

Hauptverantwortlich für die neue Kontrollinstanz ist die Datei Wgalogon.DLL im Verzeichnis \Windows\System32. Wenn die Windows-Update-Site Ihnen den Zugang verweigert und Sie stündlich Pop-up-Meldungen wegstören müssen, obwohl Ihr System lizenziert ist, können Sie sich entweder mit Microsoft in Verbindung setzen oder sich selbst behelfen. Im Internet kursieren auch Tools, die mit den nervenden Meldungen Schluss machen – beispielsweise Wgafixer und Remove WGA. Sie ersetzen einige Systemdateien und machen so den Weg auf Microsofts Update- und Download-Server wieder frei. Auch die deutschsprachige Freeware XP Antispy 3.96-4 (für Win-

dows 95/98/ME und 2000, XP, www.xp-anti-spy.org, 365 KB) bietet die Möglichkeit, die lästige WGA-Überprüfung zu deaktivieren. Der Einsatz der Tools zum Abschalten der WGA-Prüfung ist selbst auf legal lizenzierten Windows-Versionen rechtlich bedenklich.

3. So schützt MS Windows Vista

Weiterhin Bestandteil der Echtheitsprüfung unter Vista ist WGA, als Ergänzung setzt Microsoft zusätzlich auf die Software Protection Platform (SPP). Diese kombiniert verschiedene Aktivierungs- und

Prüftechniken und kann etwa zu oft verwendete Lizenzschlüssel erkennen und blockieren. Die nächste Online-Prüfung versetzt Vista dann in den Non-Genuine-Status, der einige Funktionen deaktiviert. Dem Anwender bleiben dann 30 Tage, das Problem zu lösen, siehe Infos im Kasten „Windows Vista – harte Kontrollen“.

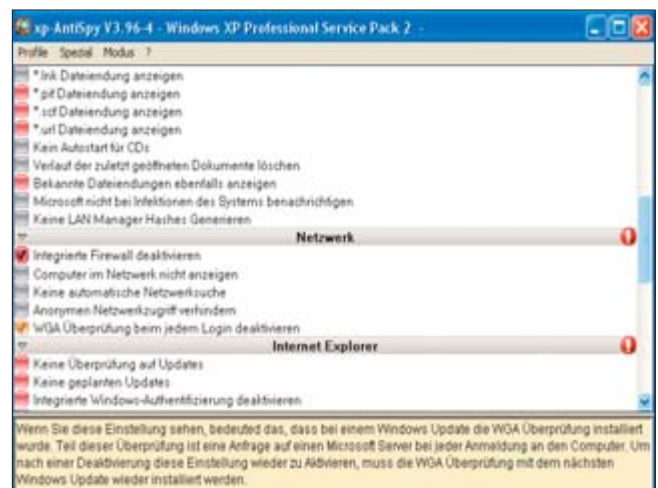
Microsoft setzt bei Vista immerhin auf drei verschiedene Aktivierungsvarianten: OEM (Original Manufacturer Equipment), Volume (Volumenlizenzen für Business-Kunden) und Retail (Einzellizenzen für Endkunden/Konsumenten). Die meisten Anwender, die einen Komplett-PC kaufen, erhalten zum Rechner eine OEM-Lizenz. Diese Vista-Version muss nicht mehr freigeschaltet werden, auf dem gekauften PC ist Vista bereits aktiviert vorinstalliert und an Bios und Hardware gebunden. Tauscht man grundlegende Hard-

Überblick MS-Kopierschutz

Inhalt	Seite
1. Windows-Raubkopien frei Haus	74
2. Windows-Echtheitsprüfung	74
3. So schützt Microsoft Windows Vista	75
Vista dauerhaft freischalten	
4. Datumstrick mit Zeitbomben-Killer	76
5. Gefälschte Aktivierungs-Server im Netz	77
6. Technik für Profis: API-Hook	77
Kästen	
Darum geht's: Microsoft-Kopierschutz umgehen	74
Ausgesperrt: Das gibt's nur nach Überprüfung	76
Windows Vista – harte Kontrollen	77

ware-Komponenten wie das Mainboard aus, muss auch die OEM-Version per Telefon oder Online-Server aktiviert werden, ebenso wie die Retail-Versionen von Vista.

Gravierende Unterschiede gibt es bei der Aktivierung von Volumenlizenzen, die in Unternehmen zum Einsatz kommen. Nach dem Flop mit den Corporate Keys für Windows XP setzt Microsoft nunmehr auf Volume Activation 2.0 für Vista und Longhorn-



WGA abschalten: Mit speziellen Tools wie XP-Antispy lässt sich die Funktion WGA Notify abschalten (Punkt 2)



Aktivierung nötig: Nach 30 Tagen muss Vista aktiviert werden (Punkt 3)

Server mit verschiedenen Varianten der Aktivierung. Ein Mehrfachaktivierungsschlüssel, der so bezeichnete Multiple Activation Key (MAK), schaltet viele Installationen frei. Das funktioniert per Proxy-basierter Aktivierung für mehrere Installationen und individuell je Einzel-PC.

Zudem können Administratoren auch einen Schlüsselmanagement-Dienst auf einem Server installieren. Dieser Key Management Service (KMS) übernimmt die Aktivierungskontrolle für das ganze Netzwerk. Die Aktivierung muss für alle beteiligten Systeme mindestens alle 180 Tage erneuert werden – sonst laufen sie automatisch nur mit begrenztem Funktionsumfang.

Vista dauerhaft freischalten

Im Internet kursieren gleich mehrere Anleitungen für das Freischalten von Vista. Da Microsoft natürlich ständig versucht, die genutzten Systemlücken zu schließen, ist ein Erfolg nicht zu hundert Prozent garantiert. Zum Redaktionsschluss konnten wir zumindest die Produkt-Aktivierung von Windows Vista mit den folgenden Tricks aushebeln:

4. Datumstrick mit Zeitbomben-Killer

Die erste illegale Freischaltmethode setzt auf eine Kombination von drei Tricks, die eigentlich nur den Aktivierungs-Zeitraum auf maximal 120 Tage verlängern. Die Kombination dieser Maßnahmen soll dann aber bewirken, dass Vista nie mehr nach der Aktivierung verlangt. Grundvoraussetzung für den Zeitbomben-Crack ist zunächst einmal, dass Vista ohne Produktschlüssel eingerichtet wurde. Diese Möglichkeit ist in der Installationsroutine von Microsoft vorgesehen, damit sich jede beliebige Vista-Version für 30 Tage testen lässt und etwa ein Home-Premium-Käufer einige Zeit den Umfang einer Ultimate-Version ausprobieren kann. Sobald nun die Installation ohne Produkt-

schlüssel abgeschlossen ist, beginnt normalerweise sofort die Aktivierungs-Uhr zu ticken: 30 Tage nach diesem Zeitpunkt läuft der Testzeitraum ab, und Vista schaltet in den Reduced Functionality Modus (RFM).

Cracker versuchten daher in einem ersten Schritt, das Systemdatum auf das Jahr 2099 vorzustellen. Der simple „2099-Bios-Trick“ wurde schon bei den Betaversionen von Vista angewendet und vor der Installation ausgeführt. Vista merkt sich damit einen sehr späten Installationszeitpunkt. Wird die Uhr dann umgehend wieder zurückgestellt, blieben theoretisch 92 Jahre bis zur Aktivierung. Um diesen Trick auch nach erfolgter Installation anwenden zu können, bedienen sich Cracker der legalen „ReArm“-Funktion. Diese setzt den Aktivierungs-Timer zurück. Steht das Systemdatum also auf 2099, wird der Timer über den Windows-Befehl

```
rundll32 slc.dll,SLReArmWindows
```

auf diesen Zeitpunkt gesetzt. Dieser Kommandozeilenbefehl lässt sich natürlich nicht beliebig oft ausführen, nach vier Mal ist Schluss. Für den Crack reicht aber offenbar ein einmaliges „ReArm“ vollkommen aus. Danach wird das Datum wieder auf den aktuellen Tag zurückgestellt.

Die Zeitbombe: Zusätzlich zum Aktivierungs-Timer tickt allerdings eine weitere Uhr. Diese misst die Zeit, die das System tatsächlich gelaufen ist – völlig unabhängig vom individuellen Installationsdatum. Um diesen Zeitähler zu umgehen, haben die Cracker einen Zeitbomben-Killer entwickelt. Dabei handelt es sich um einen Treiber, der mit Windows geladen wird. Er hält das Fortschreiten dieser internen Uhr auf. Einige Cracker bieten inzwischen eine EXE-Datei an, welche die drei Schritte (Datumsmanipulation, ReArm und Zeitbremse) zusammenfasst und vollständig automatisiert. Ein Klick auf diese Datei soll genügen, um alle Barrieren fallen zu lassen. Wer dann noch überprüfen will, ob der Timer nach der Aktion tatsächlich steht, kann über „Start, Ausführen“ den Befehl

```
slmgr.vbs -dlv
```

aufrufen. Das Vista-Script Slmgr.VBS zeigt in der letzten Zeile die Restdauer des Testzeitraums an. Ändert sich diese über mehrere Tage nicht und beträgt konstant annähernd 30 Tage, steht die Uptime-Uhr offensichtlich still. Ein erstaunlicher Nebeneffekt

Ausgesperrt: Nur nach Überprüfung

Windows Genuine Advantage Validation heißt der Vorgang, der über die Windows-Update-Seite oder den Download-Server von Microsoft die Windows-Version checkt. Diese Prüfung erledigt entweder ein Active-X-Control im Internet Explorer oder ein Plug-in in Firefox. Wer einen anderen Browser benutzt oder das automatische Ausführen von Active-X-Elementen verboten hat, muss auf einem anderen Weg die Echtheit prüfen lassen: Dazu laden Sie vor dem WGA-Test die Datei Genuinecheck.EXE über einen Link etwa auf der Windows-Update-Seite herunter und führen sie aus. Als Ergebnis bekommen Sie eine Nummer, die Sie dann einfach auf der jeweiligen Seite in das dafür vorgesehene Feld eintragen.

Schlägt die WGA-Prüfung unter Windows XP fehl, lassen sich beispielsweise Media Player 11, Internet Explorer 7 und Windows Defender nicht herunterladen und installieren. Einen Schritt weiter geht der WGA-Check in Windows Vista und sperrt sogar einige elementare Systemfunktionen. Melden WGA- oder SPP-Prüfung ein aus ihrer Sicht illegales Betriebssystem, werden folgende Systembestandteile komplett deaktiviert:

Download-Center: Online-Updates für Vista gibt es nur für geprüfte Vista-PCs. Davon ausgenommen sind allerdings kritische Sicherheits-Updates, die das Vista-Auto-Update weiterhin lädt.

Windows Aero: Die neue Oberfläche von Vista mit Transparenz-, Reflexions- und 3D-Effekten steht nach gescheiterter Überprüfung nicht mehr zur Verfügung.

Windows Defender: Der kostenlose Spyware-Scanner läuft nur noch in einem reduzierten Umfang und entfernt nur noch als kritisch eingestufte Bedrohungen vom System.

Ready Boost: Die in Vista eingeführte Beschleunigungs-Technologie soll Windows schneller machen, indem Flash-Speicher wie Arbeitsspeicher als Cache-Puffer genutzt wird.

ist außerdem, dass Windows Vista nach dieser Aktion offenbar sogar die WGA-Prüfung bestehen soll. Das bedeutet, dass gekrackte Vista-Installationen auch noch Updates und Windows-Ultimate-Extras von der Microsoft-Site beziehen und installieren können.

5. Gefälschte Aktivierungs-Server im Netz

Die meisten Windows-XP-Raubkopien werden mit einem so bezeichneten Volumen-Lizenzschlüssel freigeschaltet. Was ursprünglich als Arbeitserleichterung für Firmen-Administratoren gedacht war, fand sehr schnell Anklang in der Raubkopierszene. Die speziellen CD-Keys funktionieren zusammen mit jeder handelsüblichen Version von Windows XP Professional oder mit der XP Corporate Edition. Vorteil: Die so genannten Corporate Keys oder VLKs (Volume License Keys) schalteten Millionen Raubkopien von XP frei, eine Aktivierung ist nicht mehr erforderlich.

Bei Vista hat sich Microsoft daher für die Firmenkunden etwas Neues einfallen lassen und setzt auf die Server-basierte Lizenzverwaltung per Software Volume Activation 2.0. Hierbei erfolgt etwa beim Key Management Service (KMS) die Aktivierung einer Lizenz über den KMS-Server und nicht über Microsoft. Einen wirksamen Schutz scheint aber auch dieses Verfahren nicht zu bieten. Einige Hacker betreiben im Internet eigene KMS-Server, über die sich Vista-Business- und -Enterprise-Versionen freischalten lassen. Die Abfrage erfolgt vollautomatisch über ein spezielles, im Internet kursierendes Tool. Es geht aber auch ohne Internet-Verbindung zum Server. Im Download-Angebot einiger Hacker-Seiten befindet sich ein VM-Ware-Image für den kostenlosen VM-Ware Player (für Windows 2000/XP, www.vmware.com) und mit einem besonders vorbereiteten KMS-Server. Nach Installation von Vista Business mit einer speziellen Seriennummer ist die virtuelle Maschine auf einem PC im Netzwerk zu laden. Auf dem Nicht-VM-PC gibt man als Administrator die folgenden Kommandos ein:

```
cscript c:\windows\system32\slmgr.vbs
-skms <ip-adresse des vmware-pc>
cscript c:\windows\system32\slmgr.vbs
-ato
```

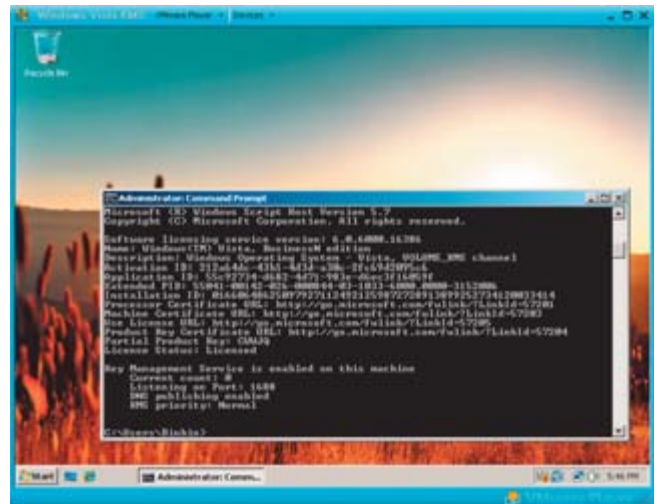
Windows ist anschließend aktiviert. Das lässt sich überprüfen mit dem Befehl

```
cscript c:\windows\system32\slmgr.vbs
-dlv
```

6. Technik für Profis: API-Hook

Technisch scheinbar überlegen, aber – anders als die beiden vorher genannten Methoden – noch mit einigen Fehlfunktionen behaftet ist der API-Hook auf die Winlogon.EXE von Vista. Es wird jedoch nur eine Frage der Zeit sein, bis er auch unter Vista funktioniert. Ein

Hook bezeichnet eine Methode, bei der das System darauf abgehört wird, ob ein bestimmter Befehl ausgesendet wird. Dieser wird abgefangen. Die erwartete Antwort wird dann durch eine manipulierte Version ersetzt. Unter XP funktioniert der Trick schon seit einiger Zeit – sowohl bei den 32- als auch bei den 64-Bit-Versionen: Der Crack installiert und registriert eine DLL-Datei (Dynamic Link Library), die bei jedem Windows-Start die API-Anfrage (Application Programming Interface) der Winlogon.EXE abfängt, über die der Login-Manager den Status der Aktivierung überprüft. Die DLL sendet postwendend eine gefälschte Ant-



Virtueller KMS-Server: Im Web gibt's Aktivierungs-Server als VM-Ware-Image, mit denen sich Vista aktivieren lässt (Punkt 5)

wort zurück, welche die Winlogon.EXE glauben lässt, sie laufe im „Abgesicherten Modus“. Da dort keine Aktivierung erforderlich ist, geht die Anmeldung ohne Schwierigkeiten weiter, und das System funktioniert auch nach Ablauf des Aktivierungszeitraums. Dieser Hook greift nicht in das System ein, sondern fängt lediglich den Informationsaustausch zwischen den einzelnen Systemkomponenten ab. Einige Cracker bevorzugen diese Methode vor allem deshalb, weil sie es für sehr unwahrscheinlich halten, dass Microsoft Updates verbreitet, die den API-Aufruf zur Überprüfung der Windows-Aktivierung ändern. ❌

Windows Vista – harte Kontrollen

Die Microsoft-Entwickler haben bei Vista die internen Prüfmechanismen verschärft, um Raubkopien oder ungültige Lizenzen des Betriebssystems zu entlarven. Wird eine Manipulation am Aktivierungsprozess erkannt, eine verdächtige, also mehrfach genutzte Seriennummer entdeckt oder schlägt eine der wiederholt nötigen Neuaktivierungen fehl, bekommt der User eine Gnadenfrist von 30 Tagen (Grace Period), in der sich Vista mit einem Pop-up meldet und auf den Missetand hinweist. Nach Ablauf der Frist wird Vista ohne gültige Aktivierung unbrauchbar und schaltet automatisch in den so genannten Reduced Functionality Modus (RFM). In diesem sind das Startmenü und viele Funktionen deaktiviert; und der Bildschirmhintergrund bleibt schwarz. Der Anwender hat dann nur noch eine Stunde Zeit zum Surfen – vor allem, um online einen legalen Schlüssel zu bestellen und direkt per Kreditkarte zu bezahlen.



Prüfung: Nach Ablauf der Testphase von 30 Tagen muss Vista aktiviert werden



Raubkopien aus dem Web

Profis finden entsprechende Download-Links für illegale Software jeder Art ganz einfach per Suchmaschine. Allerdings erst nach einer virtuellen Reise nach Russland und China.

Von **Peter-Uwe Lechner**

Reine Zeitverschwendung ist es, das deutsch- und englischsprachige Web nach illegaler Software zu durchforsten. Eine Suche auf Google.de beispielsweise nach den Begriffen „nero + warez“ liefert zwar ausgiebige Trefferlisten, in der Regel landet man aber in Endlos-Schleifen mit nervenden Pop-ups und Voting-Seiten, die nur ein Ziel haben: Die Site-Betreiber bekommen von Sponsoren und Werbe-Netzwerken Geld für die so erzielten Klicks.

Zudem wird oft auch versucht, PCs per Script zu attackieren und etwa mit Backdoors zu infizieren. Wer dennoch im Web nach seiner bevorzugten Software suchen möchte, findet auf chinesischen und russischen Servern prall gefüllte Archive. Filme gibt's zwar ebenfalls, meist handelt es sich aber um englischsprachige Movies mit Untertiteln in bescheidener Qualität. Hier ist und bleibt das Usenet unangefochten die Download-Quelle Nummer 1.

Einen Vorteil hat die Websuche: Man ist im Gegensatz zum Filesharing mit entsprechenden Tools vollkommen anonym unterwegs und braucht im Vergleich zum Usenet nichts zu bezahlen. Einzig ein schneller DSL-Anschluss und die übliche Software-Ausstattung wird benötigt (siehe Kasten „Software-Ausstattung für Warez-Profis“). Als Suchmaschine reichen www.google.cn (China) und www.google.ru (Russland) aus. Ein Online-Übersetzer sorgt zumindest dafür, dass man die grundlegende Begriffe und Inhalte der Web-Seiten versteht. Für Firefox empfiehlt sich die kostenlose Extension Translator 1.0.4.3 (<https://addons.mozilla.org/de/firefox/addon/3361>), mit der sich geöffnete Web-Seiten per Kontextmenü der rechten Maustaste in einem neuen Tab übersetzen lassen.

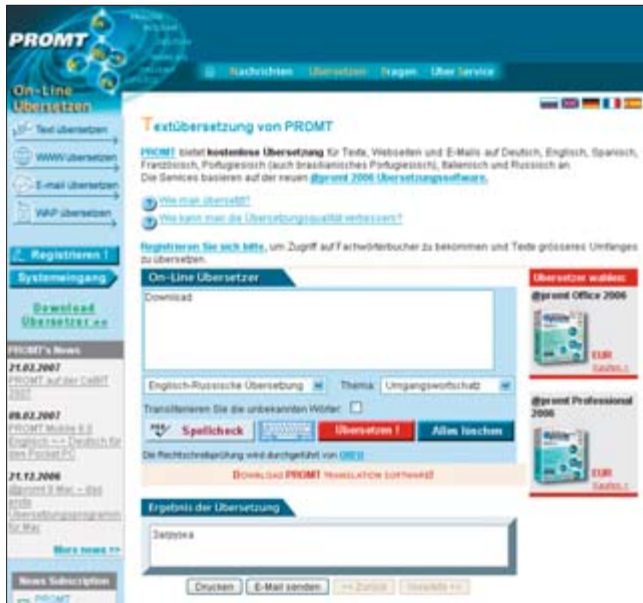
1. Illegales an jeder Ecke

Wer schon mal Urlaub in einem asiatischen Land gemacht hat, kennt die unzähligen DVD- und Software-Shops auf den Einkaufsstraßen, gleich neben dem Rolex und Gucci-Händler des Vertrauens. Zu kaufen gibt's quasi alles, was bekannt ist und sich reger Nachfrage erfreut – natürlich illegal, dafür aber meist für weniger als 5 Euro für die aktuelle Kino-Top-5-Kollektion und keine 3 Euro für Microsoft Office 2007.

Dafür bekommt man Datenträger mit billig nachgemachten DVD-Labels und schäbigen DVD-Covern aus dem Tintenstrahldrucker, auf Echtheitszertifikate verzichten die Produktpiraten in der Regel. Dass es sich bei der Software in der Regel um Kopien der englischsprachigen Originale handelt, stört versierte Anwender wenig. Oft hat man sogar Glück und bekommt eine multilinguale Version, die auch deutsch spricht.

Darum geht's: Illegale Downloads

Mit ausreichend Geduld und Kenntnis der Profi-Tricks lässt sich im Web teure Kauf-Software zum Nulltarif aufstöbern. Der Ausflug nach Russland oder China scheint auf den ersten Blick abenteuerlich und von wenig Erfolg gekrönt zu sein. Doch am Ende wird die Hartnäckigkeit mit aktueller Software belohnt.



Russisch für Anfänger: Nach der Übersetzung grundlegender Begriffe fällt die Suche nach Warez sehr viel leichter (Punkt 3)

Kein Wunder, dass vor allem das asiatische Web-Angebot reich bestückt ist und neueste Software quasi frei Haus liefert. Im Angebot sind 1:1-Raubkopien im ISO-Format zum Brennen auf CD und DVD oder Cracks zum Freischalten von Testversionen.

Doch auch russische Websites sind randvoll mit allerlei Verbotenem. Ob extrem jugendgefährdende Bilder, Raubkopien neuester Software und Filme oder Chart-Hits im MP3-Format: Auch In Russland schert sich kaum einer um den Urheberrechtsschutz.

2. Ausreichend Wartezeit einkalkulieren

Das Finden von illegaler Software klappt recht schnell, wenn man sich einmal mit der Syntax der Suchanfragen und dem Vorgehen auf den Web-Seiten vertraut gemacht hat. Zum Geduldspiel wird dann aber der Download der Warez-Archive. Viele der Web-Seiten sind auf Servern gehostet, die überlastet beziehungsweise nicht mit der eigentlich erforderlichen Bandbreite an die weltweiten Backbones angebunden sind. Die Folge: Langsamer Seitenaufbau und quälend langsame Datentransfers mit wenigen KB pro Sekunde. Die schnelle DSL-Leitung des Downloaders wird nur zu einem Bruchteil ausgelastet. Oft hat man jedoch Glück und findet über den Dateinamen des Dateiarchivs einen Mirror auf einem schnelleren Server, ein Download-Manager wie Flashget (siehe Kasten „Software-Ausstat-

tung für Warez-Profis“) übernimmt die Suche auf Wunsch sogar ganz automatisch. Vor einem ist man übrigens nie gefeit: Es kann durchaus sein, dass man sich eine zeitlich beschränkte oder funktional limitierte Testversion einer Software lädt. Und die bekommt man auch vom Hersteller – ohne lange Suche und über elend langsame Internet-Verbindungen zu den Warez-Servern. Das Risiko kann man etwa dadurch minimieren, indem man auf die Dateinamen

der Downloads achtet. Trial steht für Testversion, Retail für die Verkaufsversion.

3. Sprachbarrieren überwinden

Die Suche auf chinesischen und russischen Warez-Seiten stellt jeden Anwender vor eine erste hohe Hürde – denn kaum einer dürfte der Sprachen mächtig sein und sich in schlafwandlerischer Leichtigkeit durch die Seiten klicken, die richtigen Suchabfragen absetzen und die ausgeworfenen Inhalte sofort verstehen. Eine erste große Hilfe ist ein Stichwort-Such-Verzeichnis für in der Szene oft verwendete Begriffe in der jeweiligen Landessprache, also Chinesisch und Russisch. Hilfreich sind auch die entsprechenden Tastatur-Eingaben für kyrillische Buchstaben oder Tastatur-Schablonen. Die Stichwortlisten kann man ganz einfach selbst anfertigen, indem Wörter wie „Vollversion“, „illegal“, „Download“, „Software“ und „Retail“

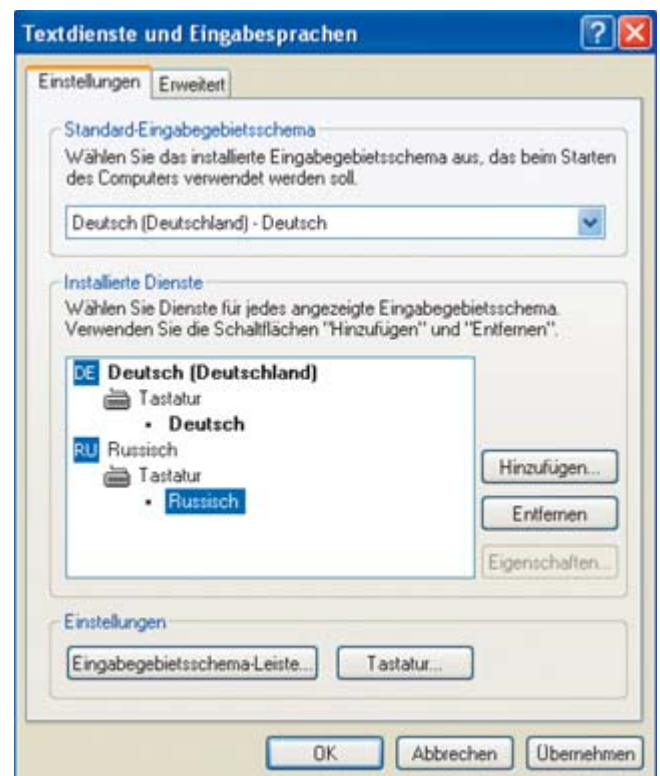
Überblick Illegale Downloads

Inhalt	Seite
1. Illegales an jeder Ecke	78
2. Ausreichend Wartezeit einkalkulieren	79
3. Sprachbarrieren überwinden	79
4. Russisch für Einsteiger	79
5. Auf Chinesisch googeln	81
6. Warez-Web-Seiten direkt ansteuern	81
Kästen	
Darum geht's: Illegale Downloads	78
Software-Ausstattung für Warez-Profis	80
Sicher surfen im isolierten Käfig	81

mit Hilfe der Web-Seite www.online-translator.com/srvurl.asp?lang=de etwa in das Kyrillische übersetzt werden.

4. Russisch für Einsteiger

Für das Eintauchen ist die Russen-Szene ist eine kyrillische Tastatur von Vorteil. Profis kaufen eine solche für wenige Euro im Zubehörhandel oder bei Ebay. Unter <http://tastatur.da.ru> findet sich eine Schablone mit kyrillischen Zeichen. Für den ersten Einstieg



Tastatur kann Russisch: Mit erweiterten Gebieteinstellungen klappt auch die Eingabe kyrillischer Zeichen (Punkt 4)



Google-China: Ein Klick auf die Flagge rechts unten öffnet die chinesische Google-Web-Seite im Browser (Punkt 5)

reicht es allerdings auch aus, die bisherige Tastatur weiter zu nutzen und das Eingabegebietsschema von Windows zu ändern. Dazu klicken Sie auf das kleine Icon „DE“

Kontextmenü „Einstellungen“. Auf dem gleichnamigen Reiter sollte „Deutsch (Deutschland) – Deutsch“ unter „Standard-Eingabegebietsschema“ aktiv sein. Unter

links neben dem Systray. Fehlt diese Schaltfläche, genügt ein rechter Mausklick in einen leeren Bereich der Windows-Symbolleiste und die Auswahl „Symbolleisten“ im Kontextmenü. Nach einem Klick auf den Eintrag „Eingabegebietsschemaleiste“ wird das „DE“-Symbol eingeblendet. Zum Ändern der Vorgaben klickt man mit der rechten Maustaste auf das Icon und wählt im

„Installierte Dienste“ steht mindestens „DE Deutsch (Deutschland)...“. Das Hinzufügen eines weiteren Eingabegebietsschemas erlaubt die Eingabe kyrillischer Zeichen. Dazu klickt man auf „Hinzufügen...“, wählt sowohl bei „Eingabegebietsschema“ als auch bei „Tastaturlayout/IME“ die Option „Russisch“ aus und übernimmt die neuen Werte mit einem Klick auf „OK“. In der Liste „Installierte Dienste“ erscheint jetzt auch „RU Russisch...“, Klicks auf „Übernehmen“ und „OK“ schließen den Vorgang ab. Der Anwender kann nun bequem zwischen der Eingabe lateinischer (deutscher) und kyrillischer Buchstaben wechseln.

Nun steht der Suche nach Downloads im russischen Web nichts mehr im Weg. Nach dem Aufruf der Website www.google.ru klickt man auf den kyrillisch geschriebenen Link hinter dem Text „Google.ru angeboten in:“. Ab sofort ist alles russisch. Die einzelnen Schaltflächen entsprechen denen der deut-

Software-Ausstattung für Warez-Profis

Für das Surfen und Laden von Software-Archiven aus dem Web empfiehlt sich die folgende Software, die sich komplett auf der  CD zur schnellen Installation befindet.

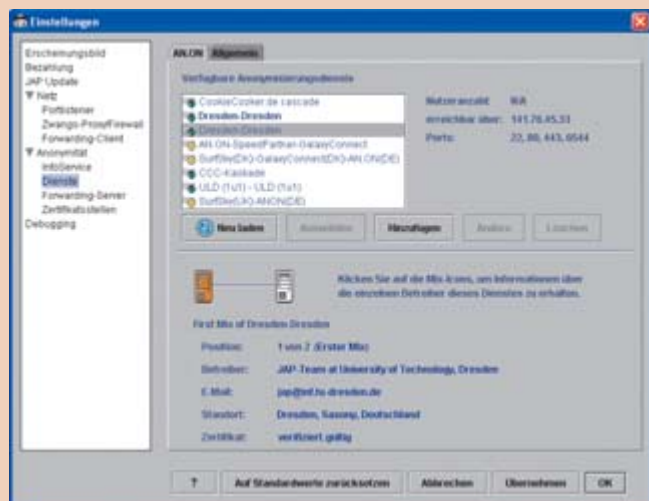
Anonym surfen: Die Fakultät Informatik der TU Dresden und weitere unabhängige Institute betreiben für den kostenlosen Anonymisierungs-Dienst JAP (für Windows 95/98/ME und 2000/XP, <http://anon.inf.tu-dresden.de>) ein Netzwerk, das aus mehreren hintereinander geschalteten Proxys – so genannten Mixen – besteht. Dadurch erfährt weder der angefragte Server noch ein Sniffer, welcher Anwender bestimmte Web-Seiten aufgerufen hat. Das Programm ist nach dem ersten Start bereits vor-konfiguriert, so dass Sie nur die Option „Anonymen Webzugriff aktivieren“ einschalten müssen. Damit der Dienst im Browser aktiv wird, muss dort als Proxyserver die Adresse 127.0.0.1 mit dem Port 4001 eingetragen sein.

Packer: Winrar (für Windows 95/98/ME und 2000/XP, www.winrar.de) ist nicht zuletzt aufgrund der Kompatibilität mit anderen Packern sehr beliebt und kann auch Dateien im ZIP-Format packen und entpacken. Diese Archive sind sogar kleiner als die mit Winzip erstellten. Außerdem kann Winrar Dateien in den Formaten ACE, ARJ, BZip2, CAB, GnuZip (GZ), ISO, JAR, LZH, UUE und TAR entpacken. Die Freeware **7-Zip 4.42** (für Windows 95/98/ME und 2000/XP, www.7zip.org) ist eine leistungsfähige Alternative zu Winrar und kommt mit gängigen Formaten wie ZIP, CAB, RAR, ARJ und anderen zurecht. Im Options-Menü können Sie die Programmoberfläche des Open-Source-Tools auf deutschsprachig umschalten.

Download-Manager: Flashget 1.82 (für Windows 95/98/ME und 2000/XP, www.amazesoft.com) beschleunigt den Download von Dateien aus dem Internet, indem es verschiedene Teile einer Datei parallel herunterlädt, um sie anschließend wieder zum Original zusammenzusetzen. Die Freeware findet gegebenenfalls Mirror-Server und kann Daten so aus mehreren Quellen gleichzeitig ziehen. Außerdem gibt es einen Scheduler,

mit dem sich Downloads vorplanen lassen. Zusätzlich werden mehrere Kategorien angelegt, die eine Sortierung ermöglichen.

Virenschutz: **Antivir Personal Edition Classic 7.04** für Windows 95/98/ME und 2000/XP, www.freeav.de) soll den PC gegen Viren, Backdoors und andere Schadprogramme schützen. Der Hintergrundwächter untersucht Download-Archive direkt nach dem Speichern auf Festplatte auf Schädlinge. Der Anwender kann zudem gezielt Suchläufe starten oder Antivir Personal Edition so konfigurieren, dass die Software zu fest gelegten Zeitpunkten automatische Kontrollläufe startet. Die Konfiguration des Programms lässt sich mittels Passwort schützen. Dank Online-Update bleibt der Virens Scanner stets auf dem aktuellsten Stand.



Anonym unterwegs: Mit einem Zusatztool für den Webbrowser wie JAP surft man ohne Rückschlüsse auf die echte Identität

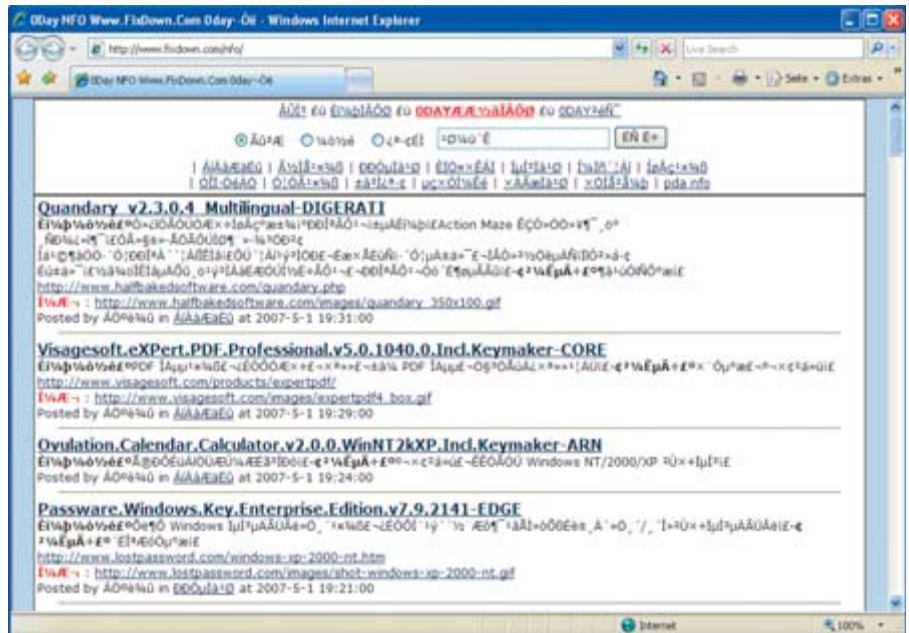
schen Google-Seite. Mit dem linken Button schaltet man die Suche für alle Internet-Seiten weltweit ein, mit dem rechten beschränkt sich die Suche auf russische Seiten – das ist die erste Wahl. Ein Klick auf die Eingabegebietsschemaeiste und Auswahl der Option „RU“ erlaubt die Eingabe kyrillischer Zeichen als Suchbegriff in das Google-Suchfeld. Hat man einige gängige Begriffe rund um das Thema WareZ und illegale Downloads mit den gesuchten Programmnamen kombiniert, finden sich in der Ergebnisliste mehrere brauchbare Fundstellen.

5. Auf Chinesisch googeln

Profis steuern direkt die Web-Seite von Google-China unter www.google.cn an und lassen sich auch dadurch nicht aus der Ruhe bringen, dass die komplette Web-Seite inklusive der Beschriftungen für die wenigen Buttons in chinesischer Sprache gehalten ist. Doch ohne Änderungen an den Einstellungen der Google-Web-Seite landen Anwender mit hoher Wahrscheinlichkeit nach der Eingabe von www.google.cn auf der deutschen Web-Seite www.google.de. Nun klickt man rechts neben dem Eingabefeld auf den Link „Sprachtools“ und scrollt bis zum Abschnitt „Verwenden Sie Googles Benutzeroberfläche in Ihrer Sprache“. Ein Klick auf „Chinesisch (vereinfacht)“ oder auf die Flagge darunter bringt die chinesische Google-Startseite zum Vorschein.

Eine erste Suche nach dem Programmnamen gefolgt von „Softview“ liefert eine sehr lange Trefferliste, schon die ersten Einträge liefern die gewünschten Fundstellen. Wer mit Firefox surft, sollte unbedingt die Gratis-Extension Google Preview (für Windows 95/98/ME und 2000/XP, <http://ackroyd.de/googlepreview/>, 17 KB) installieren. Die Erweiterung integriert Vorschaubilder in die Trefferlisten, so dass man sich schon in der Vorschau einen ersten Eindruck der Web-Seite verschaffen kann.

Alternativ dazu lässt sich jede Seite auch in einer Übersetzung aufrufen. Dazu öffnet man zunächst die Web-Seite www.google.de/language_tools?hl=de und tippt dann im Abschnitt „Übersetzen“ in das Feld „Webseite übersetzen“ für einen ersten Test die Adresse www.google.cn ein, wählt aus der Drop-down-Liste darunter den Eintrag „Chinesisch (vereinfacht) nach Englisch BETA“ aus und klickt auf den Button „Übersetzen“ rechts daneben. Anstelle der Google.cn-Sei-



Direkt-Download: Wer die richtigen WareZ-Web-Seiten kennt, spart sich die langwierige und aufwendige Suche und kann ohne Umweg mit den Downloads starten (Punkt 6)

te gibt man einfach eine der Sites ein, die eine Suche nach der gewünschten Software zu Tage gefördert hat.

6. WareZ-Webs-Seiten direkt ansteuern

Verschiedene Suchanfragen nach Vollversionen populärer Software liefern die Seiten Hybx.net, Wz222.com, 997.cn und TTBT.cn als Treffer. Also lohnt sich ein Blick in die dortigen Software-Archive. Man findet di-

verse Programme der Hersteller Adobe, Corel, Mc Afee, Microsoft, Symantec und Ulead. Größere Programme liegen als ISO-Datei zum Brennen vor, sonst sind in der Regel ZIP-Archive im Angebot.

Die zur Installation benötigten Seriennummern und Lizenzschlüssel gibt es meist als Textdatei. Täglich aktualisierte Archive mit gekrackten Anwendungen, PC-Spielen und E-Books finden sich auch auf Fixdown.com, Vipcn.com und Crsky.com.

Sicher surfen im isolierten Käfig

Das Surfen auf suspekten Web-Seiten birgt so manche Gefahr. Angreifer können beispielsweise mit manipuliertem HTML-Code versuchen, die Kontrolle über den PC des ahnungslosen Surfers zu erhalten oder Schädlinge zur Fernsteuerung einschleusen. Besser, man surft in einer isolierten Umgebung, bevorzugt unter Linux. Denn das System ist weniger anfällig für Viren und Malware als Windows. Und wenn ein Hacker tatsächlich in das Linux-System eindringt, bleibt er im virtuellen Käfig gefangen. Auf der CD gibt's das Betriebssystem Puppy Linux als virtuelle Maschine.

Das Beste: Sie müssen nichts aufwendig konfigurieren. Qemu-Puppy gibt es als fertiges Paket. Das System bringt mit Qemu seine eigene Virtualisierungssoftware mit. Damit braucht man nur einen Linux- oder Windows-PC und kann das schlanke Linux-Betriebssystem auf Mausklick starten. Die aktuelle Version setzt auf den Mozilla-Ableger Seamonkey oder Dillo als Webbrowser. Downloads lassen sich etwa auf NTFS-Partitionen oder auf einem USB-Stick speichern.



Isolationshaft: Das Linux im virtuellen Käfig ist resistent gegen Viren



Debranding für das Handy

Manche Handy-Provider arbeiten mit Tricks, um Mobilfunkkunden den ein oder anderen Euro aus der Tasche zu ziehen. Besonders heimtückisch ist das Branding von Handys.

Von Jan-Dirk Skippoe

Wer heutzutage einen neuen Mobilfunkvertrag beim Provider seiner Wahl abschließt, erhält in der Regel ein älteres Handy-Modell ohne Aufpreis oder ein topaktuelles Gerät weit unter dem normalen Listenpreis. Auch bei einer Vertragsverlängerung kann nach diesem Prinzip ein neues Handy ergattert werden. Der Nachteil dabei: Im Gegensatz zu den Originalmodellen aus dem Einzelhandel sind die Geräte der Provider an ihre Services und ihre Corporate Identity angepasst, neudeutsch „gebrandet“. Dabei lassen die Provider die Firmware der Handys von den Herstellern nach ihren Vorstellungen umprogrammieren. Ein solches gebrandetes

Handy besitzt meistens ein fest aufgebrachtes Logo des Providers auf der Geräteschale, meldet sich nach dem Einschalten mit dem Logo und ist über Menü und Tastaturbelegung auf einen bestimmten Netzbetreiber eingestellt – etwa beim Internet-Zugang, SMS- und MMS-Server.

1. Elektronische Fußfessel für das Mobiltelefon

Das Branding an sich ist nicht das Problem, da etwa auch einige PC-Hersteller ein angepasstes Windows vorinstallieren. Im Gegensatz zum Handy werden Sie diese Voreinstellungen aber mit wenige Mausklicks wie-

der los. Ein schnelles Ändern der Einstellungen, das komplette Löschen des Handy-Brandings oder das Zurücksetzen auf die Hersteller-Vorgaben ist ohne Weiteres nicht möglich. Noch nicht einmal das simple Umbelegen einer bestimmten Taste auf eine andere Funktion lässt sich vom Nutzer selbst über das Handy-Setup vornehmen. Das ist vor allem dann ärgerlich, wenn man etwa sein Mobiltelefon von T-Mobile zukünftig mit der SIM-Karte eines anderen Netzbetreibers nutzen möchte. Im Menü ist der T-Mobile-Dienst „web’n’walk“ fest eingestellt. Ein zusätzlicher negativer Aspekt des Handy-Brandings ist die Vorbelegung von Tasten, die beim Drücken ohne weitere Rückfrage zu kostenpflichtigen Services führen, beispielsweise eine teure Internet-Verbindung via GPRS (General Packet Radio Service) zum Webportal des Providers aufbauen. Das kann schnell zur Kostenfalle werden, denn schon ein unabsichtlicher und unbemerkter Tastendruck genügt, um den Gebührenzähler im Sekundentakt rasseln zu lassen. Das böse Erwachen kommt dann erst bei der nächsten Rechnung.

2. Die Schnellwahltaste mit einer Spezialfunktion belegen

Beim Branding vom Provider immer wieder gerne auf eigene Services umprogrammiert: Die Schnell taste, die eigentlich vom Kunden selbst individuell für eine häufig gebrauchte Funktion frei zu belegen ist. Oder der Menü-



Falle: Ein falscher Klick auf eine gebrandete Taste kann Ärger machen (Punkt 1)



Debranding-Dienste: Im Internet finden sich Dienstleister, die das Einspielen einer neutralen Firmware übernehmen (Punkt 4)

punkt „Sounds“ beziehungsweise „Klingeltöne“. Hier gibt's je nach Provider einen Unterpunkt wie „mehr Klingeltöne“. Ein Klick, und schon landet man auf dem Webportal des Providers, um dort im Shop neue Töne zu kaufen und sich gleich auf das Handy schicken zu lassen. Selbstredend, dass auch hier eine Internet-Verbindung aufgebaut wird. Vor allem Kinder und Einsteiger werden so gelockt und quasi übertölpelt. Denn besonders ärgerlich dabei ist, dass die kostenpflichtige Verbindung sofort und ohne Rückfrage hergestellt wird. Nur wer das Gerätdisplay genau verfolgt und die einzelnen Menüebenen stets im Blick hat, kann den teuren Gang ins Internet abwehren und stoppen. T-Mobile kennzeichnet diese Tasten übrigens mit dem Symbol „T-Zones“, Vodafone mit dem „Live“-Symbol.

3. Zurück zur Original-Software

Wer genug von der Bevormundung der Mobilfunkanbieter hat, dem stehen zwei Möglichkeiten offen. Entweder er besorgt sich ein neutrales Handy, oder man legt selbst Hand an. Webseiten wie www.handyfaq.de beschreiben detailliert, wie man das unliebsame Branding los wird. In der Regel wird die aktuelle Handy-Software ausgetauscht und mit dem Original des jeweiligen Herstellers ersetzt (geflasht). Für die gesamte Palette der Sony-Ericsson-Geräte hat das niederländische DaVinci-Team (www.davinciteam.com) eine Software entwickelt, mit der quasi jeder sein Handy vom Branding entfesseln kann. Die neue Firmware (Credit) kostet zehn Euro pro Flashvorgang, bezahlt wird mit Paypal oder Kreditkarte. Zum Flashen wird das USB-Kabel verwendet, das den meisten Geräten beiliegt. Im Download-Bereich der DaVinci-Team-Web-Seite laden Sie den USB-Flash-Treiber und den Client.

Packen Sie die Archive aus und starten den Client. Schließen Sie nun das USB-Kabel an den PC an, schalten das Mobiltelefon aus und verbinden es mit dem USB-Kabel, während Sie die Taste „c“ gedrückt halten. Windows fragt nun, welcher Treiber installiert werden soll. Wählen Sie „andere Quelle

auswählen“ und geben das Verzeichnis an, in das Sie zuvor die Treiber entpackt haben. In der Software tragen Sie Ihren Usernamen und das Passwort ein, das Sie für Ihren Credit erhalten haben. Oben rechts in der Software klicken Sie auf „Flashfiles“ und wählen in der Liste die passende Firmware für Ihr Handy. Klicken Sie den Eintrag an, und aktivieren Sie die beiden Checkboxes „Download Main Firmware“ und „Download File System Flash“. Nach einem Klick auf „Get Files“ werden die Dateien geladen. Danach drücken Sie oben auf den Button „Flash“ und wählen nacheinander die Dateien, die „MAIN“ und „FS“ im Namen führen. Unter „CDA“ wählen Sie den Eintrag aus, der dem geladenen Flash-File entspricht. Schalten Sie nun die Kontrollkästchen neben „Main“, „FS“ und „Finalization“ aktiv, und klicken Sie auf den Button „Flash“. Schalten Sie jetzt das Handy aus, und schließen Sie es mit gedrückter „c“-Taste an das USB-Kabel an. Der Flashvorgang startet und ist nach rund zehn Minuten beendet.

Frei von Riskiko ist das aber natürlich nicht. Ähnlich wie beim Aufspielen einer neuer Firmware auf einen DVD-Brenner darf die Verbindung während der Übertragung keinesfalls unterbrochen werden – sonst ist das Betriebssystem des Telefons unbrauchbar und muss zur Reparatur zum Hersteller geschickt werden.

4. Mobiltelefon flashen lassen

Wer sich nicht an den Eigenumbau traut, der findet etwa mit Firmen

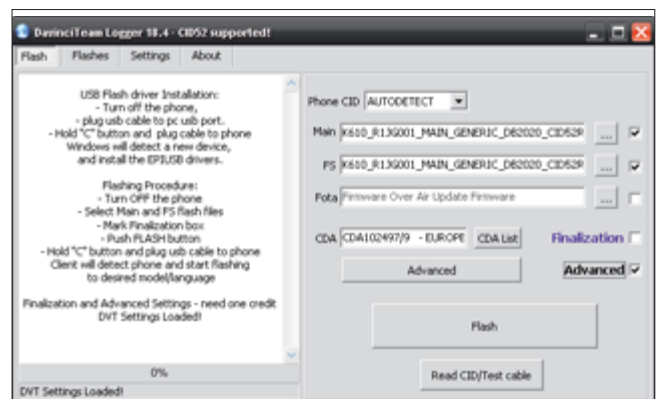
wie Smartmod (www.smartmod.de) Dienstleister für den kompletten Austausch der Software von gebrandeten Handys. Diese Anbieter verfügen über spezielle Hardware (Twister Flasher), um diesen Eingriff vorzunehmen. Das Zurücksetzen der Handy-Firmware kostet zwischen 20 und 30 Euro.

5. Vorbelegte Tasten einfach austricksen

Doch auch ohne Flashen des Mobiltelefons können Sie sich vor Kosten wappnen. Kostenlos lässt sich einfach die Internet-Verbindung ins Leere laufen. Dazu richten Sie eine neue WAP-Verbindung mit bewusst ungültigen Zugangsdaten ein und schalten diese als Standardzugang aktiv. So kommt natürlich kein Verbindungsaufbau mit dem Internet zustande, und Sie müssen nur eine Fehlermeldung bestätigen.

5. Datendienste vollständig sperren lassen

Ganz auf Nummer sicher geht man durch die Sperrung der kostenpflichtigen Datendienste, die auf das GPRS-Protokoll für WAP, E-Mail und auch das Versenden von MMS-Nachrichten setzen. Vodafone-Kunden wählen dazu die kostenlose Hotline-Nummer (08 00) 172 12 12 oder direkt vom Handy die Kurzwahl 1212 und veranlassen die Sperrung, die einmalig 4,95 Euro kostet. Kostenlos erfolgt die Sperrung für E-Plus-Kunden unter der Handy-Kurzwahl 1000. Für die Abschaltung des GPRS-Dienstes wählt man bei O2 die Nummer 55222 vom Handy aus. T-Mobile-Kunden müssen unweigerlich ihr Handy debranden oder mit der Verbindung tricksen, ein dauerhaftes Abschalten des GPRS-Datendienstes ist jedenfalls nicht möglich. ❌



Neue Software aufspielen: Mit der Software vom DaVinci-Team werden Handys von Sony Ericsson ihr Branding los (Punkt 3)



Dateneinbruch mit Nachschlüsseln

Office-Dokumente, Mailkonten, Instant Messenger – für fast jede Anwendung mit Passwortfunktion gibt es eine spezielle Knack-Software. Damit ist eine Datei blitzschnell aufgesperrt.

Von **Ramon Schwenk** und **Sascha Zäch**

Viele Anwendungsprogramme und Online-Dienste verwenden einen Passwortschutz, der jedoch oft nur eine trügerische Sicherheit vermittelt. Denn Knack-Tools liefern die vom Anwender eingesetzten Kennwörter im Klartext. Ein Segen für vergessliche Benutzer – das ideale Handwerkszeug für Datenhacker.

1. Gespeicherte Passwörter sind mit Freeware auszulesen

Um passwortgeschützte Dateien in der damit verknüpften Anwendung öffnen zu können, müssen Sie entweder das betreffende Passwort kennen oder es aus der Datei entfernen. Hacker haben besonders leichtes Spiel bei unzureichenden Kennwörtern, denn hier führt schlichtes Raten am schnellsten

zum Ziel. So ist der eigene Name oder der von Frau und Kindern ein beliebtes Passwort. Auch andere Bezeichnungen aus dem unmittelbaren Umfeld wie Wohnort, Straße, Haustiere oder Begriffe aus dem Pornobereich machen es oft leicht, Vermutungen anzustellen.

Das wichtigste Handwerkszeug von Hackern sind jedoch Passwort-Recovery-Tools, die als elektronischer Nachschlüssel arbeiten. Gleich 15 Kennwortknacker enthält die kostenlose Passwort-Knack-Suite (auf CD). Solche Utilities versuchen zunächst das bloße Auslesen oder Entfernen des Passworts innerhalb des Binärcodes der kennwortgeschützten Datei. Das Passwort wird dazu einfach auf dem Bildschirm angezeigt, überschrieben oder gelöscht. Die Profis der

Passwortknackszene bieten passende Dechiffrierer für Office-Anwendungen, Mailprogramme, Instant Messenger, Packer-Tools und andere Software an.

Hersteller von Knackprogrammen haben bei der Analyse der Dokumentenstruktur in den allermeisten Fällen einfaches Spiel: Statt eine Datei beim Speichern vollständig zu verschlüsseln, also die gesamte ursprüngliche Dateistruktur durch ein mehr oder minder undurchsichtiges Zahlen- und Buchstabenwirrwahr zu ersetzen, lassen viele Software-Entwickler die Datei in ihrem ursprünglichen Zustand und platzieren nur einen Code an einer vordefinierten Position, falls Sie beim Speichern des Dokuments ein Passwort angeben. Beim Öffnen der Datei schaut die jeweilige Anwendung nach, ob an der betreffenden Stelle ein Kennwort vorhanden ist, und fordert bei Bedarf zur Passworтеingabe auf. Diese Schutzvariante kommt bei den meisten Office-Programmen zum Einsatz. Für den Hersteller der jeweiligen Software hat dieses nachlässige Schutzverfahren den Vorteil, dass er nicht eine Vollverschlüsselungsroutine integrieren muss.

2. Wo es Knack-Tools schwer haben

Schwieriger zu knacken sind vollständig verschlüsselte Datenpakete. Als derzeit sicher gelten bei der symmetrischen Verschlüsselung die Verschlüsselungsalgorithmen AES (Advanced Encryption Standard), die auf dem inzwischen in die Jahre gekommenen Vorgänger Triple DES basieren. Der ursprüngliche DES (Data Encryption Standard) arbeitet mit der unzureichenden 64-Bit-Schlüssellänge, Triple DES mit dreifacher Schlüssellänge (168 Bit) ist etwas sicherer. Die Schlüssellänge hängt ab vom verwendeten Algorithmus. Je länger der Schlüssel ist, desto schwieriger ist es, die codierten Daten zu knacken. Lässt sich der Dateischlüssel nicht entfernen, führt das systematische Ausprobieren aller möglichen Buchstaben-, Zahlen- und Sonderzeichenkombinationen ans Ziel. Knackprogramme attackieren die Datei bei dieser Brute-Force-Methode je nach Prozessorgeschwindigkeit mit bis zu mehreren tausend Zeichenkombinationen pro Sekunde. Abhängig von der Komplexität des Schlüssels kann das Ausprobieren mehrere Stunden bis Tage dauern, und ein Volltreffer ist längst nicht in



Schnelle PDF-Decodierung: In der Regel sind Adobe-Acrobat-Dateien binnen weniger Sekunden entschützt (Punkt 2)

jedem Fall sicher. Für eine Beschleunigung beschränken Hacker die Länge des Passworts und verwenden ein Dictionary (Wörterbuch). Wörterbuchdateien mit mehreren Millionen Einträgen sind im Internet für alle wichtigen Landessprachen erhältlich und bestehen aus einer alphabetisch sortierten Liste von Namen, Bezeichnungen sowie Begriffen, die von Knackprogramm der Reihe nach ausprobiert werden.

3. Elektronische Nachschlüssel: Knackprogramme sind legal

Gegen Knackprogramme ist in den allermeisten Fällen kein Kraut gewachsen. Die von uns im Rahmen dieses Beitrags getesteten Passwortknack-Tools halten das, was sie

legt. Das gilt nicht, wenn Sie Knack-Software ausschließlich auf eigene Dateien ansetzen, deren Passwort Sie vergessen haben. In einer juristischen Grauzone bewegt sich dagegen bereits ein Firmenchef, der während der urlaubsbedingten Abwesenheit eines Mitarbeiters an geschützte Unterlagen gelangen muss und dazu ein Knackprogramm verwendet.

Für sicherheitsbewusste Anwender bedeutet dies, dass sie sich alleine auf die in Office-Programmen und in anderen Anwendungen eingebauten Kennwortschutzfunktionen keinesfalls verlassen dürfen. Hohen Schutz erzielen Sie durch ein mehrstufiges Sicherheitskonzept bestehend aus Zugangsschutz zum PC (Bios-Passwort), Windows-

versprechen. Anwender, deren persönliche Daten geknackt oder unerlaubt verändert wurden, fordern seit langem ein gesetzliches Verbot solcher Knackprogramme. Eine rechtliche Handhabung, bereits die Herstellung und Verbreitung derartiger Software auf juristischem Weg zu unterbinden, existiert in Deutschland nicht. Der Einsatz von Knack-Tools unterliegt jedoch den engen Regelungen des Strafgesetzbuchs, das das unter anderem das Ausspähen und Manipulieren fremder Daten mit Strafe be-

Überblick Dechiffrierung

Inhalt	Seite
1. Passwörter mit Freeware auslesen	84
2. Wo es Knack-Tools schwer haben	84
3. Knackprogramme sind legal	85
4. Lösung von Passwort-Problemen	85
5. Schwächen beim Benutzerkennwort	86
6. Windows-Passwort: So umgehen es Profis	86
7. Rainbow Tables als Universalnachschlüssel	87
Kästen	
Verschlüsselungsverfahren	85
So machen Sie es Angreifern schwer	86
Knackmethoden	87

Kennwort und Anwendungspasswort in Verbindung mit einem zusätzlichen Datenverschlüsselungsprogramm.

4. Lösung von Passwort-Problemen

Generell sollten Sie keine Passwörter auf dem Rechner speichern – nicht nur aus Sicherheitsgründen. Sie vergessen sie sonst rasch und können sich dann im Notfall nicht mehr einloggen.

Um bereits gespeicherte Passwörter zu löschen, gehen Sie wie folgt vor: Lassen Sie sich zunächst mit den Tools aus der Passwort-Knack-Suite (auf CD) anzeigen, welche Kennwörter gespeichert sind. Starten Sie dann die entsprechenden Anwendungen, wechseln Sie in den jeweiligen Konfigurationsdialog für die Benutzer-beziehungsweise Kennwortdaten, entfernen Sie das Passwort, und deaktivieren Sie eine eventuell

Hintergrund: Verschlüsselungsverfahren

Nachstehend finden Sie eine Liste mit den bekanntesten Chiffrier-Algorithmen, ergänzt durch eine Erklärung der Verschlüsselungsverfahren:

AES: Advanced Encryption Standard, auch Rijndael-Algorithmus genannt, wird unter anderem von US-Behörden zum Schutz geheimer Infos verwendet. Er wurde 1998 veröffentlicht und ermöglicht Schlüssellängen von bis zu 256 Bit. Damit bietet AES eine recht hohe Sicherheit.

Blowfish: Dieses schnelle Verfahren stammt aus dem Jahr 1993. Blowfish unterstützt variable Schlüssellängen von bis zu 448 Bit. Allerdings konnte seine Sicherheit bislang noch nicht mathematisch bewiesen werden.

DES/3DES: Data Encryption Standard ist der Vorgänger von AES und wurde erstmals 1974 vorgestellt. Seine Schlüssellänge beträgt nur 56 Bit, was heutigen Sicherheitsstandards nicht mehr genügt. Deshalb wurde Triple DES (auch 3DES genannt) entwickelt. Dabei kommen drei voneinander unabhängige 56-Bit-Schlüssel zum Einsatz.

RSA: Im Gegensatz zu Krypto-Algorithmen wie AES, Blowfish und DES ist das RSA-Verfahren asymmetrisch. Es kommt deshalb sehr häufig in Mail-verschlüsselungsprogrammen zum Einsatz. Präsentiert wurde RSA erstmals im Jahre 1977. Es nutzt die Multiplikation zweier Primzahlen mit mehreren hundert Stellen.



Knacker: Mit dem Password Recovery Toolkit retten Sie Dokumente, bei denen Sie Ihr Kennwort vergessen haben (Punkt 4)

vorhandene Option, die „Kennwort speichern“ oder ähnlich heißt. Falls vorhanden, klicken Sie auf „Kennwörter löschen“, um bereits im Programm gespeicherte Passwörter zu eliminieren.

Einer der populärsten Hersteller von Decodierprogrammen ist die russische Firma Elcomsoft (www.elcomsoft.de). Sie bietet unter anderem Tools für Archiv-, PDF-, Office- und Mailpasswörter an. Anders als die Kennwort-Enttarner aus der Passwort-Knack-Suite sind diese Tools jedoch kostenpflichtig. Alle Programme von Elcomsoft können auf der Website des Unternehmens

zahl des Passworts ein. Bei „Range“ lassen sich Angaben zum Aufbau des Passworts machen: nur Zahlen, nur Kleinbuchstaben, alphanumerisch mit Kleinbuchstaben. Dann beginnt der Knackvorgang mit „Start“. Das Knackprogramm nutzt dabei die Brute-Force-Methode – stures Durchprobieren aller möglichen Kombinationen. Deshalb kann der Vorgang je nach Länge und Aufbau des Passworts sowie Rechenleistung Tage oder Jahre dauern. Sehr nützlich: Das Programm beherrscht neben der Brute-Force-Methode auf der Registerkarte „Dictionary“ auch eine Dictionary Attack mit Wörterbüchern.

als Demoversionen geladen werden (einige Testversionen finden Sie auf CD). Die Programme sind zwar meist englischsprachig, die simple Oberfläche macht die Bedienung aber dennoch einfach.

Beispiel Advanced ZIP Password Recovery: Bei „Encrypted ZIP-file“ laden Sie die gewünschte ZIP-Datei ins Programm. Geben Sie nun unter „Length“ die vermutete Zeichen-

5. Windows-Schwächen beim Benutzerkennwort

Windows-Passwörter sind nicht wirklich sicher. Windows speichert sie zwar nicht im Klartext, sondern wandelt sie in alphanumerischen Code um. Wenn das Kennwort weniger als 15 Zeichen lang ist, wird es als LAN Manager Hash (kurz LM-Hash) gespeichert. Tippt nun ein Benutzer ein Windows-Kennwort ein, wird dessen Hash-Wert bestimmt und mit dem im System gespeicherten verglichen: Bei Übereinstimmung steht der Weg zu Windows offen.

LM-Hashes weisen zwei Schwachstellen auf: Alle Kleinbuchstaben werden beim Errechnen des Hash-Werts in Großbuchstaben umgewandelt. Außerdem teilt Windows Passwörter, die länger als sieben Zeichen sind, in zwei LM-Hashes auf. Beides verringert die Zahl der möglichen Zeichenkombinationen beträchtlich. So ist es selbst mit der Brute-Force-Methode möglich, Windows-Passwörter in Stunden zu knacken. Mit Verfahren wie Rainbow Tables lassen sie sich sogar sekundenschnell aushebeln. Abgelegt werden die LM-Hashes in der Datei „SAM“ im Ordner C:\Windows\system32\config.

6. Windows-Passwort: So umgehen es Profis

Bis und mit Windows ME nutzte Microsoft nur LM-Hashes als Kodiervorgang. Neuere

Codes knacken: So machen Sie es Angreifern schwer

Einfache Passwörter oder sogar für verschiedene Dienste dasselbe Passwort birgt ein Sicherheitsrisiko: Kurze Kennwörter können in Sekunden geknackt werden – mit kostenlosen Programmen aus dem Internet.

Das Problem: Komplizierte Passwörter kann sich keiner merken, zu einfache werden schnell geknackt. Die folgenden Tricks sorgen für Abhilfe:

Wörter verschmelzen: Wählen Sie zwei Wörter und schaffen Sie aus deren Silben ein neues. Aus „Katze“ und „Hund“ könnten Sie etwa das Wort „KatHuzend“ bilden. Dieses ist schon sehr schwer zu knacken. Um die Sicherheit zu erhöhen, fügen Sie zusätzlich eine Zahl und ein Sonderzeichen ein: „Kat1Hu;zend“

Satz als Vorlage: Denken Sie sich einen Satz aus und bilden Sie aus den Anfangsbuchstaben das Passwort. Aus „Ich mag Eis nur im Sommer gerne essen“ wird etwa „ImEniSge“. Würzen Sie auch ein solches Passwort zusätzlich mit einer Zahl und einem Sonderzeichen. Achten Sie darauf, dass Sie als Satzvorlage kein bekanntes Sprichwort wählen. Einige Knack-Tools probieren genau solche Varianten durch.

Hilfreiche Nachbartaste: Tippen Sie einen Begriff, indem Sie jeweils die benachbarten Tasten drücken. Dadurch werden einfache Wörter wie „Geldgier“ zu unsinnigen Zeichenfolgen („Fwksfuwe“). Wie immer lohnt es sich auch hier, Sonderzeichen und Zahlen einzusetzen.

Analogien und Gegenteile: Ersetzen Sie Teile eines Wortes durch einen analogen oder gegenteiligen Begriff. Ein schönes Beispiel ist das Wort „komfortabel“. Für „fort“ wählen wir „weg“, für „abel“ den Namen „Kain“. Das Ergebnis ist das Passwort „komwegKain“ oder noch besser „kom2weg!Kain“.

Aufwand abschätzen: Natürlich ist es am besten, möglichst sichere Passwörter zu wählen. Manchmal ist der Aufwand allerdings zu groß. Möchten Sie sich nur kurz für einen Download, einen Forenbeitrag oder einen unkritischen Web-Dienst registrieren, reicht auch ein einfaches Kennwort. Kaum jemand wird ein wirkliches Interesse daran haben, dieses zu knacken, kann er sich doch selbst registrieren. Investieren Sie lieber mehr Aufwand in den Schutz von Diensten, die wirklich kritisch sind, etwa Online-Banking, Haupt-Mailadresse und so weiter.

Windows-Versionen verwenden zusätzlich die sicherere Version namens NTLM-Hash, verzichten bei Passwörtern aus Kompatibilitätsgründen jedoch nicht auf die Speicherung der LM-Hashes. Am einfachsten beseitigen Sie diese Schwachstelle in neueren Windows-Versionen, indem Sie ein Passwort mit mindestens 15 Zeichen wählen, denn zum Bestimmen des LM-Hashes werden Passwörter nach dem 14. Zeichen abgeschnitten. Alternativ können Sie das Speichern von LM-Hashes auch mit einem Registry-Kniff verhindern.

Starten Sie den Registry-Editor mit „Start, Ausführen“ und dem Befehl regedit.exe. Klicken Sie auf „HKey_Local_Machine\System\CurrentControlSet\Control\Lsa“. Wählen Sie „Bearbeiten, Neu“ und „DWORD-Wert“, dann tippen Sie „NoLMHash“ ein. Ist der neue Eintrag ausgewählt, setzen Sie mit „Bearbeiten, Ändern“ den DWORD-Wert auf „1“. Starten Sie den Rechner neu und ändern Sie Ihr Kennwort. Dank der Schwäche der LM-Hashes lassen sich vergessene Windows-Passwörter relativ schnell zurückholen. Dazu gibt es verschiedene kostenlose Programme. Empfehlenswert ist etwa die Freeware LCP (für Win NT, 2000 und XP, www.lcpsoft.com, 2,29 MB). Sie beherrscht Brute-Force- und Wörterbuch-Angriffe und kann diese beiden Methoden sogar kombinieren. Via Menübefehl „Import“ laden Sie die LM-Hashes ins Programm. Am einfachsten geht das über die Option „Import From Local Computer“. Sie können aber auch eine SAM-Datei einlesen („Import From SAM File“) oder die LM-Hashes von einem anderen Netzwerkrechner ins Programm holen („Import From Remote Computer“). Mit „Begin Audit“ startet der Knackvorgang. LCP kommt übrigens auch mit den sichereren NTLM-Hashes zurecht, benötigt hier aber je nach Passwort einiges länger.

7. Rainbow Tables als Universalnachschlüssel

Es geht sogar noch schneller als mit LCP. Das Zauberwort heisst Rainbow Tables. Sie ermöglichen es, das Windows-Passwort innerhalb weniger Minuten auszuhebeln. Der Trick: Statt jedes Mal alle Varianten durchzuprobieren, werden einmal alle LM-Hash-Werte für mögliche Passwörter berechnet und in einer Tabelle gespeichert. Anschließend reicht es, die LM-Hash-Werte aus der SAM-Datei zu lesen und mit der Tabelle zu

vergleichen. Fast nicht zu glauben, aber probieren Sie es selbst aus: Laden Sie die kostenlose Software Ophcrack (<http://ophcrack.sourceforge.net>, 3,9 MB) herunter. Während der Installation müssen Sie angeben, ob Sie die Rainbow Tables von einer CD/DVD importieren oder aus dem Internet herunterladen wollen.

Hier liegt auch der Nachteil der Methode: Eine Tabelle ist mehr

ere hundert MB groß. Nach der Installation holen Sie die LM-Hashes mit dem Befehl „Load, From local SAM“ ins Programm. Mit „Launch“ beginnt die Passwortsuche. Alternativ können Sie Ophcrack auch als Live-CD herunterladen (484 MB). Es handelt sich um ein CD-Abbild im ISO-Format, das Sie auf einen Rohling brennen. Es enthält



Systemschwäche: Das Verfahren, das Microsoft für Windows-Kennwörter einsetzt, ist vollständig geknackt (Punkt 6)

eine bootfähige Linux-CD inklusive Ophcrack und Rainbow Tables. Damit lässt sich der Passwortschnüffler ganz ohne Installation nutzen. Es reicht, die CD einzulegen und den Rechner zu starten. Die Software sucht anschließend selbstständig nach einer Windows-Partition, extrahiert die LM-Hashes und startet den Knackvorgang. ❌

Knackmethoden: Das müssen Sie wissen

Es gibt eine Reihe wirksamer Methoden, um ein Passwort mehr oder minder schnell zu knacken. Die Kennwort-Enttarnung muss nicht mal immer mit Computern zu tun haben.

Brute Force: Der Begriff bedeutet so viel wie rohe Gewalt und beschreibt damit sehr schön das zugrundeliegende Konzept. Der Angreifer probiert systematisch alle möglichen Kombinationen durch, bis er das richtige Passwort gefunden hat.

Dictionary Attack: Ein solcher Angriff führt unter Umständen schneller zum Ziel als die Brute-Force-Methode. Zum Knacken des Passworts werden Wörter aus einer Liste verwendet. Durchgespielt wird das Ganze auch mit Wortkombinationen und rückwärts geschriebenen Begriffen. Am besten wird das Wörterbuch an die Landessprache des Nutzers angepasst und noch mit persönlichen Daten wie Namen oder Geburtsdatum ergänzt.

Rainbow Tables: Spezielle Methode zum Knacken des Windows-Passworts. Statt stur alle möglichen Kombinationen durchzuspielen, werden die LM-Hash-Werte für alle möglichen Passwörter errechnet und in einer Tabelle gespeichert. Mit Hilfe der Tabelle rekonstruiert ein moderner Computer ein Passwort in wenigen Minuten aus einem beliebigen LM-Hash-Wert.

Social Engineering: Oft machen sich Angreifer gar nicht die Mühe, mit aufwendigen Rechenmethoden ein Passwort zu knacken. Sie nutzen die Leichtgläubigkeit von Nutzern aus. Warum lange ausprobieren, wenn man einfach nach dem Passwort fragen kann, indem man sich als Systemadministrator oder Techniker ausgibt? Auch Phishing-Mails gehören in den Bereich des Social Engineering. Nutzer werden per Mail aufgefordert, unter einem bestimmten Link ihre Zugangsdaten für ihr Online-Banking-Konto oder einen anderen Internet-Dienst zu verifizieren. Dabei werden sie auf eine gefälschte Seite umgeleitet.



Hacker greifen PCs an

Das Internet ist die Gefahrenquelle Nummer eins für Ihren PC. Hacker nutzen potenzielle Schwachstellen von Computersystemen, spähen persönliche Daten aus, verändern Dokumente oder zerstören alles.

Von **Martin Danhof**

Die vernetzte Internet-Welt hat ihren Preis: Die Sicherheit gespeicherter PC-Daten und persönlicher Informationen ist durch Hackangriffe von außen gefährdet. Viele der Schlupflöcher lassen sich zwar abdichten, doch die Angreifer haben im brennenden Wettrennen oft die Nase vorn.

1. Sicherheits-Tools zum Trotz: Hohe Risiken für PC-Nutzer

Hacker verwenden Abhörprogramme zum Ausspionieren von PC-Anwendern, setzen Trojaner, Würmer und Viren ein, um Rechner lahm zu legen, oder starten heimlich Backdoor-Fernsteuerungsprogramme, über

die sie unbemerkt die Kontrolle über fremde Rechner übernehmen wollen. Andere nutzen Drive-by-Downloads (siehe Kasten) oder installieren Software-Module, die dem Nutzer beim Surfen Dialogfenster unterschieben in der Hoffnung, dass der Anwender diese vorschnell akzeptiert.

In den vergangenen beiden Jahren nahm die Zahl der bekannt gewordenen Internet-Hackangriffe drastisch zu. Dennoch vernachlässigen Software-Hersteller bei der Entwicklung von Betriebssystemen, Anwendungsprogrammen und Utilities die Sicherheit zugunsten von Benutzerfreundlichkeit und Funktionsfülle – ein nicht unerhebliches

Risiko für die Sicherheit Ihrer Daten. Ungesicherte Online-Schnittstellen und laxe Chiffrierungsmodule oder gar unverschlüsselte Kennwortübermittlungen im Klartext sind an der Tagesordnung.

2. Immer öfter Privatanwender im Visier von Hackern

Obwohl Unternehmen für versierte Angreifer immer noch das attraktivste Ziel darstellen, können auch die Systeme von Privatanwendern im Falle eines erfolgreichen Hackversuchs für zahlreiche Zwecke missbraucht werden, zum Beispiel zum Versenden von Spam-Nachrichten, zum Hosten (Bereitstel-



Überblick PC-Manipulation

Inhalt	Seite
1. Sicherheits-Tools zum Trotz: Hohe Risiken	88
2. Privatanwender im Visier von Hackern	88
3. Sicherheitslücken: Nicht nur Windows ist betroffen	89
4. Online-Hackerangriffe: Inzwischen die Regel	90
5. Systemeinbruch mit gefakten Updates	90
6. Probleme mit Software aus unbekannten Quellen	91
7. Malware-Derivate: Auch Hacker rüsten auf	91
8. Der bombensichere PC als Wunschtraum	91
Kästen	
Hacker: Ein Angreifer erzählt	90
Drive-by-Downloads: Das steckt dahinter	91

len) rechtswidriger Inhalte – Stichwort Raubkopie-Server – und für Flooding-Angriffe auf Websites in Form von Denial-of-Service-Attacken. Gehackte PCs eignen sich auch zum Weiterleiten von Daten, um beispielsweise den tatsächlichen Speicherort einer Website zu vertuschen.

Eindringversuche laufen meist nach einem festen Muster ab. Um die Kontrolle über ein System zu übernehmen, muss der Angreifer zunächst ein Programm seiner Wahl auf dem Ziel-PC ausführen, etwa unter Ausnutzung einer Sicherheitslücke in Windows oder einer anderen Software, für das eine Internet-Verbindung verwendet wird. Wenn dieses Ziel erreicht wurde, bleibt das Programm normalerweise im Hintergrund aktiv, um Befehle entgegenzunehmen und Statusinformationen an den Angreifer zu senden. Solche Angriffe werden besonders häufig ausgeführt, und die verwendeten Programme gehen zudem immer raffinierter vor, so dass sie schwieriger zu erkennen und zu entfernen sind. Gemäß der Web-Seite <http://dshield.org>, auf der Angriffsdaten gesammelt werden, wird ein ungeschütztes System durchschnittlich innerhalb von 17 Minuten gefährdet. Dshield.org ist eine freie

Online-Datenbank für Administratoren und Internet-Provider, die Anhaltspunkte über die Aktivitäten potenzieller Internet-Angreifer sammelt. Der englischsprachige Dienst soll helfen, sich gemeinsam gegen Hackerangriffe zu schützen. Dazu wertet die Datenbank die von den Benutzern eingesandten Firewall-Protokolle aus. Auf Basis der Logs sollen Muster von verdächtigen Aktivitäten frühzeitig erkannt und gemeldet werden.

3. Sicherheitslücken: Nicht nur Windows ist betroffen

Externe Angriffe über TCP/IP-Verbindungen stellen derzeit die populärste Angriffsmethode dar. Über eine Internet-Netzwerkverbindung kann jedermann weltweit auf jede beliebige IP-Adresse zugreifen. Problematisch sind hierbei die Standleitungs-ähnlichen DSL-Zugänge. DSL-Nutzer, die über eine Flatrate zum Pauschaltarif verbunden sind, verzichten oft aus

Bequemlichkeit darauf, den Online-Anschluss bei Nichtbenutzung zu unterbrechen. Dadurch sind sie über Stunden oder Tage mit der vom Provider zugewiesenen IP-Adresse online und erreichbar. Ist ein Angriff erfolgreich, bemerken die Betroffenen wegen der hohen Bandbreite die Spionage und einen damit einhergehenden heimlichen Datenklau meist nicht.

Beim Gros der Internet-Attacken handelt es sich nicht um gezielte Angriffe auf bestimmte Rechner. Vielmehr finden automatische Untersuchungsvorgänge statt, beispielsweise in Form von Portscans, über die offene Netzverbindungen eines PC geprüft werden.



Einfallstor: Hacker modifizieren Raubkopien, um damit Zugang zum System der Verwender zu erhalten (Punkt 3)



Illusion: Die von Firewall-Tools gezählten Angriffe sind meist harmlos, harte Angriffe lassen sich durchschleusen (Punkt 5)

Das systematische Scannen von IP-Adressbereichen dient auch der Suche nach Rechnern mit bestimmten Sicherheitslücken, die sich als Schlupfloch von außen eignen. Das für Netzwerke offene Vista wurde zwar viel sicherheitsbewusster als seine Vorgänger konzipiert. Dennoch ticken nach den Erfahrungen mit den Vorversionen zahlreiche Zeitbomben in dem Betriebssystem,

Linux als populäres Betriebssystem ist inzwischen betroffen. Vor allem die großen und auf vielen Rechnern installierten Distributionen Suse und Ubuntu rücken derzeit näher ins Visier von Computerhackern. Durch Updates nicht geschlossene Schwachstellen in Windows- und Linux-Betriebssystemen laden Hacker und Datenspieler geradezu ein, in die Systeme einzudringen.

4. Online-Hackerangriffe: Inzwischen die Regel

Durch das Einspielen der Patches schließen Sie die Lücken, durch die Angreifer die Gewalt über Ihren Rechner erlangen können. Dass PC-Einbrüche überhaupt gelingen können, liegt aber nur zu einem Teil an dem verwendeten Betriebssystem und der eingesetzten Software. Ganz wesentlich tragen die Unkenntnis und Gleichgültigkeit von PC-Anwendern dazu bei. Nur wenige Angriffe von außen haben ohne Zutun des Anwenders Erfolg. Über einen IP-Scan können Angreifer zwar systematisch nach offenen Ports suchen und so mögliche Angriffsziele ausmachen. Da für Hacker interessante Ports aber normalerweise erst durch eine Malware geöffnet werden, muss diese zunächst einmal auf den PC gelangen. Die meisten Gefahren gehen von Schadprogrammen aus, die Anwender selbst aktivieren. Geeignete Abwehrmöglichkeiten bieten Virens Scanner, Desktop-Firewalls und Spyware-Scanner, die alle über das Internet ausgetauschten Datenpakete kontrollieren.

Profi-Hacker: Ein Angreifer erzählt

Sein Vorname ist Victor, sein Nachname soll jedoch geheim bleiben. Er ist 30 Jahre alt und lebt in St. Petersburg, Russland. Nachdem er seine Hackertätigkeit aufgegeben hat, hat er einen legitimen Job in einer örtlichen Software-Entwicklungsfirma gefunden, und es scheint ihm Spaß zu machen. Als Victor hörte, dass Agnitum (www.agnitum.de), russischer Hersteller von Sicherheits-Software, nach Profis mit Erfahrungen bei Cyber-Sicherheitsproblemen aus erster Hand sucht, meldete er sich bei dem Virenabwehrspezialisten, um über die Malware zu sprechen.

Wie lange waren Sie als Hacker und Malware-Autor aktiv?

Als Hacker, hm, da bin ich mir nicht sicher. Das waren ungefähr zehn Jahre oder so. Es fing alles an, als ich noch studiert habe. Ich weiß noch, dass ich eines Tages auf den Server zugreifen musste, also habe ich meinen PC von einer Linux-Diskette aus hochgefahren und habe damit alle Windows-Passwörter zurückgesetzt. Ich weiß noch, wie frustriert der Systemadministrator war. So war das, komisch, schätze ich.

Damals habe ich auch andere schlechte Sachen gemacht, beispielsweise bestimmte Viren geschrieben und Phishing-Mails verschickt, um mal zu sehen, wie schnell ich Leute dazu bringen konnte, Informationen und Geld herauszurücken.

Wie schwer ist es, eigene Malware zu programmieren?

Es sind im Untergrund Tools online erhältlich, die ganz einfach eine neue Version zum Beispiel eines Trojaners aus der Original-Binärdatei erzeugen können. Obwohl das nur eine primitive Abwandlung ist, besteht trotzdem die Chance, damit an Sicherheitsprodukten vorbeizukommen, die nicht so oft aktualisiert werden wie nötig. Alles, was man braucht, ist etwas Erfahrung in der C++-Programmierung.

Können Sie uns Beispiele für solche Malware erzeugenden Tools für Windows-PCs nennen?

Die meisten von ihnen sind sowieso frei zugänglich. Pinch Builder ist ein beliebter Trojaner in Assembler-Sprache. Jeder kann sich das Muster (ungefähr 20 KB groß) herunterladen und nach eigenem Geschmack verändern. Die Original-Binärdatei greift auf einen Bereich zu, der als Geschützter Speicher – der Speicherort der Anwender-Passwörter – von Windows bekannt ist, und zieht die Informationen heraus. Das Resultat ist ziemlich eindeutig: Eine Gefährdung der Benutzerdaten.

Man kann das Tool sogar noch erweitern, dass es als Keylogger oder Spam-Roboter oder sogar als Host für zusätzliche Malware funktioniert. Die Originalversion von Pinch wurde so entwickelt, dass sie sich vervielfältigt, während der Computer das Herunterfahren einleitet. Zu diesem Zeitpunkt werden auch die Sicherheitssysteme beendet, so dass sie leicht umgangen werden können.

Was halten Sie von maßgeschneiderter Malware, die auf bestimmte Aktivitäten oder bestimmte Anwendertypen abzielt?

Es existiert bereits ein klar umrissener Markt für auf Wunsch gefertigte Viren, Programme zur Ausnutzung von Sicherheitslücken und noch nicht bekannt gegebene Sicherheitslücken. Aber wer weiß bei der Schnelligkeit und der technischen Raffinesse der heutigen Malware-Entwickler schon, ob es die Programmhersteller oder die Hacker sind, die das Spiel schließlich gewinnen werden. Nachdem ich auf beiden Seiten gearbeitet habe, würde ich sagen, dass die Hacker einen gesunden Vorsprung haben. Das Entstehen von Technologien wie Rootkits und Internet-basierten Diensten bietet ein riesiges Potenzial für Sicherheitslücken.

Konfigurieren Sie Ihre Sicherheits-Tools in jedem Fall so, dass sie auch von Ihnen ins Internet gesendete Daten prüfen, damit Ihr PC nicht als Replikationsstation dient, falls eine Malware aktiv werden sollte.

5. Systemeinbruch mit gefakten Updates

Besonders heimtückisch wie verbreitet sind Angriffe mit angeblichen Software-Updates, die etwa von Microsoft, Suse oder Ubuntu stammen sollen. Verbreitet sind ferner gefälschte Viren- und Wurmbeseitigungsprogramme. Auch angebliche Gratis-Spiele stellen eine erhebliche Bedrohung dar. Sie werden gezielt in Umlauf gebracht und enthalten in der Regel neben harmlosen Tarndateien – etwa offiziellen Updates – präparierten Code, über den sich Dritte Zugang zu Ihrem Rechner verschaffen oder über den eine Download-Routine aktiv wird und Software-Module von einem infizierten Internet-Server nachlädt.

Wenn ein PC hinter einer Firewall oder einem Proxy-Server steht, ist normalerweise keine ein- und ausgehende Datenkommunikation möglich und der Datenaustausch zwischen Malware und Angreifer schlägt fehl. Mit einem HTTP-Tunnel umgehen Hacker diese Sperre. Damit wird über eine erlaubte HTTP-Verbindung, durch die auch der Browser Kontakt zum Internet aufnimmt, eine Tunnelverbindung zu einem vom Angreifer vorgegebenen Server hergestellt. Die Datenübertragungen für Fernsteuerung und Datei-Downloads, die sonst über andere Ports laufen, werden über die Tunnelverbindung geleitet. Ein solcher Nebeneingang ins Internet kann viel Ärger verursachen, denn Desktop-Firewalls oder die Firewall-Module in DSL-Routern erkennen und blockieren diese Art der Verbindung nicht.

6. Probleme mit Software aus unbekannten Quellen

Bei der Installation von Software sollten Sie darauf achten, dass Sie die gewünschten Programme nur aus authentischen Quellen beziehen. Zum Download von Free- und Shareware sowie Demoversionen besuchen Sie am besten immer die Hersteller-Websites, auch wenn Sie an anderer Stelle auf das jeweilige Programm aufmerksam geworden sind. Seien Sie auch bei der Installation von Software von CD und DVD vorsichtig, wenn Sie nicht genau wissen, woher

die Programme stammen. Für Schutz sorgt ein Hintergrund-Virens Scanner.

Ein weiteres erhebliches Risiko geht von neuartigen Anmelde-Tools aus, die Ihren Namen, Anschrift sowie Ihre Mailadresse beispielsweise aus Office- oder Mailprogrammen auslesen und für eine heimliche Anmeldung bei einem kostenpflichtigen Internet-Dienst verwenden. Den Betroffenen flattern dann teils horrenden Rechnungen für angeblich genutzte Dienstleistungen ins Haus. Abhilfe: Lesen Sie alle Software-Dialoge sorgfältig durch, brechen Sie unaufgeforderte Downloads sofort ab, und lassen Sie Ihren PC regelmäßig mit einem aktuellen Virens Scanner durchsuchen. Wenn Sie diese Sicherheitsaspekte berücksichtigen, wird es für Spione und Saboteure erheblich schwerer, Schaden zu verursachen.

7. Malware-Derivate: Auch Hacker rüsten auf

In den vergangenen Jahren sorgten bestimmte Malware-Typen regelmäßig medienwirksam für großflächige Epidemien, und dafür, dass die Mitarbeiter in den Virenlabors optimale Erkennungsmethoden dagegen programmieren konnten. Doch bei den neuesten Malware-Generationen haben die Angreifer ihre Taktik geändert: Virenschreiber schicken Unmengen von Modifikationen ihrer neuen Kreationen in kurzem Zeitraum los. Damit steigern sie die Chance erheblich, dass zumindest ein Teil der Schädlinge durchkommt, denn durch die Vielzahl dieser Modifikationen brauchen die Abwehrspezialisten länger, ihre Tools auf die Malware abzustimmen.



Hack-Malware aktiv: So geschmacklos zeigen sich nur wenige Schädlinge (Punkt 7)

8. Der bombensichere PC als Wunschtraum

Beim Katz-und-Maus-Spiel zwischen Hackern und den Entwicklern von Sicherheitskomponenten gibt es keinen Gewinner. Mit Gewissheit lässt sich allerdings sagen, dass die Hersteller von Betriebssystemen, Anwendungsprogrammen und Sicherheitslösungen den Hackern immer hinterherhinken werden, solange sie nur reagieren. Und Anwender, die grundlegende Sicherheitspräventivmaßnahmen ignorieren, werden früher oder später Probleme mit infizierten Systemen haben. Sicherheit gibt es nicht umsonst, und Sicherheit macht Arbeit – das bedeutet, dass Sie sich fortlaufend um den Schutz Ihres PCs kümmern müssen. Passende Tools finden Sie auf CD.

Drive-by-Downloads: Das steckt dahinter

Ihr Rechner kann schon mit Spyware, Viren oder Trojanern infiziert werden, wenn Sie einfach nur eine Web-Seite besuchen, auf der Sicherheitslücken durch Malware ausgenutzt werden – entweder zufällig oder bewusst. Ein „Drive-by-Download“-Programm lädt sich automatisch ohne Ihr Wissen oder Einverständnis auf Ihren PC. Drive-by-Downloads können als eingebettete Active-X-, Java- oder Flash-Objekte aktiviert werden durch das Anklicken einer Werbung oder beim Besuch einer Website. Webserver, die ansonsten legitime Seiten hosten, können von Hackern modifiziert werden, Malware an die Rechner der Besucher weiterzugeben. Die Zahl der Web-Seiten, die Schad-Software über Drive-by-Downloads ausliefern, nahm in den vergangenen 12 Monaten drastisch zu.

So einfach schützen Sie sich: Schließen Sie Sicherheitslücken in Browser und Betriebssystem durch das Einspielen von Aktualisierungen und Patches per Online-Update. Misstrauen Sie Links, die von Unbekannten an Sie weitergeleitet werden. Erhöhen Sie die Sicherheitseinstellungen im Internet Explorer auf die Stufe „Hoch“, um die Ausführung von Active-X-Scripts zu verhindern.



Hacken lernen im Schnellkurs

Intensivkurse versprechen, Sie in einer Woche zum Hacker auszubilden. Wir wagten den Selbstversuch: Ist das in so kurzer Zeit möglich – kann man danach wirklich hacken?

Von **Andreas Kroschel**

Der Kurs findet auf Englisch statt. Hat jemand damit ein Problem? Mit dieser Frage beginnt unser Rundgang durch das Tagungshotel, das die Schulungsfirma Training Camp (www.trainingcamp.de) gemietet hat. Hier sollen wir innerhalb von fünf Tagen zu ethischen Hackern ausgebildet werden.

Zur Begrüßung: Die Frage ist in einem freundlichen Ton gestellt. Genauso freundlich erhalten wir neun Kursteilnehmer einen Überblick, wo sich was befindet – und erfahren, warum wir das eigentlich gar nicht wissen müssen: „Hier befindet sich die Bar. Doch unsere Erfahrung ist, dass Sie den Test nicht bestehen, wenn Sie Alkohol trinken. Ich zeige Ihnen auch gerne, wo sich die Diskothek be-

findet, würde Ihnen aber nicht empfehlen, sie zu besuchen, weil sie sonst wahrscheinlich den Test nicht bestehen werden. Sie haben sicherlich bereits die Fernsehgeräte auf Ihren Zimmern gesehen. Wir raten allerdings davon ab, fernzusehen ...“

Schwer wiegende Unterlagen: Eine halbe Stunde später sind wir im Besitz unserer Schulungsmaterialien: Eine Kiste mit fünf DVDs voller Hacker-Tools und zehn Kilogramm Lehrbüchern – erstere nur gegen die Unterschrift, sie nie außerhalb des Gesetzes einzusetzen, letztere müssen in fünf Tagen abrufbereit im Kopf gespeichert sein. Dann wird der bereits erwähnte Test stattfinden. Die Bücher ergeben einen ansehnlichen Turm auf dem

Tisch, und man sieht es den Gesichtern an: Wurde zu den Ausführungen vorhin noch gegrinst, erwägt im Augenblick niemand mehr, heute oder an den nächsten Abenden fernzusehen, Alkohol auch nur anzurühren oder gar ein Tanzlokal zu besuchen.

Weiß, Schwarz, Grau: Die Hutmode der Hacker

Ein Hacker-Kurs beginnt, so lernen wir am ersten Tag, keineswegs mit irgendwelchen technischen Übersichten oder Einzelheiten. Zunächst geht es erst einmal darum, wer wir sind: nämlich die Guten, also die ethischen Hacker, auch „Weißhüte“ genannt. Was wir lernen, werden wir niemals zu irgendwelchen kriminellen Zwecken einsetzen, sondern nur, um Rechner und das eigene Netzwerk abzusichern. Wer denkt, das wäre ihm vorher schon klar gewesen, wird eines Besseren belehrt: Auch bei anscheinend legalen Aktivitäten steht man schnell mit einem Bein im Gefängnis.

Schwarze Hüte: In der EDV kann die Rechtslage allerdings schnell unübersichtlich werden. ISPs (Internet Service Provider), die Administratoren von Zwischenstationen, Intrusion-Detection-Systeme und deren Betreiber – alle könnten im Fall des Falles schnell die Finger am Notruf haben. Bis man dann bewiesen hat, dass man zu den Guten gehört, ist man zunächst ein „Schwarzhut“. So heißt ein Angreifer, im deutschsprachigen Raum auch „Cracker“ genannt. Die Unschuldsvermutung greift in diesem Bereich nicht, da man ja offensichtlich kriminelle Handlungen begeht. Noch komplizierter wird es durch die verschiedenen nationalen Gesetze. So gelten in manchen Ländern Programme als Hacker-Software oder verbotene Kryptographie-Werkzeuge, die in Deutschland zum Standardumfang jeder Linux-Distribution gehören.

Graue Hüte: Zwischen den Schwarz- und den Weißhüten gibt es noch die Hacker, denen es vorrangig weder um kriminelle Handlungen noch um deren Vorbeugung geht. Sie wollen nur sich und der Welt beweisen, was sie können. Finden sie eine Sicherheitslücke und einen Weg, sie zu verwerten, können sie gar nicht anders, als diese auch zu nutzen. Ihr Ziel ist es, der Öffentlichkeit, zumindest aber dem Betreiber des Systems, einen Beleg für das Sicherheitsproblem zu liefern. Einerseits nutzen diese Hacker die gewonnenen Erkenntnisse nicht zum eigenen Vorteil aus, wie es Kriminelle tun würden; andererseits handeln sie eindeutig ungebeten und damit gegen das

Gesetz. Deshalb fallen sie in eine eigene Kategorie und dürfen sich „Grauhüte“ nennen.

Infoquellen ausspähen: Web-Archive und Job-Börsen

Die Begriffsdefinitionen und der juristische Teil sind zum Glück irgendwann vorbei. Wir sind uns einig, sie langweilig zu finden: Sowohl bei der Verhaftung als auch bei der Verurteilung würde man zeitig genug die Gründe dafür hören. Nun darf es ruhig richtig zur Sache gehen, mit bösartigen Tools und verbotenen Techniken. Doch bis dahin ist noch ein langer Weg.

Ausspähen: Hack-Angriffe laufen in Phasen ab, und die erste ist das Ausspähen. Das ist mit den meisten Methoden durchaus legal. Denn eine erstaunliche Menge an Informationen über Firmen oder Einzelpersonen ist öffentlich verfügbar, sobald sie im Internet präsent sind. So können Sie etwa in Job-Börsen erfahren, welche Art von IT-Spezialisten eine Firma sucht oder in der Vergangenheit gesucht hat – das gewährt einen guten Einblick in deren IT-Infrastruktur. Je nachdem, wie gut das Archiv einer Job-Börse ist, bekommen Sie eventuell sogar heraus, welche Server-Software dieses Unternehmen einsetzt.

Lohnender Blick zurück: In der Regel besitzen Websites kein eigenes Archiv. In diesem Fall benutzen Sie ein externes wie die „Way-Back-Machine“ unter <http://web.archive.org>. Hier lohnt es sich nicht nur, nach ehemals ausgeschriebenen Stellen zu suchen. Auch die Original-Site einer Firma kann sehr interessant sein. In der Naivität der Neunzigerjahre wurde so manches bedenkenlos online gestellt – etwa die Konterfeis und Durchwahlen von Vorständen, private Telefonnummern von Mitarbeitern, etwa für Kunden, und vielerlei Dokumente. Heute achtet man in den Unternehmen mehr auf Privatsphäre und Datenschutz – solche Infos mussten wieder von den Websites verschwinden. Außerdem hindert einen natürlich niemand daran, auf Archiv-Seiten gefundenen Mitarbeitern per Google hinterherzuschneffeln. Vielleicht sind es ja inzwischen ehemalige Mitarbeiter, die bereitwillig erzählen, warum dem so ist.

Social Engineering: Hacken ist gar nicht nötig

Unzufriedene Mitarbeiter, ob ehemalig oder nicht, werden von Sicherheitsunternehmen mittlerweile als Risiko Nummer eins eingestuft, was die nicht-technischen Möglichkeiten

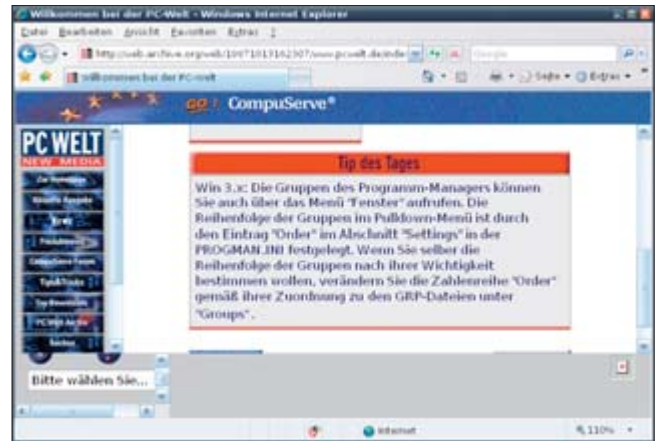
betrifft, geheime Infos über Firmen zu erlangen. Einem Hacker steht daher ein sympathisches Wesen sowie Talent zum Reden und verstehenden Zuhören gut zu Gesicht.

Mitarbeiter: Manchmal geht's noch einfacher. Ein paar Namen stehen auf der Website jeder Firma – ein Blick in deren Vergangenheit ist gar nicht nötig. Ein Anruf vom „technischen Support“, eine Frage der Außenstelle Hamburg – die meisten Mitarbeiter von Firmen werden versuchen, zu helfen. Aus der Sicht eines Sicherheitsverantwortlichen sind und bleiben Menschen der schwächste Punkt. Dieses Problem ist prinzipiell nicht lösbar: Eine Firma, in der Mitarbeiter einander so misstrauen, dass Social Engineering unmöglich wäre, hätte keine große Zukunft – das würde schließlich bedeuten, dass hier keiner den anderen unterstützt.

Endlich wird's ernst: Tricks und Tools

Mit den „weichen“ Kenntnissen, wie sie zum Social Engineering erforderlich sind, halten wir uns nicht mehr weiter auf. Im Vorfeld bereits zu wissen, mit welcher Art von IT-Infrastruktur zu kämpfen sein wird, ist sicher nützlich. Doch irgendwann muss man ran an den Feind. Die Phase des Ausspähens ist vorbei, und in den nächsten vier Phasen heißt es: Scannen, Zugriff erlangen, Zugriff aufrechterhalten, Spuren verwischen. Interessant dabei ist, dass gehackte Rechner oder Netzwerke vom Angreifer in der Regel nachträglich abgedichtet werden. Wenn das System undicht genug war, um übernommen zu werden, wissen Hacker natürlich, dass das auch anderen gelingen kann. Konkurrenz ist nicht erwünscht – und deshalb installieren sie Patches und Sicherheits-Updates oder ändern sogar eine fehlerhafte Konfiguration so, dass das System abgesichert wird. Für den eigenen zukünftigen Zugang installieren sie entweder Backdoor-Tools oder verwenden den vorgesehenen Fernzugriff des gehackten Systems.

Mit übernommenen Rechnern findet ein reger illegaler Handel statt: Oft hacken Schwarzhüte nicht, um die Opfer-Rechner selbst zu verwenden, sondern verkaufen sie an Internet-Krimi-



Das Web vergisst nichts: In den Online-Archiven findet sich auch manches, das man heute nicht mehr veröffentlichen würde

nelle, denen es am nötigen Know-how für den Aufbau eigener Bot-Netze fehlt.

Tricks & Tools: In den nächsten Tagen lernen wir Unmengen an Methoden und Tools kennen, je nachdem, ob wir auf Netzwerk-Ebene oder Betriebssysteme beziehungsweise spezielle Anwendungen angreifen wollen. Die Fülle des Stoffes ist kaum zu bewältigen, die Lektionen gehen täglich über zwölf bis dreizehn Stunden. Auch die Freizeit verbringt man am besten vor dem PC und versucht, so viel Theorie wie möglich in die Praxis umzusetzen. Kleiner Wermutstropfen: Keiner von uns schafft es, die Internet-Verbindung lahmzulegen. Teilnehmern anderer Kurse vor uns gelang das: Sie lösten durch ihre Übungsaktivitäten diverse Male beim ISP Alarm aus, weswegen die Leitung gekappt und nur nach viel gutem Zureden wieder freigeschaltet wurde.

Stunde der Wahrheit: Prüfungsangst

Nach fünf Tagen der Test: vier Stunden Zeit, einhundertfünfzig Fragen, siebzig Prozent müssen richtig beantwortet sein. Training Camp gibt eine Garantie auf seine Ausbildung: Wer durchfällt, darf so lange kostenlos die nächsten Kurse belegen, bis er besteht. Allerdings fallen Kost, Logis sowie die Gebühr für die Prüfung jedes Mal an, so dass eine Wiederholung trotzdem mit erheblichen Kosten verbunden wäre. Die Motivation, gleich zu bestehen, ist also durchaus gegeben. Am Ende schaffen es vier von neun. Natürlich ist es wie bei allen Kursen – das Vergessen setzt schnell ein, und einen Monat später würde man die gleiche Prüfung vermutlich nicht wieder bestehen. Doch das Wissen um die Methodik des Hackens bleibt erhalten. ☒



Geschützte Privatsphäre

Eine Menge Leute interessieren sich für Ihre Daten. Mit unseren Tipps surfen Sie anonym im Netz und riegeln Ihren Browser vor den Blicken Neugieriger ab.

Von **Tobias Weidemann**

Was Sie in einem Online-Casino tun oder in einer Tauschbörse zu suchen haben, geht niemanden etwas an. Doch jeder hinterlässt Spuren im Internet – immer und überall – in Form seiner IP-Adresse oder durch Cookies und andere Daten, die sich von findigen Routinen auslesen und weiterverarbeiten lassen. Ihre Privatsphäre ist noch mehr in Gefahr: Im Hinblick auf die Terrorbekämpfung hat die Europäische Union eine neue Richtlinie zur „Vorratsdatenspeicherung“ von Telefon- und Internet-Zugriffen verabschiedet. Wenn sie auch in Deutschland umgesetzt wird, müssen die Provider Daten über ihre Kunden erheben

und monatelang aufbewahren – auch ohne konkreten Verdacht. Die Behörden können dann herausfinden, wer wann welche Seite besucht hat, welche Daten er hoch- oder heruntergeladen hat und an welchem Chat er teilgenommen hat.

Die EU-Richtlinie ist heftig umstritten – einige Mitgliedsstaaten haben bereits Klage dagegen eingereicht. In Deutschland haben Gerichte erst vor einigen Monaten entschieden, dass das Speichern von IP-Daten seitens der Provider nicht nur nicht erforderlich ist, sondern gegen geltende Gesetze verstößt, da es das Recht auf Privatsphäre in unverhältnismäßiger Weise verletzt.

Terroristen und organisierte Kriminalität werden neue Gesetze wohl wenig stören: Sie haben mit Sicherheit seit langem entsprechende Vorkehrungen getroffen, um möglichst nicht ins Netz der Fahnder zu geraten. Hauptsächlich betroffen ist der Bürger, dessen Privatsphäre leidet.

Wehren Sie sich dagegen, zum gläsernen Anwender zu werden: Mit einigen wirkungsvollen Tricks verhindern Sie, dass Sie mehr Daten preisgeben als unbedingt nötig. Wir zeigen, wie Sie ungestört surfen, Dateien mit Freunden tauschen oder legal Tauschbörsen nutzen. Außerdem erfahren Sie, wie Sie Ihren Browser so absichern, dass niemand von außen spionieren oder Einstellungen an Ihrem PC verändern kann.

Gratis-Proxy-Server: Nicht immer zuverlässig

Die einfachste Methode, um unerkannt zu surfen, ist ein Proxy-Server, sprich: eine Umleitung. Damit sieht der Betreiber eines Web-Angebots nicht, welche IP-Adresse Sie aktuell haben, von welcher Website Sie kommen, welchen Browser und welches Betriebssystem Sie verwenden.

Es gibt eine Menge Proxy-Anbieter – eine Liste finden Sie etwa unter www.multiproxy.org –, aber nicht alle sind vertrauenswürdig. Gerade bei Diensten aus dem Ausland können Sie nicht sicher sein, dass der Anbieter nicht seinerseits Ihr Surfverhalten protokolliert und auswertet.

Übrigens können Sie auch selbst auf die Suche nach (zum Teil undokumentierten) Proxy-Servern gehen. Machen Sie's doch einfach wie viele Suchmaschinen, die nach Proxy-Servern fahnden. Geben Sie bei Google einige der folgenden Schlüsselbegriffe ein: „Include Form“ „Remove Scripts“ „Accept Cookies“ „Show Images“ „Show Referer“ „Rotate13“ „Base64“ „Strip Meta“ „Strip Title“ „Session Cookies“. Dabei handelt es sich um typische Schlüsselbegriffe, die in fast allen Proxy-Servern auf PHP- oder CGI-Basis enthalten sind, sofern diese nicht stark verändert wurden. Je mehr der Begriffe Sie eingeben, desto besser wird Ihre Trefferliste ausfallen.

JAP: Vertrauenswürdiger Proxy-Dienst

Auch kostenlos, aber sicherer ist eine Technologie wie JAP. Hier legen die Anbieter den gesamten Quellcode und das verwendete

Tunneling-Verfahren offen. **JAP** (Java Anonymous Proxy, auf  CD) ist ein Projekt der Universitäten Regensburg und Dresden. Dabei surfen mehrere Anwender über dieselbe IP-Adresse, leiten den Datenverkehr aber automatisch über so genannte Mixkaskaden um – das heißt: über eine Vielzahl von zusammengeschalteten Zwischenstationen. Niemand, nicht einmal der Betreiber des JAP-Netzwerks, kann im Gewirr der Verbindungen nachvollziehen, wo Daten herkommen und für wen sie bestimmt sind. Jede Zwischenstelle leitet die Daten zur nächsten weiter, erfährt aber nicht, wo sich das eigentliche Ziel befindet. Nur wenn ein Nutzer Zugriff auf die Daten sämtlicher Verbindungen hätte, ließe sich verfolgen, welche Pakete für wen bestimmt sind – das ist aber schlicht unmöglich. Zudem müssen die Betreiber der Mixkaskaden – Hochschulen und andere große Rechenzentren – dem JAP-Betreiber garantieren, dass sie Daten weder protokollieren noch austauschen.

Tor: Je mehr Teilnehmer, desto sicherer

Wie JAP ist auch **Tor** (auf  CD) ein Open-Source-Projekt und befindet sich ebenfalls noch im Entwicklungsstadium. Tor (kurz für „The Onion Router“) ist ein Netzwerk, das sich ebenfalls den Schutz vor der Überwachung des Datenverkehrs auf die Fahnen geschrieben hat. Verbindungen werden über ein Netz verteilter Server, der Onion-Router, umgeleitet. Dadurch wird der Datenverkehr deutlich schwerer abhörbar. Anders als bei JAP, wo es einige Server gibt, die die Mixkaskaden betreiben, wird hier jeder Anwender selbst zum Teil des Netzwerks. Das stellt sicher, dass auch theoretisch niemand

Zugriff auf sämtliche Teile des Netzwerks haben kann. Je mehr Teilnehmer es hat, desto sicherer wird es. Schon deswegen lohnt es sich, Tor regelmäßig einzuschalten. Sollte jemand Ihre Internet-Leitung für kriminelle Zwecke missbrauchen, besteht keine Gefahr, dass die Behörden die Aktion zu Ihnen zurückverfolgen – denn das Routing und der eigentliche Datenverkehr erfolgen unabhängig voneinander. Selbst wenn ein Angreifer ein Datenpaket ausspionieren würde, hätte er nichts von dieser Information, denn jede Anfrage wird über eine andere Rechnerkombination umgeleitet. Übrigens können Sie JAP und Tor auch kombinieren und erreichen so einen noch höheren Schutz Ihrer Privatsphäre. Die Methode frisst allerdings eine Menge Ressourcen. Probieren Sie aus, ob Ihre Internet-Leitung und Ihr PC sich dafür eignen – pauschale Systemvoraussetzungen gibt's nicht.

Steganos VPN: Anonym surfen und Daten saugen

Eine sehr professionelle und elegante Lösung, um unerkannt im Internet unterwegs zu sein, ist **Steganos Internet Anonym VPN**. Dabei handelt es sich um ein Tool für Windows 2000 und XP, das einen anonymen VPN-Tunnel (Virtuelles Privates Netzwerk) erzeugt. Es ist denkbar einfach zu bedienen. Sie können damit nicht nur wie mit Tor anonym surfen, sondern auch diverse andere Dienste nutzen, etwa Filesharing. Die Verschlüsselung erfolgt dabei mit 128 Bit und ist hinreichend sicher.

Anonymität für unterwegs: Ihr ganzes Können spielt die Steganos-Software im Internet-Café oder im öffentlichen Hot Spot per WLAN aus. Wer etwa seine Arbeit im Inter-

Überblick Sicher surfen

Inhalt	Seite
Gratis-Proxy: Nicht immer zuverlässig	94
JAP: Vertrauenswürdiger Proxy-Dienst	94
Tor: Je mehr Teilnehmer, desto sicherer	95
Steganos VPN: Anonym surfen und saugen	95
Combots: Daten tauschen unter Freunden	96
Virtueller PC: Surfen ohne Sorge	96
Browser abriegeln: So geht's	97
Kasten	
Die Tools im Überblick	95

net-Café verrichtet, kann nicht sicher sein, dass der Betreiber die Daten nicht protokolliert und für unlautere Zwecke nutzt.

Die einzige Instanz, die bei Internet Anonym VPN Ihre Aktivitäten mitprotokollieren könnte, ist theoretisch Steganos. Die Firma erklärt aber, dass sie den Datenverkehr nicht überwacht. Man kann davon ausgehen, dass das stimmt – schließlich ist der Schutz vor Überwachung das wichtigste Verkaufsargument dieser Software. Eigentlich bezahlt man bei Steganos Internet Anonym VPN nicht primär für die Nutzung der Software, sondern auch für das übertragene Datenvolumen, das – ebenso wie das Bereitstellen und Unterhalten der Server – Kosten für Steganos verursacht. Eine Monatslizenz einschließlich 25 GB Datenvolumen bekommen Sie für 11,95 Euro, eine entsprechende Jahreslizenz für 79,95 Euro. Für echte Powersauser gibt es Internet Anonym VPN Flatrate 12 Monate mit unbegrenzt Traffic zum Preis von 299,95 Euro für ein Jahr.

Internet mit Sicherheit: Die Tools im Überblick

Produkt	Funktion	Preis	Win-Betriebssysteme	Internet (Download)	Sprache	Seite
Combots Beta	verschlüsselter Dateitransfer	ab 1,99 Euro ¹⁾	XP	www.combots.de (3,03 MB)	deutsch	96
 JAP 00.07.018	anonymes Surfen	gratis	95/98/ME, NT 4, XP, Vista	http://anon.inf.tu-dresden.de (12,1 MB)	deutsch	94
Leecher Mods Pack 3	Tuning für Filesharing-Tools	gratis	95/98/ME, NT 4, 2000, XP	www.00de.de (14,1 MB)	englisch	–
 MS Virtual PC 2007	virtuelles System	gratis	2000, XP, Vista	www.microsoft.com (30,4 MB)	deutsch	96
Steganos Internet Anonym VPN	Internet-Tunnel	ab 11,95 Euro ¹⁾	2000, XP, Vista	www.steganos.de (keine Testversion verfügbar)	deutsch	95
 Tor 0.1.1.26	anonymes Surfen	gratis	95/98/ME, NT 4, 2000, XP	http://tor.eff.org (4,60 MB)	englisch	95
VM-Ware Player 1.03	virtuelles System	gratis	2000, XP	www.vmware.com (30 MB)	englisch	96

 auf CD und unter www.pcwelt.de ¹⁾ pro Monat, siehe Text



Praktisch auch fürs Arbeiten und Mailen unterwegs: Wer an öffentlichen Hot Spots surft, sichert mit Steganos Internet anonym VPN seine Privatsphäre

Steganos VPN antesten: Sie müssen nicht die Katze im Sack kaufen. Wenn Sie sich entscheiden, die Software von der Homepage des Herstellers herunterzuladen, und dort Ihre Mailadresse angeben, bekommen Sie nicht nur den Download-Link. Es gibt einen Probe-Account für drei Tage – begrenzt auf ein Datenvolumen von 100 MB. Damit können Sie testen, wie schnell der Dienst beim Surfen funktioniert. Die Geschwindigkeit beim Transfer größerer Dateien, etwa über Tauschbörsen, lässt sich allerdings nur unzureichend ermitteln.

Achtung: Während der Installation schlägt Windows Alarm und warnt Sie vor dem Tool, weil es nicht zertifiziert sei. Diesen Hinweis können Sie allerdings getrost ignorieren. Nach der Installation können Sie die Software einfach über das Windows-Startmenü aufrufen, die Seriennummer eintragen und jederzeit mit „Verbinden“ oder „Trennen“ zur anonymen Leitung wechseln.

Combots: Daten tauschen unter Freunden

Ein Produkt, das in den vergangenen Wochen für einiges Aufsehen gesorgt hat, ist die Kommunikations-Software **Combots** (www.combots.de). Ihr Anbieter Combots AG ist aus der Web.de-Gruppe hervorgegangen. Das Besondere an dem Programm ist der hohe Grad an Privatsphäre. Das datenbankgestützte System ermöglicht den verschlüsselten Austausch von Dateien nahezu beliebiger Größe – und das werbefrei und ohne Spyware. Die Daten werden über eine getunnelte Verbindung auf den Server ko-

piert. Ist der Empfänger nicht online, wird er beim nächsten Login automatisch darüber informiert, dass Dateien vorliegen. Anders als bei einer Tauschbörse kommunizieren Sie mit einem eingeschränkten Personenkreis, der nur über gegenseitige Einladungen erweitert werden kann – Spam ist also ausgeschlossen. Combots ist einfach zu installieren und zu bedienen. Anwender sollten sich übrigens nicht von der etwas verspielten Optik des Dienstes mit animierten Figuren für jeden Kommunikationspartner abschrecken lassen – sie soll eine junge Zielgruppe ansprechen.

Probetrieb mit Limit: Combots ist noch im Betastadium. Mit dieser Version lassen sich allerdings maximal 200 MB pro Datei verschieben, größere Dateien müssen Sie splitten. Dazu kann ein beliebiger Packer wie WinRar oder WinZip dienen.

Niemand liest mit: Außer dem Dienstbetreiber Combots kann niemand nachvollziehen, welche Daten tatsächlich über die Leitung geflossen sind. Pressesprecher Oliver Schwartz erklärt dazu: „Wir haben kein Interesse daran, unsere Kunden zu bespitzeln. So lange der Gesetzgeber das nicht explizit vorschreibt, werden wir daher auch nichts unternehmen, was das Recht der Kunden auf Privatsphäre beschneidet.“

Das Tool läuft unter Windows XP und kostet – je nach Vertragslaufzeit – monatlich zwischen 1,99 und 2,99 Euro. Das Konzept nennt sich allerdings Friendly-Ware. Das bedeutet, dass Sie nur bezahlen müssen, wenn Sie möchten. Combots stellt allerdings in Aussicht, dass bei hoher Systemauslas-

tung die zahlenden Kunden bei der Auslieferung der Daten bevorzugt werden.

Combots läuft noch nicht in allen Details reibungslos, Daher haben wir auch keine Version der Software auf CD. Laden Sie sich die aktuelle Version von der Website des Herstellers herunter – Sie müssen sich dort ohnehin für den Service anmelden.

Virtueller PC: Sicher surfen ohne Rücksicht auf Verluste

Wenn Sie sich mal so richtig auf zweifelhaften Websites austoben wollen, diese aber auf Ihrem Rechner keinen Schaden anrichten sollen, nutzen Sie doch einfach einen virtuellen PC. Er bildet ein komplettes System innerhalb eines Fensters oder als Vollbild nach. Sie starten ihn zusätzlich zu Ihrer bestehenden Installation. Dabei wird nicht unbedingt die Konfiguration und Hardware Ihres Rechners emuliert, sondern Sie können festlegen, wie viele Platten welcher Größe es gibt, ob etwa eine Netzwerkkarte, ein CD- oder eine DVD-Laufwerk integriert ist.

Wie das mit dem **VM-Ware Player** geht, haben wir Ihnen unter anderem in den Artikeln „Exklusiv: Ihr Zweit-PC jetzt zum Nulltarif“ (PC-WELT 1/2006, S. 56–62) und „Gratis zur Vollversion“ (PC-WELT 2/2006, S. 104–106) gezeigt, beide auf CD. Mit dem kostenlosen **VM-Ware Converter 3** (www.vmware.com/products/converter) sichern Sie komplette Windows-Rechner als virtuelle Maschine (VM), sogar über eine Remote-Verbindung im Netzwerk. Außerdem lassen sich virtuelle Maschinen von Microsoft Virtual PC und Virtual Server in das VM-Ware-Maschinenformat konvertieren. Ein Assistent begleitet bei der Auswahl von Quelle und Zielformat der VM.

Kostenloses Microsoft-Tool: Seit Jahren gibt es neben VM-Ware ein Tool, das Ähnliches kann – und zwar von Microsoft. **MS Virtual PC 2007** (auf CD) kostete in früheren Versionen rund 150 Euro – seit Ende Juli 2006 gibt's die 2004er-Version der Software aber gratis. Nach dem Erscheinen von Windows Vista hat Microsoft Anfang des Jahres die Version 2007 nachgelegt, die ebenfalls kostenlos ist.

Virtual PC 2007 läuft unter Windows 2000 SP 4, Windows XP SP 2, Windows Server 2003 und Windows Vista. Empfohlen werden eine CPU mit mindestens 1 GHz und ausreichend Plattenplatz. Die von Microsoft angebotene Gratisversion ist komplett in

deutscher Sprache. So lassen sich unter den genannten Betriebssystemen virtuelle Systeme mit MS-DOS 6.22, Windows 95/98/ME, NT 4, 2000, XP und Vista sowie OS/2 installieren. Auch Linux und andere x86-Betriebssysteme sind möglich – werden allerdings nicht offiziell unterstützt.

Virtuelles System einrichten: Beim ersten Start begrüßt Virtual PC Sie durch einen Assistenten, mit dessen Hilfe sich ein beliebiges neues System zusammenstellen lässt. Wahlweise können Sie auch eine vorgegebene Variante erstellen lassen – das geht schneller und eignet sich gerade für Einsteiger. Im nächsten Schritt geben Sie an, welches Betriebssystem Sie wünschen und wie viel Arbeitsspeicher Sie dem virtuellen PC zugestehen wollen. Außerdem müssen Sie dem System eine virtuelle Festplatte zuweisen. Falls Sie schon ein virtuelles System mit Virtual PC eingerichtet haben, können Sie dessen VHD-Datei auch für das neue nutzen. Danach booten Sie mit dem Originaldatenträger, um die Installation wie gewohnt durchzuführen.

Beachten Sie, dass Sie mit einem solchen System nicht unsichtbar sind – von außen ist nicht zu erkennen, ob Sie ein reales oder ein virtuelles System nutzen. Sie können aber zum einen das System auf Mausklick in den Ursprungszustand zurücksetzen, wenn es mit Software zugemüllt oder verändert wurde. Zum anderen können Sie so viele Kopien eines Systems erstellen, wie Sie benötigen. Damit lässt sich auch besser beurteilen, was eine Website auf Ihrem PC anrichtet.

Browser abriegeln: Sicherheitsvorkehrungen

Eine immer noch gern unterschätzte Gefahr für den Anwender sind aktive Inhalte wie Javascript-, Java- oder Active-X-Elemente. Zwar vereinfachen diese oftmals das Leben – viele Dienste auf Websites basieren darauf –, andererseits kann es aber ein Risiko sein, solche Services zu nutzen. Schließlich kann man auf diesem Weg alle möglichen Daten über Ihren Rechner auslesen und auf Ihrer Festplatte recherchieren. Beispielsweise können Firmen Ihr Surfverhalten ausspionieren und ihre Angebotsseiten so anpassen, dass Sie wahrscheinlich bestimmte weitere Seiten aufrufen. Das ist in der Regel nicht gefährlich, jedoch ein Eingriff in Ihre Privatsphäre, den Sie nicht dulden müssen. Außerdem lassen sich Einstel-



Beliebiges System: Mit Virtual PC surfen Sie in der Quarantäne-Zone. Welches Betriebssystem Sie installieren, bleibt Ihnen überlassen

lungen im System verändern, Ihre Startseite im Browser umstellen oder Ihre Lesezeichenliste um bestimmte Links erweitern. Sie tun daher gut daran, wenn Sie derartige Sicherheitsrisiken gar nicht auf Ihren Rechner lassen – das klappt mit Hilfe des Browsers.

So sichern Sie den IE ab: Im Internet Explorer 7 rufen Sie „Extras, Internetoptionen“ auf und wechseln zum Register „Sicherheit“. Klicken Sie hier auf „Stufe anpassen“ und deaktivieren Sie Active-X-Steuerelemente (die ersten drei Stellen). Wenn Sie auf die praktischen Steuerelemente nicht gänzlich verzichten möchten, wählen Sie den Punkt „Eingabeaufforderung“, so dass Sie jedes Mal gefragt werden und individuell entscheiden können. Den Download von unsignierten Active-X-Elementen sollten Sie immer unterbinden. Ähnlich sollten Sie bei Javascript und Jscript (der Microsoft-Variante von Javascript) sowie VBS (Visual Basic Script) vorgehen. Diese lassen sich gesammelt im gleichen Fenster unter „Scripting, Active Scripting“ einstellen – auch hier können Sie generell erlauben oder verbieten oder jedes Mal auf Nachfrage entscheiden. Im letzten Schritt regeln Sie noch im gleichen Fenster und nach demselben Schema den Umgang mit Java-Applets („Scripting von Java-Applets“). Zusätzlich lassen sich

unter dem Punkt „Sicherheit“ „Vertrauenswürdige Sites“ definieren, denen Sie weitergehende Rechte einräumen, sowie „Eingeschränkte Sites“, denen Sie aus irgend einem Grund misstrauen.

So geht's bei Firefox: Für Firefox gilt im Prinzip dasselbe – hier gehen Sie auf „Extras, Einstellungen“. Unter „Inhalt“ deaktivieren Sie Java und Javascript, indem Sie die entsprechenden Häkchen entfernen. Bei „Erweitert“ lässt sich für Javascript auch individuell festlegen, welche Aktionen hier erlaubt sein sollen.

In einem Punkt sind Sie übrigens mit Firefox besser aufgehoben. Der Browser unterstützt von Haus aus kein Active X – und das soll nach den Worten von Mozilla-Präsident Tristan Nitot auch so bleiben. „Active X ist aus unserer Sicht ein großes Sicherheitsrisiko, das wir dem Anwender auch in Version 2.0 nicht zumuten wollen“, erklärte der Mozilla-Chef gegenüber der PC-WELT. In der Tat reichen die Steuerungsmöglichkeiten durch Active-X-Elemente deutlich weiter als bei anderen Technologien. Hier lassen sich beliebige Routinen und Programme innerhalb des Browsers ausführen – der Anwender bemerkt das oft erst, wenn es zu spät ist. Firefox unterstützt auch in der aktuellen Version 2.0.3 kein Active X. ❌



Die Abzocker-Mafia im Web

Geschenke, Schnäppchen, tolles Einkommen ... wenn ein Angebot klasse klingt, müssen Sie auf der Hut sein. Wir sagen, wann Sie misstrauisch sein sollten und Abzocker entlarven.

Von **Tobias Weidemann**

Eigentlich klang alles ganz einfach: „Daten eingeben, registrieren, DVD abstauben“ stand unter www.dvden.de. Sascha R. zögerte nicht lange, trug seine Daten ein und freute sich auf die DVD. Abgebildet waren drei Titel aus den aktuellen DVD-Charts – darunter stand klein „Sie erhalten eine zufällige DVD bei erfolgreicher Anmeldung kostenlos“. Was Sascha R. nicht klar war und was er auch nur versteckt in den seitenlangen „Allgemeinen Geschäftsbedingungen“ hätte nachlesen können: Er hatte ein Abonnement auf DVDs abgeschlossen, das ihn monatlich 9 Euro kosten sollte. Dafür sollte er künftig einmal pro Quartal eine DVD nach Wahl des Diensteanbieters „nach

dem Zufallsprinzip“ erhalten. 27 Euro für eine DVD – das ist alles andere als preiswert. Aktuelle DVDs sind in der Regel für rund 20 Euro im Handel erhältlich – und der Kunde kann entscheiden, welchen Film er kauft. Der Dienst ist ein typisches Beispiel für Abzocke im Internet: Ein Angebot wirkt einfach, günstig, ohne Risiko – und es hat einen Pferdefuß, der erst bei näherem Hinsehen deutlich wird. In vielen Fällen geht's um einen Monatsbeitrag von wenigen Euro. Wegen einer solchen Summe werden die meisten nicht gleich vor Gericht ziehen, sondern die Ausgabe als Lehrgeld verbuchen. Und genau deshalb können die Abzocker nahezu ungestört weiter Websurfer hereinlegen.

Interessanterweise trifft es nicht nur arglose unerfahrene Anwender, die über wenig Internet-Praxis verfügen, sondern auch alte Hasen, die zu unvorsichtig sind. Wer schon zu viele AGB- und sonstige Infokästen gesehen hat, überfliegt diese ellenlangen Texte oft nicht mal mehr, sondern lässt die nervigen Dinger mit einem entschlossenen Klick auf „OK“ verschwinden. Und natürlich spielt den Anwendern nicht selten die Gier einen Streich – wer möchte nicht gern etwas kostenlos oder billiger bekommen?

So manches Angebot macht schon deshalb nicht misstrauisch, weil bekannte, seriöse Firmen oft auf ganz ähnlich scheinende Weise arbeiten. Da vergisst man schnell mal, dass sich nicht jeder an die Spielregeln hält. Der eine macht sich nur die Bequemlichkeit oder Nachlässigkeit der Kunden zunutze, andere tarnen wichtige Informationen so gut, dass die meisten Leute viel zu spät merken, worauf sie sich eingelassen haben – und am Ende des Spektrums finden sich kriminelle Methoden. Wir informieren Sie über ganz verschiedene Taktiken, mit denen die Leute im Web um ihr Geld erleichtert werden. Ausgeklammert haben wir in diesem Zusammenhang Tricks, die auf rein technischer Basis funktionieren, etwa Phishing.

1. Der Warenproben-Trick

Das Angebot: Sie heißen Produktclub, Probenzauber, Probenking, Probenbutler oder ähnlich – und haben alle dasselbe Konzept. „Wir tragen Ihre Adresse in eine Vielzahl von Websites ein, die Werbeproben verschicken, und Sie erhalten jeden Monat wertvolle Pakete mit Werbeproben oder -geschenken“ – so oder so ähnlich lauten die Versprechen der meisten Werbeproben-Sites. Oft wird auch gleich vorgerechnet, dass Sie mit Geschenken im Wert von meh-

Darum geht's: Abzocke im Web

Im Internet gibt es neben zahlreichen wirklichen Schnäppchen auch eine Vielzahl von nur scheinbar attraktiven, von unseriösen und rechtlich oder moralisch fragwürdigen Angeboten. Wir sagen, wo Sie aufpassen sollten – und was Sie tun können, wenn Sie einem Abzocker aufgesessen sind.

rerer hundert Euro rechnen können. Teilweise sind Gutscheine zu sehen, die Ihnen traumhafte Einsparmöglichkeiten vorgaukeln (etwa bei www.tricky.at, das sich auch an deutsche Anwender richtet). Damit Sie an diese Segnungen kommen, müssen Sie eine Mitgliedsgebühr bezahlen.

Das steckt dahinter: Egal, wie die Unternehmen sich nennen – uns ist kein System bekannt, bei dem Anwender wirklich in dem Maß Warenproben erhalten, wie sie es nach den Versprechungen auf der Site erwarten können. In einigen Fällen gibt's anstelle von Geschenken Werbung oder Rabattmarken im Briefkasten. Bei einigen der Sites ist nur in den AGB zu lesen, dass für die Mitgliedschaft eine Jahresgebühr verlangt wird. So bekommen viele der Teilnehmer das überhaupt erst nach Ablauf der 14-tägigen Rücktrittsfrist mit, wenn die Rechnung ins Haus flattert. Und die ist oft ganz schön hoch. Etliche Kunden zahlen nicht, weil sie sich übers Ohr gehauen fühlen – also kommen die ersten Mahnungen. In vielen Fällen binden sich Anwender sogar für zwei Jahre, wenn sie den Vertrag abschließen. Ob bei diesen Angeboten tatsächlich ein Vertrag zustande kommt, ist unklar. Um die Ansprüche einer Probchen-Site abzuwehren, müsste der Kunde vor Gericht beweisen, dass er über die genauen Vertragsmodalitäten im Unklaren gelassen wurde. Dazu ist es nötig, sich genau anzusehen, wie die Informati-

onen auf der Site im Einzelfall präsentiert werden. Schwierig ist es auch, Ansprüche gegen die Betreiber der Sites geltend zu machen. In der Regel steht in den Geschäftsbedingungen nämlich nicht, dass der Kunde eine bestimmte Zahl an Warenproben bekommt, sondern nur, dass er in eine bestimmte Zahl an Verteilern eingetragen wird. Ob etwa dann die Firmen, die die Warenproben verschicken, solche Masseneintragungen gleich herausfiltern, lässt sich nicht feststellen. Außerdem kann man kaum nachprüfen, ob die Betreiber der Proben-Sites ihre Kunden überhaupt anmelden.

2. Der Warentester-Trick

Das Angebot: Ähnlich funktioniert die Masche mit Warentests. Angeblich suchen viele Hersteller händierend nach Testkunden, die kostenlos neue Autos fahren oder teure Hardware testen wollen – und das, obwohl diese die Ware am Ende behalten dürfen oder sehr günstig erwerben können. Auch an Unterhaltungselektronik und andere hochwertige Geräte soll man auf diesem Weg kommen können. „Für unsere Produktanalysen sind wir auf die Mithilfe von Verbrauchern aus den unterschiedlichsten Einkommens-, Bildungs- und Familienverhältnissen angewiesen. Nur so schaffen wir es, die getesteten Produkte und Dienstleistungen durch einen repräsentativen Bevölkerungsschnitt bewerten zu lassen“, schreibt

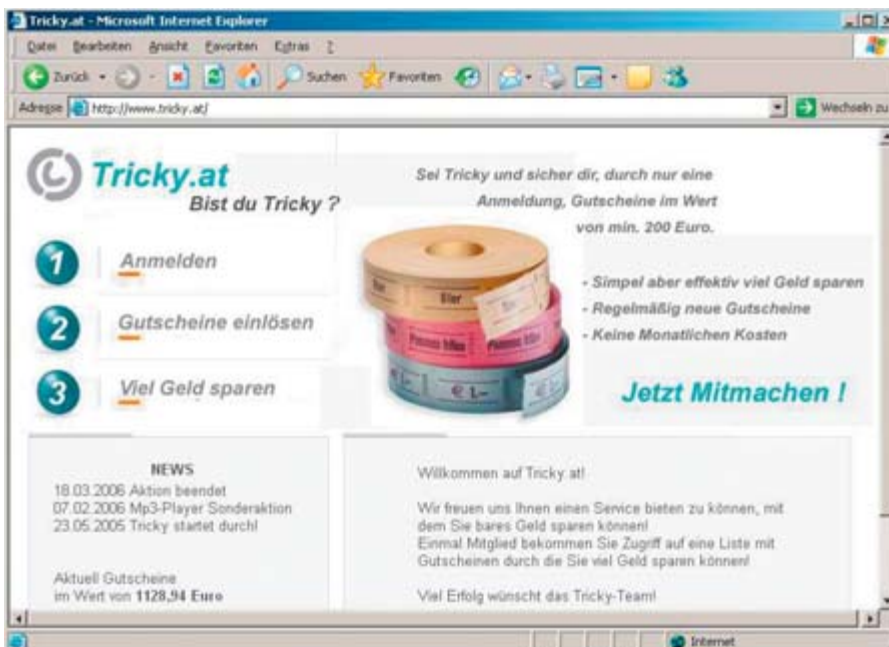
Überblick Abzocke im Web

Inhalt	Seite
1. Der Warenproben-Trick	98
2. Der Warentester-Trick	99
3. Der Probe-Abo-Trick	100
4. Der Download-Probe-Abo-Trick	100
5. Der Free-SMS-Trick	101
6. Der Get-a-free-...-Trick	101
7. Der Billig-Software-Trick	103
8. Der Nebenjob-Trick	103
9. Der Nigeria-Connection-Trick	103
10. Der Ebay-Ringtausch-Trick	103
11. Der Ebay-Zoll-Trick	105
Fazit: Vorbeugen ist besser	105
Kästen	
Darum geht's: Abzocke im Internet	98
Internet-Kriminalität: Statistik	100
Ebay: Mehr Sicherheit	101

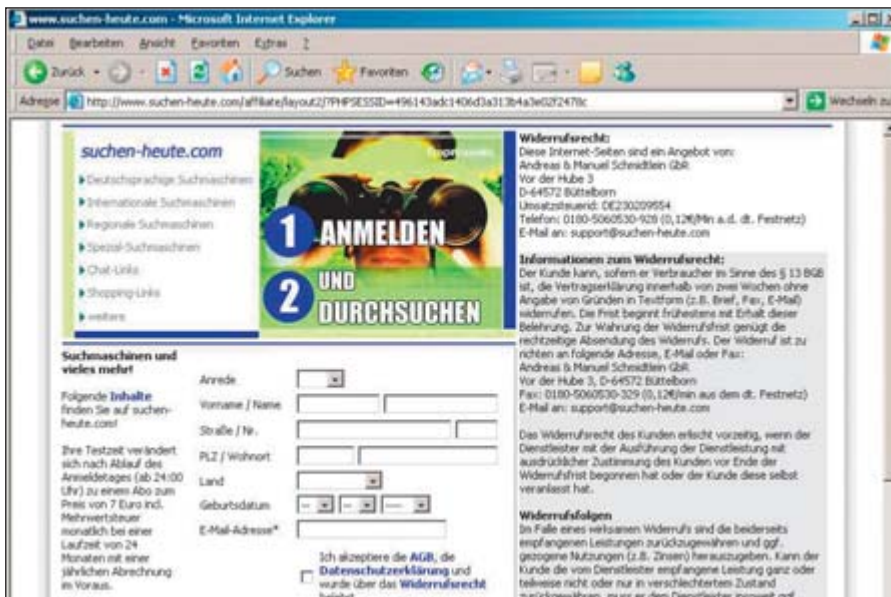
etwa das „Europäische Zentrum für Verbraucheranalysen“ (www.euceva.de) auf seiner überzeugend aussehenden Website. Man macht dem Anwender Hoffnung: „Vielleicht passen genau Sie in unser Profil!“

Das steckt dahinter: Auch hier gilt: In der Regel kostet ein solcher Vertrag nur Geld und bringt nichts ein. Mehrere Unternehmen, deren Produkte auf solchen Sites abgebildet waren, haben erklärt, dass sie für solche Angebote keine Testmuster zur Verfügung stellen.

Bei der Erstanmeldung auf der Website muss der Kunde zwar seine gesamten Adressdaten und seine Telefonnummer angeben, nicht aber eine Bankverbindung. Die erfragt etwa eine freundliche Euceva-Mitarbeiterin im persönlichen Telefongespräch zusammen mit den Kontodaten. Nun bekommt der Kunde eine schriftliche Bestätigung über den Vertrag, danach wird der Mitgliedsbeitrag abgebucht. Dieses Verfahren macht es dem Kunden schwerer, nachzuweisen, dass er über einige Feinheiten des Vertrags im Unklaren gelassen wurde. Für 7 Euro im Monat gibt's nun die Aussicht auf wertvolle Waren, wie auf der Website an mehreren Stellen versprochen wird. Auf diese Pakete darf er lange warten – viele Kunden berichten in Foren, dass sie keine



Katze im Sack: Gutscheine verspricht Tricky.at – doch für was für Gutscheine genau der Anwender 120 Euro zahlen soll, erfährt er vorher nicht (Trick 1)



Kein Grund für ein Abo: Fast alle Informationen auf den Heute-Sites der Schmidlein-Brüder bekommen Sie auch gratis im Internet (Trick 3)

Waresgeschenke erhalten haben, dafür aber Mailwerbung von zahlreichen Werbepartnern. Ganz schnell allerdings kommen in vielen Fällen Mahnschreiben, wenn der unzufriedene Kunde nicht bezahlt. In einigen Fällen melden sich auch Inkassounternehmen.

men. Der verhinderte Wartentester sollte deshalb frühzeitig und deutlich reagieren, indem er etwa der Rechtmäßigkeit der Forderung widerspricht und gegebenenfalls das Geld einer bereits erfolgten Abbuchung zurückholt. Die Inkassounternehmen dro-

hen in aller Regel mit hohen Gebühren und damit, der Gläubiger werde vor Gericht gehen. Allerdings ist fraglich, ob eine solche Firma an einem Rechtsstreit interessiert ist. Wir kennen keinen vergleichbaren Fall, in dem die Drohung, vor Gericht zu gehen, tatsächlich umgesetzt wurde.

3. Der Probe-Abo-Trick

Das Angebot: Einen Web-Service testen, von Club-Vorteilen profitieren oder DVDs ausleihen, sprich: zur Probe für eine Weile Vorteile nutzen, die nicht jeder hat – und das gratis. Da sagt man schnell mal ja – abmelden kann man sich schließlich vor Ende des Testzeitraums.

Das steckt dahinter: Das Angebot einer kurzfristig kostenlosen Mitgliedschaft ist oft blankes Kalkül. Leicht vergisst der Kunde, rechtzeitig zu kündigen. Und besonders ärgerlich: Er hat es oft schwer, zu beweisen, dass er korrekt gekündigt hat.

Ein Unternehmen, das in den vergangenen Monaten einige Schlagzeilen gemacht und die Verbraucherschützer auf den Plan gerufen hat, ist die Firma Andreas & Manuel Schmidlein GbR aus Büttelborn. Sie bietet eine Reihe von Sites mit Informationen zu verschiedenen Themen an, etwa www.hausaufgaben-heute.com, www.lehrstellen-heute.com, www.fabrikverkauf-heute.com oder www.suchen-heute.com. Alle Sites haben eins gemeinsam: Die Informationen, die dort zu finden sind, gibt's problemlos auch auf kostenlosen Websites. Außerdem verpflichtet der Anwender sich mit seiner Anmeldung zu einem zweijährigen Abo mit einer monatlichen Grundgebühr von 7 Euro, sofern er nicht bis 24 Uhr am selben Tag seinen Test-Account kündigt oder innerhalb der nächsten zwei Wochen von seinem Widerrufsrecht Gebrauch macht. Bei jedem Gratistest-Angebot sollte man die AGB sorgfältig lesen. Damit ein gültiger Vertrag zustande kommt, müssen die Spielregeln klar auf der Site zu finden sein – im Fall der Schmidlein-Websites war das nicht immer der Fall.

4. Der Probe-Download-Trick

Das Angebot: Anonym im Usenet alles herunterladen, was das Herz begehrt – und das erst mal gratis. Das bieten zum Beispiel Centurionet (www.centurionet.com) oder Firstload (www.firstload.de) an. Lange Zahlenkolonnen auf der Startseite sollen zeigen, wie viele hunderttausend Filme, Musikstü-

Internet-Kriminalität: Das sagt die Statistik

Statistiken zur Kriminalität rund ums Internet zu bekommen, ist schwierig. Nur zehn Bundesländer weisen diese Delikte überhaupt detailliert aus, in den anderen Bundesländern verschwinden sie in den Zahlen über andere Straftaten.

Interessant: Jeder zweite zur Anzeige gebrachte Fall in Zusammenhang mit Warenbetrug hat das Tatmittel Internet. Die gute Nachricht: Je nach Tatbestand liegt die Aufklärungsquote bei Internet-Betrugsdelikten bei bis zu 94 Prozent. „Die Täter hinterlassen einfach zu viele Spuren“, erklärt ein Polizeisprecher. Insgesamt werden 83,5 Prozent der angezeigten Web-Betrügereien durch die Behörden aufgeklärt (Stand 2004). Es ist also durchaus sinnvoll, im Betrugsfall Anzeige zu erstatten – vor allem, wenn der Gegner in Deutschland oder in der EU sitzt.



1) Ware kommt abhanden, wird nicht ausgeliefert 2) Es wird nicht gezahlt oder Geld unterschlagen



Volles Programm: Centurionet möchte besser sein als Bit Torrent und Co. (Trick 4)

cke, Bilder und Programme quasi auf Abruf für den Anwender bereitstehen.

Das steckt dahinter: Auch hier gibt's Test-Accounts. Viele Anwender berichten in Foren davon, dass die Kündigung während des Testzeitraums ignoriert und das Geld für die Mitgliedsgebühr eingefordert wurde. Der Unterschied zu anderen Probe-Abos: Die Unternehmen haben ein Druckmittel mehr, um an ihr Geld zu kommen. Denn die Anwender fürchten, dass bei einer Klage vom Gericht überprüft würde, was man mit einem solchen Download-Dienst anstellt – und da bleiben im Regelfall nur wenige Anwendungen, die nicht mit dem Urheberrecht in Konflikt kommen.

Allerdings wissen auch die Anbieter solcher Dienste, dass ihre Werbung klar eine bestimmte Zielgruppe adressiert und ihr Geschäftsmodell ebenso angreifbar ist wie dessen Nutzung. Sie dürften daher kein Interesse an vor Gericht ausgetragenen Vertragsstreitigkeiten haben. Falls Sie korrekt und rechtzeitig gekündigt haben, sollten Sie das belegen, falls nicht, müssten Sie nachweisen, dass Sie sich bei Abschluss des Vertrags nicht über die Auswirkungen Ihrer Anmeldung im Klaren sein konnten. Laden Sie sich also etwa die AGB herunter.

5. Der Free-SMS-Trick

Das Angebot: Ein Klassiker. Sie bekommen etwas gratis – zum Beispiel einige SMS, die Sie übers Internet verschicken dürfen. Sie investieren nur etwas Zeit und gehen scheinbar kein Risiko ein. Ein Beispiel hierfür ist der Dienst www.1sms.de.

Das steckt dahinter: Wenn es nicht um ein Abo geht und Sie mit den paar kostenlosen SMS nur geködert werden sollen, geht es

wohl eher darum, an „qualifizierte Adressen“ zu kommen, also an Adressen im Paket mit weiteren Informationen, die man an Andere – etwa für Werbezwecke – verkaufen möchte. So werden Sie vielleicht noch gefragt, für welche Themen Sie sich interessieren, welches Auto Sie fahren oder wie alt Sie sind. All diese Daten sind für Firmen bares Geld wert. Genauer verraten hier oft die AGB und das übrige Kleingedruckte. Achten Sie darauf, ob Sie irgendwo der Weiterverwendung Ihrer Daten, etwa als Informationen für „Partner der Firma“ zustimmen, und deaktivieren Sie diesen Punkt nach Möglichkeit. Seriöse, bekannte Unternehmen werden Ihre Daten nicht ohne Ihre Zustimmung weitergeben, ansonsten ist aber äußerste Vorsicht angebracht.

6. Der Get-a-free-...-Trick

Das Angebot: Dienste wie www.freepay.com sind bislang vor allem in den USA bekannt, sie kommen aber auch in Europa in Mode. Die genannte Site leitet deutsche Besucher auf eine teils amüsant übersetzte deutsche Version um. Hier sollen Sie sich mit Ihren Adressdaten anmelden – Postfach-Adressen sind zumeist nicht erlaubt. Danach werden Sie mit Online-Werbung beliefert oder müssen an Umfragen teilnehmen. Nach der Anmeldung werden Sie aufgefordert, Mailadressen Ihrer Freunde, Bekannten und Kollegen anzugeben, denen Sie den Dienst empfehlen und ebenfalls die An-

meldung nahelegen. Wahlweise müssen sich diese auch über einen bestimmten Referrer-Link anmelden, den Sie bekommen. So sieht das System, dass der Kontakt über Sie erfolgt ist. Als Belohnung sollen Sie ein hochwertiges technisches Gerät erhalten, etwa ein Luxus-Handy oder einen MP3-Player. Voraussetzung: Eine bestimmte Zahl Ihrer Freunde und Kollegen meldet sich auf Ihre Werbung hin ebenfalls bei dem Dienst an und „erfüllt“ „ein Angebot“, wie es auf der Homepage heißt. Was das genau bedeutet, ändert sich immer wieder mal.

Das steckt dahinter: Den iPod oder das Notebook bekommen Sie in den meisten Fällen tatsächlich. Sie müssen sich das aber hart erarbeiten. Es geht wieder ums Datensammeln – in der Regel sogar ganz offen. Sie stimmen zu, kostenlose „Verbraucherinformationen“, sprich: Werbung, zu bekommen. Gleichzeitig rekrutieren Sie in einer Art Schneeballsystem weitere Interessenten für den Dienst. Nach einer festgelegten Zahl von Anmeldungen, die Sie generiert haben, bekommen Sie dann die versprochene Ware. Der Haken: Die Zahl der zuwerbenden Personen ist sehr hoch – die meisten Teilnehmer werden das wohl nicht erreichen. Das ganze System basiert auf einer Art Mischkalkulation, da der Betreiber des Dienstes auf diese Weise viele Adressen bekommt, ohne dass er dafür eine Prämie herausrücken muss. Dass einige Ihrer Freunde und Kollegen es wenig lustig finden könnten,

Ebay: Mehr Sicherheit

Auf Ebay wird viel geschimpft – der Umgang mit unzuverlässigen Bietern sei nachlässig, Support-Anfragen würden mit unpassenden Standard-Textbausteinen beantwortet, Power-Seller bevorzugt, sogar Förderung oder Duldung krimineller Aktivitäten werden dem Online-Auktionshaus immer wieder in Foren unterstellt. Sicher könnte Ebay an vielen Stellen mehr tun. Allerdings kann man auch den Veranstalter eines Flohmarkts nicht für sämtliche Waren der einzelnen Anbieter verantwortlich machen.

Ebay ist verständlicherweise daran interessiert, nicht in Verruf zu geraten. Denn durch Meldungen über Betrugsfälle bei Auktionen werden vor allem wenig erfahrene Anwender verschreckt. Diese trauen sich dann nicht, Waren zu ersteigern oder anzubieten, weil sie sich nicht sicher fühlen. Ebay hat daher nicht nur Sicherungen wie den Treuhänder-Service eingerichtet, sondern auch zusammen mit der Polizei eine Kampagne unter dem Motto „Online kaufen – mit Verstand“ gestartet. Ziel ist es, über die Website www.kaufenmitverstand.de Anwender zu informieren, wo die Fallstricke bei Ebay-Auktionen liegen und mit welchen Sicherheitsvorkehrungen man den meisten Problemen aus dem Weg gehen kann. Praktisch: Auf der Website finden sich „7 Goldene Regeln für den sicheren Online-Kauf“, die übrigens nicht nur für Ebay-Transaktionen hilfreich sind, sowie eine mit Bildern versehene Safety Card, ähnlich wie man sie aus dem Flugzeug kennt. Die finden Sie zum Ausdrucken als PDF auch auf CD.



wenn Sie deren Mailadresse irgendwo eintragen, ist ein weiterer Grund, von solchen Angeboten die Finger zu lassen.

7. Der Billig-Software-Trick

Das Angebot: Windows Vista für 50 Dollar, Auto CAD für 100 Dollar, Adobe Creative Suite CS3 Premium für 150 Dollar – und das alles legal dank besonderer Preiskalkulation und Großbestellungen. Wer würde da nicht auch ein Schnäppchen machen wollen? Neben Viagra-Spam und Phishing-Post gibt's zunehmend Mails, in denen Software in der OEM-Version – also ohne Support durch den Hersteller – für einen Bruchteil des regulären Preises angeboten wird.

Das steckt dahinter: Wer genau die Software verkauft, erfährt der Kunde entweder gar nicht, oder der Anbieter ist eine unbekannte Firma ohne Postadresse und Telefonnummer, allenfalls mit einer Mailadresse. In vielen Fällen muss der Kunde auch eine Zahlung per Vorkasse leisten oder seine Kreditkartendaten an ein Unternehmen im Ausland übermitteln, das er nicht kennt. Darauf einzugehen, ist sehr leichtsinnig. Wir haben nachgefragt, was es mit solchen Angeboten auf sich hat: „Typischerweise müsste der Kunde schon beim Preis bemerken, dass es hier nicht mit rechten Dingen zugehen kann“, erklärt Alexander Hopstein von Adobe. Der Anwender erwirbt hier in nahezu allen Fällen Raubkopien, die aber, das räumt der Pressesprecher ein, immer aufwendiger produziert werden. Im Fall von Adobe müsste man von vornherein misstrauisch sein: Nach Photoshop 6.0 gab es keine OEM-Versionen der teureren Adobe-Produkte mehr. Und ob Ihnen ein solcher Anbieter, von dem Sie nur die Mailadresse

Gratis-iPod oder -Notebook: Die meisten Anwender gehen leer aus, weil sie nicht genügend neue Adressen liefern. Auch ansonsten lohnt sich ein Blick in die (recht verworrenen und schlecht übersetzten) allgemeinen Geschäftsbedingungen des Anbieters (Trick 6)

und die Kontonummer kennen, wirklich die vorab bezahlte Software schickt, ist ohnehin sehr stark zu bezweifeln.

8. Der Nebenjob-Trick

Das Angebot: Besonders perfide machen sich manche Betrüger die schlechte Lage auf dem Arbeitsmarkt zunutze. Meist arbeiten sie per Mail, zunehmend auch per Kleinanzeige mit einem Internet-Link. Wer in einer Stellenbörse online einen Job sucht, zieht wohl ihre Angebote besonders an. Gesucht werden deutsche Mitarbeiter und „Repräsentanten“ für eine ausländische Firma, die etwa ein Konto unterhalten sollen, einige Zahlungen weiterleiten sollen oder ähnliches. Das Ganze könne problemlos von zu Hause aus erledigt werden. Klingt nach einer leichten Arbeit ohne Risiko.

Das steckt dahinter: Dieser Trick ist für die Betroffenen wirklich gefährlich. Sie erhalten etwa auf ein von Ihnen eingerichtetes Konto die erwarteten Summen. Nachdem Sie diese weitergeleitet haben – meist abzüglich einer zunächst großzügig erscheinenden Beteiligung für Ihre Arbeit, bekommen Sie Post von der Polizei oder Staatsanwaltschaft. Das auf Sie angemeldete Konto wurde für Geschäfte verwendet, bei denen der Käufer betrogen wurde. Dieser fordert nun sein Geld zurück. Eventuell müssen Sie den Geprellten deren Schaden ersetzen, in jedem Fall haben Sie Ärger. In anderen Fällen geht es um Geldwäsche. Dann könnten Sie sich sogar der Beihilfe schuldig machen.

9. Der Nigeria-Trick

Das Angebot: Sie bekommen Mails aus Afrika oder Osteuropa, in denen Ihnen beispielsweise vorggaukelt wird, jemand befände

sich in einer Notlage, und Sie könnten mit einer Überweisung, die Sie über Ihr Konto laufen lassen, helfen oder gar das Vermögen einer Familie, eines Dorfes oder einer unterdrückten Minderheit vor einem bösen Regime retten. Auch hier wird Ihnen ein beachtlicher Prozentsatz der Summe als Lohn für die Mühe versprochen.

Das steckt dahinter: Diese Strategie ist wohl eine der ältesten – es gibt sie mindestens seit 15 Jahren –, erst kamen Faxe und Briefe, jetzt Mails. Der Name entstand, weil die ersten dieser Betrugsversuche aus Nigeria kamen. Und so wild und unglaublich die Geschichten auch klingen, es gibt immer wieder Leute, die aus gutem Willen oder Geldgier auf so etwas hereinfallen. Zunächst versucht man, Ihr Vertrauen zu gewinnen. Dann werden Sie aufgefordert, eine geringe Gebühr für Überweisungs- oder Anwaltskosten zu überweisen – ein kleiner Betrag verglichen mit dem, was Sie später bekommen sollen. Nur so könne das Geschäft abgewickelt werden. In der Regel hören Sie dann nichts mehr von den Betrügern. Es gibt aber auch Fälle, in denen eine Zahlung nach der anderen gefordert wird. Je mehr ein Betrugsoffer investiert hat, desto schwerer wird es, das Geld verloren zu geben und sich einzugestehen, dass man reingelegt wurde. Hüten Sie sich übrigens davor, die Sache selbst vor Ort erledigen zu wollen. Im April 2002 flog ein Deutscher wegen einer solchen Geschichte nach Afrika. Er wurde entführt und erst gegen Lösegeld wieder freigelassen. Mehr zu diesem Thema finden Sie unter www.nigeria-connection.de.

10. Der Ebay-Ringtausch-Trick

Das Angebot: Es gibt eine Vielzahl von Abzock-Tricks rund um Ebay, die wir in den vergangenen Jahren immer wieder angeprangert haben. Besonders gefährlich ist dieser raffinierte Trick: Ein Anbieter aus dem Ausland verkauft etwa einen Computer, und bittet den Käufer, das Geld doch auf das Konto eines Freundes in Deutschland zu überweisen. Der Käufer willigt ein, schließlich spart er dadurch die hohen Kosten für eine Auslandsüberweisung.

Das steckt dahinter: Das kann ein kostspieliger Fehler sein. Die Sache geht in eine ähnliche Richtung wie Trick 8. In vielen Fällen gehört das Konto wiederum einem (nichts ahnenden) anderen Verkäufer, bei dem der Ebayer aus dem Ausland seiner-

seits Ware bestellt hat. Nachdem das Geld dort eingegangen ist, versendet der Verkäufer die gewünschte Ware. Der erste Kunde, der das Geld überwiesen hat, hört nichts mehr von dem Händler aus dem Ausland. Wütend erstattet er nach einigen Wochen Anzeige und versucht, das Geld zurückzubekommen. Dabei wird natürlich auch überprüft, wer der Inhaber des Kontos ist, an das das Geld gegangen ist.

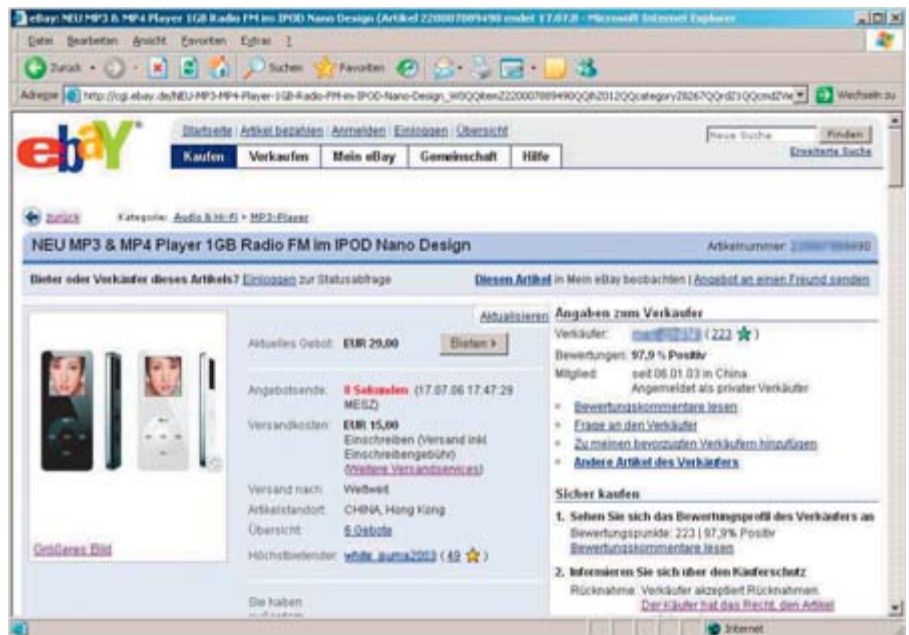
Natürlich muss der Wert der Waren einigermaßen ähnlich sein. Aber auch eine Differenz kann der angeblich überweisende Kunde aus dem Ausland erklären: „Oh, ich habe gerade gesehen, dass ich zu viel überwiesen habe. Nein, teure Überweisung zurück lohnt nicht, packen Sie das Restgeld ins Paket.“

Vorsicht ist geboten: Auf ein Konto, das nicht auf den Namen des Verkäufers lautet, sollte man grundsätzlich nicht überweisen – und auch als Verkäufer sollte man skeptisch werden, wenn Geld von einem anderen kommt als dem, der die Ware ersteigert hat. Freilich lässt sich das nicht auf jedem Kontoauszug feststellen, und natürlich kann das auch ganz banale Gründe haben (Käufer ist etwa die Lebensgefährtin mit anderem Namen). Fragen Sie aber nach. Und nutzen Sie lieber den Treuhand-Service.

11. Der Ebay-Zoll-Trick

Das Angebot: Sie haben ein Gerät von einem Power-Seller aus Fernost erworben, der Ihnen verspricht, dass keine weiteren Kosten durch den Zoll hinzukommen. Sie erhalten die Ware und denken, alles sei o.k. Mehrere Monate später bekommen Sie Post vom deutschen Zoll, der hohe Gebühren einfordert. Die Preisersparnis ist dahin – eventuell haben Sie nun mehr ausgegeben als bei einem Kauf in Deutschland.

Das steckt dahinter: Der Händler hat das Gerät wahrscheinlich als geringwertige Ware (bis 22 Euro) oder als Geschenk deklariert, und der Zoll hat diese Falschdeklaration bei einer anderen Transaktion dieses Händlers bemerkt. Daraufhin wurden sämtliche Geschäfte des Händlers überprüft und bei den anderen Käufern das Geld nachgefordert. Nicht vom Händler, der eigentlich für die Verzollung verantwortlich wäre, will man das Geld haben, sondern vom Käufer: „Sie wurden Zollschuldner, weil Sie an diesem vorschriftswidrigen Verbringen beteiligt waren, obwohl Sie wussten oder vernünftiger Weise hätten wissen müssen, dass



Vorsicht, Zoll: Wenn der Artikel von außerhalb der EU importiert wird, werden oft nachträglich Zollgebühren fällig – für den Käufer (Trick 11)

Sie damit vorschriftswidrig handeln“, heißt es in bestem Amtsdeutsch. Zu versuchen, den Betrag vom Händler wiederzubekommen, wäre aufwendig und wenig erfolgversprechend. Deshalb gilt: Informieren Sie sich vorher über die geltenden Zollbestimmungen. Hier spielt nicht nur das Land eine Rolle, aus dem die Ware kommt, sondern auch die Warengruppe. Die Bestimmungen sind so kompliziert, dass Sie aus der Webseite www.zoll.de auch nicht schlau werden. Sie brauchen in den meisten Fällen die Hotline unter Telefon (069) 46 99 76 00.

Fazit: Vorbeugen ist besser

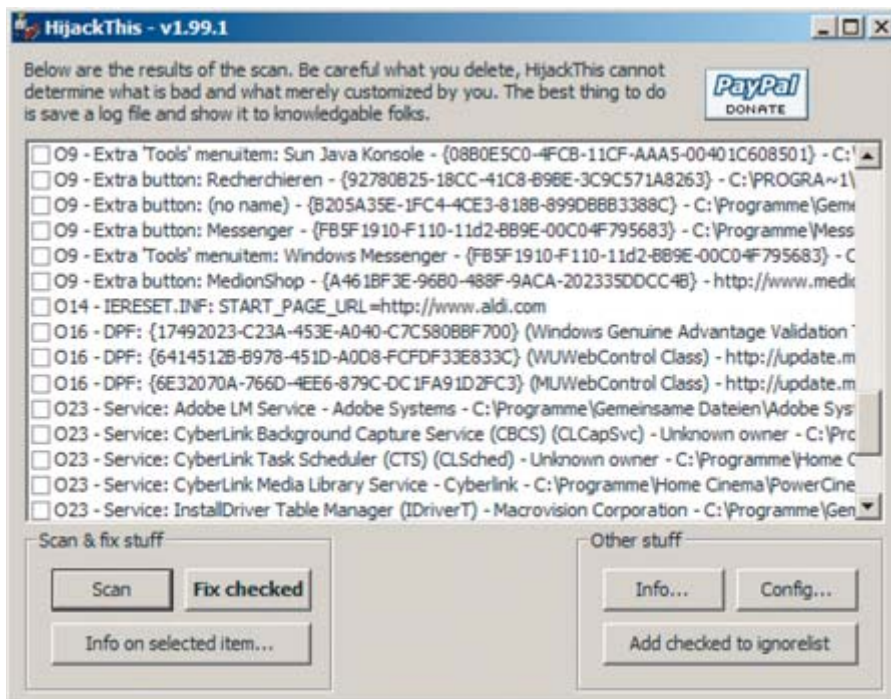
Oft ist es besser, auf ein besonders verführerisches Geschäft zu verzichten, als sich auf das Risiko einzulassen, sich damit eine Menge Ärger einzuhandeln. Vor den meisten Gefahren kann man sich mit etwas gesundem Misstrauen schützen: Lieber dreimal lesen und nach dem Haken suchen als blauäugig einen riskanten oder ungünstigen Vertrag unterschreiben. Niemand hat etwas zu verschenken, und ein Schaden wird Ihnen später wahrscheinlich nur ersetzt, wenn Sie das gerichtlich einklagen. Das bedeutet nicht nur viel Ärger, sondern endet oft erfolglos, etwa wenn es sich um Briefkastenfirmen oder Unternehmen aus dem Ausland handelt, die nur schwer zu belangen sind. In solchen Fällen bleiben Sie dann auch auf Anwalts- und Gerichtskosten sitzen.

Wenn das Kind schon in den Brunnen gefallen ist, sollten Sie zunächst Hilfe im Internet suchen. Oft sind schon andere auf dieselbe Masche hereingefallen. Hilfreich sind beispielsweise Foren wie Computerbetrug.de (<http://forum.computerbetrug.de>), 123Recht.net (www.123recht.net) oder das Ärger-Forum (www.aerger-forum.de).

Für Sascha R. war die Lektüre der Forenbeiträge hilfreich. Bei Computerbetrug.de erfuhr er nicht nur, dass auch andere bereits mit dem Angebot DVDn Probleme hatten, sondern er fand auch heraus, dass die Widerrufsbelehrung zu dem Zeitpunkt seines Vertragsabschlusses nicht ausreichend war. Deshalb hatte für seinen Vertrag die Widerrufsfrist noch gar nicht begonnen, und er konnte problemlos per Einschreiben vom Vertrag zurücktreten.



Nigeria-Connection: Die Masche ist alt – und funktioniert immer wieder (Trick 9)



Diagnose: Viren tot!

Hat sich Ihr PC einen Virus, Wurm oder Trojaner eingefangen, dann müssen Sie schnell und richtig handeln. Wir erklären Schritt für Schritt, wie Sie Schädlinge erkennen und entfernen.

Von **Tristan Bestle**

Kaum ein Tag vergeht ohne Hiobsbotschaften über neue Malware, die Ihren PC gefährdet. Im Idealfall ist Ihre Antiviren-Software (AV) durch ein Signatur-Update bereits darauf vorbereitet, so dass Sie den Angriffen von Viren und Trojanern gelassen entgegensetzen können. Läuft Ihr AV-Programm allerdings mit veralteten Signaturen oder gibt es zu der neuesten Plage noch kein Update, so ist es für den Schädling leicht, Ihren PC zu infizieren. Die Folge ist, dass sensible Informationen wie Passwörter und Bankverbindungsdaten auf Ihrem PC nicht

mehr sicher sind. Hat sich beispielsweise ein Trojaner in Ihrem System eingenistet, sendet dieser die Daten an den Hacker, sobald Sie online gehen. Daher ist es nicht zu empfehlen, mit dem vermutlich infizierten Rechner online nach dem neuesten Viren-Update zu suchen oder Infos einzuholen. Doch wie den Virus dann entfernen? Mit ein paar Grundkenntnissen und den richtigen Programmen können Sie sich gezielt auf die Suche nach Eindringlingen machen und diese dauerhaft beseitigen oder zumindest außer Gefecht setzen. Doch Vor-

sicht: Wann und wie Sie im Detail vorgehen, entscheidet darüber, ob Sie den Schädling auch wirklich loswerden.

1. Virus – oder doch alles okay?

Falls sich Ihr Rechner ungewöhnlich verhält, muss das nicht gleich mit einem Virus oder einem Trojaner zu tun haben. Reagiert beispielsweise der PC nicht mehr, kann er auch überlastet sein. Oder zeigt Ihr Internet-Browser eine Seite nicht an, dann hat vielleicht ein Fehler in der Web-Seite verhindert, dass Firefox & Co. die Seiten aufbauen. Wenn sich solche Vorkommnisse allerdings häufen, sollten Sie sich auf die Suche nach Eindringlingen auf Ihrem Rechner machen.

Infektionswege: Die meisten Schädlinge kommen heute per Mail. Unbedarfte Benutzer öffnen mit Malware infizierte Anhänge. Aber auch beim Surfen kann Ihr PC ein Schadprogramm einfangen, indem Sie Webseiten ansteuern, die durch Ausnutzen von Sicherheitslücken schädlichen Code in Ihr System einschleusen. Dabei ist die Gefahr umso größer, je länger Sie keine Sicherheits-Updates eingespielt haben.

Tipp: Aktivieren Sie unter Windows XP unter „Systemsteuerung, Sicherheitscenter“ die Option „Automatische Updates“. Anwender älterer Windows-Versionen sollten mindestens einmal pro Woche im Internet Explorer über „Extras, Windows-Update“ nach aktuellen Updates suchen und diese installieren. Alternativ holen Sie sich die aktuellen Fassungen unter <http://windowsupdate.microsoft.com/>. Auf dieser Site finden Sie übrigens eine neue Version von Windows-Update, das Ihren PC nicht nur nach

Darum geht's: Viren gründlich entfernen

Antiviren-Software arbeitet nicht immer so effektiv, wie uns die Hersteller das versprechen. Die Programme nützen Ihnen nur dann etwas, wenn sie aktuell sind und auf die neuesten Schädlinge reagieren können. Zudem löschen die Tools oft nicht alle Einträge der Eindringlinge, sondern lassen Reste auf dem System zurück. Wir zeigen Ihnen, was Sie beim Entfernen von Viren & Co. beachten müssen und wie Sie Ihr System gründlich von Malware reinigen.



Unentbehrlich: Eine Antiviren-Software wie das kostenlose Antivir darf auf keinem Rechner fehlen

fehlenden Updates für Windows durchsucht und diese aufspielt, sondern sich auch um das Update-Management von MS-Office und anderen Microsoft-Produkten kümmert.

2. Erster Check mit AV-Tool

Vermuten Sie, dass sich ein Virus oder Trojaner in Ihrem System eingenistet hat, dann lautet das erste Gebot: Keine Panik und vor allem den Rechner nicht überstürzt herunterfahren. Die meisten Viren entfalten ihre volle Wirkung beim Neustart des Betriebssystems, wenn Sie vorher nichts gegen sie unternommen haben. Die Schädlinge nisten sich meist in den Autostart-Einstellungen ein, die in der Registry abgelegt sind.

Als erstes sollten Sie offline gehen und den PC mit Ihrer Antiviren-Software wie **Antivir PE Classic** (auf CD) scannen. Wird ein Virus entdeckt, ist es am sichersten, die infizierte Datei löschen zu lassen.

Heute gibt es kaum noch klassische Viren, die andere Dateien, etwa Systemdateien, infizieren. Die von der AV-Software gemeldete infizierte Datei ist daher meistens schon

der Virus selbst. Haben Sie den Verdacht, eine wichtige Systemdatei sei verseucht, dann stecken Sie die Datei lieber in Quarantäne. Fast alle AV-Tools bieten diese Funktion an.

Achtung: Deaktivieren Sie über „Start, Einstellungen, Systemsteuerung, System, Systemwiederherstellung“ die Systemwiederherstellung. Sonst landen Viren in Systemdateien nach einem Rechnerneustart wieder in ihrem Ordner.

Makroviren: Der falsche Weg ist das Löschen von Schädlingen, wenn beispielsweise Dateien wie Word-Dokumente befallen sind. Einen Makrovirus erkennen Sie daran, dass sich das Programm ungewöhnlich verhält: Beispielsweise poppen Meldungen wie „This one's for you, Bosco.“ auf, Text wie „WAZZu“ schreibt sich wie von Geisterhand an den unterschiedlichsten Orten in das Dokument, oder die DOC-Dateien wandeln sich von selbst in eine DOT-Vorlagendatei um. Besteht der Verdacht auf einen solchen Virus, beseitigen Sie diesen, indem Sie die Datei im reinen Text-Format speichern. Dabei gehen allerdings auch die Formatierung und Makros verloren.

Scan wiederholen: Nachdem Ihr Antiviren-Programm die Datei gelöscht hat oder Sie selbst aktiv geworden sind, scannen Sie sämtliche Festplatten und Speichermedien Ihres Systems nach weiteren Viren. Meistens verteilt der Eindringling seine Einträge auf mehrere Stellen im System. Manchmal schlägt die Antiviren-Software bei der ersten Fundstelle Alarm und sucht dann nicht

Überblick Viren entfernen

Inhalt	Seite
1. Viren, Trojaner – oder doch alles okay?	106
2. Erster Check mit AV-Tool	107
3. Viren und Trojaner manuell suchen	107
4. Port-Verbindungen überwachen	108
5. Malware manuell sicher löschen	109
Kästen	
Darum geht's: Viren entfernen	106
Wichtige Sicherheits-Software	107
Überblick: Autostart	108

alle anderen möglichen Stellen ab. Nach dem Scannen starten Sie Ihren PC mittels Kaltstart neu. Das heißt, Sie fahren Windows herunter und schalten den PC aus, wenn das nicht automatisch geschieht. Andernfalls könnten manche Viren im Arbeitsspeicher aktiv bleiben. Scannen Sie Ihr System nach einem Neustart nochmals, und vergewissern Sie sich, dass Ihre Antiviren-Software keine weiteren Schädlinge findet. Ist diese Aktion abgeschlossen, aktivieren Sie wieder die Systemwiederherstellung.

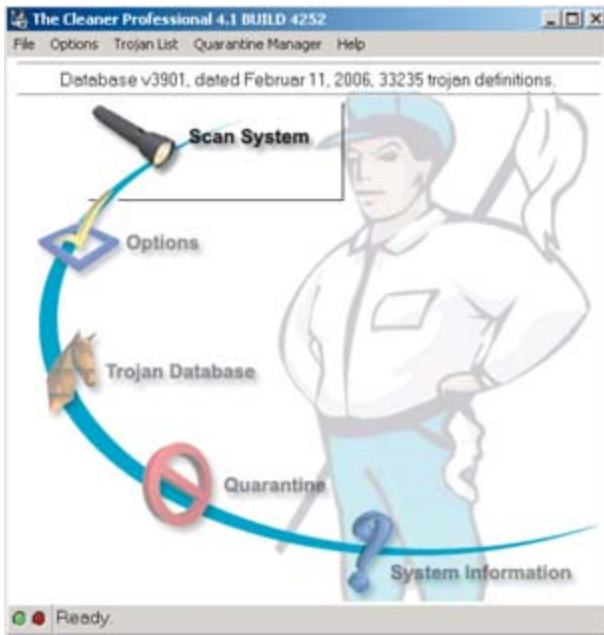
Virenentfernungs-Tools: Kann auch Ihre Antiviren-Software den Eindringling nicht löschen, brauchen Sie spezielle Tools, die die meisten AV-Hersteller auf ihren Websites kostenlos anbieten. Mittlerweile gibt es Software, die das System speziell auf Trojaner hin scannt und diese entfernt – beispielsweise die englischsprachige Shareware **The Cleaner Professional** (auf CD).

3. Schädlinge manuell suchen

Die meisten Programme – egal ob Spezial-Tool oder AV-Software – können das System

Im Überblick: Wichtige Sicherheits-Software

Produkt	Kategorie	Preis	Win-Betriebssysteme	Internet (Download)	Sprache	Seite
Antivir PE Classic 7.0	Antiviren-Software	gratis	98/ME, NT 4, 2000, XP	www.free-av.de (rund 10,5 MB)	deutsch	107
Hijack This 2.0 Beta	Diagnose-Software	gratis	98/ME, NT 4, 2000, XP	www.merijn.org (200 KB)	englisch	–
Starter 5.6.2.8	Start-Manager, Prozess-Viewer	gratis	98/ME, NT 4, 2000, XP	http://codestuff.cjb.net (460 KB)	deutsch	108
The Cleaner Professional 4.2	Antitrojaner-Software	49 Euro	98/ME, NT 4, 2000, XP	www.moosoft.com (4,5 MB)	englisch	107
Trojancheck 6.02	Start-Manager, Prozess-Viewer	gratis	98/ME, 2000, XP	www.trojancheck.de (1,2 MB)	deutsch	108
Zone Alarm 7 Free	Firewall	gratis	98/ME, 2000, XP	www.zonelabs.de (11 MB)	deutsch	109



Spezial-Tool: The Cleaner Professional findet Trojaner auf dem System und macht sie unschädlich

nicht vollständig säubern. Gerade in der Registry bleiben oft Einträge zurück. Sie sollten daher immer manuell überprüfen, ob sich noch Reste der Malware im System befinden. Dieser Check wird auch fällig, wenn auf dem PC keine Antiviren-Software installiert ist oder die Signaturen veraltet waren. In der Regel installieren sich Schädlinge so, dass sie sich beim Start des Systems unbe-

merkt automatisch laden. Manchmal werden hinter den Parametern auch Leerzeichen eingefügt, damit die restlichen Einträge am Bildschirm nicht mehr zu sehen sind. Sie sollten deshalb immer an den Rand scrollen.

System.INI: In diese Datei tragen sich Trojaner meist unter „Shell=“ ein. Der Programmaufruf von Explorer.EXE ist an dieser Stelle in Ordnung. Wenn dahinter allerdings

merkt automatisch laden. Das Programm läuft meistens im Hintergrund und wird aktiv, wenn der Benutzer etwa online geht. Trojaner lassen sich somit dort aufspüren, wo sie sich eintragen können, um heimlich zu starten. Manche schreiben sich in die Dateien Win.INI, System.INI, Autostart.BAT oder Config.SYS, die Sie in Windows mit „Start, Ausführen, Sysedit“ einsehen und bearbeiten können.

Win.INI: Vor allem früher wurde diese Datei öfter benutzt, um den Trojaner beim Systemstart zu laden. Eventuelle Eintragungen sind dort unter den Parametern „Load=“ oder

weitere Einträge stehen, gehen Sie dem besser nach, indem Sie zum Beispiel die laufenden Prozesse überwachen.

Registry: Ein beliebter Ort für versteckte Programmstarts ist die unübersichtliche Registrierdatenbank, die Sie über „Start, Ausführen, Regedit“ öffnen können.

Kontrollieren Sie darin, ob sich etwa Einträge unter „Hkey_Clases_Root\Exefile\Shell\Open\Command“ befinden. Standardmäßig steht dort nur „%1“%*“. Bei einem Trojaner-Befehl steht vor der Zeichenkette noch der Pfad für ein Programm. Bei Verdacht löschen Sie den Eintrag.

Vorsichtig vorgehen: Änderungen in der Registry sollten Sie nur vornehmen, wenn Sie wirklich sicher wissen, dass die Einträge tatsächlich von einem Trojaner stammen. Mit Hilfe eines Start-Managers können Sie nach und nach jedes unbekannte Programm deaktivieren, das automatisch mit dem PC startet. Haben Sie versehentlich eine benötigte Software abgeschaltet, lässt sie sich später einfach wieder aktivieren. Auf Trojaner spezialisiert ist der Start-Manager **Trojancheck**: Mit der Freeware können Sie überprüfen, welche Programme und Daten Ihr Rechner automatisch beim Start lädt.

Infos zu Schädlingen: Möchten Sie wissen, ob eine Datei, die Trojancheck meldet, ein Virus oder ein Trojaner ist, dann suchen Sie die Datei einfach über Google. Anhand der Beschreibungen finden Sie schnell heraus, ob die Datei zum System, zu einem wichtigen Programm oder Dienst gehört oder ob es sich um einen Schädling handelt. Sie können auch die Prozessdatenbank der PC-WELT einsehen (www.pcwelt.de/wiki).

Prozess-Viewer: Trojanern kommen Sie auch auf die Schliche, indem Sie einen Prozess-Viewer einsetzen, zum Beispiel die kostenlose Software **Starter** (auf CD). Damit stellen Sie fest, welche Programme gerade aktiv sind. Die meisten Trojaner tarnen sich mit geschickt gewählten Namen, so dass Sie sie auf den ersten Blick für Programme halten, die zum Betriebssystem gehören. Überwachen Sie daher öfter die laufenden Programme. Dann wird Ihnen auch auffallen, wenn plötzlich ein Programm dabei ist, das vor zwei Tagen noch nicht da war.

4. Port-Verbindung überwachen

Trojaner finden Sie auch, indem Sie die Kommunikations-Kanäle Ihres PCs überwachen, die Ports. Ein belegter Port bedeutet,

Autostart: Quellen für Programmaufrufe

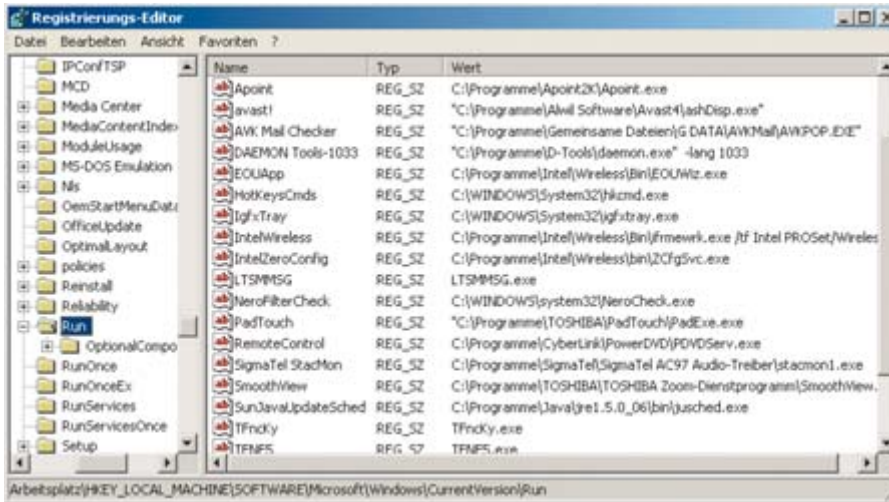
Wir listen die Autostart-Möglichkeiten für Programme unter Windows auf. Nicht jede Option gibt es in jeder Windows-Version.

Registry

- „Hkey_Local_Machine\System\CurrentControlSet\Services“
- „Hkey_Local_Machine\Software\Microsoft\Windows\CurrentVersion“: Darin die Werte unter „RunServicesOnce“, „RunServices“, „RunOnce\Setup“, „RunOnce“, „RunOnceEx“ und „Run“
- „Hkey_Current_User\Software\Microsoft\Windows\CurrentVersion“: Darin die Werte unter „RunServicesOnce“, „RunServices“, „RunOnce“ und „Run“
- „Hkey_Current_User\Software\Microsoft\Windows NT\CurrentVersion\Windows“: Darin die Werte unter „Run“ und „Load“ „Hkey_Clases_Root\exefile\shell\open\command“

Startordner

- %windir%\All Users\Startmenü\Programme\Autostart
- %windir%\Startmenü\Programme\Autostart
- %windir%\Profiles\<Benutzername>\Startmenü\Programme\Autostart
- Dokumente und Einstellungen\All Users\Startmenü\Programme\Autostart
- Dokumente und Einstellungen\<Benutzername>\Startmenü\Programme\Autostart



Die Registry: Hier tragen sich Viren und Trojaner am häufigsten ein, um sich automatisch während des PC-Starts zu aktivieren und von da an immer aktiv zu sein

dass hier ein Trojaner lauern könnte. Am besten überprüfen Sie die Ports direkt nach dem Start des Rechners, solange Sie noch offline sind. Das geht zum Beispiel mit dem Windows-eigenen Kommandozeilen-Programm Netstat. Geben Sie unter „Start, Ausführen“ zuerst den Befehl „cmd“ ein und in das neue Fenster den Befehl „netstat -a“. Ist ein Port belegt, dann lautet der entsprechende Status „Listening“. Anhand der ausführlichen Port-Liste unter www.multi-online.com/security/Portliste.php lässt sich in den meisten Fällen erkennen, ob es sich um einen Trojaner handelt und um welchen. Um ein Gefühl dafür zu bekommen, welche Ports standardmäßig belegt sind, rufen Sie Netstat regelmäßig auf.

Mit der Port-Liste können Sie den Trojaner allerdings nicht immer genau bestimmen: Hacker-Tools, mit denen nahezu jeder einen Trojaner erstellen kann, geben dem Autor die Möglichkeit, die Ports frei zu wählen. Viele legen die Kommunikation ihrer Schädlinge auf Ports, die eigentlich für harmlose Anwendungen reserviert sind. Sie sollten sich also nicht allein auf die Überwachung der Ports verlassen, sondern die beschriebenen Methoden kombinieren.

Firewall: Eines der effektivsten Mittel, mit dem sich Trojaner aufspüren lassen, ist eine Systemüberwachung per Firewall. Versucht ein Trojaner beispielsweise, aus Ihrem Rechner heraus zu seinem Programmierer Kontakt aufzunehmen, erkennt dies eine Firewall sofort. Sie zeigt an, welches Programm unaufgefordert eine Verbindung herstellen will und über welchen Port das versucht

wird. Eine Firewall darf daher auf keinem System mit Netzwerkverbindung fehlen. Für Privatanwender empfehlen wir die kostenlose Firewall **Zone Alarm** (auf CD).

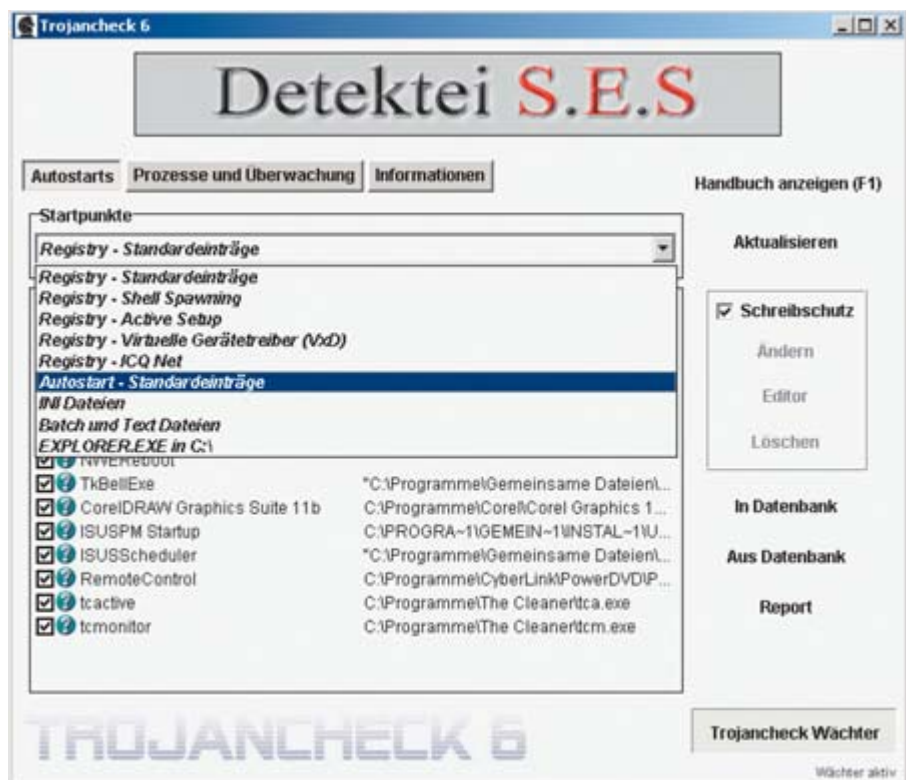
5. Malware manuell löschen

Haben Sie bei Ihrer Suche in der Registry einen Trojaner-Eintrag gefunden, notieren Sie sich zuerst den Eintrag und löschen ihn dann. Anschließend starten Sie das System

neu und entfernen die zuvor notierte Datei von Ihrem Rechner. Lässt sich der Trojaner auf diese Weise nicht beseitigen, starten Sie Ihren Rechner im „Abgesicherten Modus“ und versuchen es erneut. In den abgesicherten Modus kommen Sie, wenn Sie die <F8>-Taste drücken, während Ihr PC hochfährt.

Einfacher und schneller säubern Sie Ihr System, indem Sie den Trojaner mit Hilfe des Prozess-Viewers beenden, das Programm auf dem System suchen und es dann löschen. Nach einem erneuten Systemstart sollten Sie sämtliche Einträge in der Registry und die Dateien noch einmal überprüfen. Danach löschen Sie mögliche weitere Trojaner-Einträge in der Registry. Das geht über „Start, Ausführen, Regedit“ und „Bearbeiten/Suchen“. Sollte nach einem Neustart eine Fehlermeldung über eine nicht gefundene Datei erscheinen, haben Sie noch nicht alle Einträge des Trojaners aufgestöbert. Vergessen Sie nicht, die Systemwiederherstellung vor der Säuberung zu deaktivieren und danach wieder zu starten.

Achtung: Sie sollten sicher sein, dass es sich bei dem zu löschenden Programm um einen Trojaner handelt. Wenn Sie wichtige Systemdateien entfernen, kann Ihr PC anschließend seinen Dienst verweigern. ❌



Trojancheck: Alle Orte, die potenziell schädliche Programme wie Viren und Trojaner enthalten können, zeigt Ihnen dieses Freeware-Tool auf einen Blick an



Bot-Armeen greifen an

Auf tausenden PCs warten gefährliche Tools auf das Kommando für das Bombardement auf Firmen-Server mit korrupten Anfragen. Kriminelle versuchen so Unternehmen zu erpressen.

Von **Arne Arnold**

Kriminelle haben ein neues und sehr lukratives Ziel für sich entdeckt. Sie erpressen kleine und große Firmen, die im Internet präsent sind, um hohe Geldsummen. Das funktioniert teilweise sehr viel einfacher als bei üblichen Schutzgelderpressungen. Denn die Gangster müssen gar nicht selbst in Erscheinung treten und können anonym weltweit von jedem beliebigen Ort aus zuschlagen – zu jedem Zeitpunkt ohne weitere Vorwarnung. Als Druckmittel dient ihnen dabei eine Armee von Bot-Rechnern, die spielend fast jeden Server lahm legen können. Die erpressten Firmen kön-

nen sich gegen die Attacken kaum wehren. Wir erklären den technischen Hintergrund und zeigen, wie die Abzocke abläuft.

Botnets: Die schlafende Gefahr auf Ihrem Rechner

In Branchen, in denen das ganze Geschäftsmodell von der IT abhängig ist, können die Downtime-Kosten schnell sehr hoch werden. So schätzt Contingency Research beispielsweise für Online-Shops die Ausfallkosten auf über 100.000 Dollar pro Stunde, für ein Bankrechenzentrum auf 2,5 Millionen und für das Online-Broking gar auf 6,5 Mil-

lionen Dollar. Zuerst gerieten Online-Wettbüros ins Visier von Kriminellen. Die Gauner forderten von den Site-Betreibern bis zu 60.000 Euro, damit die Web-Seiten auch weiterhin erreichbar sind. Die Wettbüros wendeten sich an die Polizei und investierten bis zu 150.000 Euro in Sicherheitstechnik. Derart hohe Investitionen waren durchaus angebracht, denn die befürchteten Attacken gehen von Bot-Netzwerken aus – kurz Botnets genannt. Diese Netze bestehen aus mehreren tausend Rechnern von Privatleuten, auf denen die Gangster heimlich schädlichen Code eingeschleust haben. Die PCs lassen sich vom Programmierer des Codes über einen zentralen Server im Internet fernsteuern. Bis es soweit ist, verhalten sich die befallenen Rechner fast gänzlich unauffällig. Die Besitzer der Rechner haben dabei keine Ahnung, dass ihr PC teil einer Angriffsarmada ist.

Ist eine erpresste Firma nicht bereit zu zahlen, starten die Kriminellen einen Denial-of-Service-Angriff (DoS-Angriff) über ihr Bot-Netzwerk. Dabei stellen die Bot-PCs korrupte Anfragen an den Server der Firma. Verbreitet ist das Syn-Flooding. Normalerweise wird die Kommunikationssitzung zwischen PC (Client) und Server in drei Schritten aufgebaut: Der Client sendet „SYN“, der Server antwortet mit „SYN-ACK“ und der Client bestätigt das mit „ACK“. Beim Syn-Flooding schickt der Client das „ACK“ nicht

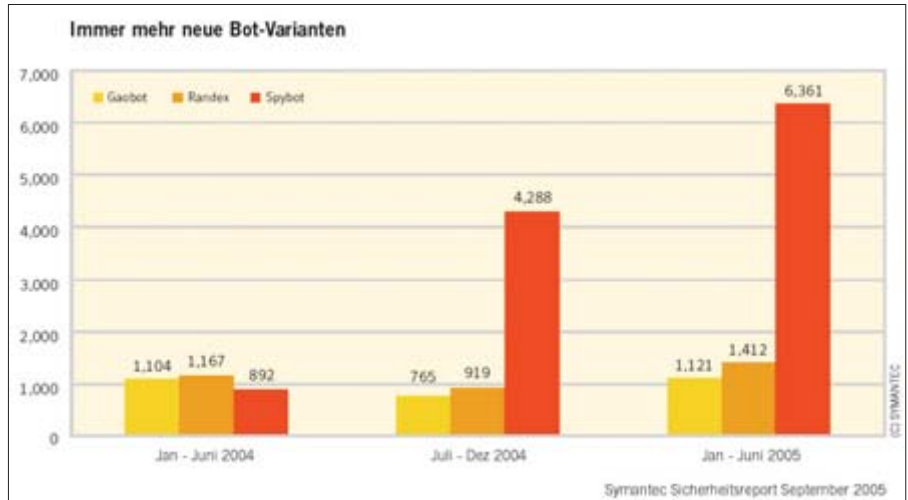
ab, die Verbindung ist also halb geöffnet. Da es auf einem Server nur eine beschränkte Anzahl halb offener Verbindungen geben kann, sind der Rechner und damit auch die darauf laufende Website nicht mehr für normale Anfragen erreichbar.

Erpressung: Kriminelle entdecken das Internet

Die Sicherheitsfirma Messagelabs berichtet von einer Studie, laut der 17 von 100 befragten US-Unternehmen bereits mit erpresserischen DoS-Angriffen bedroht wurden. Experten schätzen, dass hinter den Erpressungsversuchen meist das organisierte Verbrechen steht, das mehr und mehr auch im Internet tätig wird. Das Know-how für die Angriffe holen sich die Verbrecher von Hackern, die ihrerseits feststellen, dass es sehr lukrativ ist, ein Bot-Netzwerk aufzubauen und zu vermieten.

Aktienbetrug: Kursmanipulation durch Online-Tricks

Wer weiß, wie sich der Kurs einer Aktie entwickelt, kann richtig viel Geld verdienen. Dabei ist es fast egal, ob der Kurs steigt oder fällt. Hauptsache, er bewegt sich in die von den Kriminellen gewünschte Richtung. Für fallende Kurse lässt sich wiederum mit DoS-Angriffen sorgen. Das dafür nötige Bot-



Verbreiteter Bot-Schädling: Laut der Sicherheitsfirma Symantec stieg die Zahl der Varianten des Schädlings Spybot (roter Balken) innerhalb eines Jahres am stärksten

Netzwerk kann jeder anmieten, der einen entsprechenden Preis bezahlt. Ist ein Unternehmen aufgrund eines Angriffs nicht über das Internet erreichbar, wird die Aktie sehr wahrscheinlich fallen.

Bekannt wurde ein Fall mit umgekehrtem Vorzeichen. Kriminelle verschickten eine Pressemitteilung, die angeblich von der Firma Concorde America stammte. Darin wurden die Expansion des Unternehmens angekündigt. Innerhalb kurzer Zeit verdoppelte sich der Wert der Aktie.

Schutz: Betroffen sind auch Privatanwender

Ziel der Angriffe von Bot-Armeen sind zwar Firmen, doch betrifft das Thema natürlich auch die Privatanwender. Denn auf ihren Rechnern versteckt sich der gefährliche Code und bezieht den Anwender in ein kriminelles Vorgehen ein. Zudem wird während des Angriffs die Internet-Verbindung stark beansprucht. Schnellen Schutz vor den gefährlichen Bot-Programmen bringen eine Antiviren-Software und eine Firewall. ☒

So funktionieren Bot-Netzwerke

Der Begriff Bots ist abgeleitet vom Wort „Roboter“. Denn die befallenen Rechner lassen sich vom Programmierer des Codes fernsteuern wie eine Armee von Robotern. Mehrere hundert bis einige tausend Bot-Rechner zusammen bilden ein Bot-Netzwerk. In Fachkreisen wird gelegentlich auch der Begriff Zombi für einen Bot-Rechner verwendet.

1. Schritt: Verbreitung

An erster Stelle kommt die Verbreitung des schädlichen Codes. Am häufigsten geschieht das wie bei einem Internet-Wurm, der sich per Mail verbreitet. Auf einem infizierten Rechner sucht er nach weiteren Mailadressen und verschickt sich an diese über ein mitgebrachtes Mailprogramm weiter. Auch Trojaner werden oft für den Aufbau eines Botnets eingesetzt. Sie verbreiten sich etwa über Sicherheitslücken in Windows.

2. Schritt: PC besetzen

Will ein Programmierer ein Bot-Netzwerk aufbauen, passt er oft bestehende Würmer oder Trojaner an seine Bedürfnisse an. Typisch für solch einen angepassten Code ist, dass er nur wenige Schadensroutinen auf dem befallenen System ausführt. Dazu zählt der Versuch, Antiviren-Tools und Firewall-Programme lautlos zu umgehen. In der Regel löscht der

Code aber keine Anwenderdateien und spioniert auch keine Daten aus. Er versucht vielmehr, sich versteckt zu halten, damit der Besitzer des PCs nicht misstrauisch wird.

Nur wenn eine Internet-Verbindung besteht, meldet sich der befallene Rechner bei einem Server an und wartet im Hintergrund auf Kommandos von seinem Programmierer. In der Regel läuft das über einen IRC-Server (Internet Relay Chat).

3. Schritt: Angreifen

Ein schlagkräftiges Botnet besteht aus fünf bis 10.000 Rechnern mit einer schnellen Verbindung ans Internet. Haben sich die einzelnen Rechner am IRC-Server angemeldet, kann der Programmierer von dort aus die Art und den Zeitpunkt für die Attacke festlegen. Häufig werden die Botnets für DoS-Attacken (Denial of Service) genutzt. Dabei senden sie manipulierte Anfragen an Internet-Server, womit diese für gewöhnliche Aufgaben blockiert sind. Eine gut konfigurierte Firewall kann DoS-Attacken zwar abwehren, doch der Angriff läuft ja nicht nur von einem PC, sondern von vielen tausend Rechnern aus. Die Abwehr ist somit wesentlich schwieriger. Bei DoS-Attacken, die von Botnets ausgehen, spricht man auch von DDoS-Angriffen (Distributed Denial of Service).



Großer Lauschangriff

Keylogger sind Tools zur Bespitzelung von Anwendern. Ihre einzige Aufgabe: Den Benutzer heimlich ausspionieren, seine Aktivitäten festhalten und alle Web-Adressen notieren.

Von **Christoph Metzger**

Keylogger sind Programme, die sich auf dem Rechner eines Opfers einnisten, dessen Eingaben mitprotokollieren und diese Daten anschließend an einen „Auftraggeber“ übermitteln. Das passiert komplett im Hintergrund, ohne dass der Anwender etwas bemerkt, denn je unauffälliger sich das Schadprogramm verhält, desto geringer ist die Chance der Enttarnung. Problematisch wird es vor allem, wenn die Signaturen des Keyloggers dem auf dem Zielsystem installierten Virenschutzprogramm noch nicht bekannt sind. Dann sind Homebanking, Zugangsdaten, TANs, Kreditkartennummern und Paypal-Konten in Gefahr.

Auch wenn Sie an fremden PCs surfen, laufen Sie Gefahr, dass Sie ausspioniert werden. Möglicherweise protokollieren Keylogger im Hintergrund sämtliche Tastaturklicks mit. Wenn Sie an einem fremden System etwa Ihre Bankdaten oder Login- und Passwortdaten eingeben, sollten Sie das nur unter Vorbehalt tun.

1. Die Methoden der Desktop-Spanner

Wächterprogramme laufen im Hintergrund und speichern regelmäßig detaillierte Berichte über Ihre PC-Aktivitäten oder versenden diese per Mail oder über eine direkte

TCP/IP-Verbindung. Einmal installiert, führen sie ihre Tätigkeit vollautomatisch und ohne weitere Benutzereingriffe durch. Bei der Installation registrieren sich Keylogger dazu für einen Autostart. Über einen Eintrag in der Registry unter einer meist unverfänglich wirkenden Tarnbezeichnung sorgt ein Keylogger für die automatische Ausführung beim Systemstart. Die Aufzeichnung enthält alle PC- und Internet-Aktivitäten und arbeitet wahlweise textbasiert durch das Extrahieren aller auf dem Desktop vorhandenen Textinformationen oder grafisch wie ein herkömmlicher Videorekorder. Das Nutzerprotokoll umfasst Angaben über geöffnete Anwendungen, besuchte Web-Seiten, Chat-Unterhaltungen, Mausklicks, geladene Bilder, Mails und aktive Anwendungen samt Zeitstempel. Sogar eine vollständige Fernsteuerung des Rechners wie bei einem Trojaner ist mitunter vorgesehen.

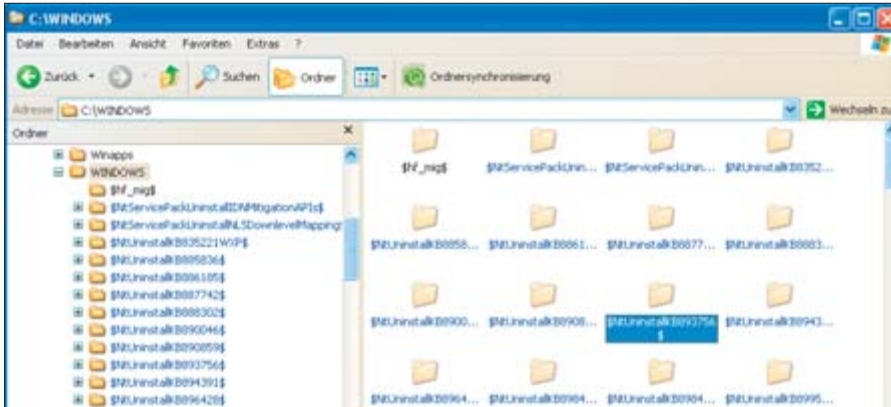
2. Protokoll-Software spioniert Sie systematisch aus

Neben Aufnahmen Ihres Monitors enthalten aktuelle Spionageprogramme einen Rekorder für die auf Internet-Seiten eingegebenen Formulardaten, eine Benutzerverwaltung, die die Protokollierung gezielt bei bestimmten Anwendern aktiviert, sowie eine Pausenfunktion zur automatischen Unterbrechung und Wiederaufnahme der Aufnahme. Über die Erkennung von Schlüsselwörtern und eine daran gekoppelte Alarmfunktion verschicken Schnüffelprogramme unbemerkt Kurzmitteilungen, falls der Anwender eine Seite aufruft oder ein Dokument bearbeitet, das einen bestimmten Begriff enthält. Dadurch kann der Angreifer bei Bedarf einschreiten, etwa durch einen Fernzugriff auf den PC.

Betrachtet man die von Keyloggern eingesetzten Mechanismen zur Tarnung und Spionage von Benutzerdaten, zeigt sich eine verblüffende Ähnlichkeit mit herkömmlichen Trojanern. So verwundert es kaum, dass immer wieder Trojaner in Umlauf sind, die als klassischer Keylogger arbeiten.

3. So erkennen und beseitigen Sie Schnüffel-Software

Wer sich nicht sicher ist, ob möglicherweise Keylogger, Fernsteuerungs-Tools oder Protokoll-Software auf dem eigenen Rechner aktiv sind, sollte sein System genau inspizieren. Hinweise zum generellen Schutz vor



Gut getarnt: Bei den in diesem Ordner abgelegten Dateien scheint es sich um Systemupdates zu handeln – es sind jedoch die verschleierte Protokolle (Punkt 3)

Viren und Würmern finden Sie im Beitrag ab Seite 94. Die in diesem Beitrag gezeigten Tipps & Tricks gelten auch für die Vorbeugung vor Keyloggern.

Ein Ansatzpunkt zur Aufdeckung von Spionage sind die zahlreichen Bildschirmfotos und Protokolldateien, die irgendwo auf der Festplatte abgelegt werden müssen und eine beachtliche Größe annehmen können. Bei einer Monitauraufösung von 1280 x 1024 Punkten kommen bei einem Screenshot alle 15 Sekunden abhängig von der verwendeten Komprimierung schnell zwischen 450 und 700 MB an Daten zusammen. Häufig muss hierfür das Windows-Verzeichnis erhalten, denn dort befinden sich unzählige Dateien und Ordner mit nichtssagenden Dateinamen. Ein Keylogger könnte sich aber auch in einem Windows-Verzeichnis unter einem

Namen einnisten, der kaum von dem einer wichtigen Systemdatei zu unterscheiden ist. Dann ist detektivisches Gespür gefragt. Suchen Sie daher nach Dateien und Ordnern, die besonders viele Dateien ähnlicher Größe aufweisen und deren Dateinamen Regelmäßigkeiten erkennen lassen.

Klicken Sie die suspekten Datei mit der rechten Maustaste an, und wählen Sie „Eigenschaften, Version“. Hinter „Beschreibung“ sollte ein aussagekräftiger Name stehen, hinter „Copyright“ der Hersteller. Je nach Auskunftsfreudigkeit des Herstellers sind in den Feldern „Kommentare“ oder „Besondere Beschreibung“ weitere Infos hinterlegt. Falls Sie mit den Informationen nichts anfangen können, hilft eine Google-Recherche nach dem Dateinamen. Gleiches gilt für den Fall, dass in der Datei keine weiterführen-

Überblick Keylogging

Inhalt	Seite
1. Methoden der Desktop-Spanner	112
2. Software spioniert systematisch aus	112
3. Schnüffel-Software erkennen	112
4. Bildschirmtastatur nutzen	113
5. Hintergrundtasks aufdecken	114
6. Kommunikation unterbrechen	114
Kästen	
Diese Big-Brother-Tools sind legal	113
Keylogging: Wenn der Arbeitgeber spioniert	114
Virtueller PC als Hochsicherheitsumgebung	115

den Informationen vorhanden sind und daher auf der Registerkarte „Version“ nichts angezeigt wird.

4. Bildschirmtastatur nutzen

Ein Großteil der Keylogger-Programme klinkt sich direkt nach dem Tastaturtreiber ein und protokolliert sämtliche Eingaben mit. Bildschirmtastaturen sind allerdings ein eleganter und einfacher Weg, um sie auszuwickeln. Eine Bildschirmtastatur ist eine virtuelle, also nur auf dem Monitor angezeigte Tastatur in einem Programmfenster, die mit der Maus bedient wird. Gedacht waren diese Hilfsprogramme ursprünglich für behinderte Menschen. Windows enthält zwar eine solche Tastatur, allerdings ist die-

Kaum zu glauben: Diese Big-Brother-Tools sind legal

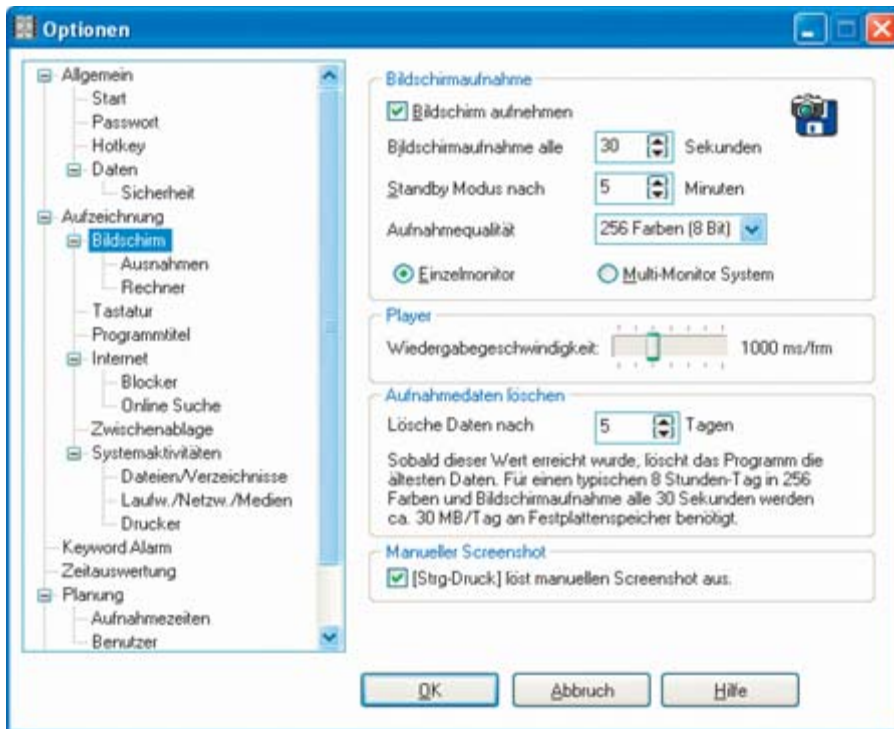
Manchmal ist es notwendig, einen Computer zu überwachen. Sei es, dass man wissen möchte, ob jemand während der Abwesenheit des Besitzers am Gerät war und was derjenige dort gemacht hat, sei es, um feststellen zu können, womit sich der Nachwuchs beschäftigt.

Orvell Monitoring: Orvell (www.protectcom.de) ist mit einer umfangreichen Überwachungstechnik für Bildschirmaufnahmen, Tastenanschläge und Web-Adressen ausgestattet. Der Anwender entscheidet, ob es sichtbar oder im Stealth-Modus ausgeführt werden soll. Außerdem muss er eine Tastenkombination zum Aufruf der „Kommandozone“ angeben – ohne die lässt sich Orvell Monitoring im Stealth-Modus nicht aufrufen. Das Kernmodul der Software ist die Tastaturüberwachung. Hier werden alle Tastenanschläge aufgezeichnet. In der Praxis funktioniert das ganz gut. Nur findet man einzelne Buchstabenlöschungen oder -ersetzungen mitten im Text wieder, was etwas verwirrend sein kann. Trotzdem ist getippter Text sehr gut rekonstruierbar. Auch die Software wird überwacht: Orvell Monitoring merkt sich Start- und Endzeit aller Programme.

Gut gelöst ist die Screenshot-Funktion: Standardmäßig macht Orvell Monitoring alle 30 Sekunden ein Bildschirmfoto, das Intervall kann aber auch größer oder kleiner gewählt werden. Interessant: Bei Eingabe von frei definierbaren Begriffen – vordefiniert ist „Sex“ – wird die Häufigkeit der Screenshots erhöht, so dass man genau erfährt, was der Anwender getan hat. Zudem kann das Tool den Administrator per Mail alarmieren, wenn bedenkliche Aktivitäten (beispielsweise USB-Stick angesteckt) einsetzen.

Home Keylogger: Die Freeware (www.kmint21.com) mit Stealth-Funktion beschränkt sich auf das Protokollieren von Tastaturanschlägen.

Eblaster/Spector Pro: Wie eine Kamera macht Spector Pro (www.spectorsoft.de) Aufnahmen dessen, was der Anwender auf seinem Monitor sieht. Spector kann mehrere hundert Aufnahmen pro Stunde versteckt auf der Festplatte ablegen. In den Programmoptionen stellt der Administrator ein, wie häufig und detailliert (Farbe oder schwarzweiß, hohe oder niedrige Qualität) Spector aufnehmen soll. Eblaster vom gleichen Hersteller ist auf das Mitschneiden von Mails, Chats und Instant Messages spezialisiert.



Trick: Mit heimlich geschossenen Bildschirmfotos lässt sich zwar der Desktop-Inhalt aufnehmen, ein kurzes Fotointervall reicht für virtuelle Tastaturen nicht aus (Punkt 4)

se nicht sicher. Besser ist beispielsweise die Freeware **Virtual Keyboard** von Andrej Koch (für Windows 95/98/ME, 2000 und XP, Download unter www.andrej-koch.de, 317 KB), die zudem nicht installiert werden muss. Sie geben die Dateien einfach in das Fenster ein und kopieren Sie anschließend in die notwendigen Felder. Das Konzept

funktioniert so gut, dass einige Banken und Mailprovider, etwa www.safe-mail.net, für ihre Kunden eine solche virtuelle Tastatur für die Anmeldung und die Eingabe von Daten bereitstellen. Allerdings eignen sich diese virtuellen Keyboards kaum für den täglichen Einsatz, dazu sind sie zu unflexibel. Für die Eingabe sensibler Daten sollten Sie

aber, besonders an öffentlichen Rechnern wie Internet-Cafés, auf eine virtuelle Tastatur zurückgreifen.

5. Hintergrundtasks aufdecken

Schnüffelpprogramme laufen mit wenigen Ausnahmen als Hintergrundprozess, den Sie mit Hilfe eines erweiterten Taskmanagers aufspüren können. Mit dem Taskmanager von Windows kommen Sie hier nicht weiter, denn einige der Spione schleichen sich an diesem Bordwerkzeug vorbei. Besser Sie verwenden das englischsprachige **Process Explorer** von Sysinternals (für Windows 2000, XP und Vista, Download unter www.sysinternals.com, 1,46 MB), das auch solche Prozesse anzeigt, die der Windows-Taskmanager versteckt.

Standardmäßig sehen Sie, ähnlich wie im Windows-Taskmanager, eine Liste aller laufenden Prozesse in der oberen Fensterhälfte. Process Explorer zeigt hier alle Tasks in einer anschaulichen Baumstruktur an und liefert zahlreiche Informationen. So erfahren Sie, auf welche DLL-Dateien, Registry-Einträge und Systemkomponenten ein Task zugreift und ob bestimmte Teile einer Anwendung gerade nicht verfügbar sind. Sie erhalten die Infos im unteren Bereich des Programmfensters, sobald Sie einen Task markieren und „View, View Handles“ wählen. Eine Alternative zu Process Explorer ist **Process Viewer** (für Windows 95/98/ME, NT4, 2000 und XP, Download unter [## Keylogger: Wenn der Arbeitgeber lauscht](http://www.</p></div><div data-bbox=)

Welcher Chef würde nicht gerne wissen, welche Websites seine Mitarbeiter vom Büro-PC aus besuchen? Zwar sind Server mit pornographischem oder anderweitig problematischen Inhalten in den meisten Firmennetzwerken ohnehin blockiert. Doch oft funktionieren die Filter nicht richtig. Und an eine eventuell vorhandene betriebliche Vereinbarung zur Internet-Nutzung halten sich längst nicht alle Mitarbeiter.

Der Einsatz von Überwachungs-Software greift in die Rechte der Mitarbeiter ein und ist grundsätzlich unzulässig, es sei denn ein Gesetz oder eine Rechtsvorschrift erlauben dies, es liegen besondere Gründe vor, oder die betroffenen Mitarbeiter haben ihre explizite Zustimmung erteilt. Die detaillierte Aufzeichnung der PC- und Internet-Nutzung eines oder aller Anwender stellt einen Umgang mit personenbezogenen Daten dar, der den Reglementierungen des Bundes- und Landesdatenschutzgesetzes unterliegt. Besondere Gründe können unter Umständen vorliegen, wenn der Arbeitgeber gegenüber einem einzelnen Arbeitnehmer ein berechtigtes Interesse nachweisen kann und ein schutzwürdiges Interesse des Betroffenen nicht entgegensteht. Das kann zum Beispiel zur Aufdeckung

von kürzlich stattgefundener Straftaten der Fall sein, wenn ein durch Tatsachen begründeter Verdacht gegen einen Mitarbeiter vorliegt.

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

Auch Betriebsvereinbarungen können ein Aufzeichnen aller Computeraktivitäten innerhalb eines Unternehmens regeln – es bedarf jedoch generell der Einbeziehung des Betriebsrats, sofern ein solcher existiert. Außerdem muss der Mitarbeiter gesondert und im Vorfeld auf die Protokollierung hingewiesen worden sein.

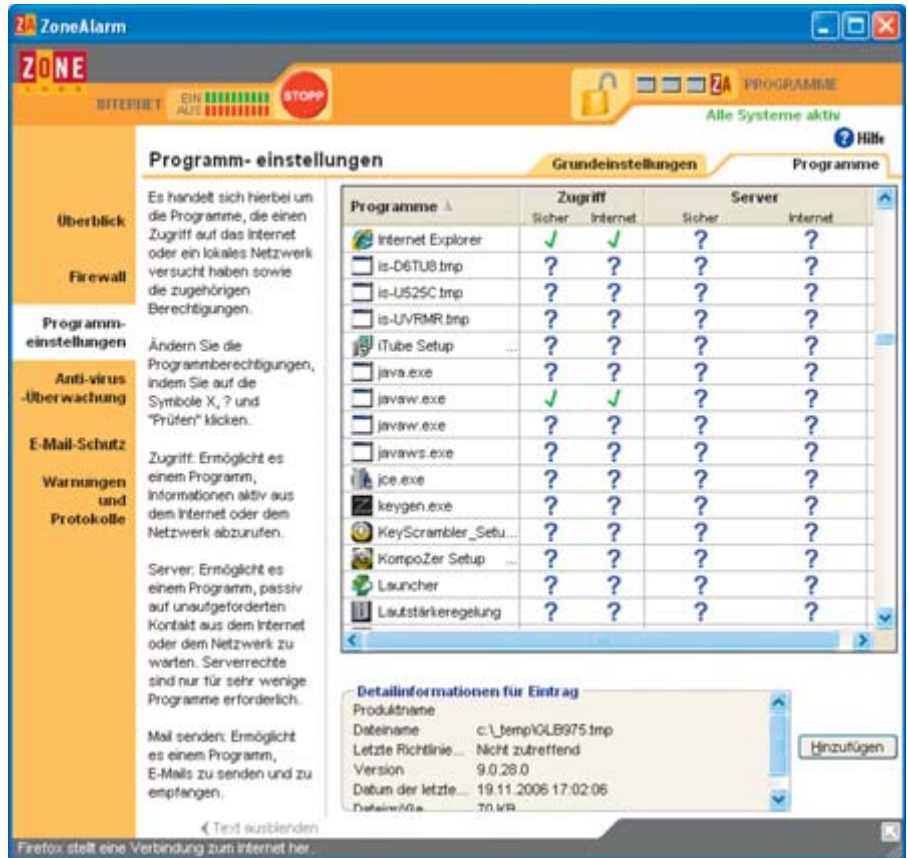
Eine Besonderheit sind Helpdesk-Tools, mit denen sich die Support-Mitarbeiter über das Netzwerk an Client-PCs aufschalten und beispielsweise Wartungsarbeiten durchführen können. Solche Tools verlangen die Zustimmung des Anwenders, bevor der Fernzugriff möglich ist.

prcview.com, 1,46 MB). Besonders gut an dem Programm ist, dass es auch die Pfade anzeigt, in denen die gerade laufenden Programme liegen. Anhand der Verzeichnisnamen können Sie grob abschätzen, bei welchem es sich um ein unerwünschtes Programm handeln könnte. Für die Nutzung von Process Explorer und Process Viewer müssen Sie als Administrator angemeldet sein. Auf Ihrem Dienst-PC werden Sie aber wohl keine Administratorrechte haben, so dass sich die Existenz von Spionage-Tools wahrscheinlich nicht nachweisen lässt.

6. Kommunikation unterbrechen durch Desktop-Firewalls

Zur Erkennung von Keyloggern und Protokoll-Software, die Daten über das Internet verschicken, eignen sich Desktop-Firewalls optimal. Firewalls bieten zwar keinen generellen Schutz davor, dass Sie sich ein bösartiges Programm einfangen, blockieren aber die Kommunikationswege. Dieser Schutz greift auch dann, wenn Sie in der Firewall-Software das lokale Netzwerk als sichere Zone eingetragen haben.

Jedes Programm, das etwas nach draußen senden möchte und dazu Ports auf Basis von TCP/IP benutzt, muss die Firewall passieren. Das gilt auch in der umgekehrten Richtung, wenn beispielsweise eine Fernsteuerungs-Software auf Ihren PC angesetzt wird. Als Vorbeugemaßnahme vor heimlichen Bespitzelungen sollten Sie die Liste derjenigen Programme, denen Sie innerhalb der Fire-



Freigegebene Programme: Achten Sie darauf, nicht vorschnell einem Task mit vielversprechendem Namen den Netzwerkzugriff zu erlauben (Punkt 5)

wall eine Erlaubnis zur Datenkommunikation im lokalen Netzwerk oder über das Internet erteilt haben, von Zeit zu Zeit kontrollieren und alle Programmnamen aus der Befugnisliste löschen, deren Bedeutung Ihnen

nicht ganz klar ist. Handelt es sich dabei etwa um ein Mailprogramm, das Sie versehentlich entfernt haben, müssen Sie die Netzwerkkommunikation beim nächsten Programmstart wieder erlauben. ❌

Ausgesperrt: Virtueller PC als Hochsicherheitsumgebung

Eine technisch interessante Methode, sich vor PC-Bespitzelung zu schützen, sind virtuelle Umgebungen, etwa auf Basis von **VM-Ware Player** (www.vmware.com) oder **Virtual PC 2007** (auf CD und unter www.microsoft.com). Das Gastsystem ist dabei vom eigentlichen Betriebssystem getrennt und hat im besten Fall eine komplett andere Software-Struktur. Viren, die zwischen verschiedenen Betriebssystemen, etwa Windows und Linux, springen können, gibt es zwar, allerdings sind sie aufwendig zu erstellen und existieren derzeit nur als Beispielcode. Deswegen sollten Sie in der virtuellen Maschine eine Linux-Distribution einsetzen. Besonders einfach ausprobieren können Sie das Surfen in einer virtuellen Maschine mit **QEMU-Puppy Linux 2** (auf CD), das nicht einmal installiert werden muss. Deutlich mehr Komfort ermöglicht eine vollwertige Distribution wie **PC Linux OS** (www.pclinuxos.de): Das System bietet optisch und funktional einiges, ist aber dennoch relativ schlank. Dadurch ist die Distribution schnell wieder geladen und einsatzbereit. Die zusätzliche Ladezeit wiegt den enormen Sicherheitsvorteil auf alle Fälle auf.

Richten Sie in Ihrer Virtualisierungs-Software einen neuen PC ein, dann starten Sie PC Linux OS. Direkt auf dem Desktop befindet sich nach dem Booten eine Verknüpfung namens „Install PCLinuxOS“. Nach Eingabe des Root-Passworts „root“ rufen Sie damit einen Assistenten auf, der Sie durch die Installation führt.

Vor- und Nachteile der virtuellen Umgebung: Damit ist eine sichere Surf-Umgebung eingerichtet. Sollte auf dem Windows-PC ein Keylogger installiert sein, scheitert dieser an der Virtualisierungs-Software, da die virtuelle Umgebung sich vor den normalen Keyboard-Treiber einklinkt. Windows-Trojaner sind ebenfalls außer Gefecht gesetzt, da die unterschiedlichen Architekturen einen Übergriff verhindern.

VM-Ware und Virtual PC speichern die virtuelle Umgebung, wenn Sie das Fenster schließen und die entsprechende Rückfrage bestätigen. Wenn Sie anschließend die Umgebung erneut aufrufen, stellt die Software den letzten Zustand wieder her. Alternativ entscheiden Sie sich am Ende einer Sitzung, sämtliche Änderungen einfach zu verwerfen.



Sicher bleibt es unsicher

Die kommenden Monate bringen einige Herausforderungen für PC-Anwender. Welche schwerwiegenden Bedrohungen sind zu erwarten – und wie kann man sich dagegen wehren?

Von Gaby Salvisberg

Die Unsicherheit bei Anwendungen, Netzwerken und Betriebssystemen bleibt auch im laufenden Jahr bestehen. Welche Bedrohungen nehmen zu, welche ab? Und wie lassen sich die Fallen umgehen? Im Text finden Sie drei Icons. Rot: Wir erwarten eine Zunahme dieser Bedrohung. Gelb: Die Bedrohung wird sich kaum verändern. Grün: Die Gefahren nehmen eher ab.

1. Adware

 Dabei handelt es sich um Software-Komponenten in durch Werbung finanzierten Anwendungen. Solche Software

blendet etwa gelegentlich Werbebanner ein. Reine Adware gefährdet die Sicherheit nicht zwingend; trotzdem kann Adware Ihre Surf-gewohnheiten ausspionieren, was sie zur Spyware macht. Nach unseren Einschätzungen wird sich nicht viel verändern. Heute gibt es genügend Alternativen (Freeware, Open Source), um nicht zu Adware greifen zu müssen. Abhilfe: Lesen Sie die Lizenz- und Datenschutzbedingungen jeder angeblich kostenlosen Software genau. Mit Tools wie **Ad-Aware** (für Win 95/98/ME, NT 4, 2000, XP und Vista, auf  CD und unter www.lavasoft.de, 2,34 MB) können Sie Ad-

ware zudem beseitigen; nur läuft dann oft das Programm möglicherweise nicht mehr, das die Adware enthalten hat.

2. Backdoors

 Wie der Name („Hintertüren“) andeutet, eröffnet ein Backdoor-Trojaner ungebetenen Gästen einen Zugang zum PC. Meist pflanzt er dem PC auf diesem Weg weitere Schädlinge ein, schließt ihn via Internet an ein Bot-Netz an oder spioniert Daten aus. Backdoors können durch fast jede andere Art von Schädlingen ins System geraten, oft durch Würmer oder in gezielt versandten Mails, in denen etwa behauptet wird, die Beilage sei ein wichtiges Update.

3. Boot-Sektor-Viren

 Man steckt eine Diskette in einen infizierten PC, worauf auch sie zum Virenträger wird. Benutzt man die Disk wiederum im nächsten Computer, steckt sich dieser ebenfalls an. Auch wenn sich heute noch einzelne PCs von alten Disketten einen Schnupfen holen, ist dieses Virenkonzept Schnee von gestern. Die meisten Virens Scanner können Boot-Sektor-Viren entdecken. Stellen Sie sicher, dass das Scannen der Boot-Sektoren in Ihrem Antivirenprogramm eingeschaltet ist.

4. Bot-Netze

 Das Schaffen so genannter Bot-Netze ist heutzutage das hauptsächliche Bestreben eines Virenschreibers. Dabei schließt ein Angreifer unbemerkt von deren Besitzern infizierte PCs via Internet zu einem Netzwerk zusammen, das er fernsteuern kann. Benutzt wird das Bot-Netz dann für Spam und kriminelle Aktivitäten, wie Angriffe auf Firmenserver. Bot-Netze können sehr groß werden. Im Jahr 2005 hat die holländische Polizei ein Bot-Netz mit weltweit über 1,5 Millionen Rechnern entdeckt. Bisher ist dieser Rekord noch ungeschlagen.

5. Browser-Hijacker

 Es ist ärgerlich, wenn im Webbrowser plötzlich eine unerwünschte Webseite als Start- oder Suchseite eingetragen ist. Wird ein Browser durch einen eingeschleppten Schädling auf diese Weise entführt (englisch „hijacked“), lässt sich die Startseite ohne Eingriffe in die Innereien von Windows meist nicht mehr ändern. Von diesen Hijackern war bisher praktisch nur der Internet

Explorer betroffen. Da viele Leute auf alternative Browser (Firefox, Opera) umsteigen und weil der IE 7 besser geschützt ist, dürfte diese Erscheinung eher ab- als zunehmen.

6. Cyber-Erpressung

 Diese Art des Verbrechens wird gern unter dem Deckmantel der Anonymität begangen. Erpresser drohen beispielsweise Firmen, mithilfe eines Bot-Netzes ihre Server anzugreifen, siehe DDoS-Attacken. Auch im kleineren Rahmen wurden Erpressungsfälle gemeldet: Es gibt Würmer, die etwa alle Excel- oder Word- Dokumente auf der Festplatte des Opfers verschlüsseln. Will der Anwender seine Dateien zurückhaben, muss er den Gaunern Geld für ein Entschlüsselungs-Tool bezahlen. Laut Kaspersky Lab nahm Cyber-Kriminalität im vergangenen Jahr generell stark zu. Das wird sich auch 2007 kaum ändern. Abhilfe: Wer erpresst wird, meldet sich rasch bei der Polizei.

7. Dialer

 Vor lästigen Einwahlprogrammen, die sich übers Modem heimlich mit teuren Nummern verbinden, müssen sich immer weniger Anwender fürchten. Einerseits haben wir dies der zunehmenden Ablösung der Einwahlmodems durch Breitbandgeräte zu verdanken, andererseits auch den besseren Kontrollen der kostenpflichtigen Zugangsnummern. Siehe auch Handy-Dialer.

8. DDoS-Attacken

 Oft ein Werkzeug zur Cyber-Erpressung. Bei einer Denial of Service-Attacke (DoS) wird etwa ein Webserver so lange mit Mülldaten überflutet, bis unter der Last zusammenbricht. Werden die Kräfte mehrerer verschiedener Systeme für den Angriff auf einen Server gebündelt, spricht man von einer Distributed Denial of Service-Attacke. Weil die hierfür verwendeten Bot-Netze eher wachsen, gehen wir von einem zunehmenden Trend aus. Abhilfe: Als Anwender kann man nicht viel gegen DDoS-Attacken tun, außer den PC sauber zu halten, damit er nicht dafür missbraucht wird.

9. Fuzzing

 Eine auch „fuzz testing“ genannte Methode zum Aufspüren von Sicherheitslecks in Software. Dabei wird die zu prüfende Anwendung automatisch verschiede-

ndem Datenmüll ausgesetzt. Die Reaktionen darauf landen in einer Protokolldatei, die sehr häufig Hinweise auf Schwachstellen aufzeigt. So findet man Lücken oft viel schneller als durch manuelles Ausprobieren oder durchs Analysieren des Programmcodes. Laut den Experten von Symantec haben nun auch Schädlingsschreiber diese Methode für sich entdeckt. Durch Fuzzing aufgedeckte Lecks werden wahrscheinlich zunehmen. Das Problem betrifft die Software-Entwickler, die sehr schnell auf die gefundenen Lecks reagieren müssen.

10. Geldwäschejobs

 Die mit Cyber-Erpressungen, Phishing et cetera ergaunerten Gelder müssen natürlich gewaschen werden. Hierfür rekrutieren die Täter per Massenmails so genannte Finanzagenten, die gegen ein Entgelt ihre Bankkonten für den Transfer des Geldes zur Verfügung stellen. Dies gilt als Geldwäsche und ist strafbar. Oft hängt am Ende aber nur der Finanzagent in den Maschen des Gesetzes, während die Cyber-Kriminellen davonkommen.

11. Handy-Dialer

 An PCs gibts immer weniger Modems, die von Dialern missbraucht werden könnten. Bleibt noch das Handy: Im September 2006 wurde von Kaspersky ein Handy-Dialer auf Java-Basis entdeckt, der auf verschiedenen Geräten läuft. Er verschickte automatisch mehrere SMS an eine kostenpflichtige Nummer (3 US-Dollar pro Nachricht). Klar wäre es denkbar, dass solche Schädlinge in nächster Zeit Schule machen. Doch dem stehen die Behörden und Handy-Netzbetreiber im Weg: Sie sperren Nummern von böswilligen Anbietern. Zudem wurden in den meisten Ländern die Kontrollen und Hürden für die Registrierung solcher Nummern erhöht. Der eine oder andere Abzocker wird es vielleicht wieder mal versuchen; aber die Ge-

Überblick Die Angstmacher

Inhalt	Seite
Gefahren 1-8	116
Risiken 9-14	117
Bedrohungen 15-22	118
Angriffe 23-27	119

fahr war letztes Jahr schon relativ gering und wird nächstes Jahr kaum wesentlich steigen.

12. Handy- & Smartphone-Würmer

 Mobiltelefone, Organizer und Kombinationen davon (Smartphones) sind nicht vor Schädlingen gefeit. Die Weiterverbreitung von einem Handy oder Smartphone zum nächsten erfolgt meist automatisch via Bluetooth oder in per MMS verschickten Dateien. Bekannt sind Würmer und Trojanische Pferde für Smartphones mit Symbian als Betriebssystem. Geräte mit Windows Mobile oder Palm OS sind bisher kaum davon betroffen. Wer sein Handy oder Smartphone per USB oder Bluetooth mit dem Desktop-PC verbindet, sollte aufpassen: Es gibt Handy-Schädlinge, die sich beim Datenaustausch vom Smartphone auf den PC übertragen können – und umgekehrt. Abhilfe: Nehmen Sie via MMS oder Bluetooth ankommende Dateien nicht an. Bluetooth-Empfang



Browser-Hijacker: Durch Verbesserungen im neuen Internet Explorer 7 nehmen diese Attacken deutlich ab (Punkt 5)



Vorsicht: Bei jeder noch so verlockenden Meldung drücken Sie auf „Nein“ oder „Ablehnen“ (Punkt 12)

nur im konkreten Bedarfsfall aktivieren – und auch dann nur im für andere Nutzer „unsichtbaren“ Modus.

13. Instant-Messenger-Spam

Instant-Messenger von ICQ, AOL, MSN und Yahoo bleiben nicht von Spammern verschont. Stellen Sie das betroffene Programm so ein, dass neue Kontakte erst um Autorisierung bitten müssen, bevor sie Ihnen Nachrichten schicken können.

14. Instant-Messenger-Würmer

Von infizierten PCs aus verschickt ein solcher Wurm automatisch Nachrichten an die Personen auf der im Instant Mes-

senger gefundenen Kontaktliste. Für den Empfänger sehen die Nachrichten aus, als kämen sie vom Bekannten persönlich.

15. Keylogger/Passwortspione

Ein Keylogger fängt die vom Benutzer auf seinem PC getippten Eingaben ab. Wer jemandem einen Keylogger unterjubelt, hat es weniger auf den Inhalt der Mails oder Briefe abgesehen, sondern auf geheime Zugangsdaten und Passwörter, etwa von Online-Spielen, Mailkonten und Online-Banking-Diensten. Einen anderen Ansatz verfolgen die Passwortspione: Sie versuchen, die bereits gespeicherten Passwörter aus dem befallenen System auszulesen.

16. Mailwürmer

Diese Schädlinge verbreiten sich von infizierten PCs aus, indem sie sich selbst automatisch an alle gefundenen Adressen mailen. Zwar werden viel weniger Exemplare verschickt, es gibt aber mehr Varianten pro Wurmtyp. Dieser Umstand hält die Antivirenlabors auf Trab, denn oft sorgen nur geringfügige Änderungen im Wurmcode dafür, dass wieder eine neue Signatur für den Virens Scanner nötig ist.

17. Nigeria- und Lotterie-Abzocke

In Nigeria nahm diese Masche vor Jahren (damals noch in Briefform) ihren Anfang, weshalb man sie heute noch so

bezeichnet. Die Gauner unterbreiten dem potenziellen Opfer einen Geschäftsvorschlag. Angeblich wolle man eine große Geldsumme außer Landes bringen, wofür man vom Empfänger etwas Hilfe benötige. Als Entgelt für diese Hilfe winkt eine hohe Provision.

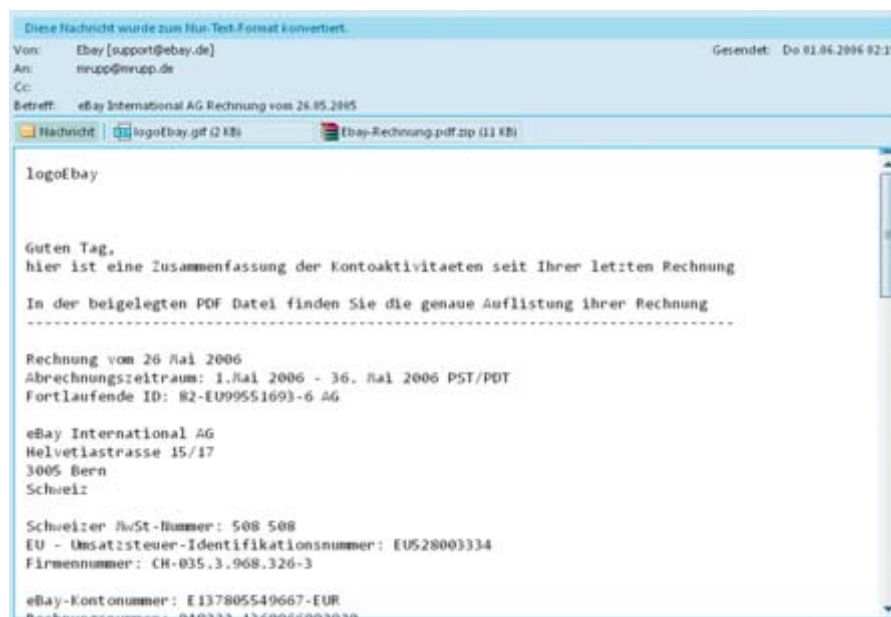
In eine ähnliche Kerbe hauen die Lotterie-Abzocker. Man habe in einer Lotterie den Hauptgewinn gezogen und solle sich doch bitte melden. Wer auf eine der Maschen reinfällt, wird in beiden Fällen gebeten, einen Vorschuss zu leisten, weil ja Transaktionsgebühren anfallen. Vom Vorschuss sieht man natürlich nie wieder was, geschweige denn vom versprochenen Gewinn. Allzu stark wird die Masche nicht mehr zunehmen. Die Kriminellen müssen immer mehr Leute mit ihren Mails belästigen, bis sie endlich einen Dummen finden.

18. Office-Schädlinge

In Microsoft Office wurden letztes Jahr zahlreiche Sicherheitslücken gefunden, die von Microsoft größtenteils gestopft wurden. Die Lücken steckten fast alle samt in der OLE-Funktion, die es erlaubt, Inhalte von anderen Dateien in ein Office-Dokument einzubetten. Laut Alexander Gostev, Virenspezialist bei Kaspersky Lab, ist kein Ende in Sicht. In seinen Augen hat Microsoft seinen Job nur unvollständig erledigt. Er schrieb in einem Bericht: „Man hätte sich nicht nur auf das Stopfen der jeweils gefundenen Sicherheitslücken beschränken dürfen; Microsoft hätte stattdessen die gesamte OLE-Technologie überarbeiten müssen.“ Die Gesamtzahl der potenziell angreifbaren Stellen in OLE-Objekten betrage über hundert. Schädlingsschreiber werden besonders auch das neue Office 2007 nach verwundbaren Stellen abklopfen, was zu einer Zunahme von Schädlingen führen wird.

19. Phishing

Darunter versteht man das betrügerische Aushorchen von Passwörtern aller Art, indem das Opfer per Mail auf eine gefälschte Webseite gelockt wird. In den neuen Versionen sowohl von Firefox als auch des Internet Explorer ist ein Phishing-Filter eingebaut. Nutzen Sie ihn, aber verlassen Sie sich nicht ausschließlich darauf. Abhilfe: Loggen Sie sich niemals über einen per Mail erhaltenen Link in Ihre Online-Konten ein. Verwenden Sie zum Mailen am



Soll verleiten: Je schockierender die Nachricht, desto eher klicken die Anwender auf den Link, der auf eine EXE-Datei führt; in diesem Fall ein Passwortspion (Punkt 15)

besten der Thunderbird-Mail-Client. Neben einem trainierbaren Spam-Filter (Phishing ist Spam) gibt es auch eine Funktion, die vor Mails warnt, die etwas phishig riechen.

20. Polymorphe Malware

Das sind Schädlinge, die sich selbst laufend verändern und so den Virenschannern ihre Erkennung erschweren. Laut Auskünften von Symantec erwartet man in dieser Kategorie eine Zunahme. Die Schadensroutinen selbst ändern sich jedoch nicht: Einpflanzen von Backdoors, Diebstahl von Daten und so weiter.

21. Rootkits

Wer einen Backdoor auf einem PC verstecken will, verpackt ihn in ein Rootkit. So lassen sich Schädlinge sehr tief im Betriebssystem verbergen. Lange Zeit haben sich die Virenschannern an diesen Schädlingstarnkappen die Zähne ausgebeissen. Inzwischen gibt es einige Produkte, die in der Lage sind, sie aufzuspüren. Dennoch werden es die Schädlingsschreiber nicht dabei bewenden lassen und weiterhin zu Rootkit-ähnlichen Technologien greifen.

22. Spam

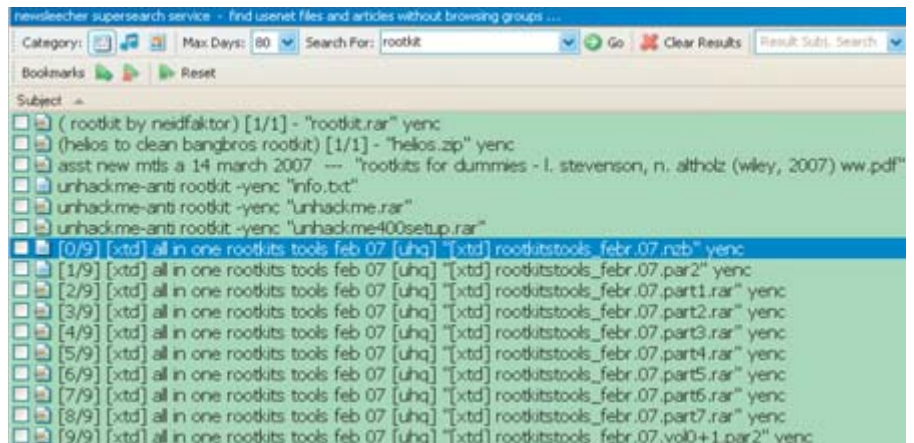
Das nervigste Übel im PC-Alltag ist die Flut der unerwünschten Werbe-mails. Für den Versand von Spam werden heute in mindestens 80 Prozent der Fälle sogenannte Zombies verwendet, also PCs, die zu einem Bot-Netz gehören. Im Januar 2006 waren etwa 60 Prozent aller verschickten Mails Spam. Heute geht man von über 90 Prozent aus. Auch wenn immer mehr Länder gesetzliche Maßnahmen gegen Spammer ergreifen, ist die Tendenz weiter steigend. Abhilfe: Spam-Filter einsetzen, etwa jenen des Providers oder des Mailers. Es gibt nur eines, was das Übel an der Wurzel packt: Nichts bei einem Spammer kaufen!

23. Spyware

Solche Programme gehören zu den Trojanischen Pferden. Sie spionieren Nutzerdaten aus und übermitteln sie im Hintergrund online an den Hersteller.

24. Trojanische Pferde

Das größte Wachstum in allen Schädlingsskategorien ist laut Kaspersky Lab bei den Trojanischen Pferden zu verzeichnen. Das sind unscheinbare Pro-



Laden und unterschreiben: Fertig einsatzbereite Rootkits lassen sich von jedermann aus Newsgroups herunterladen und verwenden (Punkt 21)

gramme, die teils mit Würmern und teils durch Sicherheitslücken eingeschmuggelt werden. Zu den Trojanern zählen auch Backdoors, Keylogger, Rootkits und Spyware.

25. Viren

Diese altbekannten Zeitgenossen identifizieren bestehende Dateien und hoffen darauf, dass der Benutzer sie unbemerkt per Mail, auf CD oder Diskette weitergibt, wodurch sich der Virus auf einem neuen Rechner einnisten und natürlich weiter verbreiten kann. Neue Viren im klassischen Sinn werden aktuell nur noch wenige gesichtet. Die Führung bei den sich selbst verbreitenden Schadprogrammen haben längst die Würmer übernommen.

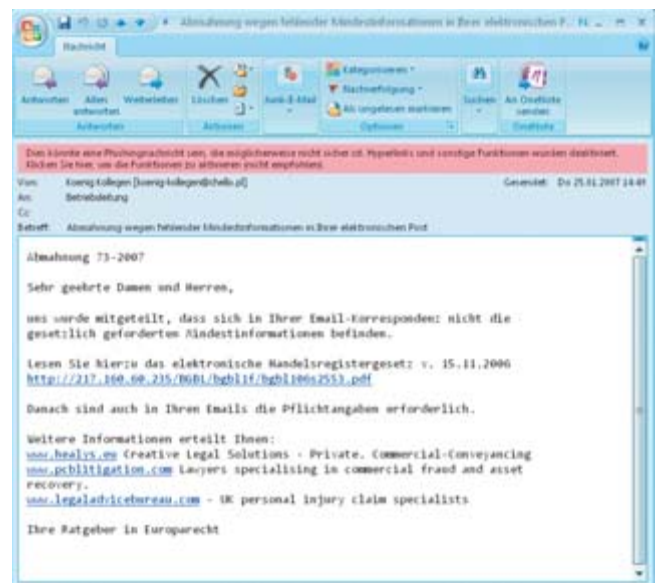
26. Zero-Day-Attacken

Seit 2006 zeigt sich laut Kaspersky eine Anpassung der Cyber-Kriminellen an die Microsoft-Update-Intervalle. Neue Sicherheitslecks werden in der Hackerszene nicht sofort, sondern direkt nach dem monatlichen Patch-Day veröffentlicht. So haben die Virenschreiber fast einen ganzen Monat Zeit, entsprechende Schad-Software zu entwickeln. Zeitplanung wird beim Verbreiten von Schädlingen ohnehin große-

geschrieben. Große Spam- oder Wurmwellen brechen bevorzugt in der Nacht von Sonntag auf Montag los. So bleibt den Fachleuten wenig Zeit für eine Reaktion – am Montagmorgen klicken dann tausende auf den falschen Link.

27. Web-2.0-Angriffe

Mit Web 2.0 verschmilzt der PC mit dem Internet. Anwendungen werden damit nicht mehr lokal auf der Festplatte installiert, sondern direkt via Web genutzt. Die Schädlingsschreiber werden versuchen, die Web-2.0-Anwendungen zu attackieren, um entweder private Daten zu stehlen oder um den Anwendern weiteren Schadcode unterzubeln. Bisher zwar noch kaum gesehen, aber zu erwarten.



Werbeblut: Spam-Mails sind lästig. Außerdem besteht die Gefahr, in der Flut eine Phishing-Mail zu übersehen (Punkt 22)



Sicherheits-Mythen

Hartnäckig halten sich eine Reihe von Behauptungen rund ums Thema PC-Sicherheit, an denen bei genauem Hinsehen nicht viel dran ist. Wir klären auf und sagen, was Sache ist.

Von **Christoph Metzger**

Das größte Sicherheitsproblem im Bereich von PC-Technik ist der Anwender, der durch Leichtsinns und Unwissenheit Angreifern die Türen öffnet. Einen Teil dazu tragen Behauptungen bei, die seit langem kursieren, sich jedoch bei genauem Hinsehen als Fehlinformation entpuppen.

1. Ein paar offene Ports schaden nicht weiter

Trotz einer gewissen Anzahl offener Ports ist mein Rechner sicher. Teilweise falsch!

Wer offene Ports im Internet anbietet, läuft immer Gefahr, dass diese kompromittiert werden. Damit ein Programm überhaupt mit dem Internet kommunizieren kann, muss es

auf Ihrem Rechner eine bestimmte Tür öffnen – einen Port. Wenn Anwendungen oder Systemdienste bestimmte Ports offen halten, kann der Rechner über diese Ports Anfragen von Clients entgegennehmen, verarbeiten und beantworten.

Eine Gefahr stellen offene Ports allerdings nur dar, wenn das Programm, das dort antwortet, fehlerhaft ist. Im eher harmlosen Fall stürzt die Software einfach ab. Im schlimmsten Fall erlaubt es dem Anfrager, Schädlinge einzuschleusen oder gar vollständig auf das System zuzugreifen. Sie sollten deswegen dafür sorgen, dass nur wirklich notwendige Ports offen sind. Eine einfache Grundregel: Es ist grundsätzlich sicherer, Ports zu schlie-

ßen, noch bevor eine Desktop-Firewall an dieser Stelle etwas zu tun bekommt.

2. Rootkits – die findet mein Virens Scanner doch

Antivirenprogramme verhindern, dass sich Rootkits auf dem Rechner einnisten können. Falsch!

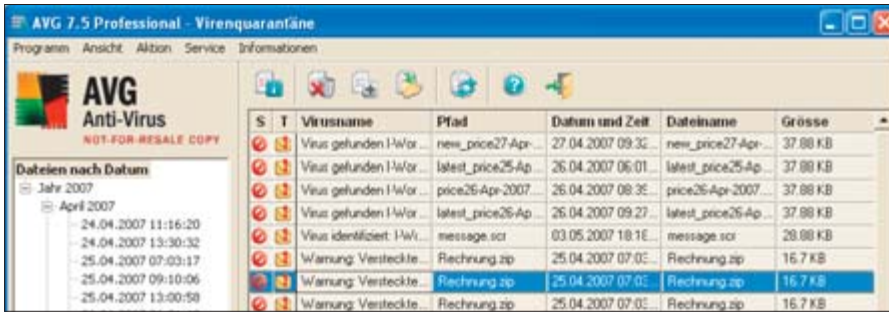
System-Stealth-Techniken (Stealthing wörtlich: verbergen, verschleiern) breiten sich bei Software zu bösartigen Zwecken stark aus. Stealthing-Verfahren kommen vor allem bei Rootkits zum Einsatz und verschleiern das Vorhandensein einer Datei in einem System durch Abfangen der entsprechenden API-Funktionen des Betriebssystems und durch das Überlisten von Explorer-ähnlichen Programmen. Ziel des Ganzen: Der tatsächliche Inhalt eines Dateidatensatzes soll dem Anwender nicht angezeigt werden. Auch der Taskmanager wird dabei so manipuliert, dass er es einer bösartigen Anwendung ermöglicht, ihr Vorhandensein im Arbeitsspeicher und in der Liste der ausgeführten Prozesse zu verbergen. Der Großteil heutiger Antivirenprogramme ist noch nicht in der Lage, Rootkits zuverlässig zu erkennen und entsprechend zu reagieren, so dass die meisten komplexen Schadprogramme mit so ausgefeilten Methoden vermutlich unentdeckt bleiben.

3. Dateien nach Malware-Funden bereinigen lassen

Die Hersteller von Virenabwehrprogrammen lassen den Anwender im Glauben, eine mit Viren oder Würmern infizierte Datei ließe sich nach einem Fund per Mausklick bereinigen. Falsch!

Nachdem die Antiviren-Software einen Virus entdeckt hat, ist der nächste Schritt dessen Entfernung. Das kann eine ziemliche Herausforderung sein, da die meisten Viren dazu neigen, sich zu vervielfältigen, zu mutieren und zusätzliche schädliche Programmteile online nachzuladen. Ein Wurm oder Virus kann an zahlreichen Speicherorten vorhanden sein, mehrere Viren können nebeneinander existieren und Komponenten austauschen, um der Entfernung zu entgehen, indem sie sich gegenseitig als Backup-Punkte dienen.

Angesichts der Komplexität des Problems ist es nicht verwunderlich, dass Antivirenprogramme es oft nicht schaffen, gefundene Malware vollständig auszuschließen. Die Auf-



Virenquarantäne: Reparaturversuche bei verseuchten Dateien scheitern in vielen Fällen. Zurück bleiben unbrauchbare Dokumente und defekte Programme (Punkt 3)

gabe, feindlichen Code aus einer Datei zu entfernen und dabei gleichzeitig die ursprüngliche Version zu erhalten, erweist sich insoweit als knifflig, und Antivirenprogramme löschen oft mehr als unbedingt nötig und hinterlassen so ein Programm oder eine Komponente, die nicht funktionsfähig oder völlig nutzlos ist.

4. Anonym surfen blockiert Rückschlussmöglichkeiten

Wer mit einer Software-Tarnkappe im Internet surft, kann anstellen, was er möchte, ohne dass seine Identität herausgefunden werden kann. Falsch!

Durch den Einsatz von Anonymisierungs-Diensten wie JAP (auf CD) ist es möglich, Ihre Online-Aktivitäten zu verschleiern und eine Verfolgung Ihrer Surf-Gewohnheiten zu erschweren. Sobald Sie eine Website unter Zwischenschaltung eines Anonymisierers besuchen, wird statt Ihrer echten IP-Adresse im Protokoll des Servers eine Tarnadresse des zur Verschleierung verwendeten Proxy-Dienstes gespeichert. Je mehr Server es sind und je häufiger Ihre IP-Adresse wechselt, desto besser die Tarnung. Anhand der Proxy-Protokolle und den Aufzeichnungen Ihres Providers können Ermittlungsbehörden dennoch Ihre Identität ermitteln und nachvollziehen, welche Seiten Sie besucht haben. Ein aufwendiger Kreuzvergleich ist nur bei besonders schweren Vergehen und in der Regel nur nach einer richterlichen Anordnung möglich, doch Sie selbst können ja nicht nachvollziehen, wann und wer Ihre Daten auswertet.

5. Microsoft durchleuchtet Windows-Anwender

Windows sendet heimlich Seriennummern, Anwenderdaten und persönliche Informationen an Microsoft. Teilweise falsch!

Seit Windows XP mit der eingebauten Zwangsaktivierung auf dem Markt ist, gibt es immer wieder Gerüchte über Microsoft-Spionage. Die schlimmsten Spekulationen befürchten das Senden persönlicher Informationen wie Passwörter, Systemeinstellungen, Mails oder Informationen über installierte und möglicherweise raubkopierte Software direkt an Microsoft. Technisch ist eine Spionage möglich. Die Phone-Home-Aktivitäten von Windows sind aber nach derzeitigem Kenntnisstand weitgehend harmlos. Die mit den Microsoft-Servern ausgetauschten Infos erfolgen in den allermeisten Fällen im Klartext und sind damit leicht nachvollziehbar. Das lässt sich mit einem Sniffer wie Whireshark nachprüfen, denn fast alle Daten werden im Klartext übertragen, eine Verschlüsselung findet so gut wie nie statt. Grundsätzlich nicht auszuschließen ist allerdings, dass Microsoft in einer Version des Windows-Update-Tools die bei Online-Updates abgefragten Daten ausweitet.

Überblick Halbwahrheiten

Inhalt	Seite
1. Offene Ports schaden nicht	120
2. Rootkits finden auch Virens Scanner	120
3. Dateien lassen sich bereinigen	120
4. Anonym blockiert Rückschlüsse	121
5. Microsoft durchleuchtet Anwender	121
6. Firewalls verhindern Attacken	121
7. Firefox ist rundum sicher	122
8. Alternativpfade schützen	122
9. Wenige Stunden entscheiden	122
Kasten	
Schnüffel-Tools nur aus dem Untergrund?	121

6. Desktop Firewalls verhindern Online-Attacken

Wer ein Firewall-Tool auf seinem PC installiert hat, ist immun gegen Angriffe aus dem Internet. Falsch!

Immer mehr Programme greifen auf das Internet zu. Desktop-Firewalls haben also immer mehr zu kontrollieren. Es ist paradox: Anwender fordern ständig mehr Sicherheit. Gleichzeitig nehmen sie in Kauf, dass sich auf den Festplatten immer mehr Firmen tummeln. Die werten munter private Daten aus, bieten Update-Services an oder installieren im schlimmsten Fall Hacker-Software. Das alles ist die Folge von Kopierschutzmanie, Web 2.0 und anderen Verschmelzungen zwischen PC und Internet. Bald schon mutiert jeder PC zum Webserver.

Schnüffel-Tools: Nur aus dem Untergrund?

Hacker und Cracker bringen Spyware und Trojaner in Umlauf. Teilweise falsch!

Der wohl überwiegende Teil der in Umlauf befindlichen Spionageprogramme stammt aus der Hacker- und Cracker-Szene. Darüber hinaus gibt es auch andere Urheber. Unter dem Stichwort Bundestrojaner setzt der Staat Spionage-Software gezielt zur Bepitzelung verdächtiger Personen ein. Bereits seit 2005 spähen Geheimdienste heimlich via Internet die Computer von Verdächtigen aus. Das hat ein Sprecher des Kanzleramts vor dem Bundestags-Innenausschuss bestätigt. Auch das BKA soll künftig einen Trojaner verwenden dürfen, um unerkannt Datenspionage durchzuführen. Installiert werden soll das Tool bei Verdächtigen mit Hilfe der Internet-Provider – es klinkt sich einfach in einen Download ein. Experten halten einen solchen heimlichen Spitzeldienst bei der gegenwärtigen Rechtslage für unzulässig, ja für verfassungsrechtlich bedenklich.

Auch in Firmen werden Überwachungs-Tools eingesetzt, um Mitarbeiter zu kontrollieren – oft auf äußerst wackeliger rechtlicher Grundlage. Die eingesetzten Programme zeichnen automatisch sämtliche PC-Aktivitäten auf. So werden beispielsweise regelmäßig der Windows-Bildschirm abfotografiert und die Adressen aller besuchten Websites gespeichert.



Browser-Empfehlung: Sicherer als der IE ist Firefox allemal, dennoch plagen auch den Open-Source-Browser Bugs (Punkt 7)

Von dieser Entwicklung sind aktuelle Desktop-Firewalls völlig überfordert. Firewall-Programme sind zwar für die Sicherheit enorm wichtig. Sie blockieren Zugriffe von außen auf PC oder Netzwerk. Sie kontrollieren aber auch den ausgehenden Datenverkehr und wollen so trotz aller Vorsichtsmaßnahmen eingeschmuggelten Schädlingen das Leben schwer machen.

Die Masse an Daten, die zwischen PCs und dem Internet ausgetauscht wird, ist allerdings nicht mehr zuverlässig zu überwachen. Meldungen der Sicherheits-Software verwirren die Anwender höchstens: Darf das Programm Svchost.EXE auf das Internet zugreifen? Ja oder nein? Es braucht jetzt neue technische Konzepte, die solche Entscheidungen zuverlässig übernehmen – damit verunsicherte Anwender ihren PC nicht versehentlich zur Freibeuterzone erklären.

7. Firefox ist ein rundum sicherer Browser

Der Internet Explorer ist eine der größten Sicherheitslücken in Windows – Firefox dagegen ist sicher. Falsch!

Verheerende Sicherheitsmängel in Browsern sind Surfer vor allem vom Internet Explorer



Stunden zählen: Manche Hersteller lassen sich Zeit mit Online-Updates (Punkt 9)

plorer gewohnt. Seit Jahren jagt ein wichtiger Patch den anderen. In puncto Sicherheit besser als beim Internet Explorer sieht es bei Firefox aus: Er ist gegen viele Attacken immun. Und trotzdem ist es an der Zeit, sich von einem gefährlichen Vorurteil zu verabschieden: Wer mit Firefox surft, ist nicht automatisch sicher vor allen Online-Gefahren.

Firefox ist nicht eng mit dem Betriebssystem

verzahnt wie der Internet Explorer. Der IE ist zwar eine eigenständige Software, kann aber dennoch einen starken Einfluss auf Windows nehmen. Dafür sorgen Active-X-Controls, das Zonenmodell und Browser Helper Objects, die den Internet Explorer erweitern. Fehler im Microsoft-Browser haben somit häufig auch weitreichende Auswirkungen auf die Systemsicherheit.

Doch auch in Firefox schlummern aller Wahrscheinlichkeit nach etliche Gefahren in Form von Programmierfehlern, zudem ist der Browser erweiterbar. Obwohl der Quellcode für jeden einsehbar ist, enthalten die Codezeilen wie jede Software Mängel, die erst nach der Veröffentlichung der jeweiligen Version entdeckt werden. Dass in der Vergangenheit immer wieder auch schwerwiegende Sicherheitslecks der Risikostufe „hoch“ in Firefox gefunden wurden, zeigt ein Blick auf die Bugliste. Als einer der Garanten dafür, dass Firefox-Anwender in der Vergangenheit weniger häufig Opfer von Internet-Attacken wurden, galt die vergleichsweise geringe Verbreitung des Browsers. Doch mit zunehmender Popularität ist Firefox ein lohnendes Ziel für Hacker.

Anwender profitieren aber bei Firefox von der offenen Kommunikation der Open-Source-Gemeinde. Die Entwickler dokumentieren alle Fehler auf der Mozilla-Website (www.mozilla.org). In der Regel erschien bislang bereits kurz nach der Entdeckung eines Sicherheitslecks eine neue Browser-Version, die den Fehler behob. Sie müssen also nicht auf den monatlichen Patchday von Microsoft warten, um eine Sicherheitslücke zu schließen.

8. PC mit Alternativpfaden sicher einrichten

Wenn Sie bei der Installation von Software den Standardpfad ändern, sind Malware-Angriffe unmöglich. Falsch!

Installieren Sie wenn möglich das Betriebssystem und sämtliche Anwendungen nicht in die standardmäßig vorgegebenen Pfade, sondern geben Sie benutzerdefinierte Speicherorte an. Ziel ist es dabei, einige relevante Standardvoreinstellungen so zu verändern, dass Schädlingsprogramme, die auf ein standardisiertes Betriebssystem vertrauen, keine Angriffsfläche mehr finden. Tatsache ist: Die Einnistung von Trojanern, Würmern und Viren können Sie durch diesen Trick immerhin erschweren, jedoch keineswegs verhindern. Für Malware-Programmierer ist es nämlich ein Leichtes, statt eines festen Pfads die Angabe zum tatsächlichen Speicherpfad aus der Registry auszulesen. Zudem verlangen manche älteren Software-Add-ons Standardpfade. Ansonsten verweigert die Zusätze ihren Dienst.

9. Der Kampf wird in wenigen Stunden entschieden

Ohne Antiviren-Software geht es heute nicht mehr. Wer den Virenschanner täglich aktualisiert, dem können neue Schädlinge nichts anhaben. Falsch!

So gut wie alle Virenschanner und Anti-Spyware-Tools lassen sich über das Internet auf den neuesten Stand bringen. Klar – ein Malware-Scanner mit seit Wochen nicht mehr aktualisierter Suchdatenbank kann gerade erst in Umlauf gebrachte Schädlinge nicht erkennen und macht das Abwehrprogramm dadurch wirkungslos.

Damit Sie umgehend ein Update für Ihre Antiviren-Software erhalten, wenn es verfügbar ist, müssen Sie die Software entsprechend konfigurieren. Eine gute Lösung ist eine Einstellung, die immer dann nach Updates sucht, wenn Sie online gehen. Doch die Hersteller von Virenabwehrprogrammen reagieren unterschiedlich schnell auf neue Gefahren. Unsere Tests in der Vergangenheit belegen: Wirklich schnell ist kein Anbieter. Die Spitzenreiter unter den Herstellern liefern aber immerhin im Schnitt innerhalb der ersten vier Stunden nach dem Bekanntwerden eines neuen Schädlings die nötigen Signaturen. Andere Hersteller reagieren teilweise mit wesentlich größerer Verzögerung – so kann es zu Infektionen kommen. ☒

Impressum

Redaktion

Lyonel-Feininger-Straße 26, 80807 München,
leserbrief@pcwelt.de

Chefredakteur: Andreas Perband (ap)
(verantwortlich, Anschrift der Redaktion)

Stellvertreter des Chefredakteurs: Wolfgang Koser (wk)

Stellvertretender Chefredakteur:

Dr. Hermann Apfelböck (ha)

Chef vom Dienst: Andrea Kirchmeier (ak)

Koordination Sonderhefte: Tom Dassel (td)

Redaktion: Dr. Hermann Apfelböck (ha), Arne Arnold (afa),
Andreas Kroschel (akr), Tobias Weidemann (tw)

Freie Mitarbeiter Redaktion: Tristan Bestle, Martin Danhof,
Sebastian Deichsbach, Klara Gehmach, Simone Gissler, Tim
Kaufmann, Margrit Kuther, Peter-Uwe Lechner, Lukas Merten,
Christoph Metzger, Johannes Richard, Gabi Salvisberg, Ramon
Schwenk, Jan-Dirk Skippoe, Markus Weber, Claudius Wirt,
Sascha Zäch

Freie Mitarbeiter Layout: Alex Dankesreiter

Freie Mitarbeiter Schlussredaktion: Andrea Röder

Heft-CD/DVD: Bettina Künnast (Leitung/bek), Michael Braun

Redaktionsassistent: Ursula Istavrinis (Leitung),

Heike Meironik, Thamar Thomas-Isbrücker, Christa Vetter

Koordination www.pcwelt.de: Stefan Willeke (Leitung/sw)

DTP-Produktion/Disposition: Andreas Förth (leitend)

DTP-Layout: Bianca Aumeyer, Anton Paunert

Design: h2Design.de

Titelgrafik: UweBeyer

Bildnachweis: Titel-Illustration: Mauritius Images.

Sofern nicht anders angegeben: Anbieter

Copyright: Das Urheberrecht für angenommene und veröffentlichte Manuskripte liegt bei der IDG Magazine Media GmbH. Eine Verwertung der urheberrechtlich geschützten Beiträge und Abbildungen, insbesondere durch Vervielfältigung und/oder Verbreitung, ist ohne vorherige schriftliche Zustimmung des Verlages unzulässig und strafbar, soweit sich aus dem Urheberrechtsgesetz nichts anderes ergibt. Eine Einspeicherung und/oder Verarbeitung der auch in elektronischer Form vertriebenen Beiträge in Datensysteme ist ohne Zustimmung des Verlages unzulässig.

Anzeigenabteilung

Tel. 089/36086-210, Fax 089/36086-263

E-Mail: media@pcwelt.de

Anzeigenleitung (Associate Publisher):

Christoph Burkhart (-294) (verantwortlich für Anzeigen und für die Vorstellung der New-Media-Inhalte im „Promotion“-Teil der PC-WELT und auf CD/DVD, Anschrift des Verlages)

Anzeigenverkaufsleitung IT:

Uta Kruse, PLZ 4, 5 (-355)

Mediaberatung Markenartikel:

Julia Wursthorn (-219)

Key Account Manager Print, CD/DVD:

PLZ 0, 1, 2, 8, 9: Bettina Schwarz (-132);

PLZ 3, 6, 7: Thomas Ströhlein (-188)

Junior Mediaberater: Christine Thonhauser (-293)

Anzeigenverkaufsleitung Ausland: Iris Haug (-854)

Anzeigenleitung Online: Petra Sesser (-516)

Marketing: Karin Hecker (-617)

Leitung Marktforschung: Frank Heublein (-785)

E-Commerce & Syndication: Andreas Koschinsky (-644)

Leitung Anzeigendisposition: Rudolf Schuster (-135)

Anzeigendisposition: Michael Steinbrückner

(-291, Fax -99291), Mail: msteinbrueckner@idgcom.de

Digitale Anzeigenannahme: Andreas Frenzel, leitend (-239),
Manfred Aumaier (-602)

Datentransfer: ISDN: 089/208070 und 089/36086-493;

FTP: www.idgverlag.de/dispoenter; Mail (max. 20 MB):

AnzeigendispoPrint@pcwelt.de

Anzeigenpreise: Es gilt die Anzeigenpreisliste 24 (1.10.2006).

Bankverbindungen:

Deutsche Bank AG, Konto 6662266, BLZ 700 700 10;

Postbank München, Konto 220 977-800, BLZ 700 100 80

Anschrift für Anzeigen: siehe Anschrift des Verlages

Erfüllungsort, Gerichtsstand: München

IGS Anzeigenverkaufsleitung für ausländische

Publikationen: Tina Ölschlager (-116)

Verlagsrepräsentanten für Anzeigen

Frankreich: F. Bonnin, 5 Rue Chantecoq, 92808 Puteaux, Tel.:

0033-1-4197-0, Fax 0033-1-4197-6202. NL: Florence Schmit,

Richard Holkade 8, 2033 Haarlem, Tel.: 0031-23-5461090.

Großbritannien: Shane Hannam, 29/31 Kingston Road,

GB-Staines, Middlesex TW 18 4QG, Tel.: 0044-1-784210210. USA

East: Chip Zaborowski, 500 Old Connecticut Path, P.O. Box 9377,

Framingham, MA 01701-9377, Tel.: 001-508-87907 00. USA

West: Larry Arthur, 501 Second Street, S. 114, San Francisco,

CA 94107, Tel.: 001-415-2434141. Taiwan: The Infopro Group,

Sophia Yu, 8F, 131 Sec 3 Nanking E Road, Tel.: 00886-2-2715-

3000. Japan: Noriko Nozaki, 8th Floor 3-4-5, Hongo Bunkyo-

Ku, Tokio 113-0033, Japan, Tel. 0081-3-5800-4851. Singapur:

J. Yu, No. 80 Marine Parade Road, #17-01A Parkway Parade,

S-449269, Tel.: 0065-3458383. Hongkong: V. Chan, S.1707,

K. Wah Centre, 191 North Point, Tel.: 00852-28613238. Korea:

C.H. Park, Rm. 1806/7, Golden Tower 191, 2-ka, Choongjungro,

Seodaemun-ku, Seoul, Tel.: 0082-2364-4182/3

Vertrieb

Gesamtvertriebsleitung: Josef Kreitmair (-243)

Vertriebsassistent: Melanie Stahl (-738)

Leitung Vertriebsmarketing: Matthias Weber (-154)

Marketingkoordination: Stefanie Kusseler (-451)

Junior Specialist Online: Ines Pariente (-506)

Vertrieb Handelsauflage: MZV

Moderner Zeitschriften Vertrieb GmbH,

Breslauer Straße 5, 85386 Eching,

Tel. 089/31906-0, Fax 089/31906-113,

E-Mail: mzv@mvz.de, Internet: www.mzv.de

Produktion: Heinz Zimmermann (Leitung)

Druck: Mayr Miesbach GmbH · Druck · Medien · Verlag

Am Windfeld 15, 83714 Miesbach, Tel. 08025/294-267

Kundenservice: Abonnements, Archivhefte, Sonderhefte,
Umtausch defekter CDs/DVDs: PC-WELT-Kundenservice
Postfach 810580, 70522 Stuttgart, Tel. 0711/7252-277, Fax -377,
Schweiz: Tel. 071/3140615, Österreich: Tel. 01/2195560,
Mail: shop@pcwelt.de

Haftung: Eine Haftung für die Richtigkeit der Beiträge
können Redaktion und Verlag trotz sorgfältiger Prüfung nicht
übernehmen. Die Veröffentlichungen in der PC-WELT erfolgen
ohne Berücksichtigung eines eventuellen Patentschutzes.
Auch werden Warennamen ohne Gewährleistung einer freien
Verwendung benützt.

Copyright: IDG Magazine Media GmbH,
Lyonel-Feininger-Straße 26, 80807 München,
Tel. 089/36086-0, Fax 089/36086-501

Verlag

IDG Magazine Media GmbH,

Lyonel-Feininger-Straße 26, 80807 München

Tel. 089/36086-0, Fax 089/36086-501, www.pcwelt.de

Geschäftsführer: York von Heimbürg

Verlagsleitung: Canio Martino

Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über
die Presse vom 8.10.1949: Alleiner Gesellschafter der
IDG Magazine Media GmbH ist die **IDG Communications
Media AG**, München, die 100%ige Tochter der International
Data Group Inc., Boston, USA, ist.

Vorstand: York von Heimbürg, Keath Arnot, Pat Kenealy

Mitglieder der Konzerngeschäftsführung: Josef Lohner

Aufsichtsratsvorsitzender: Patrick J. McGovern

ISSN 1860-7926



Aktuelle Tests finden Sie unter:
www.pcwelt.de

Windows Vista ausreizen

Installieren & konfigurieren

Vista ist auf den meisten neuen PCs bereits vorinstalliert und sofort startklar. Wer hingegen von Windows XP umsteigen oder Vista neu installieren möchte, muss die eine oder andere Hürde meistern. Dazu zählen etwa das Vorbereiten der Hardware mit passenden Treibern, das Überprüfen der Kompatibilität vorhandener Software sowie das Sichern von Daten. Nach dem ersten Vista-Start sollte das System konfiguriert und per Online-Update auf den aktuellen Stand gebracht werden.



Tuning-Guide



Schneller, schöner, besser. So lässt sich das Tuning für Windows Vista kurz beschreiben. Verschiedene immer wiederkehrende Tätigkeiten können etwa leicht automatisiert werden. Windows Explorer und Desktop werden an die individuellen Anforderungen angepasst und mit so genannten Gadgets um neue Funktionen erweitert. Und für betagte und weniger leistungsstarke Rechner empfiehlt PC-WELT eine Art Frischzellenkur, bei

der unnötiger Ballast zugunsten von mehr Geschwindigkeit abgeworfen wird.

Vista absichern: Schutz mit Bordmitteln

Glaubt man den Aussagen von Microsoft, dann ist Windows Vista sehr viel sicherer als seine Vorgänger. Mit der überarbeiteten Firewall, dem Anti-Spyware-Tool Windows Defender sowie der konsequenten Arbeit mit eingeschränkten Benutzerrechten sollen bössartige



Schädlinge und Hacker ausgesperrt bleiben. Die PC-WELT-Experten zeigen Schritt für Schritt die optimale Nutzung der einzelnen Sicherheitsfunktionen von Windows Vista und geben Ratschläge, wie Ihre wichtigen Daten und das komplette System damit geschützt werden.

Vista-Interna nutzen

Microsoft hat den Vista-System-Komponenten Shell, Gruppenrichtlinien, Services und Registry im Vergleich zu Windows XP zahlreiche neue Funktionen und grundlegende Änderungen spendiert. Vor allem Power-User und Administratoren profitieren von den Neuerungen, zu denen auch bereits bekannte Utilities aus den XP- und 2003-Server-Resource-Kits zählen. PC-WELT kennt die besten Tipps und Tools für den Praxiseinsatz.



PC-WELT Sonderheft-Abo

Ihre Vorteile: Bequeme E-Mail-Vorabinfo über kommende Sonderhefte mit Abbestellmöglichkeit • Sie entscheiden vor jedem neuen Heft, ob Sie es haben möchten • 1 Euro Preisvorteil pro Heft • Versandkostenfreie Lieferung • Service jederzeit kündbar

Jetzt risikolos anfordern: www.pcwelt.de/shop, **Tel.** 0711/7252-277 **Fax:** 0711/7252-377, **E-Mail:** shop@pcwelt.de