SECURITY

CHIP

Hacker-Tools vom Staat

Vorsicht, Sicherheitsamt vertreibt verbotene Tools!

Sicherheits-CD
mit 50 Top-Tools

Vollversion 1
Magical Security
Verschlüsselt Dateien

Vollversion 2
Safe One
Legt geheime Laufwerke an

SECURITY

€ 9,95

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

Ein Sonderheft von CHIP Ausgabe 2/08

Sicher im Web

Schäuble-Blocker für alle
Firewall total, Spyware killen, Daten codieren

Mit Tarnkappe ins Web
Anonym surfen, WLAN-Hotspot sicher nutzen

WLAN lückenlos sichern
Windows & WLAN-Router richtig einstellen

SPECIAL

Webseite bauen & absichern
Planen & aufbauen mit Joomla, XSS & Crawler aussperren, Formulare und Blog schützen

PLUS: Alle Tools auf Heft-CD

AUF CD!

Vollversion Magical Security
Verschlüsselt wichtige Dokumente ganz einfach per Knopfdruck

AUF CD!

Vollversion Safe One
Das Steganos-Tool legt geheime, virtuelle Laufwerke auf dem PC an

AUF CD!

Die 50 besten Security-Tools
Alles gratis: Netzwerk-Analyse, Browser & Plugins, Webdesign- & CMS-Tools

02

4196627809952

Bleiben Sie wachsam!

Andreas Vogelsang
Redaktionsleiter
CHIP-Sonderhefte

Liebe Leser,

„Vorsicht, bald hackt das BKA!“ – diese Warnung stand über dem Editorial des letzten CHIP-Sonderheftes zum Thema „Security“ im Januar 2007. Was vor einem knappen Jahr noch ungläubiges Staunen hervorrief, hat heute leider gar nichts Sensationelles mehr an sich. Kein Wunder: Mit seinen zeitweise im Wochenrhythmus abgefeuerten Vorschlägen zur Stärkung der inneren Sicherheit auf Kosten der Grundrechte der Bürger hat Bundesinnenminister Schäuble im vergangenen Jahr erfolgreich ausgetestet, wie weit er gehen kann. Und der Gewöhnungseffekt sorgte dafür, dass auch die abstrusesten Äußerungen zur Bespitzelung der Bürger durch Onlinedurchsuchungen oder andere Aktionen mittlerweile kaum mehr als ein Schulterzucken hervorrufen.

Lassen Sie sich nicht einlullen. Der Mann und seine Behörden meinen es ernst. Das ist spätestens seit dem Sommer klar, als mein Kollege Roman Leipold in CHIP 9/2007 den ominösen Bundestrojaner als PC-Wanze enttarnte, die – noch – mit immensem Aufwand im PC des überwachten Bürgers installiert wird. Noch! Denn Sie können davon ausgehen, dass der technische Aufwand sinken wird und sich die Überwachungsaktionen ausweiten werden – so wie das beim Telefon schon seit Jahren der Fall ist.

Lassen Sie sich nicht ausspähen. Weder staatliche Schnüffler noch Internet-Mafiosi oder neugierige Nachbarn gehen Ihre privaten Daten etwas an. Beim Schutz Ihrer Privatsphäre hilft Ihnen dieses Heft. Wir zeigen Ihnen, wie Sie Ihre Hardware vor Schnüffelattacken und Schadprogrammen absichern und auch im Internet unangreifbar werden. Denn in unserem Special „Sicherer Webauftritt“ erfahren Sie nicht nur, wie Sie mit dem CMS-Tool Joomla eine gelungene Webpräsenz aufbauen, sondern auch, wie Sie sie effektiv schützen – vor Attacken durch Cross-Site Scripting (XSS), geknackten Kontaktformularen oder übereifrigen Suchmaschinen.

Viel Spaß mit Ihrem sicheren PC!

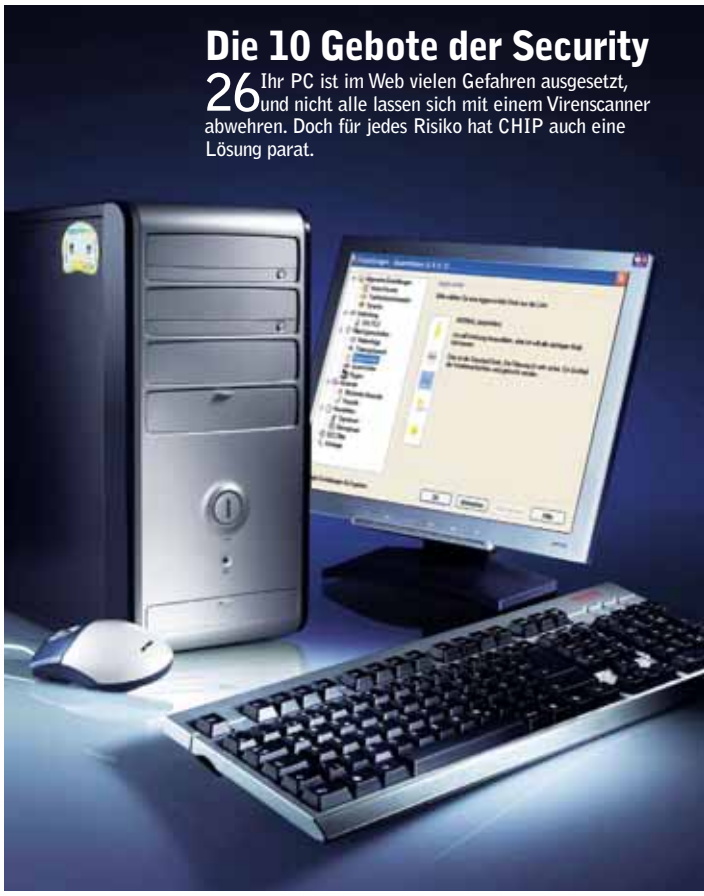
INHALT

Report: So arbeitet die Internet-Mafia

6 Das organisierte Verbrechen macht sich auch im Internet rücksichtslos breit. CHIP war undercover in den Mafia-Kreisen unterwegs – und enthüllt die kriminellen Methoden.

Security-Suiten im Test

12 Schützen die bekannten Suiten von Symantec, Kaspersky, G Data & Co. auch vor den neuen Bedrohungen durch die Internet-Mafia? CHIP hat sieben Pakete auf ihren Malware- und Phishing-Schutz getestet.



Die 10 Gebote der Security

26 Ihr PC ist im Web vielen Gefahren ausgesetzt, und nicht alle lassen sich mit einem Virenscanner abwehren. Doch für jedes Risiko hat CHIP auch eine Lösung parat.

AKTUELL

PC SICHER MACHEN

SICHER SURFEN

Webbrowser im Test

50 Wir haben uns die neuesten Versionen von Firefox, Opera, Internet Explorer und dem Apple-Browser Safari angesehen. Diesmal gab es einen Überraschungssieger.

Risiko Tauschbörse

62 Über die IP-Adresse lässt sich jeder Surfer identifizieren – besonders leicht bei Gnutella-basierten Tauschbörsen wie eMule oder BearShare.

Auf Heft-CD

Zwei Vollversionen – Ashampoo Magical Security und Steganos Safe One – und die 50 besten Freeware-Tools zu den Themen Security, Netzwerk, Browser, PHP und Content Management sind die Highlights der Heft-CD dieser Ausgabe. Mehr zu den Programmen erfahren Sie ab 18.

SPECIAL: SICHERER WEB-AUFTRITT

39 Gewinnspiel, 98 Vorschau, 98 Impressum

Gewinnspiel

Preise im Gesamtwert von über 1.650 Euro zu gewinnen!

Beteiligen Sie sich an unserer Umfrage, und gewinnen Sie mit etwas Glück eine von drei FritzBoxen von AVM oder eines von zehn Sicherheitspaketen „BitDefender Total Security 2008“. Mehr Infos gibt’s auf 39.

Auf den Spuren der Internet-Mafia

KNOW-HOW

Attacken im Internet

Die Mafia schreckt vor nichts zurück – auch nicht im Web. Anschläge sind zwar selten, dafür aber umso heftiger. Die Waffe ist meist ein Botnetzwerk.

Distributed Denial of Service (DDoS)
Mit einem einzigen PC lässt sich nur wenig Schaden anrichten. In ihren Botnetzen kontrolliert die Internet-Mafia allerdings Tausende PCs. Auf einen Befehl hin schicken die Bots ohne Unterlass Anfragen an das Opfer. In der Summe werden damit riesige Datenraten erzeugt, die der Empfänger nicht mehr bewältigen kann. Bei einem Angriff auf die Root-DNS-Server, die im Internet für die Zuordnung von IP-Adressen und Namen zuständig sind, wurden Spitzenwerte von mehr als 900 MBit/s gemessen.

Estland, 27.04.2007
Um die Politik zu beeinflussen, wird Estland wochenlang attackiert.

Israel, 17.05.2006
Aggressive Spammer zwingen die Firma Blue Security zum Aufgeben.

USA, 21.10.2002
Eine Attacke legt die Root-DNS-Server lahm – vermutlich nur ein Testlauf.

Irland, 18.01.2002
Der Provider Cloud Nine wird abgeschossen, die Hintergründe werden niemals bekannt.

Foto: iStockphoto

Das organisierte Verbrechen macht sich auch im Internet rücksichtslos breit. CHIP war undercover in den Mafia-Kreisen unterwegs – und enthüllt die kriminellen Methoden.

Auf Heft-CD

- AntiVir PE Classic (Security)
- Spybot – Search & Destroy (Security)
- XP-AntiSpy (Security)

Plötzlich sind wir mittendrin – im Hackerforum „Zloy“. Dort trifft sich die russische Internet-Mafia. Es dauert einen Moment, bis wir uns zurechtfinden. Dann sehen wir, was wir gesucht haben: Zwischen kyrillischen Schriftzeichen erkennen wir Screenshots, Preislisten und ICQ-Kontakte. Auf dem Online-Schwarzmarkt wird geboten, was es bei Ebay nicht zu kaufen gibt: Trojaner, Botnetze, Kontodaten, Kreditkartennummern – und natürlich Passwörter.

Über Wochen hinweg haben wir die Spuren der russischen Mafia verfolgt, haben beobachtet, wie Geschäfte gemacht und neue Schädlinge produziert werden. Von außen eine stark abgeschottete, unzugängliche Szene. Doch nachdem unser Undercover-Team sie erst einmal infiltriert hat, ist der Rest ein Kinderspiel.

Ganz offen bietet das organisierte Verbrechen seine Dienste an. Es fürchtet weder Staatsgewalt noch Sicherheitsfirmen. Muss es auch nicht. Und die seltenen Rückschläge steckt die Szene ganz locker weg. So wie den vom 11. September 2007, als das Bundeskriminalamt (BKA) und die deutsche Staatsanwaltschaft einen ihrer größten Erfolge gegen eine international organisierte Phishing-Bande verzeichnen konnten. 18 Monate liefen die Untersuchungen. Die Ermittler verfolgten die Geldströme und observierten die Täter. Am Ende wurden acht Personen festgenommen – zwei Frauen und sechs Männer. Sie stammen aus Deutschland, der Ukraine und der Russischen Föderation und gelten als Urheber unzähliger Phishing-Attacken. Mit gefälschten E-Mails der Deutschen Telekom, Ebay und vieler anderer Firmen lockten sie ihre Opfer und verursachten einen Schaden von mehreren hunderttausend Euro.

Der bisher größte Schlag der deutschen Strafverfolger – er war lediglich ein Mückenstich für die Internet-Mafia. Bereits zehn Tage später rollte die nächste Phishing-Welle über Deutschland hinweg. Die Lücke, die die Bande hinterlassen hatte, war blitzschnell geschlossen: Erneut überschwemmten gefakte Mails der Volks- und Raiffeisenbanken die Postfächer. Ihr Ziel: Die Opfer sollen ihre Kontodaten preisgeben – also PINs, TANs und sämtliche Passwörter.

Illegale Angebote In einschlägigen Foren gibt es alles zu kaufen, beispielsweise auch geklaute Kreditkartendaten.

Handel im Netz: Wie der Untergrund kommuniziert

Wir begeben uns undercover in die dunkelsten Ecken des Internets, in denen das organisierte Verbrechen seine Deals macht. Die Suche nach den Hintermännern des Milliardengeschäfts beginnt in einem harmlos wirkenden Forum. Denn die wichtigsten Anlaufstellen der Internet-Mafia sind frei zugängliche Webseiten – vor allem Foren. Diese erste Adresse muss man kennen, alle weiteren sind dort verlinkt. Schnell kommt man dann auf Seiten wie „Carder-Biz“, „Anti-Chat“ oder „Zloy“. Dort treffen sich alle Beteiligten, tauschen Informationen über Sicherheitslücken aus und bieten ihre Waren an. Und alles ist in Bewegung: Während das eine Forum plötzlich nicht mehr erreichbar ist, entstehen an anderer Stelle zwei neue.

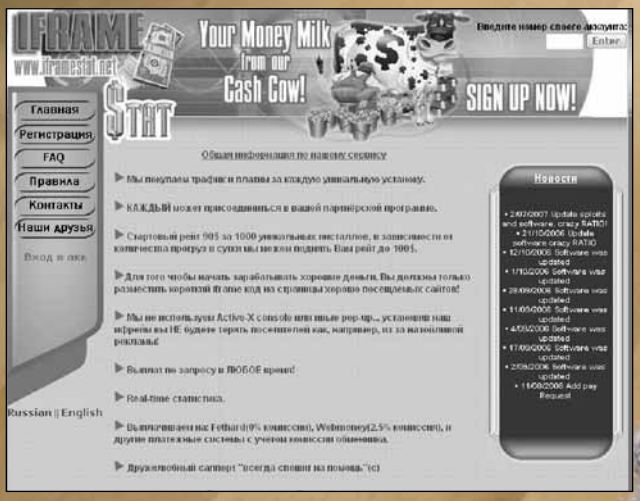
Wo man auch unterwegs ist, überall trifft man auf dieselben Namen – auf das „Infected Team“ etwa, das sein Botnetzwerk für Spam und Angriffe anbietet. Mittlerweile ist es so erfolgreich, dass es eine eigene Webseite hat. Andere wiederum begnügen sich mit einem einfachen Forenbeitrag, der sich in Copy & Paste-Manier hundertfach im Netz wiederholt – etwa der Hacker Morozov, der den Trojaner-Baukasten „Power Grabber“ anbietet. Er wirbt mit einem Screenshot und einer kurzen Beschreibung für seinen auf Onlinebanking spezialisierten Schädling – und mit seiner ICQ-Nummer. Denn wer ins Geschäft kommen möchte, erfährt die Details im virtuellen Zwiegespräch.

Chatten ist in der Szene sehr beliebt – besonders ICQ. Das ICQ-Protokoll er- →

laubt das Routing über Socks Proxys – und das garantiert Anonymität. Daraus entstehen, fast schon von selbst, zwei neue Geschäftszweige. So haben sich etwa die Besucher des Nomerkov-Forums auf das Beschaffen möglichst kurzer und eingängiger ICQ-Nummern spezialisiert. Denn wie bei einer Telefonnummer kommt es auch an dieser Stelle darauf an, dass sich die ICQ-Adresse leicht merken lässt. Und so versuchen Hacker wie Komarik und Krockus mit Tools wie „Malefic Brute“ an die Passwörter solcher ICQ-Accounts zu gelangen. Bei Preisen zwischen sieben und 70 Dollar pro erfolgreichem Hack ist das ein sehr einträgliches Geschäft.

Allerdings haben die ICQ-Hacker auch Ausgaben. Denn sie sind auf die Botnetz-Betreiber und ihre Zombie-Rechner angewiesen. Auch die kann man mieten. Die „Fraud Crew“ zum Beispiel bietet für 70 Dollar pro Monat eine Proxy-Flatrate. Dafür hat der Kunde dann Zugriff auf rund 700 Rechner. Die braucht ein ICQ-Hacker auch, denn bereits nach wenigen fehlgeschlagenen Login-Versuchen von derselben IP-Adresse ist bei ICQ für gewöhnlich Schluss. Mit einem Netz von 700 Socks Proxys lässt sich die Brute-Force-Attacke ganz einfach auf viele Accounts und viele IP-Adressen verteilen.

Professionell Maßgeschneiderte Tools sind profitabel. An dieser Stelle steht gerade ein Trojaner-Tarnwerkzeug zum Verkauf.



Kuhhandel Mit Angeboten wie diesem will man Webseiten-Betreiber animieren, gefährliche iFrames einzubauen.

Grauzone Die an dieser Stelle angebotenen Webdesigns werden oft genutzt, um schnell Seiten für Scheinfirmen aufzubauen.

Do it yourself Trojaner aus dem Baukasten

Dass sich die Mafia besonders gern im Web trifft und austauscht, hat seine Gründe. Der wichtigste heißt Arbeitsteilung. Anstatt selbst ein Team aufzubauen und zu organisieren, setzen die Mafiosi auf freie Mitarbeiter. So gibt es für jeden Bereich Spezialisten – etwa Informatikstudenten. Sie verdienen als Handlanger der Internet-Mafia wesentlich mehr als in jedem Praktikum. Es gibt sogar das Gerücht, dass sie direkt von der Universität abgeworben werden, um Trojaner zu programmieren.

Unser Undercover-Team stellt inzwischen fest: Der aktuelle Liebling der Phisher heißt „Pinch 3“. Das Trojaner-Bastelset erzeugt einen kleinen, aber mächtigen Spion. Startet das Opfer diese Datei, werden sämtliche Passwörter ausgelesen und per E-Mail oder HTTP zum Hacker geschickt. Doch die Do-it-yourself-Trojaner haben einen für die Phisher gravierenden Nachteil: Da sich die Spionagetools aus dem Baukasten in großen Teilen ähneln, ist es für die Sicherheitsfirmen ein Leichtes, eine Signatur zu schreiben, die gleich Hunderte von Varianten erkennt. Im Forenjargon heißen solche Trojaner danach „burned“ – also verbrannt.

Doch davon lässt sich die Szene nicht beeindrucken. Anstatt die Trojaner immer wieder neu zu schreiben und auf diese Weise den Signaturen zu entkommen, werden heutzutage Downloader

oder Dropper programmiert. Das sind bescheidene Programme, deren einzige Aufgabe im Nachladen der eigentlichen Malware besteht. Die derzeit kleinste Variante hat lediglich 474 Byte – halb so viel wie ein leeres Word-Dokument. Oft wird das Programm um Funktionen erweitert, die Schutzsoftware wie Firewalls und Virenscanner deaktivieren.

Um sicherzugehen, dass nicht auch die Downloader irgendwann verbrannt sind, boomt in den Foren ein Angebot an EXE-Packern und -Cryptern. Die Hacker interessiert es allerdings nur wenig, dass die Malware-Files damit kleiner werden. Viel wichtiger ist die Tatsache, dass sich mit dem Komprimieren und Verschlüsseln der Dateien auch deren Signaturen ändern. Diese Methode ist so erfolgreich, dass sich Sicherheitsfirmen wie Symantec gezwungen sehen, von der Fingerabdruck-Methode „Signatur" Abstand zu nehmen und neue Techniken anzuwenden – etwa die verhaltensbasierte Analyse. Damit erkennt ein Sicherheitsprogramm einen Downloader etwa daran, dass er zuerst versucht, die Firewall zu deaktivieren, und Sekunden später ein weiteres Tool aus dem Netz lädt.

Die Programme, auf die unser Ermittlerteam stößt, haben eines gemeinsam: Sie werden immer professioneller. Selbst den Experten fällt es mittlerweile schwer, „gute" und „böse" Applikationen auseinanderzuhalten. Das einfachste Angriffswerkzeug sind noch die sogenannten Joiner – Programme, die harmlose Dateien, etwa Bilder oder Scherzsoftware, mit dem Trojaner bündeln. Wer dieses Paket öffnet, holt sich die Online-Mafia sofort auf seinen Rechner.

Trojaner zu kaufen ist nicht schwer. Eine Phishing-Bande muss sich nur überlegen, was sie braucht, und schon kann es losgehen. Doch wie bezahlt man die gefährliche Ware? Um das herauszufinden, versuchen wir, den bereits erwähnten Trojaner „Power Grabber" zu kaufen. Laut Beschreibung ist die Software in der Lage, unbemerkt Passwörter auszuspionieren – zum Beispiel beim Onlinebanking. Wie in der Szene üblich, erreichen wir den Verkäufer per ICQ. Der ist misstrauisch und will von uns wissen, woher wir die Adresse haben. Wir geben das Forum an und bekommen im Gegenzug eine neue ICQ-Adresse. Dort erst geht es richtig zur Sache. Der Trojaner ist schon etwas älter: Das weiß der Hacker – und das wissen wir. In gebrochenem Englisch feilschen wir um den Preis. Das einzig Neue an dem Trojaner wäre die durch einen Crypter veränderte Signatur. Deswegen will der Hacker 300 WBZ – sprich Dollar. Hinter WBZ steht der Epayment-Anbieter WebMoney Transfer, der im Untergrund sehr beliebt ist und seine Währung 1 : 1 in Dollar umwandelt.

Zum Schein geht unser Ermittlerteam auf den Deal ein und bekommt eine Bankverbindung bei WebMoney genannt. An dieser Stelle brechen wir den Handel ab. Schließlich wollen wir dem Hacker nicht auch noch Geld in den Rachen werfen. Hätten wir den Preis gezahlt und der Anbieter sein Wort gehalten, dann hätten wir den Trojaner bei einem russischen Download-Portal – ähnlich wie RapidShare – in einem verschlüsselten RAR-Archiv herunterladen können.

KNOW-HOW

Was Phishing-Angriffe kosten

In einschlägigen Foren gibt es alles zu kaufen, was für eine Phishing-Attacke nötig ist. Für rund 250 Dollar kann sich jeder Hobbyhacker professionell ausstatten.

Trojaner (spioniert die Opfer aus)	**100 Dollar**
Crypter (tarnt den Trojaner)	**50 Dollar**
Bots (verschicken Spam)	**5 Dollar pro 100 Stück**
Proxys (decken den Hacker)	**70 Dollar pro Monat**
ICQ-Adresse (ermöglicht Verhandlungen)	**20 Dollar**

Malware-Geschäfte Wie der Hacker anonym bleibt

Wäre es möglich, den Hacker durch seine Kontonummer ausfindig zu machen? Vermutlich nicht. Ein Konto bei WebMoney scheint auf den ersten Blick zwar wenig anonym. „Das Geld wird aber nie direkt überwiesen, sondern fließt über mehrere Kanäle", erklärt Sicherheitsexperte Eugene Kaspersky.

Er skizziert den typischen Ablauf: Um nicht selbst mit dem Schadprogramm in Verbindung gebracht zu werden, akquirieren die Hacker Mittelsmänner. In einer Spamnachricht – wie sie vermutlich jeder kennt – wird diesen ein lukrativer Nebenjob versprochen. Die einzige Aufgabe der Strohmänner besteht darin, ein Konto zu verwalten und eingehendes Geld auf ein anderes Konto zu überweisen. Für das Erledigen dieser Aufgabe dürfen die Mittelsmänner einen gewissen Anteil behalten. Üblich ist ein einstelliger Prozentsatz. Das Konto, auf das das Geld überwiesen wird, haben die Hacker meist unter falschem Namen im Ausland angelegt. Am Ende holen sie den Gewinn schließlich an einem Geldautomaten ab.

Fast dieselbe Masche kommt bei Phishing-Attacken zum Einsatz. Erbeutet der Phisher Daten wie PIN, TAN und Kontonummer, überweist er das Geld per Onlinebanking an einen Mittelsmann. Der leitet es an einen oder oftmals auch mehrere Strohmänner weiter. Die wiederum transferieren das Geld schließlich auf verschiedene Konten, die den Phishern gehören.

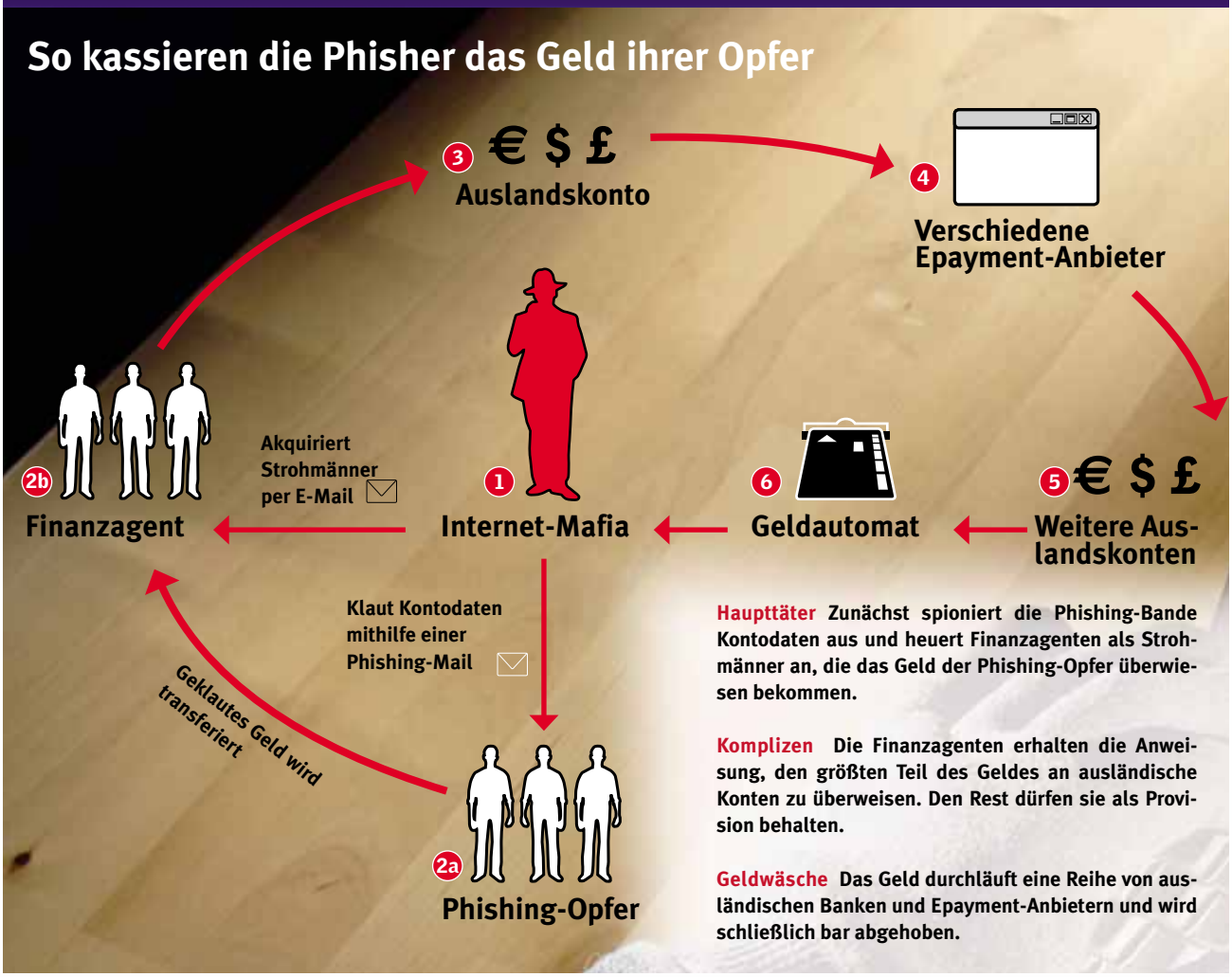
In Deutschland steht – anders als in den USA oder den meisten anderen Ländern – diese Art von Geldwäsche unter Strafe. Selbst wer sich nicht darüber im Klaren ist, dass er an einer illegalen Handlung mitwirkt, wird bestraft.

Das wahre Ausmaß des illegalen Treibens wird erst offenbar, wenn man nicht nur auf die Beiträge in den Foren achtet, sondern auch auf die Werbung und die Affiliate-Links. Denn ist das Botnetz aufgebaut, lässt es sich für mehr als nur Angriffe auf weitere Internetnutzer und deren Kontodaten nutzen.

Häufig begegnet man deshalb in den Foren Werbung von Traffic-Händlern. Zwei Varianten sind üblich: Die einen verkaufen Traffic. Wer glaubt, dass seine Webseite zu schlecht besucht ist und legale Optimierungsmaßnahmen nicht helfen, das Google-Ranking zu verbessern, kann an dieser Stelle einfach Klicks und →

KNOW-HOW

So kassieren die Phisher das Geld ihrer Opfer



Besucher einkaufen. Die Botnetz-Betreiber fangen daraufhin an, Blogs und Foren mit Kommentaren und Links voll zu spammen, die möglichst viele Besucher auf die Seite locken sollen.

Die anderen dagegen kaufen Traffic ein. Auf zahllosen Webseiten wie beispielsweise iFrame.biz begegnet unseren Undercover-Surfern Werbung von Phishern für das schnelle Geld. Das Angebot: Wer in seine Webseite ein angeblich ungefährliches iFrame einbaut, der bekommt jeden Besucher bezahlt. Das Geschäft ist allerdings gefährlich und wenig einträglich. Für 1000 Besucher pro Tag bekommt ein Webseitenbesitzer gerade mal 25 US-Cent. Die Webseite im iFrame enthält jedoch in den allermeisten Fällen gefährliche Downloads oder Adware – entgegen den Beteuerungen des Verkäufers, das Angebot sei legal und vollkommen harmlos.

Einige Pornoseiten-Betreiber, die in den Weiten des Internets schlicht untergehen, greifen ebenfalls gern auf die Internet-Mafia und deren Botnetze zurück. Die bietet nämlich gegen Entgelt an, ihre Opfer auf Pornoseiten umzuleiten: Die mit Bots infizierten Opfer bekommen beim Ansurfen beliebiger Webseiten neben den ohnehin schon zahlreichen Werbebannern auch noch Pornowerbung angezeigt – eine Masche, die sich offenbar für viele richtig auszahlt.

In vielen Fällen lassen sich die dunklen Verbindungen nicht mehr nachweisen. Allerdings gibt es ein paar eindeutige Hinweise auf dubiose oder kriminelle Webpräsenzen. So besitzen viele dieser Webangebote kein Impressum, dafür aber ICQ-Adressen als Kontakte und weisen englische Formulierungen auf, die an automatische Übersetzungsdienste wie Babelfish erinnern.

Die Täter Wer hinter den krummen Geschäften steckt

Wer sich hinter den Machenschaften im Internet verbirgt, ist die mit Abstand spannendste Frage. Selbst Experten, die sich bereits seit Jahren mit diesem Thema beschäftigen, können unserem Ermittlerteam keine zufriedenstellende Antwort liefern. So äußerte ein Hacker auf der Sicherheitsmesse BlackHat den Verdacht, dass die klassische russische Mafia dahintersteckt. Andere Insider wiederum hängen der Verschwörungstheorie an, dass vor allem Ex-Mitarbeiter des aufgelösten sowjetischen Geheimdienstes KGB bei den Betrügereien im Internet ihre Finger im Spiel haben. Sogar das BKA scheint sich nicht ganz sicher zu sein. Auf die Frage, ob sich dahinter bereits etablierte Organisationen verbergen, heißt es: „Das können wir so pauschal nicht sagen.“ Valentin Pletzer

Sicher surfen: Welche Suite schützt wirklich?

Niemand sollte sich ungeschützt ins Internet begeben. Doch nicht jede Internet-Security-Suite deckt alle wichtigen Bereiche ab. CHIP schickt sieben Kandidaten in den Härtetest.

Sie denken, auf Phishing fällt nicht einmal mehr Ihre Oma herein? Und wer einfach nur aufpasst, wohin er surft und was er anklickt, ist im Internet sicher? Dann hat die Phishing-Mafia schon gewonnen. Denn die Angriffe werden immer routinierter und zahlreicher.

Allein im September verzeichnete das IT-Unternehmen Sophos 5400 neue infizierte Webseiten – und das Schema dahinter ist immer dasselbe. In mehr als der Hälfte aller Fälle wird eine Webseite gehackt und ein iFrame eingebaut. Wer so eine Webseite besucht, lädt auch ein gefährliches JavaScript. Das wiederum sorgt dafür, dass eine verschlüsselte EXE-Datei ausgeführt wird, die den wahren Schädling holt und installiert.

Der beste Schutz vor solchen Angriffen sind und bleiben aktuelle Security-Suiten. Unser Test zeigt allerdings, dass es noch genügend Raum für Verbesserungen gibt. Erscheinungsbild und Funktionsweise neuartiger Schädlinge ändern sich nämlich mittlerweile so schnell, dass herkömmliche Scans nicht mehr genug sind. In unserem Test mussten die neuen Suiten für 2008 deshalb diesmal nicht nur die knapp 1400 derzeit aktiven Viren erkennen, sondern vor allem auch verschlüsselte und gepackte Malware. Eine Disziplin – so viel sei schon verraten –, in der sich die Scanner nicht gerade mit Ruhm bekleckerten.

Immer mehr Anwender legen Wert auf Performance und Verständlichkeit der Produkte; deshalb fließen diese Kategorien noch stärker als bisher in unsere Tests ein. Denn was nützen die aufwendigsten Schutzmechanismen, wenn der Anwender sie aufgrund fehlender

Foto: N. Schäffler

Kenntnisse oder wegen des hohen Ressourcenverbrauchs abschaltet?

Viren & Trojaner Schädlinge erkannt, aber nicht entfernt

Trojaner und gefährliche Webseiten dominieren im Augenblick die Malware-Charts. Trotzdem ist das Anti-Virus-Modul zweifellos der wichtigste Bestandteil einer Security-Suite. Allerdings muss der Scanner heutzutage nicht nur Viren, sondern sämtliche bösartigen Programme erkennen.

BEKANNTE MALWARE: In dieser Kategorie unseres Tests gibt es in diesem Jahr keinerlei Überraschungen. Sämtliche Internet-Security-Suiten erkennen 100 Prozent der Malware, die auf der Wildlist steht – dem Verzeichnis der im Internet aktiven Schädlinge. Dabei macht es keinen Unterschied, ob ein Scandurchgang manuell gestartet wird oder ob der Hintergrundwächter aktiv ist.

AKTIVE SPYWARE, BOTS & ADWARE: Wie schon im Vorjahr wollten wir wissen, ob die Security-Suiten bereits aktive Schadsoftware erkennen und restlos entfernen können. Die Zahl der verwendeten Malware wurde von sechs auf zehn erhöht. Damit jedoch haben die Suiten so ihre Probleme – denn mindestens ein Eindringling geht nahezu jedem Produkt durch die Lappen. Schlimmer noch: Wird ein Schädling erkannt, heißt das nicht automatisch, dass die Software ihn auch entfernt.

Am besten schlägt sich noch Symantec mit der Norton Suite: Sie vernichtet 70 Prozent der schadhaften Dateien und ihrer Registry-Einträge. Alle anderen schaffen es nur in rund 50 Prozent der Fälle, den Schädling nach dem Erkennen auch zu entfernen. An dieser Stelle sollten die Hersteller auf jeden Fall gründlich nachbessern.

KOMPRIMIERTE MALWARE: Ein einfacher, aber effektiver Trick der Malware-Produzenten besteht darin, alten Trojanern durch EXE-Packer eine neue Signatur zu verpassen. Die Hersteller der Security-Suiten wiederum kontern, indem sie versuchen, die Dateien vor dem Scannen zu entpacken. Das klappt aber vielfach →

FAZIT

Den perfekten Rundum-Schutz gibt es nicht. Trotzdem haben wir von den Testkandidaten mehr erwartet. Besonders gravierend: Wenn der Schädling einmal auf dem PC ist, versagen die Suiten. Einen Phishing-Schutz im Browser gibt es nicht. Wenigstens bemühen sich viele Hersteller, die Systemauslastung zu reduzieren – doch selbst da sind sie noch weit vom Ideal entfernt. Die erst nach dem Test erscheinende ESET Smart Security soll immerhin bis zu 30mal schneller laufen als die Testkandidaten.

INFO

Tops & Flops der Security-Suiten

Jedes der getesteten Security-Pakete hat seine speziellen Stärken und Schwächen – CHIP verrät sie Ihnen.

Kaspersky bietet ein starkes Anti-Phishing-Tool bei guter Performance an. Der Malware-Schutz könnte jedoch besser sein.

Norton besitzt kein Anti-Spam-Modul. Das kostet die Suite den Sieg – trotz verbesserter Performance.

G Data spürt fast alle Schädlinge auf, doch der Rechner wird dabei viel zu stark ausgelastet.

F-Secure zeigt kaum Schwächen, ist allerdings weder sicher noch schnell genug für eine Empfehlung.

BitDefender ist zwar preiswert, bietet jedoch kaum Schutz vor Phishing. Sparen Sie also nicht am falschen Ende!

Panda bestätigt: Sicherheit hat ihren Preis. Zwar verfügt die Suite über anständige Erkennungsraten, doch das kostet viele Ressourcen.

Avira, ein Produkt ohne große Stärken, lässt den Angreifern genügend Raum, um Malware auf den Rechner zu schleusen.

nicht. Besonders schlecht schneidet dabei die Security-Suite von Avira ab: Sie erkennt nur rund 63 Prozent der von uns getesteten Samples. Und wir haben nur vier Schädlinge in mehr als 500 verschiedenen Variationen getestet.

FEHLALARME UND REAKTIONSZEIT: Zu jedem Vergleich der Scan-Engines gehört auch ein False-Positive-Test, also die Frage, ob ungefährliche Programme fälschlicherweise blockiert werden. An dieser Stelle machen die Security-Suiten alles richtig: Kein Produkt kommt bei 150000 Dateien auf eine Fehlalarm-Quote von mehr als einem Promille.

Anders sieht das Bild bei den Reaktionszeiten auf neu entdeckte Schadprogramme aus: Symantec, ein Unternehmen, das nach eigener Aussage sehr viel Zeit in die Qualitätskontrolle steckt, braucht bis zu neun Stunden, um eine passende Signatur auszuliefern. Besser macht das die Internet-Security-Suite G Data. Sie erledigt diese Aufgabe dank zwei verschiedener Scan-Engines schon innerhalb einer halben Stunde.

Phishing & Spam Kaum Schutz vor Betrug

Phishing ist für die Internetmafia ein attraktives Millionengeschäft. Das erklärt auch den steilen Anstieg an betrügerischen Mails und Webseiten. Ein ausgereifter Phishing-Schutz sollte deshalb in keiner Security-Suite fehlen.

E-MAIL-FILTER: User wollen immer ein sauberes Postfach, ohne sich mit der aufwendigen Konfiguration eines Filters beschäftigen zu müssen. Im Test

Kaspersky Die Suite alarmiert nicht nur visuell, sondern auch akustisch – mit einem besonders unangenehmen Geräusch.

Avira Die Firewall von Avira meldet zwar viel, sagt aber nichts Konkretes. Resultat: Der User weiß nicht, was er tun soll.

mussten deshalb alle Suiten ohne Training 250 E-Mails als erwünschte und unerwünschte Nachrichten interpretieren. Kleine Gemeinheit: Die Filter der Anbieter Google, GMX und Web.de hatten bereits ihre Arbeit erledigt.

Trotz der erschwerten Bedingung gab es kein Ergebnis, das schlechter war als 73,1 Prozent. Doch die Security-Suiten hatten damit eigentlich erst einmal wenig zu tun. Denn schon das Testprogramm Microsoft Mail von Windows Vista erkennt dank eingebautem Filter selbst Spamnachrichten. Einen besseren Schutz bieten lediglich Kaspersky und F-Secure, die sich in etwa die Waage halten. Kaspersky entdeckt zwar mehr Spammails, dafür sortiert F-Secure keine echten E-Mails fälschlicherweise in den Spamordner.

Norton Die Norton Internet Security Suite wirkt extrem aufgeräumt. Für manche ist das allerdings des Guten zu viel.

BROWSER-SCHUTZ: Nicht einmal die Hälfte aller Security-Suiten kümmern sich um das Phishing-Problem dort, wo es auftritt: im Webbrowser und nicht nur im E-Mail-Client. Denn immer häufiger finden sich gefährliche Links nicht nur in E-Mails, sondern auch in Blogs, Foren und scheinbar harmlosen Webseiten. Die drei rühmlichen Ausnahmen Kaspersky, Symantec und G Data erkannten bei unserem Test alle Phishing-Seiten, alle anderen bieten dagegen keinerlei Schutz.

NETZWERK-SCHUTZ: Ebenfalls zum Thema Phishing rechnen wir die ARP-Spoofing-Attacke – ein Angriffsszenario, das bereits erfolgreich in öffentlichen Netzen demonstriert wurde. Der Hacker leitet durch einen simplen Trick den Datenverkehr über seinen Rechner und liest dann ganz bequem die Passwörter aus. Katastrophal: In unseren Tests erkannte keine einzige Security-Suite diesen Angriff!

Performance & Bedienung Weniger Last, zu wenig Infos

Sicherheit um jeden Preis – so hätte in den vergangenen Jahren das Motto der Internet-Security-Suiten lauten können. Die Firmen packten ohne Rücksicht auf Verluste eine Funktion nach der anderen in die Pakete. Die Folge: Die Rechner wurden immer langsamer, die Produkte immer komplizierter – und der Benutzer hatte das Nachsehen. Doch jetzt scheinen die Hersteller umzudenken: Einige Programme verbrauchen weniger Res-

sourcen, arbeiten schneller und sind deutlich einfacher zu bedienen.

Das schlägt sich schon in der Startzeit nieder. 55 Sekunden benötigt ein frisches Vista zum Starten auf unserem Testrechner. Nur fünf Sekunden länger braucht das System mit F-Secure – ein sehr guter Wert. Das andere Extrem: Die Suite von G Data verzögert den Vista-Start um stattliche 80 Sekunden.

Doch während der eine oder andere einen langsameren Start noch hinnehmen mag – auf kostbaren Arbeitsspeicher will niemand verzichten. Um den größten Speicherfressern auf die Spur zu kommen, haben wir gleich zwei Werte ermittelt. Die sogenannten „Private Bytes" geben an, wie viel RAM eine Anwendung exklusiv belegt. Dieser Speicher steht also keiner anderen Anwendung zur Verfügung. Doch erst mit dem zweiten Wert, dem „Working Set", wird das Bild vollständig. Je mehr Speicher eine Suite an dieser Stelle belegt, umso wahrscheinlicher ist es, dass Windows auf die Auslagerungsdatei zurückgreifen muss. Dann wird die Festplatte zum Flaschenhals.

Beim RAM-Test schneidet BitDefender am besten ab: Wird gerade kein Scandurchlauf gestartet, schrumpft der Verbrauch auf 66 MByte Private Bytes und lediglich 7 MByte Working Set – ein Wert, von dem die Panda-Security-Suite weit entfernt ist: Sie bringt die RAM-Kapazität mit 110 MByte und 222 MByte an ihre Grenzen.

Doch auch bei Downloads aus dem Internet machen sich die Sicherheitsprogramme bemerkbar. Der Internet Explorer etwa lädt die Dateien zuerst in den Cache der temporären Internetdateien, ehe er sie an ihren Bestimmungsort kopiert. Das Problem: Manche Virenscanner nehmen beide Vorgänge unter die Lupe – einer sollte jedoch reichen. Denn der doppelte Scan macht den Download zu einer wahren Geduldsprobe. So dauert das Herunterladen einer 100-MByte-Datei für Kaspersky-Nutzer satte 51 Sekunden, während F-Secure das in 20 Sekunden schafft – fast genauso schnell, als würden Sie gar keinen Scanner einsetzen.

Wird die Datei nicht umbenannt, sondern nur von einer Festplatte auf die nächste kopiert, sind alle Scanner so intelligent, die Datei kein weiteres Mal einem vollen Check zu unterziehen. Und auch beim E-Mail-Download konnten wir bei keinem der getesteten Produkte eine Verzögerung feststellen.

Doch wie schnell und schlank eine Security-Suite auch sein mag – erst wenn der User problemlos damit umgehen kann, ist echte Sicherheit gewährleistet. Deshalb bewerteten wir auch die Qualität der Informationen der Firewall- und Malware-Meldungen – und da besteht bei fast allen Herstellern Nachholbedarf. Alle Firewalls geben zwar detaillierte Informationen zu den Anwendungen aus, die eine Internetverbindung aufbauen möchten, doch eine echte Entscheidungshilfe ist das nicht. Denn mit kryptischen IP-Adressen können die meisten User kaum etwas anfangen. Dateinamen oder das Programm-Icon dagegen kann ein Virenschreiber leicht fälschen und damit den Nutzer in die Irre führen.

Ähnlich problematisch sind die Meldungen bei den Virenscannern. Sie bezeichnen eine befallene Datei zwar als bösartig, sagen dem User aber nicht klar, was er nun machen soll. Allein die Internet-Security-Suite von Norton nimmt dem Benutzer die Entscheidung ab. Sie verschiebt einen Virus automatisch in Quarantäne. Das kann der User jederzeit rückgängig machen, falls sich die Suite geirrt haben sollte.

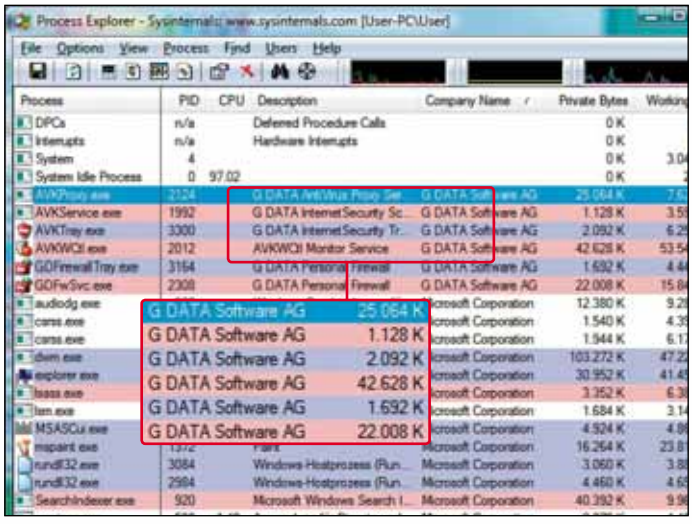
Valentin Pletzer →

INFO

OneCare 2.0: Microsoft macht in Sicherheit

Eigentlich gar keine schlechte Idee, die Microsoft da hatte: Zusätzlich zum Virenscanner und der Firewall enthält die Security-Suite auch noch ein Backup, einen Systemoptimierer und eine zentrale Oberfläche, über die sich alle Rechner im Netzwerk kontrollieren lassen. Leider scheitert das Ganze jedoch an der Ausführung. Der Virenscanner ist bestenfalls Mittelmaß, einen Spamfilter gibt es nicht, und der Rest ist eigentlich nur eine Oberfläche für die in Windows bereits enthaltenen Programme Defrag und Windows Firewall. Für rund 50 Euro Jahresabo ein teurer Spaß. Platz für ein Online-Backup stellt Microsoft auch bereit, allerdings nur für Bilder. Und weil 10 GByte nicht billig sind, kostet der Service zusätzlich 20 Euro im Jahr.

OneCare 2.0 Microsofts Security-Suite ist immer für einen Fehlalarm gut. Die Firewall auf dem dritten PC ist längst aktiv.



G Data Die Security-Suite von G Data belegt ziemlich viel Arbeitsspeicher und bremst so das System stark aus.

Übersicht	CHIP TESTSIEGER 12/2007 PLATZ 1	CHIP PREISTIPP 12/2007 PLATZ 2	PLATZ 3	PLATZ 4	PLATZ 5
Produkt	**Kaspersky Internet Security 7.0**	**Norton Internet Security 2008**	**G Data Internet Security 2008**	**F-Secure Internet Security 2008**	**BitDefender Internet Security 2008**
Anbieter	Kaspersky	Symantec	G Data	F-Secure	BitDefender
Preis (ca.)	40 Euro	30 Euro	40 Euro	40 Euro	30 Euro
Internet	www.kaspersky.de	www.symantec.de	www.gdata.de	www.f-secure.de	www.bitdefender.de
Anzahl der Lizenzen	1	1	1	1	1
Kosten Telefon-Hotline (deutsch)	0,12 Euro/Minute	0,20 Euro; ab 3. Minute 1,89 Euro/Minute	0,0409 Euro/Minute	0,12 Euro/Minute	0,12 Euro/Minute
Gesamtwertung	76 Punkte	75 Punkte	65 Punkte	61 Punkte	60 Punkte
	■■■■□	■■■■□	■■■□□	■■■□□	■■■□□
Malware-Schutz	62	75	61	65	62
Phishing-Schutz	93	65	80	51	38
Ergonomie	73	86	54	66	81
Preis/Leistung	**Gut**	**Gut**	**Befriedigend**	**Befriedigend**	**Gut**
Malware-Schutz					
Erkennungsrate bekannter Malware	100 %	100 %	100 %	100 %	100 %
Erkennungsrate bei aktiver Malware	90 %	100 %	90 %	90 %	100 %
Entfernte aktive Malware (Dateien)	50 %	70 %	50 %	60 %	50 %
Entfernte aktive Malware (Registry)	60 %	70 %	10 %	60 %	30 %
Erkennungsrate inaktiver komprimierter Malware	81,81 %	90,75 %	85,18 %	82,45 %	77,56 %
Fehlalarme bei Virenscans	6	1	9	7	17
Wartezeit für neue Signaturen (gemessen Jan. bis Aug. 2007)	ca. 1 Stunde	ca. 9 Stunden	ca. 0,5 Stunden	ca. 3 Stunden	ca. 2,5 Stunden
Firewall-Aktivität bei Angriffen	– (Firewall stürzt ab)	Mittlere Auslastung	Hohe Auslastung	Mittlere Auslastung	Kaum Auslastung, aber viele Meldungen
Phishing-Schutz					
Erkennungsrate bei unerwünschten E-Mails	92,8 %	– (Modul nur per Download)	73,1 %	86,9 %	73,1 %
Fehlalarme bei Spam-Erkennung	4	Modul nur per Download	12	0	12
Erkannte Phishing-Seiten	100 %	100 %	100 %	Keine	Keine
Anbindung an E-Mail-Client	POP3/IMAP und Outlook-Plugin	Outlook/Eudora/Netscape Mail	POP3/IMAP	POP3/IMAP und Outlook-Plugin	POP3 und Outlook-Plugin
Abwehr gegen ARP-Spoofing	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz	Kein Schutz
Ergonomie					
Vista-Bootzeit [1]	69 Sekunden	74 Sekunden	80 Sekunden	60 Sekunden	74 Sekunden
Arbeitsspeicherbedarf Private Bytes	60 MByte	68 MByte	136 MByte	197 MByte	66 MByte
Arbeitsspeicherbedarf Working Bytes	9 MByte	8 MByte	151 MByte	48 MByte	7 MByte
Scandauer (Sauberes System 18,8 GByte)	12 Min. 9 Sek.	9 Min. 54 Sek.	17 Min. 22 Sek.	9 Min. 39 Sek.	5 Min. 6 Sek.
Verzögerung beim Mail-Abholen	Nicht messbar	Nicht messbar	Nicht messbar	Nicht messbar	Nicht messbar
Download-Zeit (für 100 MByte)	51 Sekunden	23 Sekunden	22 Sekunden	20 Sekunden	27 Sekunden
Verzögerung beim Dateikopieren	–	–	–	–	–
Hilfe bei Firewall-Meldungen	Standardmäßig abgeschaltet	Kaum Meldungen	Nutzer muss alles selbst entscheiden	Einige Standardprogramme voreingestellt	Nutzer muss alles selbst entscheiden (kompliziert)
Hilfe bei Malware-Meldungen	Nutzer muss entscheiden (mit Empfehlung)	Automatische Quarantäne, kleine Notiz	Nutzer muss entscheiden (mit Empfehlung)	Nutzer muss entscheiden (mit Empfehlung)	Nutzer muss entscheiden (mit Empfehlung)
Boot-CD vorhanden/ updatefähig/NTFS-tauglich	–/–/●	–/–/–	●/●/●	●/–/–	●/●[2]/●
Zusatzfunktionen	Kindersicherung	Passwort-Safe	Kindersicherung, Werbeblocker, Datenschredder	Kindersicherung	Kindersicherung, Mobile Antivirus
Bedienbarkeit	Einfache Installation; Oberfläche richtet sich eher an Profis	Einfache Installation; Einstellungen für Experten sehr versteckt	Einfache Installation; Virenscan benötigt jedes Mal die Bestätigung der Vista UAC	Einfache Installation; sehr aufgeräumte Benutzeroberfläche	Einfache Installation; optional tiefer gehende Einstellungsmöglichkeiten

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

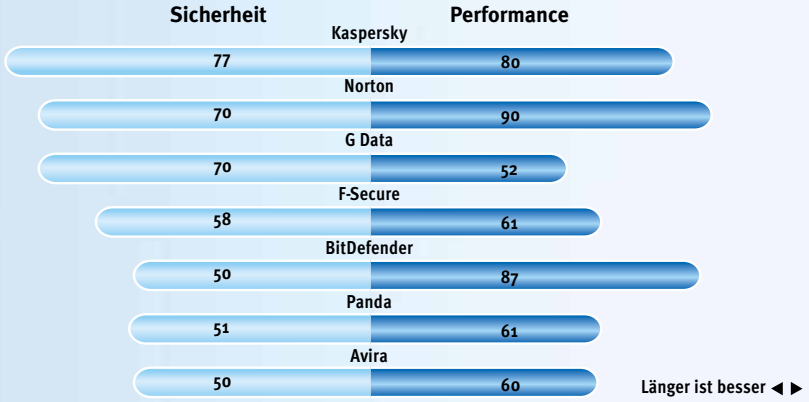
● Ja
– Nein

[1] Ohne Suite: 55 Sekunden
[2] Via Internet

PLATZ 6	PLATZ 7
Panda Internet Security 2008	**Avira Premium Security Suite**
Panda Security	Avira
80 Euro	40 Euro
www.pandasecurity.com	www.avira.de
3	1
Keine Telefon-Hotline	1,99 Euro/Minute
55 Punkte	52 Punkte
■■□□□	■■□□□
63	62
38	38
64	58
Mangelhaft	**Ausreichend**
100 %	100 %
100 %	100 %
60 %	60 %
50 %	40 %
71,78 %	62,46 %
3	5
ca. 6 Stunden	ca. 3 Stunden
Mittlere Auslastung	Mittlere Auslastung
73,1 %	73,1 %
12	12
Keine	Keine
POP3 und Outlook-Plugin	Outlook (Express)/ Windows Mail/Thunderbird
Kein Schutz	Kein Schutz
64 Sekunden	75 Sekunden
110 MByte	110 MByte
222 MByte	34 MByte
7 Min. 9 Sek.	6 Min. 53 Sek.
Nicht messbar	Nicht messbar
24 Sekunden	37 Sekunden
–	–
Kaum Nachfragen; viele Meldungen	Nutzer muss alles selbst entscheiden (kompliziert)
Nutzer muss entscheiden (mit Empfehlung)	Nutzer muss entscheiden (mit Empfehlung)
●/●/–	–/–/–
Kindersicherung, Tuning, Backup	–
Einfache Installation; mehr Funktionalität (z.B. Backup) als andere Security-Suiten	Einfache Installation; Einstellungsmöglichkeiten richten sich an Experten

Sicherheit & Performance sind gefragt

Zwei Dinge zeichnen eine gute Security-Suite aus: Sie muss sicher sein, und sie darf das System nur möglichst wenig belasten. In dieser Grafik stellen wir die Sicherheitswertung den Ergebnissen im Performance-Test gegenüber.



Kauf-Check Security-Suiten

☑ **Phishing-Filter** E-Mails zu durchsuchen reicht nicht. Achten Sie darauf, dass die Suite Phishing nicht nur mit dem Spamfilter bekämpft, sondern auch im Browser.

☑ **Virenscanner** Aktuelle Anti-Viren-Tools finden bekannte Malware schnell und zuverlässig. Das gilt jedoch oft nur für inaktive Schädlinge. Wichtig ist aber auch, dass sie bereits gestartete Angreifer finden.

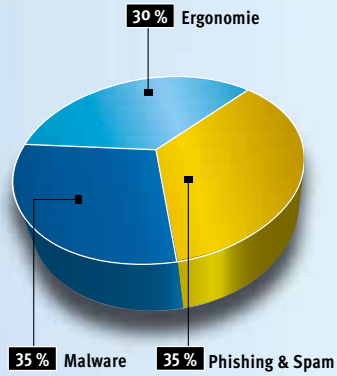
☑ **False-Positive-Rate** Ob beim Spamfilter oder bei der Viren-Erkennung: Beobachten Sie, wie oft die Suite danebenlangt und gute Tools sowie echte Mails blockiert.

☑ **Arbeitsspeicherbedarf** Achten Sie unbedingt auf einen geringen Arbeitsspeicherverbrauch – vor allem dann, wenn Ihr Rechner weniger als 1 GByte RAM besitzt.

☑ **Verständlichkeit** Selbst Profis können so manchen Warnhinweis nicht erklären. Wichtig ist, dass Sie verstehen, was die Security-Suite Ihnen mitteilen will.

☑ **Performance** Alle getesteten Produkte nehmen Einfluss auf die Geschwindigkeit Ihres Systems. In der Tabelle links erfahren Sie, wie sehr Bootzeit, Downloads und E-Mails ausgebremst werden.

So testet CHIP Security-Suiten



In Kooperation mit dem Viren-Testlabor AV-Test (**www.av-test.de**) haben wir die Erkennungsraten der Scanner einem harten Test unterzogen. Diesmal wollten wir in erster Linie wissen, ob bereits aktive Malware gefunden und komplett entfernt wurde. Außerdem mussten die Scanner zeigen, ob sie mit EXE-Packern getarnte Malware zuverlässig erkennen. Zudem erwarten wir von jedem Paket einen wirkungsvollen Phishing-Schutz. Verständliche Sicherheitswarnungen sind für jede Suite ein Muss.

ALLE PROGRAMME AUF HEFT-CD

Top-Tools fürs Web 2.0

Webserver einrichten, Heim-Netzwerke aufbauen, anonym surfen, System vor Angriffen schützen: Auf der Heft-CD finden Sie das Komplettpaket der besten Gratis-Tools für alle Internet-PCs.

Das Internet präsentiert alle nur denkbaren Informationen und Angebote. Aber nicht jede Website ist Ihnen wohlgesonnen. Hinter scheinbar seriösen Seiten verbergen sich Hacker, die unbemerkt Trojaner, Viren oder Rootkits in Ihr System schleusen.

Der Schaden kann immens sein: Verlust der privaten Daten, heimliches Durchforsten Ihres Rechners und das Ausspähen Ihrer Passwörter und Bankdaten sind nur einige Beispiele.

Mit den Tools auf der Heft-CD schützen Sie sich effektiv vor Schnüffelattacken und Schädlingen: Setzen Sie etwa den Gnu Privacy Guard (GnuPG) ein, um Ihre vertraulichen Daten zu verschlüsseln – und dank der Thunderbird-Erweiterung Enigmail können Sie sicher sein, dass nur befugte Adressaten Ihre E-Mails lesen.

Firefox ist ein sehr guter und komfortabler Browser – und mit den richtigen Plugins auch noch bombensicher: Mit NoScript schalten Sie ganz einfach Java und JavaScript ab und schützen sich so vor gefährlichen Internetseiten. Adblock Plus stoppt automatisch nervige Werbung und Popups – und mit der Firefox-Erweiterung FoxTor schalten Sie per Knopfdruck den Anonymisierer Tor bequem ein und aus.

Haben es einige Schädlinge auf Ihre Festplatte geschafft, helfen nur noch zuverlässige Tools wie AntiVir PE Classic oder Avast! 4 home weiter. Sie suchen gezielt nach Viren auf Ihrem System und löschen sie endgültig.

Die Freeware A-squared HiJack Free durchsucht den Rechner nach Hijackern, Spyware, Adware und Trojanern. Über einen Link zu Google holen Sie zu jeder von dem Programm gefundenen Datei schnell alle Informationen ein.

Außerdem auf der Heft-CD: alle Tools zum Einrichten von Servern und Datenbanken sowie privaten Blogs und Onlinegalerien.

VOLLVERSION I: ASHAMPOO MAGICAL SECURITY

Vertrauliche Daten schützen

Features
➔Schützt Dokumente
➔Sichere AES-Verschlüsselung
➔Sehr einfache Bedienung

Beschreibung Wichtige Dokumente sollten Sie nicht ungeschützt auf der Festplatte speichern: Mit der Vollversion Ashampoo Magical Security nutzen Sie die sichere AES-Verschlüsselung (Advanced Encryption Standard) zum Codieren von sensiblen Daten. Im Gegensatz zu vielen anderen Tools ist die Bedienung kinderleicht – zwei Mausklicks genügen, und Ihre vertraulichen Unterlagen sind versiegelt. Sie können die geschützten Daten auch brennen oder per E-Mail versenden.

Tipp Um das Programm freizuschalten, fordern Sie am Ende der Installation einen kostenlosen Schlüssel an, den Sie anschließend in der Vollversion eintragen.

➔CD-CODE Vollversion

VOLLVERSION II: STEGANOS SAFE ONE

Verschlüsselte Laufwerke einrichten

Features
➔Kann zwei Datensafes anlegen
➔Passwortgenerator
➔Nutzt externe Speicher als Schlüssel

Beschreibung Wenn Sie Ihren PC mit mehreren Personen teilen oder ein Notebook besitzen, sollten Sie Ihre vertraulichen Daten niemals ungeschützt auf dem Rechner lassen. Mit Steganos Safe One legen Sie per Knopfdruck bis zu zwei virtuelle, verschlüsselte Laufwerke an. Diese Datensafes fassen jeweils bis zu 1 GByte an Daten. So können Sie Ihre Dokumente wirklich sicher auf der Festplatte ablegen und brauchen keine Angst zu haben, dass Unbefugte an Ihre Daten kommen.

Tipp Wenn Sie sich keine Passwörter merken möchten, können Sie externe Datenspeicher wie USB-Sticks, MP3-Player oder ActiveSync-fähige Handys als Zugangsschlüssel nutzen.

➔CD-CODE Vollversion

HINWEISE ZUR CD

So legen Sie los

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

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

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

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

DIE 50 TOP-TOOLS

→ CD-CODE ◎ BROWSER

→ CD-CODE ◎ NETZWERK

→ CD-CODE ◎ PHP/CMS

→ CD-CODE ◎ SECURITY

ALLE PROGRAMME AUF HEFT-CD

Die 50 besten Tools

Das Internet ist aus dem Alltag kaum wegzudenken – umso wichtiger ist der Schutz vor potenziellen Angreifern und Schädlingen. Die besten Gratis-Tools finden Sie auf der Heft-CD.

VLC MEDIA PLAYER

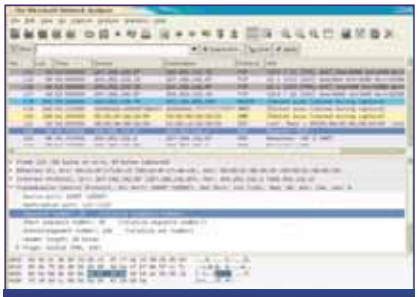
Alle Formate spielen

Features
→ Spielt alle gängigen Formate ab
→ Unterstützt Streaming
→ Individuell einstellbar

Beschreibung Der VLC Media Player spielt nahezu alle Audio- und Videodateien ab, darunter MP3, DVD, Video-CD, MPEG und DivX. Die Besonderheit: Der Player unterstützt MPEG- und DivX-Streaming und kann damit auch Videos schon während des Downloads abspielen. So können Sie bereits beim Herunterladen prüfen, ob Sie die richtige Datei erhalten.

Tipp Verschiedene Skins für den Player finden Sie unter **www.videolan.org/vlc**.

→CD-CODE Netzwerk



WIRESHARK

Netzwerke prüfen

Features
→ Analysiert den Netzwerkverkehr
→ Erkennt mehr als 470 Protokolle
→ Findet Sicherheitslücken

Beschreibung Wireshark ist eines der beliebtesten und umfangreichsten Tools zur Netzwerkanalyse. Es untersucht den Datenverkehr auf Protokollebene. Die Freeware arbeitet perfekt auf Ethernet, Token Ring und FDDI. Wireless LANs können Sie unter Windows nur eingeschränkt untersuchen.

Tipp Eine komplette Anleitung finden Sie unter **www.wireshark.org**. Wer die WinPcap-Bibliothek installiert hat, kann den Netzwerkverkehr auswerten.

→CD-CODE Netzwerk

ADBLOCK PLUS

Werbung abschalten

Features
→ Geniale Firefox-Erweiterung
→ Stoppt Werbung
→ Eigene Regeln definieren

Beschreibung Mit dem Firefox-Plugin Adblock Plus unterbinden Sie nervige Pop-ups und Werbung im Browser. Sie können vordefinierte Regeln nutzen und eigene festlegen. Erscheint trotzdem ein störendes Banner, klicken Sie einfach mit der rechten Maustaste auf das Objekt – danach blockt das Firefox-Addon das Banner künftig automatisch.

Tipp Das Surfen ohne Werbung hat den positiven Nebeneffekt, dass auch der Seitenaufbau schneller vonstatten geht.

→CD-CODE Browser

TOR-, PRIVOXY- & VIDALIA-PAKET

Sicher und unerkannt surfen

Features
→ Anonymisiert den Datenverkehr
→ Blockt Werbung
→ Schützt vor Angriffen

Beschreibung Lassen Sie sich nicht ausspionieren! Das Paket aus Tor, Privoxy und Vidalia bietet Ihnen mehr Schutz im Internet. Tor anonymisiert Ihre Vorgänge, indem es Ihre Datenkommunikation durch ein verteiltes Netzwerk von Servern leitet. Diese Server (Onion Router) schützen Sie vor Webseiten, die Ihre persönlichen Profile sammeln – und vor Angreifern, die Ihren Datenverkehr abhören. Die EXE-Datei enthält neben Tor noch ein Control-Panel und das kostenlose Privoxy – ein Webproxy, der für zusätzlichen Schutz und mehr Privatsphäre im Internet sorgt. Sie können Privoxy zusätzlich als Werbeblocker nutzen.

Tipp Für Firefox gibt es einige Addons, mit denen Sie Tor per Knopfdruck ein- und ausschalten, etwa FoxTor. Auf der Heft-CD finden Sie auch den vorkonfigurierten Sicherheitsbrowser XeroBank.

→CD-CODE Netzwerk

JAP

Spuren im Netz verwischen

ahnender User. Mit JAP bremsen Sie die Spione aus und surfen nahezu anonym durch das Internet. Wenn Sie mit dem kostenlosen Tool auf Webseiten zugreifen, bekommen weder der angefragte Server noch der Provider mit, welche Internetseiten Sie ansteuern. Dabei bedient sich JAP eines einfachen Tricks: Ihre Verbindung wird unter allen JAP-Nutzern versteckt. JAP folgt dem Peer-to-Peer-Prinzip: Je mehr User den Dienst nutzen, desto schwieriger ist das Aufspüren einzelner Aufrufe. Einen zusätzlichen Schutz vor Lauschangriffen auf Ihre Internetverbindung bietet das Programm, indem der Datenverkehr über drei Proxyserver läuft. Pro Station wird Ihre Verbindung dann zusätzlich verschlüsselt.

Features
→ Surfverhalten verschleiern
→ Anonyme Verbindungen aufbauen
→ Automatische Konfiguration

Beschreibung Schnüffelangriffe im Internet nehmen rapide zu. Besonders gefragt sind die privaten Informationen nichts

Tipp Einen ausführlichen Workshop zum Einsatz von JAP sowie des Tor-, Privoxy- & Vidalia-Pakets finden Sie ab 60.

→CD-CODE Netzwerk

GALLERY CONSTRUCTOR

Galerien basteln

Features
→ Legt automatisch Webalben an
→ Diashows gestalten
→ Einfache Bedienung

Beschreibung Wer schnell und unkompliziert eine Onlinegalerie anlegen möchte, liegt mit diesem Tool genau richtig. Der Gallery Constructor generiert aus ausgewählten Bildern Miniaturansichten und bindet sie in Internetseiten ein. Auf Wunsch können sich die Besucher Ihrer Homepage die Originalbilder oder eine Diashow ansehen.

Tipp Das Programm nutzt fertige Vorlagen, und ein Wizard hilft beim Einrichten der Seiten.

→CD-CODE PHP/CMS

GNU PRIVACY GUARD

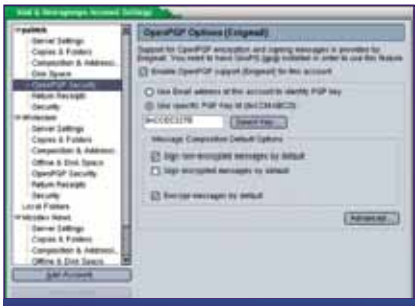
Dokumente codieren

Features
→ Verschlüsselt Daten
→ Hoher Sicherheitsstandard
→ Mit vielen Tools kompatibel

Beschreibung Das Open-Source-Programm Gnu Privacy Guard (GnuPG) kryptographiert Dokumente über die Kommandozeile. Das Tool unterstützt aber auch zahlreiche Mail- und Chatprogramme. GnuPG unterstützt etwa die Verschlüsselungsalgorithmen ElGamal, DSA, RSA, AES, Blowfish und Twofish.

Tipp Eine Liste der unterstützten Tools sowie Frontends finden Sie unter **www.gnupg.org**.

→CD-CODE Netzwerk



ENIGMAIL

Mails verschlüsseln

Features
→ Addon für Thunderbird
→ Nutzt GnuPG
→ Verschickt sichere Nachrichten

Beschreibung Enigmail erweitert Thunderbird mit dem Feature, Nachrichten verschlüsselt zu verschicken. Das Addon codiert E-Mails mit der Schutzsoftware GnuPG. So versenden Sie vertrauliche Nachrichten, ohne befürchten zu müssen, dass nicht-autorisierte Personen mitlesen.

Tipp Um die Erweiterung zu installieren, müssen Sie die Datei lediglich mit Thunderbird öffnen.

→CD-CODE Netzwerk

MAMBO

Netzseiten verwalten

Features
→ Umfangreiches CMS
→ Viele Erweiterungen
→ Individuell anpassbar

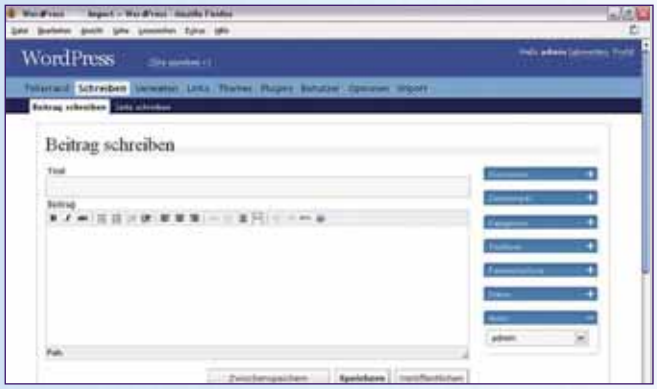
Beschreibung Mambo ist ein leistungsstarkes Content Management System (CMS), mit dem Sie Ihre Webseiten up to date halten. Auch das Anlegen von Onlineshops und anderen Webangeboten ist mit Mambo kein Problem.

Tipp Um das Tool nutzen zu können, benötigen Sie MySQL, PHP und den Apache-Server. Viele Erweiterungen finden Sie unter **http://source.mambo-foundation.org**.

→CD-CODE PHP/CMS

WORDPRESS

Professionelle Weblogs gestalten



Features
➜ Umfangreiches Blogtool
➜ Diverse Vorlagen und Themes
➜ Leichte Bedienung

Beschreibung Machen Sie mit beim Web 2.0, und basteln Sie Ihre eigene Newsseite oder ein persönliches Onlinetagebuch. WordPress ist ein professionelles und einfach zu bedienendes Blogprogramm, mit dem Sie in regelmäßigen Abständen Text- und Bildbeiträge auf Ihrem Webspace veröffentlichen. Wählen Sie einfach die gewünschte Vorlage – und schon können Sie Ihre Beiträge online stellen. In der Vorschau sehen Sie sofort, wie andere Leser Ihren Blog wahrnehmen. Der Upload von Bildern erfolgt über einen einfachen Dateidialog, um die Anpassung ans Layout kümmert sich WordPress. Zudem lassen sich einzelne Beiträge mit einem Passwortschutz oder mit einem Kommentarfeld für die Leser versehen.

Tipp Für WordPress gibt es zahlreiche Erweiterungen und Themes im Internet, mit denen Sie Ihren Blog aufwerten können. Hilfe und Tutorials finden Sie unter der Adresse **http://codex.wordpress.org**.

➜CD-CODE PHP/CMS

JOOMLA

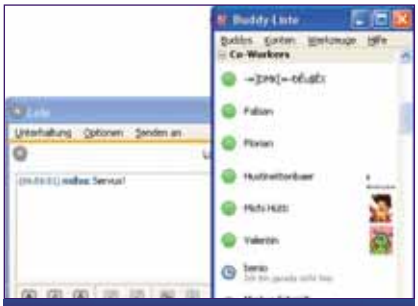
Netzdienste basteln

Features
➜ Webauftritt gestalten
➜ Vielseitiges CMS
➜ Bedienung per Browser

Beschreibung Das Content Management System (CMS) Joomla ist mit dem Tool Mambo verwandt. Wie sein Konkurrent ist auch Joomla sehr umfangreich und lässt sich individuell anpassen. Es eignet sich beispielsweise zum Gestalten eigener Webshops und anderer Dienstleistungen. Das Programm steuern Sie über einen Browser.

Tipp Ab 72 zeigen wir Ihnen auf neun Seiten, wie Sie mit Joomla eine professionelle Webpräsenz aufbauen können.

➜CD-CODE PHP/CMS



PIDGIN

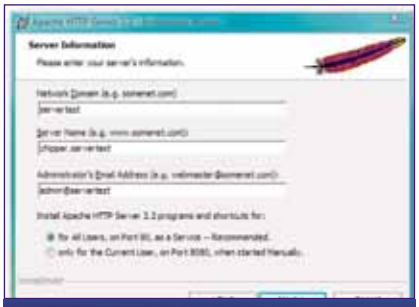
Stets erreichbar sein

Features
➜ Instant-Messenger
➜ Unterstützt zahlreiche Protokolle
➜ Viele Themes und Plugins

Beschreibung Pidgin ist ein kostenloser Instant-Messenger für alle Netzwerke. Das Tool ist unter anderem kompatibel zu ICQ, AIM, MSN, Yahoo und zum IRC-Netzwerk. Sie können sich gleichzeitig in die verschiedenen Protokolle einwählen und die meisten Funktionen des jeweiligen Messengers nutzen.

Tipp Mit Plugins lässt sich Pidgin individuell gestalten. So können Sie den Messenger etwa transparent setzen.

➜CD-CODE Netzwerk



APACHE HTTP-SERVER

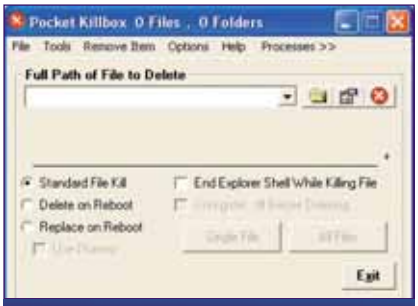
Webserver anlegen

Features
➜ Richtet einen Server ein
➜ Sehr flexibel
➜ Zahlreiche Anleitungen

Beschreibung Das Open-Source-Programm ist der beliebteste Webserver. Apache ist modular aufgebaut, was eine sehr individuelle Konfiguration ermöglicht. Der HTTP-Server ist die perfekte Lösung für User mit soliden Grundkenntnissen.

Tipp Einen Webserver einzurichten erfordert einige Kenntnisse. Ausführliche Hilfe finden Sie auf der offiziellen Website unter **www.apache.de**.

➜CD-CODE Netzwerk



POCKET KILLBOX

Alles löschen

Features
➜ Entfernt hartnäckige Spyware
➜ Keine Installation nötig
➜ Kinderleichte Bedienung

Beschreibung Pocket KillBox ist ein Tool, das Spyware und andere Daten löschen kann, die sich mit Windows-Bordmitteln nicht entfernen lassen wollen. Das Programm startet ohne Installation. Nach dem Öffnen können Sie sofort einzelne Dateien oder ganze Verzeichnisse angeben, die Pocket KillBox löschen soll.

Tipp Nach dem Löschvorgang muss das System neu gestartet werden.

➜CD-CODE Security

AZUREUS (VUZE)

Alle Daten bequem saugen

Features
→ BitTorrent-Client
→ Neue Oberfläche
→ Verbesserte Funktionen

Beschreibung BitTorrent-Clients gibt es wie Sand am Meer – aber nur wenige bieten zahlreiche Funktionen und gute Einstellmöglichkeiten. Zu den derzeit besten Clients gehört Azureus: In der neuen Version bringt das Programm unter dem Namen Vuze eine grundlegend überarbeitete Oberfläche mit, die Videoportalen wie YouTube ähnelt: Sie können sich Vorschaubilder von den Angeboten anzeigen lassen und thematisch in unterschiedlichen Rubriken suchen. Die umfangreich ausgestattete Freeware bietet alle wichtigen Funktionen, um schnell an die gewünschten Dateien zu kommen, etwa Multi-Download, Prioritäten setzen, Vorschau, IRC-Client und Statistikfunktion.

Tipp Damit Azureus (Vuze) auf Ihrem System startet, müssen Sie die Java Runtimes installiert haben. Ausführliche Hilfestellungen finden Sie im Web unter **http://azureus.sourceforge.net**.

→CD-CODE Netzwerk

FIREFOX 3.0 BETA

Schnell und sicher

Features
→ Verbesserte Schutzmechanismen
→ Zoomfunktion
→ Schneller als der Vorgänger

Beschreibung Die neue Firefox-Version bringt viele Detailverbesserungen mit: Die Entwickler haben die Bookmark-Verwaltung überarbeitet, bessere Schutzmaßnahmen eingebaut und ordentlich an der Geschwindigkeit geschraubt. Ebenfalls neu ist die Zoomfunktion.

Hinweis Firefox 3 befindet sich noch im Beta-Stadium. Sie sollten das Tool aus diesem Grund nicht als Standardbrowser nutzen. Die Vorabversion dient ausschließlich Testzwecken.

→CD-CODE Browser

ZONEALARM

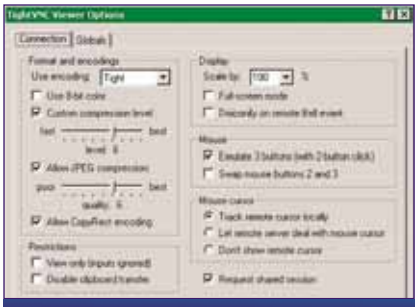
Angreifer aussperren

Features
→ Verschleiert den PC im Internet
→ Schützt vor Angriffen
→ Automatische Konfiguration

Beschreibung Das Freeware-Tool ist eine zuverlässige Firewall, die vor Hackern schützt. Ein großer Vorteil von ZoneAlarm besteht in seiner besonders einfachen Bedienung und der „Stealth"-Funktion, mit der Sie unsichtbar im Internet unterwegs sind.

Tipp Im Gegensatz zu vielen anderen Firewalls verlangt ZoneAlarm keine manuelle Konfiguration. Daher eignet sich die Freeware auch für unerfahrene User.

→CD-CODE Security



TIGHTVNC

PCs fernsteuern

Features
→ Fremde PCs fernwarten
→ Daten privat tauschen
→ Einfache Installation

Beschreibung Mit TightVNC steuern Sie fremde Rechner, als ob Sie direkt davor sitzen würden. Sie sehen den Bildschirminhalt des entfernten Computers und können sowohl die Maus als auch die Tastatur einsetzen.

Tipp Das Tool erlaubt auch einen einfachen Datentransfer und funktioniert plattformunabhängig. Hilfe zum Einrichten der Software finden Sie unter **www.tightvnc.com**.

→CD-CODE Netzwerk

ANTIVIR PE CLASSIC

Viren vernichten

Features
→ Schützt vor PC-Schädlingen
→ Zuverlässig und schnell
→ Echtzeit-Scanner

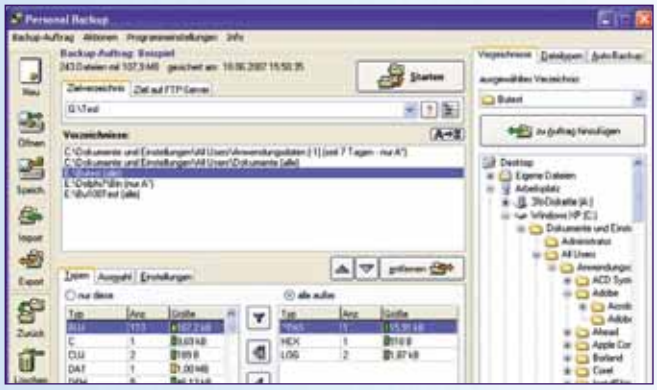
Beschreibung Mit AntiVir stehen dem Anwender gleich zwei Sicherheitsfeatures zur Verfügung: Während der integrierte Echtzeit-Scanner laufend Ihr System überwacht, können vorsichtige User mit dem Prüftool einzelne Downloads, komplette Ordner oder die ganze Festplatte manuell nach PC-Schädlingen durchsuchen.

Tipp Ein kostenloses Handbuch finden Sie unter **www.free-av.de.**

→CD-CODE Security

PERSONAL BACKUP

Persönliche Daten sichern



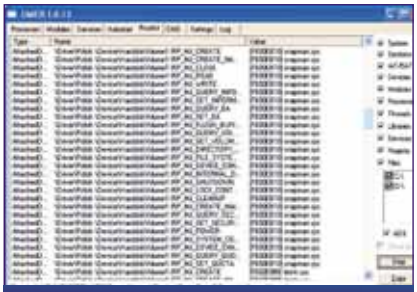
Features
→ Legt Backups an
→ Verzeichnisse frei wählbar
→ Kann Daten komprimieren

Beschreibung Mit Personal Backup sichern Sie Ihre persönlichen Daten in einem beliebigen Zielverzeichnis auf Ihrer Festplatte oder in einem Netzwerk. Unterverzeichnisse bindet das Tool automatisch ein. Praktisch und platzsparend: Auf Wunsch speichert Personal Backup die Daten komprimiert. Filterfunktionen erlauben ein bequemes Backup von ausgewählten Dateien, etwa aller Word-Dokumente. Das Anlegen eines Backups können Sie manuell starten oder automatisch vornehmen lassen – zu einem festgelegten Zeitpunkt oder auch bei jedem An- oder Abmelden des Benutzers.

Tipp Um Ihre Daten zuverlässig zu schützen, sollten Sie regelmäßig neue Sicherheitskopien anlegen. Speichern Sie die Backups nicht auf der Partition Ihres Betriebssystems.

Hinweis Das Anlegen eines automatischen Backups beim Herunterfahren funktioniert unter Windows Vista nicht.

→CD-CODE Security



GMER

Rootkits enttarnen

Features
→ Schädlinge bekämpfen
→ Keine Installation nötig
→ Immer einsatzbereit

Beschreibung Schnell und einfach: Gmer durchsucht Ihren Rechner nach Rootkits und schützt Sie so vor unerwünschten Gästen. Das Programm benötigt keine Installation und kann auf externen Speichermedien, etwa USB-Sticks, platziert werden.

Tipp Das Tool durchsucht den Rechner nach allen laufenden Prozessen, versteckten Modulen, Dateien oder Registrierungsschlüsseln. Gefundene Rootkits können Sie sofort entfernen.

→CD-CODE Security

PHPMYADMIN

Daten verwalten

Features
→ Datenbanken per Browser pflegen
→ Erledigt die wichtigsten Aufgaben
→ Unterstützt SQL-Statements

Beschreibung Das Tool ist ein PHP-Programm zum Anlegen und Administrieren von Datenbanken. Da Sie phpMyAdmin per Browser bedienen, benötigen Sie beim Verwalten keinen speziellen Rechner.

Tipp Das Open-Source-Programm bietet eine grafische Oberfläche (WYSIWYG). Umfassende Programmierkenntnisse in SQL sind in phpMyAdmin daher nicht erforderlich.

→CD-CODE PHP/CMS

OPERA

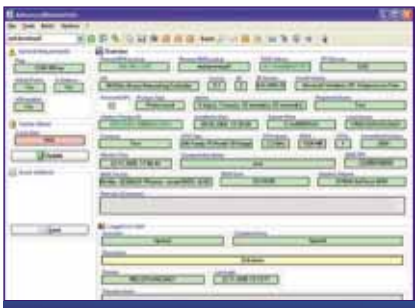
Besser surfen

Features
→ Neue Rendering-Engine
→ Integrierter E-Mail-Client
→ Verbesserter Schutz

Beschreibung Mit dieser Vorabversion testen Sie die neuen Funktionen des umfangreichen Browsers. Opera vereint alle wichtigen Webprogramme unter einem Dach, etwa einen E-Mail- und BitTorrent-Client. Zusätzlich bietet es zahlreiche Widgets.

Achtung Eine ältere Opera-Version sollten Sie vor der Installation löschen. Einen Test der wichtigsten Webbrowser finden Sie ab 50.

→CD-CODE Browser



ADVANCEDREMOTEINFO

Netz durchforsten

Features
→ Analysiert Netzwerke
→ Kann Rechner herunterfahren
→ Screenshot-Funktion

Beschreibung AdvancedRemoteInfo liefert Ihnen zahlreiche Informationen über alle Netzwerkrechner. Die Software übermittelt alle wichtigen Daten – von der IP-Adresse bis zum eingeloggten User. Mit der Screenshot-Funktion können Sie alle Änderungen einfach und übersichtlich dokumentieren.

Tipp Das Tool kann andere PCs im Netz herunterfahren. Manuelles Ausschalten wird somit überflüssig.

→CD-CODE Netzwerk

XAMPP

Komplettes Serverpaket

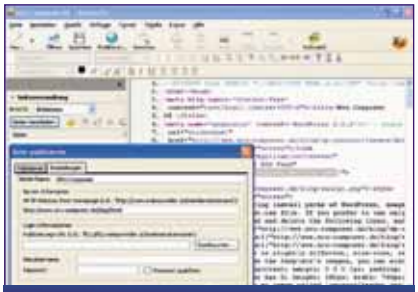
XAMPP sparen Sie sich dagegen viel Aufwand: Die Datei beherbergt ein komplettes Softwarepaket, das alle notwendigen Programme zur Einrichtung und Wartung eines Webservers mitbringt. Die Abkürzung „XAMPP“ steht für „X“ (alle beliebigen Betriebssysteme), „Apache“, „MySQL“, „PHP“ und „Perl“. Im XAMPP-Paket sind zahlreiche Tools enthalten: So finden Sie darin neben den Hauptprogrammen etwa auch den FileZilla FTP Server, OpenSSL, phpMyAdmin, SQLite sowie das XAMPP Control Panel, XAMPP Security und ADODB.

Features
→ Alle wichtigen Tools in einer Datei
→ Automatische Einrichtung
→ Leicht konfigurierbar

Beschreibung Einen Server einzurichten erfordert einiges an Arbeit und solide Kenntnisse. Bis die einzelnen Komponenten eingerichtet sind und einwandfrei laufen, können Wochen vergehen. Mit

Tipp Hilfe und weiterführende Informationen finden Sie im Internet unter **www.apachefriends.org.**

→CD-CODE PHP/CMS



KOMPOZER PORTABLE

Homepages bauen

Features
→ Grafische Oberfläche
→ Nutzt die Gecko-Engine von Mozilla
→ FTP-Dateimanager

Beschreibung Der KompoZer ist ein kostenloser HTML-Editor, der auf der Gecko-Engine von Mozilla basiert. Die Bedienung geht leicht von der Hand. Das Programm besitzt eine grafische Oberfläche, in der Sie Text, Bilder und Tabellen schnell zu einer eigenen HTML-Seite zusammenbauen. Auch das Anlegen von Formularen ist mit KompoZer kein Problem.

Tipp Erleichtern Sie sich das Arbeiten, indem Sie die Registerfunktion nutzen.

→CD-CODE PHP/CMS

IMGBURN

Images brennen

Features
→ Unterstützt die wichtigsten Formate
→ Arbeitet ressourcenschonend
→ Einfache Bedienung

Beschreibung ImgBurn ist ein Tool, mit dem Sie im Handumdrehen Images brennen. Das Programm unterstützt alle gängigen Formate wie BIN, CDI, GCM sowie GI, IBQ, IMG, ISO und MDS.

Tipp Die Bedienung des Programms könnte kaum einfacher sein: Zum Brennen ziehen Sie die Datei einfach in das Programmfenster und bestätigen Ihre Auswahl. Den Rest übernimmt dann ImgBurn für Sie.

→CD-CODE Security

A-SQUARED HIJACK FREE

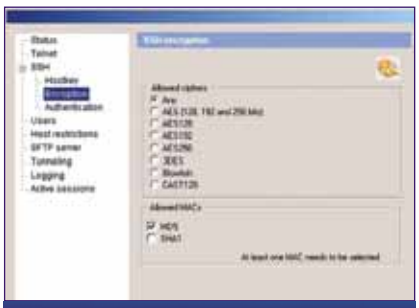
Rechner säubern

Features
→ Durchsucht den PC nach Schädlingen
→ Zeigt offene Ports an
→ Generiert eine Liste der Schädlinge

Beschreibung A-squared HiJackFree durchsucht Ihren PC nach Hijackern, Spyware, Adware, Trojanern und Würmern. Zusätzlich zeigt es alle auf Ihrem Rechner installierten Autostarts, Explorer-Addons, Dienste, offenen Ports, Hosts und laufenden Prozesse an.

Tipp Über einen Link zu Google können Sie sich zu jeder Datei Informationen anzeigen lassen. Schädlinge löschen Sie einfach per Knopfdruck.

→CD-CODE Security



FREESSHD

Sichere Verbindung

Features
→ PCs administrieren
→ Verschlüsselte Übertragung
→ Daten tauschen

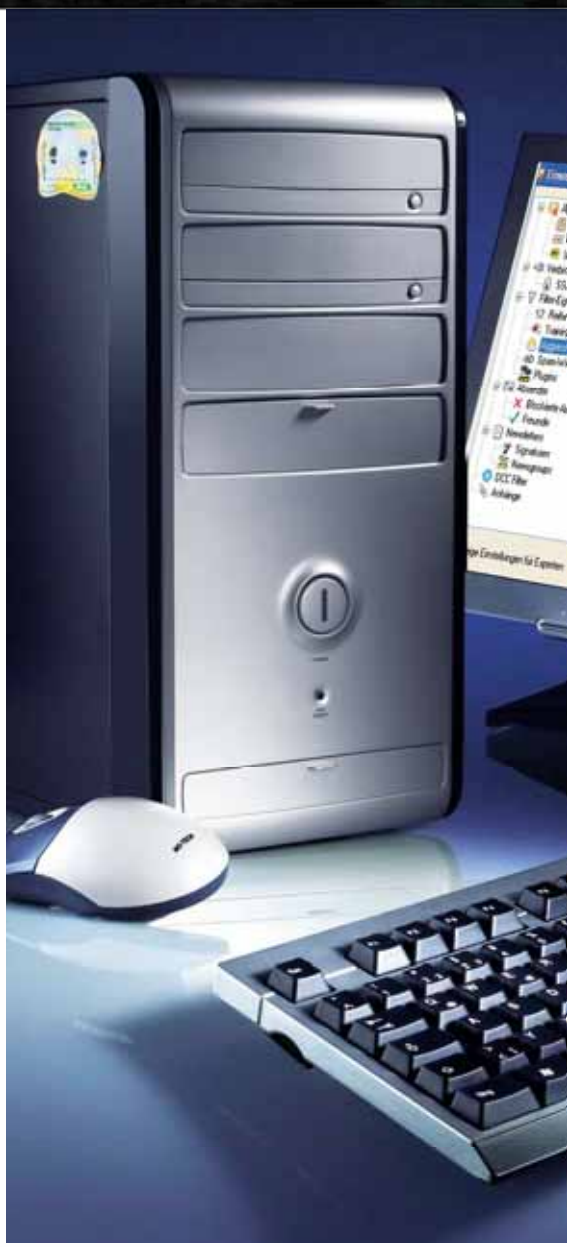
Beschreibung FreeSSHd bietet eine 2048-Bit-verschlüsselte Übertragung über eine Secure Shell (SSH) und einen integrierten SFTP-Server. Damit ist das Steuern von Remote-PCs kein Problem mehr. Das Tool eignet sich besonders zur Fernwartung anderer Rechner im Netzwerk.

Tipp Das Programm benötigt die Ports 22 (SSH) und 23 (Telnet), um eine externe Verbindung aufbauen zu können.

→CD-CODE Netzwerk

10 Gebote für mehr Sicherheit

Ihr Rechner ist im Internet vielen Gefahren ausgesetzt, und nicht alle lassen sich mit einem Virenscanner abwehren. Wir zeigen Ihnen, was sonst noch erforderlich ist.



Alle Computer, die in irgendeiner Form mit der Außenwelt kommunizieren, sind in Gefahr, von Schadprogrammen befallen zu werden. Und es gibt praktisch keinen PC, der von der restlichen Welt komplett abgeschottet wäre. Zwar muss ein Rechner nicht unbedingt an ein Netzwerk angeschlossen sein. Um absolute Sicherheit zu haben, müssten Sie jedoch auch auf Datentransfers verzichten, also auf das Öffnen oder Kopieren von Dateien, die auf CD, DVD oder USB-Stick vorliegen. Das ist jedoch keine praktikable Lösung.

Vorsicht ist also angesagt. Auf den folgenden Seiten stellen wir Ihnen daher die größten Bedrohungen für die Sicherheit Ihres PCs vor und zeigen Ihnen, wie Sie sich dagegen wappnen.

1 Updates: Computer immer aktuell halten

Risiko Software wird immer komplexer und muss gleichzeitig in immer kürzerer Zeit entwickelt werden. Das heißt, dass die Programme aus immer mehr Code bestehen, der immer weniger getestet wurde. In der Folge enthalten sie mehr Fehler und bieten Hackern damit auch mehr Angriffspunkte. Davon ist nicht nur das Betriebssystem betroffen, sondern auch die zugehörigen Anwendungen – unter anderem der Browser, die Firewall und natürlich auch die E-Mail- und Messenger-Applikationen.

Lösung Meist vergeht einige Zeit, bis jemand die Schwachstellen findet und der Hersteller entsprechende Sicherheitspatches bereitstellt. Sobald jedoch ein solcher Patch verfügbar ist, sollten Sie ihn sofort herunterladen und installieren. Falls das angeboten wird, sollten Sie der Software erlauben, im Internet selbstständig nach Updates zu suchen und sie einzurichten. So ist gewährleistet, dass die Sicherheitslücken so schnell wie möglich geschlossen werden.

Ganz besonders bei Windows ist es wichtig, dass Sie die Patches rasch installieren. Dabei unterstützt Sie unter XP und Vista das Windows Update, das in der neuesten Windows-Version nicht nur das Betriebssystem, sondern auch die Office-Anwendungen von Microsoft auf dem aktuellen Stand hält. Für alle Anwendungen ohne automatische Update-Funktion sollten Sie – etwa über Outlook – einen Alarm einrichten, der Sie regelmäßig daran erinnert, im Internet nach Aktualisierungen zu suchen und sie zu installieren.

Denken Sie immer daran: Sie sind nur dann einigermaßen sicher im Internet unterwegs, wenn bei Ihrem PC alle bekannten Sicherheitslecks gestopft sind.

2 E-Mail: Kommunizieren nur mit Virenscanner

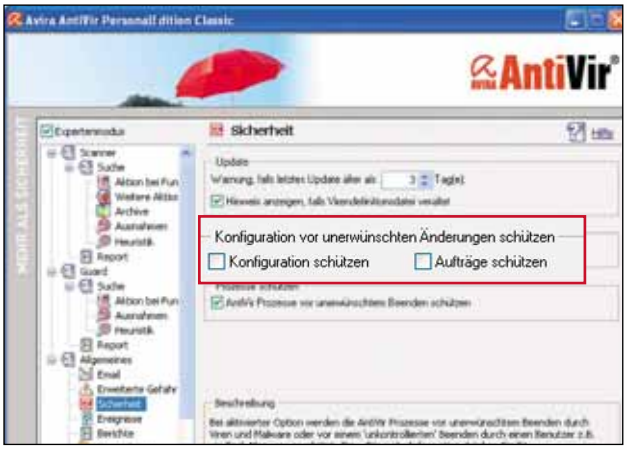
Risiko Die am häufigsten genutzte Internetanwendung ist die Kommunikation per E-Mail. Daher sind Attacken per Mail bei Hackern sehr beliebt. Seit man die Nachrichten nicht nur im reinen Text-, sondern auch im HTML-Format verschicken kann, beschränken sich die Angriffe nicht mehr allein auf die Infizierung von Dateianhängen. Stattdessen werden auch eingebettete Programmzeilen in JavaScript oder VBScript dazu genutzt, um heimlich unerwünschte Programme nachzuladen. Diese Anwendungen öffnen dann meist eine Hintertür zu Ihrem Rechner und verwandeln ihn beispielsweise in eine Ausgangsbasis für das Versenden von Spammails.

Lösung Setzen Sie Ihren E-Mail-Client möglichst nur im Zusammenspiel mit einem Virenscanner ein, der die eingehenden Nachrichten auf Schadcode untersucht. Dazu ist allerdings in der Regel ein kommerzielles Programm wie beispielsweise von Symantec oder Kaspersky erforderlich. Das beliebte und kostenlose AntiVir PersonalEdition Classic von Avira (**www.freeav.de**) öffnet zwar im Expertenmodus ein Konfigurationsfens-

Auf Heft-CD

- A-squared Anti-Dialer (Security)
- AVG Anti-Virus Free (Security)
- Spybot – Search & Destroy (Security)

Foto: K. Satzinger



E-Mail-Viren Der Virenscanner sollte vor ungewollten Veränderungen an seiner Konfiguration geschützt werden.

ter namens „Email“. Die dortigen Einstellungen erlauben es dem Programm jedoch nur, Ihnen beim Fund eines Virus eine Nachricht zu schicken.

Achten Sie beim Einsatz eines Virenscanners darauf, dass er immer aktuell ist. Jedes Programm bietet eine Funktion für automatische Aktualisierungen. Darüber hinaus haben Sie normalerweise auch die Möglichkeit, die Update-Suche selbst zu starten. Das empfiehlt sich beispielsweise dann, wenn der Rechner längere Zeit nicht eingeschaltet war und die Virendefinitionen daher nicht mehr aktuell sind. Bevor Sie irgendetwas anderes mit Windows machen, sollten Sie in diesem Fall erst einmal ein Update des Virenscanners anstoßen. Anschließend können Sie dann wieder die automatische Aktualisierung dafür Sorge tragen lassen, dass die Software über die neuesten Informationen verfügt.

Viele E-Mail-Provider bieten mittlerweile für eingehende Nachrichten eine eigene, Server-basierte Prüfung auf enthaltene Viren an. Sie ist allerdings in der Regel kostenpflichtig und lediglich in den erweiterten E-Mail-Diensten der Firmen enthalten.

3 Spam: Schutzmaßnahmen aktivieren

Risiko Spammer versenden gern HTML-Mails – dadurch hoffen sie, mehr über den Empfänger der Nachricht zu erfahren. Dazu platzieren sie im HTML-Code Links auf Bilder, die beim Öffnen der Nachricht automatisch nachgeladen werden. Der Adressat der E-Mail bekommt davon nichts mit, die Bilder sind teilweise nur ein Pixel groß. Wenn eine solche Grafik vom Server abgerufen wird, weiß der Absender zum einen, dass es sich um eine gültige Mailadresse handelt, und zum anderen kann er anhand der IP-Adresse Rückschlüsse auf den Standort seines Opfers ziehen. Diese Informationen erhöhen den Wert einer Mailadresse beim Weiterverkauf.

Lösung Die meisten Mailprogramme enthalten heute einen Schutzmechanismus, der das automatische Nachladen von eingebetteten Bilddateien verhindert. Microsoft Outlook beispielsweise ruft die Bilder erst ab, wenn Sie nach einer Rückfrage des Programms die Erlaubnis dazu erteilen. Sie finden die Einstellung unter „Extras | Optionen“ auf der Registerkarte „Sicherheit“.

Damit Spam gar nicht erst bis zu Ihrem Mailclient durchdringt, sollten Sie einen Provider mit Spamfilter wählen. Alle größeren Anbieter, wie Yahoo, GMX oder Web.de, bieten eine solche Funktion auch in den kostenlosen Varianten ihrer Maildienste an.

Bei GMX etwa finden Sie die Anti-Spam-Funktionen in der Rubrik „Spamschutz“. Sie bietet verschiedene Möglichkeiten an, E-Mails zu überprüfen:

- Der „Textmuster-Profiler“ analysiert eingehende Nachrichten und vergleicht sie mit den E-Mails im Ordner „Spamverdacht“. Findet er dabei eine hohe Übereinstimmung, verschiebt GMX die Mails automatisch zu den anderen verdächtigen Dokumenten.
- Der „Briefkopf-Analyzer“ sucht nach Schlüsselwörtern wie zum Beispiel „Viagra“. Wird er fündig, setzt GMX die E-Mail in den Spamordner.
- Der „Spamserver-Blocker“ prüft die eingehenden Mails auf gefälschte Absenderadressen. Zwar lassen sich die Mailadressen leicht manipulieren, nicht jedoch die IP-Adressen der Server, welche die Nachrichten verschicken. Auf diese Weise lässt sich gleichfalls viel unerwünschte Werbung aussortieren.

Weiterhin bietet GMX auch Funktionen zum Anlegen von Black- und White-Listen. Dort können Sie Absender aufnehmen, die entweder grundsätzlich vertrauenswürdig sind – oder unerwünscht und daher nicht bis zu Ihrem Postfach durchgelassen werden sollen.

Schließlich überprüft GMX die eingehenden Mails noch anhand von zwei Anti-Spam-Listen: Die globale Liste enthält eine Sammlung von Servern, die zum Versand von Spam genutzt werden. →

Die Administratoren der GMX-Server verwalten darüber hinaus eine eigene Spamliste, die durch die GMX-User täglich erweitert wird.

Was mit dem Spam geschehen soll, können Sie einstellen. Sie können die Nachrichten sofort löschen lassen oder auch im Ordner „Spamverdacht“ speichern. Auf diese Weise haben Sie noch ein Sicherheitsnetz, falls eine E-Mail fälschlicherweise als Spam identifiziert und nicht zugestellt wurde.

Aber Achtung: Der Inhalt des Ordners „Spamverdacht“ wird von GMX regelmäßig gelöscht. In welchen Zeitintervallen das geschieht, können Sie jedoch individuell festlegen.

Sie können den Spamfilter noch effizienter machen, indem Sie ihn trainieren. Dazu löschen Sie die Spammails nicht nur, sondern markieren sie – entweder mit dem Schild „Durchfahrt verboten“ aus der Übersicht oder indem Sie sie per Drag & Drop in den Ordner „Spamverdacht“ verschieben.

Falls Ihr eigener E-Mail-Provider keinen Spamfilter anbietet, können Sie auf ein zusätzliches Tool wie beispielsweise die Freeware Spamihilator (**www.spamihilator.com**) zurückgreifen. Dieses Programm schaltet sich zwischen den E-Mail-Server und den Posteingang auf Ihrem Computer und führt eine Vorsortierung der Nachrichten durch. Es identifiziert Spam mit einem lernfähigen Filter und einer Liste von Schlüsselwörtern. Mithilfe von Plugins lässt sich das Tool auch um Funktionen wie Black- und White-Listen erweitern. Spamihilator ist kompatibel zu praktisch allen verbreiteten E-Mail-Programmen.

Spam Zum Schutz vor Spam bietet Outlook an, Bilder in HTML-Mails erst nach ausdrücklicher Zustimmung zu laden.

4 Phishing: Aktuelle Browser-Generation nutzen

Risiko Während die bislang aufgeführten Punkte lediglich Bedrohungen für Ihren Rechner und die darauf gespeicherten Daten darstellen, geht es beim Thema Phishing direkt an den Geldbeutel. Denn die Internetgangster bedienen sich immer dreisterer Methoden, um an Ihr Geld zu kommen. Sie schicken Ihnen beispielsweise eine offiziell aussehende E-Mail von Ihrer Bank, die Sie nach Ihren Zugangsdaten fürs Onlinebanking und nach einer TAN-Nummer fragt. Und mit diesen Daten wird anschließend Ihr Konto geplündert.

Beim Vorgehen der Betrüger gibt es mehrere Varianten: Häufig enthält die Phishing-Mail einen Link, der vorgeblich auf die Website Ihrer Bank verweist. Falls Sie ihn anklicken, leitet Sie jedoch ein Skript im Hintergrund auf eine Seite des Phishing-Betrügers um. Diese Seite sieht der Startseite Ihrer Hausbank meist täuschend ähnlich. Dort erwarten Sie dann Eingabefelder für PIN und TAN. Füllen Sie diese aus, landen die Daten in einer Datenbank des Phishers.

Die Adresse der Site des Betrügers stimmt allerdings nicht mit der Adresse Ihrer Bank überein. Sehen Sie daher genau hin, was Ihr Browser beim Überstreichen des Links mit der Maus unten in seiner Statuszeile anzeigt.

Ein weiterer beliebter Trick sind Veränderungen an der Hosts-Datei von Windows. Diese Datei dient in kleinen, lokalen Netzwerken dazu, URLs in IP-Adressen zu übersetzen, um die anderen Computer im Netz identifizieren zu können. Wenn nun jemand in dieser Datei einer URL eine IP-Adresse zuweist, landen Sie nach Eingabe der URL in den Browser bei einer komplett anderen Webadresse. Es gibt einige Trojaner, die die Benutzer auf diese Weise auf illegale Server umleiten. Sie sollten die Datei daher regelmäßig kontrollieren, Sie finden sie unter \Windows\system32\drivers\etc.

Lösung Die aktuelle Browser-Generation ist mit einem Phishing-Schutz ausgestattet. Er gleicht die angesteuerten URLs mit einer Datenbank von Phishing-Sites ab und weist Sie darauf hin, wenn Sie eine gefährliche Adresse ansteuern. Besitzer älterer Browser-Versionen können sich mit Zusatzprogrammen schützen. Für Firefox gibt es etwa die Netcraft-Toolbar (**https://addons.mozilla.org/firefox/1326**). Sie bekommen sie auf der Homepage von Netcraft (**http://toolbar.netcraft.com**) auch für ältere Versionen des Internet Explorer. Um die Hosts-Datei von Windows gegen Veränderungen zu schützen, sollten Sie sie mit einem Schreibschutz versehen.

Ganz allgemein gilt: Seien Sie im Zweifelsfall immer misstrauisch. Banken fordern Ihre Kunden niemals per E-Mail zum Eingeben von PIN und TAN auf. Außerdem sollten Sie prinzipiell nie dem Link in einer Mail folgen, die angeblich von Ihrer Bank kommt. Tippen Sie die Adresse der Bank im Zweifelsfall direkt in die Adresszeile Ihres Browsers ein. Falls Sie die Informationen, auf welche die E-Mail verweist, dort nicht finden und Sie sich immer noch unsicher sind,

Spam Ein Spamfilter gehört bei den kostenlosen Mailservices mittlerweile zum Standard.

kontaktieren Sie den Kundendienst Ihrer Bank telefonisch, oder löschen Sie die Nachricht.

5 Computerviren: Abwehren und suchen

Risiko In den vergangenen Jahren sind mit Trojanern, Rootkits und Keyloggern völlig neue Formen von Schadprogrammen erschienen. Anders als frühere Generationen zielen sie nicht mehr darauf ab, die gespeicherten Daten zu zerstören. Stattdessen wollen sie die Kontrolle über Ihren PC übernehmen und vertrauliche Informationen ausspähen.

Die längste Historie der genannten Virenformen haben Trojaner. Sie wurden benannt nach dem Trojanischen Pferd aus der griechischen Mythologie. Trojaner sind Programme, die sich auf dem Computer einnisten, Daten sammeln und übers Internet an den Hacker schicken. Meistens hat sie der Anwender unbewusst selbst installiert – über eine Anwendung, die er auf seinen PC geladen hat, über Downloads aus Tauschbörsen oder Filesharing-Dienste.

Aktuell werden Trojaner vor allem über illegale Webseiten verbreitet, auf denen Registriernummern kommerzieller Programme zu finden sind. Falls der Browser nicht perfekt geschützt ist, installieren diese Sites im Hintergrund den Trojaner auf dem Rechner. Der sammelt anschließend Daten wie etwa den Benutzernamen und das Passwort für den Internetzugang oder Kreditkarten-Informationen und gibt sie an den Programmierer des Trojaners weiter.

Eine ähnliche Funktion erfüllen Keylogger, die es als Hardware und Software gibt. Sie überwachen einfach nur die Eingaben an der Tastatur. Je nach Intelligenz des Programms zeichnet es entweder den kompletten Datenstrom oder nur bestimmte Informationen auf, beispielsweise eingegebene Passwörter, Konto- oder Kreditkartendaten.

Ein Software-Keylogger speichert diese Daten dann entweder auf der Festplatte oder gibt sie übers Internet direkt an den Hacker weiter. Die Hardwarevariante dagegen besteht aus einem kleinen Gerät, das aussieht wie ein Adapter und zwischen PC und Tastatur gesteckt wird. Diese Keylogger besitzen entweder einen eigenen Speicher oder übermitteln die aufgezeichneten Daten per Funk.

Zwar ist ein Hardware-Keylogger ohne Weiteres mit dem bloßen Auge zu erkennen. Da jedoch PCs meist unter dem Schreibtisch stehen, werden die Geräte häufig erst mit einiger Verzögerung entdeckt. Außerdem sind mittlerweile auch Tastaturen mit integriertem Keylogger auf dem Markt, bei denen das Überwachungsgerät gar nicht mehr zu sehen ist.

Perfekt getarnt sind in der Regel auch Rootkits. Sie vereinen die Fähigkeiten von Trojanern und Keyloggern mit Backdoor-Funktionen. Das bedeutet, dass der Hacker sich nicht nur unbemerkt Zugang zu Ihrem PC verschaffen, sondern ihn auch als Ausgangsbasis für weitere Aktionen nutzen kann, beispielsweise zum Versenden von Spammails. Rootkits ersetzen meist Teile des Betriebssystemkerns durch eigene Versionen und sind daher nur schwer zu identifizieren.

Lösung Trojaner, Keylogger und Rootkits haben eines gemeinsam – sie tun alles, um nicht bemerkt zu werden. Deswegen sollten Sie darauf achten, dass solche Programme von vornherein überhaupt keine Chance bekommen, sich auf Ihrem Rechner einzunisten.

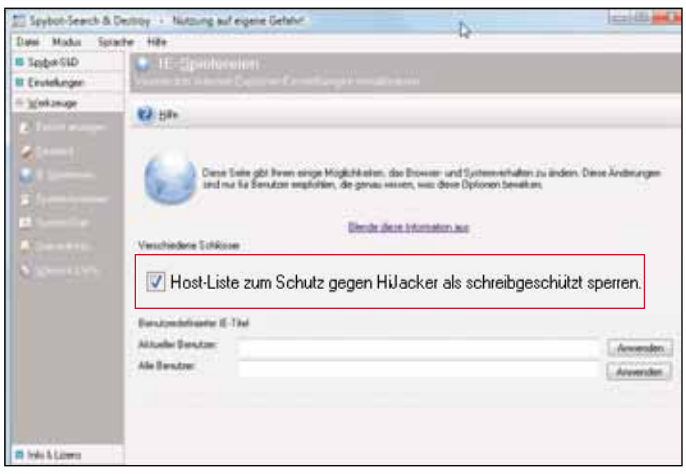
Die Grundvoraussetzung dafür ist der Einsatz einer Firewall und eines Virenscanners mit aktuellen Virendefinitionen. Zudem sollten Sie Ihren PC von Zeit zu Zeit auf Rootkits untersuchen, beispielsweise mit den Programmen Stinger von McAfee (**http://vil.nai.com/vil/stinger**), Rootkit Revealer von Microsoft (**www.microsoft.com/technet/sysinternals/Utilities/RootkitRevealer.mspx**) oder BlackLight von F-Secure (**www. f-secure.de/blacklight**). Von der Software Ice Sword (**www.blogcn.com/user17/pjf/blog/44731756.html**) erhalten Sie darüber hinaus Hinweise auf verdächtige Prozesse, und sie sagt Ihnen auch, wie Sie diese am besten wieder von Ihrem Computer entfernen.

Die einfache Version der Hardware-Keylogger erkennen Sie daran, dass das Gerät als Stecker zwischen Tastatur und Rechner sitzt. Schwieriger wird es, wenn der Keylogger in die Tastatur integriert ist. Werden Sie also misstrauisch, wenn jemand ohne erkennbaren Grund Ihre Tastatur ausgetauscht hat.

6 Dialer: Vorwahlen sperren lassen

Risiko Eine weitere Gefahrenquelle für Internetnutzer bilden Dialer. Dabei handelt es sich um Programme, die die Internetverbindung nicht über den normalen Provider herstellen, sondern über einen teuren und meist illegalen Anbieter, der entweder im Ausland residiert oder eine 0900-Nummer benutzt.

Doch nicht alle Dialer sind illegal: Es gibt auch eine große Gruppe legaler Programme, mit denen kostenpflichtige Internetdienste ihre Bezahlvorgänge abwickeln. So waren etwa Anfang 2006 nach Angaben der Webseite Dialerschutz (**www.dialerschutz.de**) bei der Bundesnetzagentur rund 1,77 Millionen Dialer legal registriert. Die Zahl hat sich in den letzten Jahren kontinuierlich nach oben entwickelt. Übernimmt jedoch ein solcher legaler Dialer die Einwahl, muss der Kunde explizit auf die Kosten des Dienstes hingewiesen werden. Auf der Website der Bundesnetzagentur können Sie übrigens nach dem Betreiber einer 0900- →



Adware & Spyware Im erweiterten Modus von Spybot – Search & Destroy gibt es eine Funktion zum Schutz der Hosts-Datei.

Nummer in einer Datenbank suchen und ihn beim Verdacht des Missbrauchs auch melden (**http://app.bundesnetzagentur.de/Dialer2005**).

Illegale Dialer installieren sich ohne Zustimmung des Users im Hintergrund und ersetzen die Verbindung zum Standardprovider durch ihre eigenen Daten. Das böse Erwachen für den Anwender kommt dann mit der Telefonrechnung am Monatsende.

Lösung Das Risiko, mithilfe von Dialern betrogen zu werden, ist in den letzten Jahren mit der zunehmenden Verbreitung von Breitbandanschlüssen geringer geworden. Denn eine Bedrohung stellen die Programme nur für solche Benutzer dar, die über ein analoges Modem oder per ISDN ins Internet gehen.

Bei den meisten DSL-Anschlüssen hingegen sind die Zugangsdaten heute in einem Router und / oder DSL-Modem abgelegt, dessen Einstellungen durch Benutzernamen und Passwort vor unbefugten Zugriffen gesichert sind. Außerdem müssen die Gebühren, die bei nicht registrierten, also illegalen Dialern aufgelaufen sind, seit Mitte 2005 nicht mehr bezahlt werden.

Beim Erkennen und Beseitigen von Dialern helfen Ihnen das bereits erwähnte Spybot – Search & Destroy oder das Programm A-squared Anti-Dialer (**www.tu-berlin.de/www/software/hoaxlist.shtml**). Außerdem bietet die Telekom genauso wie andere Telekommunikations-Anbieter auch die Sperrung bestimmter kostenpflichtiger Vorwahlen an, die dann von Ihrem Anschluss nicht mehr erreicht werden können. Somit haben Dialer dann keine Chance mehr, teuere Verbindungen aufzubauen.

Dialer In der Datenbank der Bundesnetzagentur können Sie die Betreiber von legalen Dialern ausfindig machen.

7 Adware: Hilfe von Tools und Popup-Blockern

Risiko Weniger gefährlich als ein Virus, dafür aber unglaublich lästig ist Adware. Das ist Software, die sich auf Ihrem Rechner einnistet und anschließend bunte Werbebotschaften anzeigt oder zusätzliche Toolbars im Webbrowser und dubiose Suchseiten einrichtet.

Die Werbung stammt oft von einem Programm, das sich über die eingeblendete Werbung finanziert. Einige Tools, so etwa einige Download-Manager, sind in zwei Versionen verfügbar: kostenlos, aber mit Werbeeinblendungen, oder kostenpflichtig ohne die nervigen Anzeigen. Teilweise lässt sich das Adware-Modul der Software gezielt deinstallieren – dann jedoch funktioniert meistens auch das Programm nicht mehr.

Eine andere Adware-Infektionsquelle sind diverse Internetseiten aus den Kategorien Sex und Warez, die im Hintergrund oder beim Download von Programmen, Filmen und Bildern auch Werbebanner und -fenster installieren.

Dialer Dieses Tool untersucht Ihren Rechner auf illegale Dialer und schützt ihn mit einem Guard-Programm.

Lösung Um Ihren PC von der unerwünschten Werbung zu reinigen, gibt es spezielle Programme. Dazu zählen etwa Spybot – Search & Destroy, Ad-Aware 2007 Free von Lavasoft (**www.lavasoft.de/products/ad_aware_free.php**) oder Spyware Doctor (**www.pctools.com/de/spyware-doctor**). Die ersten beiden Anwendungen sind gratis, Spyware Doctor kostet rund 35 Euro.

Weitere Werbeeinblendungen, die sich im Browser als Popups öffnen, stoppen Sie mit einem Popup-Blocker, einer Funktion, die in sämtlichen aktuellen Browsern enthalten ist. Für ältere Versionen des Internet Explorer gibt's den Popup-Blocker der Google Toolbar, Firefox lässt sich mit Adblock Plus (**https://addons.mozilla.org/firefox/1865**) nachrüsten. Opera hingegen hat bereits länger eine entsprechende Funktion.

8 Hoaxes: Keine Reaktion ist die richtige Reaktion

Risiko Während die bisher genannten Bedrohungen einen realen Hintergrund haben, täuscht ein Hoax eine Gefährdung des Users nur vor. Ein Hoax ist eine Falschmeldung über eine angebliche Bedrohung, die sich jedoch ironischerweise ähnlich schnell ausbreitet wie ein echter Virus. Die Weitergabe erfolgt per E-Mail, über Messenger-Programme oder auch via Handy als SMS. Abgesehen davon, dass er Ängste und Verwirrung schürt, kann ein Hoax keinen Schaden anrichten. Teilweise werden Hoaxes jedoch als Lockmittel für den Besuch von Websites eingesetzt, die beim Anwender Viren oder Adware installieren.

Die erste bekannt gewordene Hoax-Meldung, die vor einem Virus namens

„Good Times“ warnte, wurde 1994 millionenfach verbreitet. Der Virus sollte angeblich in einer E-Mail versteckt sein und beim Öffnen der Nachricht die Festplatte löschen können.

Auch E-Mails der sogenannten Nigeria Connection werden als Hoaxes gewertet. Das Muster ist immer gleich: Ein angeblicher Millionär aus Nigeria oder einem anderen weit entfernten Staat will Ihnen für die Hilfe bei einer Finanz-Transaktion und gegen einen kleinen Vorschuss Teile seines Vermögens überschreiben. Tatsächlich werden Sie nach dem Überweisen des Vorschusses niemals wieder etwas von dem Mann hören. Die ausführlichste deutschsprachige Liste von Hoaxes finden Sie auf den Seiten der TU Berlin (**www.tu-berlin.de/www/software/hoaxlist.shtml**).

Manche der Hoax-Mails sind so gut gemacht, dass man sich im ersten Moment fragt, ob es sich nicht doch um eine echte Nachricht handelt. Einen Hoax können Sie jedoch meistens daran identifizieren, dass er eine oder mehrere der folgenden Eigenschaften aufweist:

- Sie werden aufgefordert, die Nachricht an mehrere Personen weiterzuleiten.
- Das Thema der E-Mail ist häufig ein Virus, eine Erbschaft, ein gutes Geschäft oder ein Glücksspielgewinn.
- Oft wird eine namhafte Firma als Leumund vorgeschoben, die mit der Sache in Wirklichkeit nichts zu tun hat.
- In den E-Mails finden Sie normalerweise keine absoluten Zeitangaben, wie „1. Dezember 2007“, sondern nur relative wie „letzten Freitag“ oder „gestern“.

Lösung Wenn Sie einen Hoax erhalten, gibt es nur eine richtige Reaktion: Antworten Sie nicht, leiten Sie die Mail nicht weiter, sondern löschen Sie sie und melden Sie sie Ihrem Spamfilter, damit solche Post beim nächsten Mal gleich im Papierkorb landet.

Hoaxes Auf der Website der TU Berlin finden Sie eine ständig aktualisierte Liste von Hoax-Meldungen.

9 Social Engineering: Schweigen ist Gold

Risiko Die größte Gefahrenquelle im IT-Bereich sind die Anwender selbst. Kevin Mitnick, einer der bekanntesten Hacker aller Zeiten, hat die meisten seiner Angriffe auf Firmennetzwerke mit Social Engineering vorbereitet. Diese Methode setzt darauf, dass Mitarbeiter am Telefon vertrauliche Informationen preisgeben, wenn man nur geschickt genug fragt oder sie unter Druck setzt.

Meist fängt der Datensammler bei der Putzfrau oder der Sekretärin an und versucht, sich ein Bild über die Abläufe innerhalb der Firma oder über die Organisation und die Hierarchiestufen zu machen. Mit diesen Informationen arbeitet er sich Stufe für Stufe weiter nach oben, bis er genügend Hintergrundwissen besitzt, um bei einem Mitarbeiter mit erweiterten Zugriffsrechten auf das Netzwerk anzurufen und ihn mit einer plausibel klingenden Begründung nach Usernamen und Passwort zu fragen.

Statistisch gesehen ist diese Methode, an fremde Daten zu kommen, übrigens wesentlich erfolgreicher als eine Brute-Force-Attacke, die automatisiert verschiedene Kombinationen aus Benutzernamen und Passwort abfragt.

Lösung Vor Social Engineering sind Sie nur sicher, wenn Sie am Telefon oder per E-Mail grundsätzlich keine sicherheitsrelevanten Daten an Personen weitergeben, die Sie nicht kennen. Bleiben Sie auch dann unnachgiebig, wenn der Anrufer versucht, Sie in die Enge zu treiben. Informieren Sie nach einem solchen Anruf Ihren Vorgesetzten und einen Mitarbeiter aus dem Bereich Datensicherheit oder aus der IT-Abteilung.

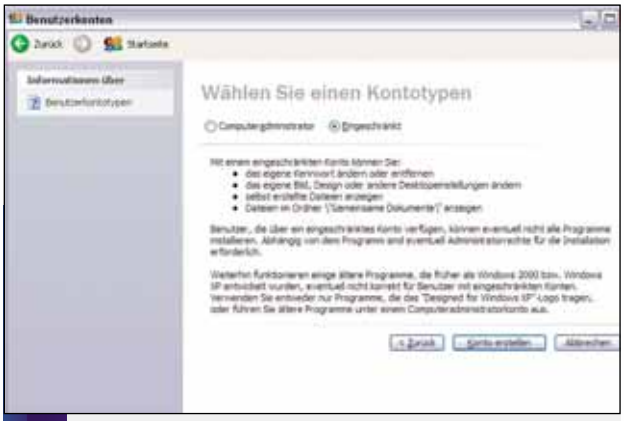
10 Ganz allgemein: Sicherheit ernst nehmen

Risiko Im Internet gibt es viele gefährliche Ecken und Winkel. Bereits ein einfacher Download ist eine potenzielle Gefahr für die Sicherheit Ihrer Daten – laden Sie also Dateien nur aus sicheren Quellen herunter. Websites mit dubiosen Inhalten, etwa Seriennummern oder Programmen zum Generieren von Registrierungsschlüsseln, verbreiten oft auch Trojaner, Rootkits und Viren.

Lösung Insbesondere wenn Ihr Rechner von mehreren Personen genutzt wird, sollten Sie strenge Sicherheitsrichtlinien einhalten. Gehen Sie niemals mit Administratorrechten ins Internet, und installieren Sie neben Virenscanner und Firewall weitere Schutzsoftware wie etwa Spybot oder A-squared Anti-Dialer.

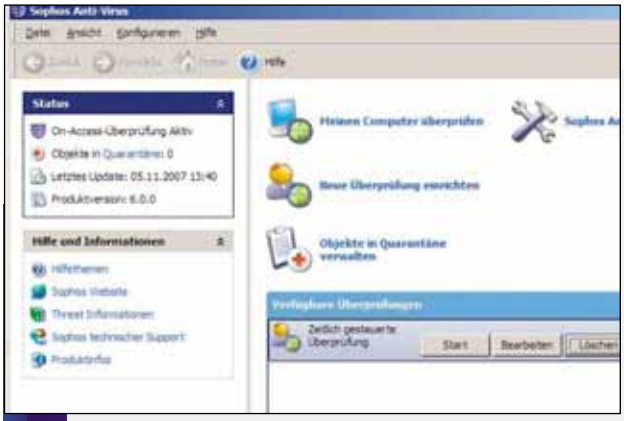
Andreas Hitzig

Adware & Spyware Das Tool Ad-Aware hilft Ihnen beim Entfernen von Adware und Spyware.



1 Eingeschränktes User-Konto

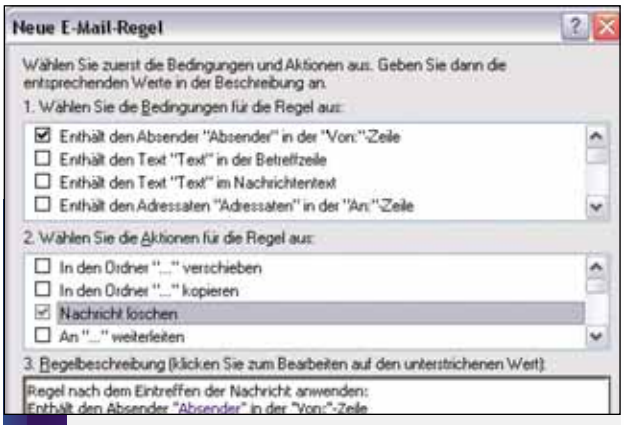
Schalten Sie die automatische Windows-XP-Anmeldung aus, und wählen Sie den klassischen Weg über die Eingabe von Kennung und Passwort. Legen Sie danach unter „Systemsteuerung | Benutzerkonten“ ein neues Benutzerkonto an, geben Sie dem Konto einen beliebigen Namen, klicken Sie auf „Weiter“, und wählen Sie die Option „Eingeschränkt“. Verwenden Sie künftig dieses Konto zum Surfen. Schadprogramme aus dem Internet haben dann keinen Zugriff auf Ihr System.



2 Virenschutz installieren

Virenscanner blockieren Viren und Würmer, die per E-Mail oder auf anderen Wegen aus dem Internet auf den Rechner gelangen. Neben den kommerziellen Programmen bieten auch Freeware-Scanner einen guten Schutz. Installieren Sie die Antiviren-Software Ihrer Wahl, und achten Sie darauf, den Virenschutz regelmäßig zu aktualisieren (mindestens einmal pro Woche), denn sonst kann das Tool neue Viren und Würmer nicht aufspüren.

Sicher in 10 Minuten



5 Spammails ausfiltern

Zwar nicht gefährlich, aber sehr lästig sind unerwünschte Werbemails. Fast jedes Mailprogramm erlaubt es deshalb, mithilfe von Filterregeln Spammails automatisch auszusortieren. Wer den Mailclient Outlook Express einsetzt, öffnet dazu das Menü „Extras“ und wählt die Optionen „Nachrichtenregeln“ und „E-Mail“. Erkannte Spammails lassen sich in ein besonderes Verzeichnis verschieben oder gleich löschen – und das Spam-Aufkommen wird spürbar geringer.

6 Dateien verschlüsseln

Vertrauliche Daten auf dem PC sollten Sie unbedingt verschlüsseln. Windows XP bietet dazu die EFS-Verschlüsselung an, allerdings nur in der Professional Edition. Für Benutzer der Home Edition von XP schafft zum Beispiel das Freeware-Programm EasyCrypto Deluxe Abhilfe. Die Software verschlüsselt Ihre Dateien und macht sie für alle unlesbar, die das Passwort nicht kennen. EasyCrypto bekommen Sie unter **www.handybits.com** im Untermenü „Collection 2002“.

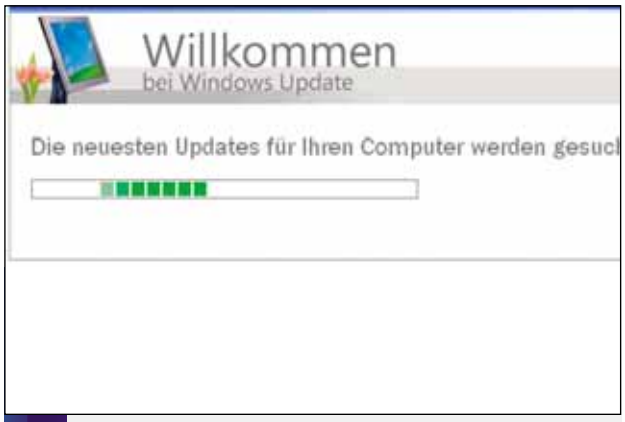
3 Firewall aktivieren

Eine Firewall wehrt Hackerangriffe und Würmer ab. Windows XP verfügt ab dem Service Pack 2 über einen sogenannten Portblocker – die einfachste Art einer „Brandschutzmauer“. Um die XP-Firewall einzuschalten, wechseln Sie in die Systemsteuerung und öffnen das Applet „Netzwerk- und Internetverbindungen“. Klicken Sie danach auf „Windows Firewall“, und aktivieren Sie sie. Auf der Registerkarte „Ausnahmen“ legen Sie die Programme fest, deren Daten die Firewall passieren dürfen.

4 Spyware abblocken

Wenn plötzlich Werbung auf dem Bildschirm erscheint, die irgendwie zu den eigenen Interessen passt, ist Spyware dafür verantwortlich. Um diese Schnüffelprogramme loszuwerden, empfehlen sich Tools wie Spybot – Search & Destroy (**www.safer-networking.org/de**), Ad-Aware (**www.lavasoft.com**) oder XP-AntiSpy (**www.xp-antispy.org**). Die – in der Regel kostenlose – Software spürt die lästigen Spione auf und entfernt sie von der Festplatte.

Schon mit ein paar Mausklicks können Sie Ihren Windows-PC vor Angriffen von Viren, Würmern und Hackern sehr gut schützen. Alle Tools, die Sie dazu brauchen, finden Sie auf der Heft-CD.



7 Windows aktuell halten

Alle Sicherheitsmaßnahmen nützen wenig, wenn das Betriebssystem nicht up to date ist. Wer die Auto-Update-Funktion von XP ausgeschaltet hat, sollte einmal im Monat nach sicherheitsrelevanten Updates suchen und sie umgehend installieren. Dazu gehen Sie im „Hilfe- und Supportcenter“ auf „Windows Update“. Windows stellt nun eine Verbindung zum Microsoft-Server her und sucht selbstständig nach Aktualisierungen. Hat Windows dann Updates gefunden, klicken Sie auf „Installieren“.

EXTRA-TIPP

Adobe-Reader & Co. updaten

Auf fast jedem PC sind der Adobe Reader, der Adobe Flash Player und die Java Runtime von Sun installiert. Mit diesen Erweiterungen öffnen Sie im Browser PDFs oder betrachten multimediale Webinhalte. Ein Browser kann noch so aktuell sein – er bleibt ein Einfallstor für Schädlinge, wenn er für die Anzeige von Multimedia-Inhalten auf veraltete und unsichere Erweiterungen zurückgreifen muss. Bringen Sie diese drei Browser-Erweiterungen aus diesem Grund regelmäßig auf den neuesten Stand.

Adobe Reader 8.1

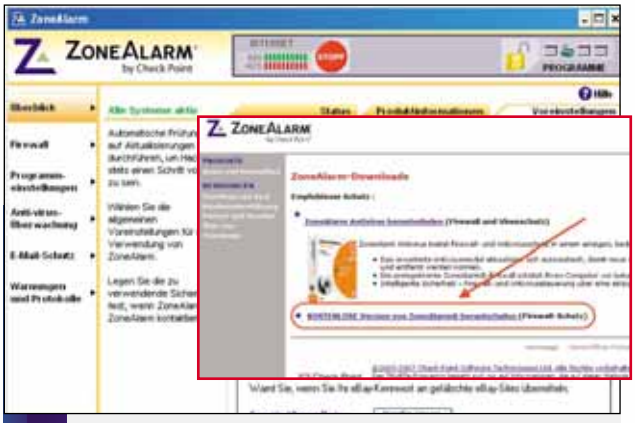
Die aktuellste Fassung des beliebten PDF-Betrachters erhalten Sie unter der Webadresse **www.adobe.com/de/products/acrobat/readstep2.html**.

Adobe Flash Player 9

Installieren Sie die neueste Version des Flash Players auf Ihrem Computer. Sie bekommen die kostenlose Software unter der Webadresse **www.adobe.com/de/products/flashplayer**.

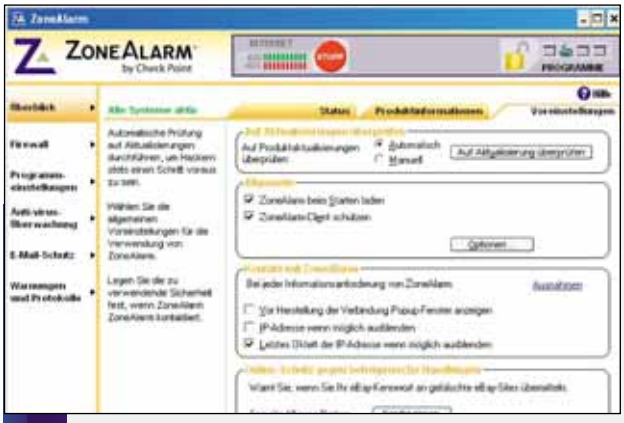
Sun Java Runtime Environment

Starten Sie das Herunterladen der Java-Bibliotheken unter der Webadresse **http://java.sun.com/javase/downloads/index.jsp**. Weiter unten auf dieser Webseite finden Sie das Java Runtime Environment (JRE) 6 Update 3 und klicken auf „Download“.



1 ZoneAlarm installieren

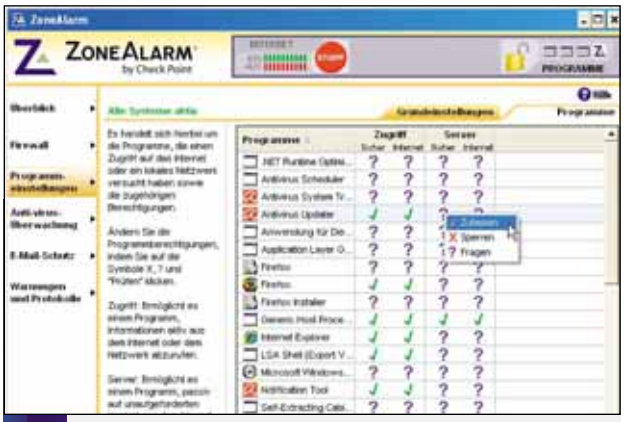
Falls Sie ZoneAlarm lieber von der Herstellerseite herunterladen, statt es von der Heft-CD zu installieren, sollten Sie darauf achten, die kostenlose Version downzuloaden. Bevor Sie mit der Konfiguration von Zone Alarm beginnen, überprüfen Sie die installierte Version auf Updates. Starten Sie dazu ZoneAlarm, und wechseln Sie im Menü „Überblick“ auf die Registerkarte „Voreinstellungen“. Starten Sie an dieser Stelle über die Schaltfläche „Auf Aktualisierungen überprüfen“ die Suche nach Updates.



2 ZoneAlarm einrichten

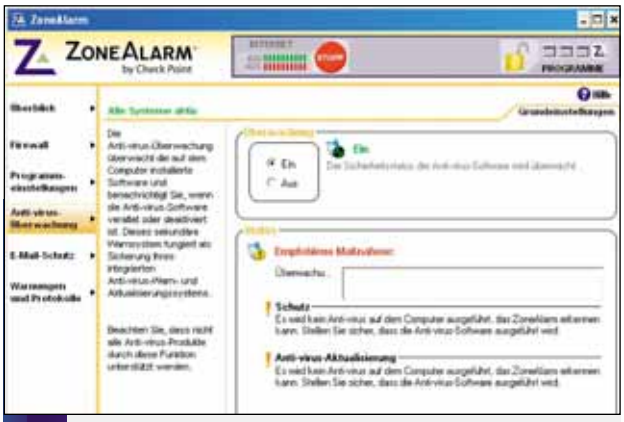
Vergewissern Sie sich zunächst, dass Sie in der linken oberen Ecke die grüne Meldung „Alle Systeme sind aktiv“ sehen. In den „Voreinstellungen“ geben Sie nun auch an, ob ZoneAlarm beim Booten von Windows starten und vor unbefugtem Herunterfahren gesichert werden soll. Schränken Sie die Kommunikation mit dem Hersteller ein: Aktivieren Sie dazu alle drei Optionen in der Rubrik „Kontakt mit ZoneAlarm“, damit Sie über den Datenaustausch im Bilde sind und er anonym erfolgt.

Angreifer aussperren



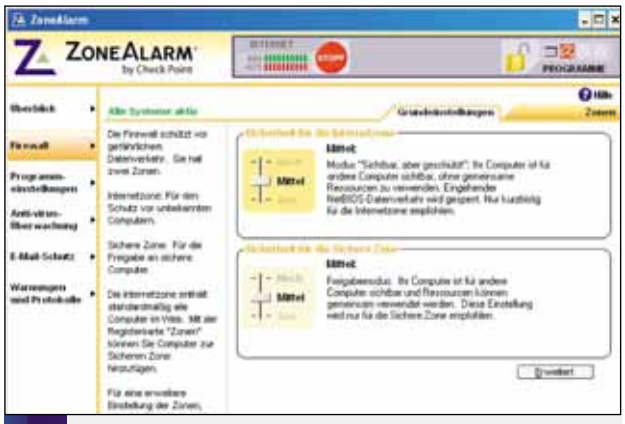
5 Rechte zuweisen

Die Kommunikation einer Anwendung mit dem Web steuern Sie über die „Programmeinstellungen“: Müssen Programme beim Aufbau einer Verbindung um Erlaubnis fragen („Mittel“) oder wird über den Lernmodus das Vorgehen einmal festgehalten und dann angewendet („Niedrig“). Auf der Karte „Programme“ können Sie jede Anwendung gesondert behandeln. Sie regeln etwa unter „Zugriff“, ob sie mit dem Web kommunizieren darf, und über „Server“, ob aus dem Web Kontakt zu ihr aufgebaut werden darf.



6 Mailverkehr überwachen

ZoneAlarm kann Ihren Virenscanner überwachen und meldet, wenn er veraltete Definitionen verwendet oder durch ein drittes Programm beendet wurde. Im Bereich „E-Mail-Schutz“ bietet Ihnen ZoneAlarm eine Kontrolle eingehender E-Mails an. Dabei untersucht die Firewall eintreffende Mailanhänge auf potenzielle Risiken. In der kostenlosen Variante schlägt das Tool allerdings nur bei VB-Skripten Alarm. Daher sollten Sie auf keinen Fall auf den Einsatz eines zusätzlichen Virenscanners verzichten.



3 Sicherheitszonen festlegen

ZoneAlarm teilt die Welt in zwei Zonen ein: die „Internetzone“ und die „sichere Zone“ – Ihr lokales Netz. Im Menü „Firewall“ legen Sie über die „Grundeinstellungen“ die jeweilige Sicherheitsstufe fest. Auf der Stufe „Mittel“ etwa ist Ihr PC im Web sichtbar, Ressourcen wie Datei- oder Druckerfreigaben können jedoch nicht geteilt werden. Für Ihr lokales Netz steht in der Gratisvariante von ZoneAlarm nur die Einstellung „Mittel“ zur Verfügung, die eine gemeinsame Nutzung von Ressourcen gestattet.

4 Regeln definieren

In der Registerkarte „Zonen“ legen Sie fest, welche Adressbereiche zur „sicheren Zone“ gehören; dies können Hosts, einzelne IP-Adressen, Adressbereiche und Subnetze sein. Um eine neue Zone festzulegen, klicken Sie auf „Hinzufügen“ und wählen die passende Option aus. In einem Heimnetz schalten Sie über „IP-Bereich“ den Adressbereich frei, den Ihr DHCP-Server vergibt. Befinden sich auch PCs mit manueller IP-Vergabe, etwa für BitTorrent, in Ihrem Netz, fügen Sie diese anschließend über „IP-Adresse“ hinzu.

Jeder Ausflug ins Internet kann Ihr System gefährden. CHIP zeigt Ihnen, wie Sie mit ZoneAlarm Ihren PC oder Ihr Netzwerk vor fremden Zugriffen schützen.

7 Protokolle auswerten

ZoneAlarm informiert Sie über die Vorkommnisse auf Ihrem PC. In den „Grundeinstellungen“ legen Sie fest, wie detailliert das geschehen soll. In der „Protokollanzeige“ sehen Sie auch, welche Schutzmaßnahmen die Firewall ergriffen hat. ZoneAlarm unterteilt die Warnmeldungen in „Firewall“- und „Programmbezogene“ Meldungen. Sie sollten die Warnmeldungen regelmäßig kontrollieren – bei Meldungen mit der Bewertung „Hoch“ suchen Sie in der Internet-Datenbank von ZoneAlarm „weitere Infos“.

EXTRA-TIPP

Zusätzliche Funktionen

ZoneAlarm kann noch mit einigen hilfreichen Zusatzfunktionen aufwarten.

- **Proxyserver:** Befinden Sie sich hinter einem Proxy, geben Sie die Werte über „Überblick | Voreinstellungen“ und den Button „Optionen“ ein.
- **Phishing:** Einen Phishing-Schutz für Ebay-Aktivitäten finden Sie unter „Überblick | Voreinstellungen“. Sie werden gewarnt, wenn Sie Ihr Ebay-Passwort an eine andere Seite übertragen.
- **Warnmeldungen:** Das Protokollieren der Warnmeldungen lässt sich anpassen. Im Bereich „Warnungen und Protokolle“ finden Sie eine erweiterte Ansicht. Dort legen Sie fest, ob die Protokolldatei täglich archiviert werden soll, wo sie gespeichert wird und wie das Format des Protokolls aussieht.
- **Spielemodus:** Spielen Sie häufig im Netzwerk oder im Internet, sind Sie sicherlich auch schon durch ständig eintreffende Warnhinweise genervt worden, die ein zeitnahes Reagieren auf das Spielgeschehen so gut wie unmöglich machen. Um den Unmut der Spieler zu vermeiden, bietet ZoneAlarm einen Spielemodus an, der die meisten Warnungen unterdrückt, sodass Sie ungestört spielen können. Sie aktivieren den Spielemodus über das Kontextmenü von ZoneAlarm in der Statuszeile.

Nie mehr Spam-Terror

Aktien, Viagra, Gewinnspiele – Schwärme von Werbemails überfallen uns. Genug! So stoppen Sie die Spam-Attacken.

Wie Krähen über die Saat fallen Spamroboter über Mailadressen im Internet her. Auf irgendeiner Seite pickt eine dieser Krähen Ihre Anschrift heraus – und dann nimmt der Spamterror kein Ende mehr. Besonders Nachrichten mit PDF-Anhängen attackieren derzeit den geplagten User. Als wäre das noch nicht genug, stechen dem Surfer im Web auch noch grell blinkende Werbebanner in die Augen und kreischen ihm Flash-Sounds in die Ohren.

Zeit für eine Radikallösung: Der ganze Werbemüll muss weg – dauerhaft! Fangen Sie mit dem Mailprogramm an, danach nehmen Sie sich die Browser vor, Firefox und Internet Explorer. Wir zeigen Ihnen die unkomplizierte Lösung – die aber noch viel Potenzial für Feinjustage bietet.

Auf Heft-CD

- A-squared HiJack Free (Security)
- Spamihilator (Security)
- Spybot – Search & Destroy (Security)

Spamihilator Das Top-Tool gegen Spam

Welchen Mailclient Sie auch verwenden, bei allen hilft eine bequeme und zuverlässige Lösung gegen Spam: die Freeware Spamihilator (**www.spamihilator.com**). Sie hängt sich zwischen Postfach und Mailprogramm und sortiert gleich bei der Übertragung lästige Werbebotschaften aus. Einfach installieren und dem Assistenten folgen – schon sind Sie eine gehörige Portion Spam los.

Der Spamihilator hat einen großen Vorteil gegenüber den Filtern von GMX & Co.: Er lässt sich genau auf die Spammails anpassen, die den Anwender am meisten quälen – etwa der Aktienspam mit PDF-Dateien oder Botschaften auf Russisch oder Chinesisch.

Der kleine Wermutstropfen: Bisher stürzt der Spamihilator beim Abrufen von IMAP-Postfächern ab. IMAP steht

Foto: M. Fiorito

für „Internet Message Access Protocol“ und bedeutet, dass alle Mails auf dem Mailserver bleiben und dort verwaltet werden. GMX und andere Freemail-Dienste bieten solche Postfächer für wenige Euro im Monat an.

Spamihilator-Autor Michael Krämer arbeitet derzeit daran, die Fehler zu beheben. Alternativen gibt es allerdings sowieso kaum: Denn die meisten Freeware-Lösungen aus dem Bereich Spamschutz haben die E-Mail-Abfrage per IMAP gar nicht erst auf der Agenda.

Prüfstationen inbegriffen Spezialfilter einrichten

Was den Spamihilator so gut macht: Er setzt nicht nur auf einen Filter, sondern jagt die Mails durch eine Kette von Prüfstationen.

Der effektivste Filter wird gleich mitinstalliert: DCC – die Abkürzung für „Distributed Checksum Clearinghouse“. Er funktioniert so: Jeder PC mit diesem Filter schickt eine Prüfsumme über die eben erhaltene Mail an einen der DCC-Server. Der Server zählt die Häufigkeit einer Checksumme. Überschreitet ein Zähler die kritische Masse, stuft DCC diese Mail als Spam ein. Die Checksumme berücksichtigt sogar Variationen, wie sie in Spammails vorkommen. Einziger Nachteil: Das Abfragen der Daten kostet Zeit – beim Mail-Aufkommen im Test fiel das jedoch kaum ins Gewicht.

Falls der DCC-Filter versagt, springen andere ein, etwa ein Wortfilter, der klassische Spambegriffe aussiebt, ein Bayes-Filter, der die Ansammlung bestimmter Begriffe („Sex“, „Viagra“ usw.) untersucht und sich sogar trainieren lässt, ein Attachment-Plugin, das nicht nur unerwünschte, sondern sogar gefährliche Nachrichten aufhält – und weitere Filter mehr.

Und wie bekommen Sie die Spams mit PDF-Anhängen oder in kyrillischer Schrift weg? Ganz einfach: mit weiteren Spamfiltern, die Sie unter der Adresse **www.spamihilator.com/plugins/index.php** finden, etwa diese:

ALPHABET SOUP: Verscheucht mit sinnlosen Zeichenketten versehene Mails.

EMPTY MAIL: Sortiert Nachrichten aus, die keinen oder nur wenig Text enthalten – derzeit noch ein typisches Kennzeichen für PDF-Spams.

Nervend Spam-Nachrichten, in PDF-Dokumente verpackt, preisen den Kauf bestimmter Aktien an.

MYSTIC SIGNS: Schmeißt Mails in kyrillischer Schrift raus – und wehrt Versuche ab, andere Filter mit Sonderzeichen zu verwirren.

RFC VALIDATOR: Erkennt Mails, die nicht dem Standardformat entsprechen.

SCRIPTS: Filtert alles, was gefährliche Programmzeilen im HTML-Code aufweist.

SERVER TESTER: Enttarnt gefälschte Absenderadressen, wie sie gern von Spammern genutzt werden.

Die Plugins installieren Sie per Doppelklick auf die heruntergeladene Datei. Und voilà, die Vogelscheuchen-Armee gegen Spam-Krähen steht Gewehr bei Fuß!

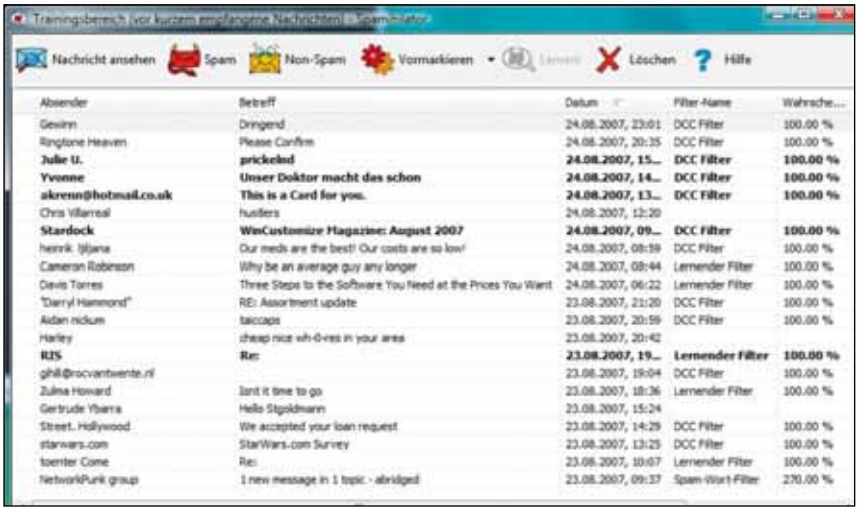
Richtig anlernen Echte Mails von Spam trennen

Wo gehobelt wird, fallen Späne. Auch der Spamihilator schmeißt zunächst Mails in den Papierkorb, die dort nicht hineingehören. Newsletters etwa sind immer in Gefahr, aussortiert zu werden – dies ist aber nicht im Sinne des Anwenders. Die Lösung: Schalten Sie den Newsletter-Filter vor alle anderen. Denn er lässt anhand einer Whitelist die erwünschten Infomails passieren. Dafür muss man ihm jedoch erst sagen, welche das sind.

Dazu öffnen Sie die Einstellungen, indem Sie mit der rechten Maustaste auf das Spamihilator-Icon rechts unten klicken und „Einstellungen“ wählen. Dort suchen Sie „Newsletter | Signaturen“ und klicken auf den Button „Neu“. Geben Sie nun einen typischen Begriff aus dem Betreff des Newsletters ein, beispielsweise „ShortNews“. Die meisten Rundmails gehen an eine bestimmte sichtbare Adresse – alle anderen Empfänger sind ausgeblendet. Diese Adresse geben Sie noch im Bereich „Newsgroups“ ein, und ab sofort ist der Newsletter gerettet.

Die Kunst besteht jetzt darin, die Mailfilter in der richtigen Reihenfolge zu schalten. Denn wenn etwa ein erwünschter Newsletter kommt, sollen sich die anderen Filter erst gar nicht mit ihm aufhalten. Also gehen Sie wieder in die Einstellungen und klicken unter „Filtereigenschaften“ auf „Reihenfolge“. An dieser Stelle markieren Sie einen Filter und schieben ihn mit den Pfeiltasten links nach oben oder unten – je weiter oben er steht, desto eher greift er. Eine mögliche Reihenfolge ist etwa:

1. **NEWSLETTER-PLUGIN**
2. **SCRIPTS-FILTER** →

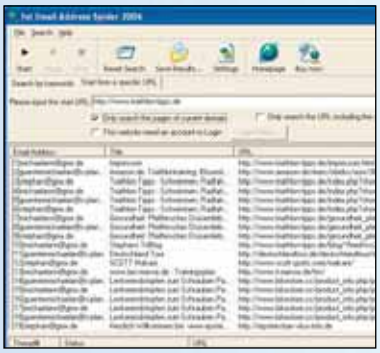


Erkennungsdienst Im „Trainingsbereich“ von Spamihilator erklären Sie dem Programm, welche Mails gut und welche böse sind. Das beugt späteren Fehlentscheidungen vor.

INFO

Verrät Ihre Webseite E-Mail-Adressen?

Webseiten-Betreiber können sich dem Selbsttest unterziehen: Wie viele E-Mail-Adressen verrät meine Webpräsenz den Spam-Krähen? Dazu setzen Sie den 1st Email Address Spider von **www.123hiddensender.com** ein. Um die Adressen exportieren zu können, brauchen Sie die Vollversion für 130 Dollar. Für den Selbstcheck ist jedoch die Testversion völlig ausreichend. Und so gehen Sie am besten vor:



Adressen-Sammler Der 1st Email Address Spider liest die Mailadressen aus Webseiten aus.

Mail-Postfächer finden Nach dem Start des Programms schließen Sie den Registrierdialog mit „Close“. Im Hauptfenster klicken Sie auf „Start from a specific URL“ und geben als Start-URL den Domainnamen Ihrer Webseite an. Aktivieren Sie dann die Option „Only search the pages of current domain“ – sonst geht der Spider auch auf verlinkte Seiten. Klicken Sie auf „Start“, und verfolgen Sie den Fortschritt.

Adressen verschlüsseln Die Auswertung nehmen Sie als Grundlage, um die Adressen auf Ihrer Webseite zu entfernen – die Spalte „URL“ verrät den Deeplink, unter dem der Spider fündig wurde. Soll die Adresse sichtbar, aber nicht sammelbar sein, verschlüsseln Sie sie für die Suchspider. Die richtigen Verschlüsselungsmethoden erfahren Sie auf der Website **www.antispam.de/wiki/Harvester**. Eine der besten Methoden ist übrigens diese: Schreiben Sie die Mailadresse in eine Bilddatei – zum Beispiel mit Paint. Dieses Bild schneiden Sie längs in zwei Teile, speichern sie einzeln und setzen sie erst auf der Webseite wieder zusammen – beispielsweise in einem Div-Tag.

3. **MYSTIC-SIGNS-FILTER**
4. **DCC-FILTER**
5. **SERVER TESTER**
6. **RFC VALIDATOR**
7. **EMPTY-MAIL-FILTER**
8. **ALPHABET SOUP**
9. **ATTACHMENT-FILTER**
10. **SPAM-WORT-FILTER**
11. **LERNENDER FILTER**

Nun sollten Sie festlegen, was passieren soll, wenn eine Mail als Spam oder Non-Spam identifiziert wird: Unter „Wenn der Filter eine Spam-Mail findet ...“ wählen Sie beim Newsletter-Plugin die Option „fahre mit dem nächsten Filter fort“. Bei „Wenn der Filter eine Non-Spam-Mail findet ...“ klicken Sie „beende den Filterprozess“. Alle anderen Plugins stellen Sie im Falle einer Spammail auf „Filterprozess beenden“ und bei Non-Spams auf „Fortfahren“.

Freunden können Sie einen Passierschein ausstellen: In den Spamihilator-Einstellungen klicken Sie auf „Absender“ und „Freunde“ und hinterlegen alle Adressen, die der Spamihilator nicht zu überprüfen braucht. Bei manchen Mailclients funktioniert das per Drag & Drop aus dem Adressbuch.

In den ersten Tagen des Einsatzes von Spamihilator sollten Sie gelegentlich noch mal den Papierkorb durchforsten. Sie finden ihn über einen Doppelklick auf das Spamihilator-Icon. Fälschlich aussortierte Mails holen Sie sich mit „Wiederherstellen“ zurück.

Es lohnt sich, den Spamihilator zu trainieren: Nach dem Abholen der Mails geht man dazu in den „Trainingsbereich“ – wieder über das Icon, die rechte Maustaste und den gleichnamigen Menüpunkt. Korrigieren Sie das Verhalten des Tools, indem Sie falsche Treffer oder nicht erkannten Spam markieren. Nach einigen Malen merkt sich der Spamihilator die Korrektur, und nur noch selten verirrt sich Spam in Ihr Postfach – endlich Ruhe! Na ja, bis auf das, was einen beim Surfen sonst noch nervt.

IE7pro Internet Explorer ohne Werbung

Extrem hohen Nervfaktor hat etwa Onlinewerbung. Zum Glück gibt es schnelle Hilfe für die wichtigsten Webbrowser. Beim aktuellen Internet Explorer etwa ist das die Erweiterung IE7pro von **http://ie7pro.softonic.de**. Nach der Installation gehen Sie über „Extras | IE7Pro Preferences“ in die Einstellungen. Unter „Werbefilter“ aktivieren Sie den „Flash-Blocker“, den „Werbefilter“ und die „Standardregeln“, starten den Internet Explorer neu – und genießen das Web werbefrei.

Weg mit der Onlinewerbung Adblock Plus für den Firefox-Browser entfernt Bannerwerbung von Webseiten, die Bilder bleiben erhalten.

Adblock Plus Firefox von Werbung befreien

Die Stärke des Firefox-Browsers liegt in der großen Entwicklergemeinde, die hinter ihm steht. Kein Wunder also, dass es die ausgereiftere Freeware-Lösung für diesen Browser gibt: AdBlock Plus (**http://adblockplus.org/de/**). Dieser Werbefilter lässt nichts mehr durch.

Holen Sie sich die jüngste Version, und installieren Sie sie. Dabei erlauben Sie Firefox, falls der Dialog kommt, dass er grundsätzlich von dieser Seite Add-ons installieren darf. Später brauchen Sie nämlich noch Filterregeln. Denn nach einem Neustart steht Adblock Plus zwar zur Verfügung, blockt aber noch keine Werbung. Dazu gehen Sie auf die Webseite **http://adblockplus.org/de/subscriptions** und klicken bei den folgenden Filterlisten auf „Abonnieren“:

CÉDRICS LISTE
ABP TRACKING FILTER
FILTER VON DR. EVIL

WICHTIG Die beiden Optionen „Automatisch aktualisieren“ und „Filter aktivieren“ müssen aktiviert sein. Und das war es dann auch schon – Werbung, ade!

Stephan Goldmann

Mitmachen & gewinnen!

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

Preise im Gesamtwert von über 1.650 Euro zu gewinnen!

3 x FRITZ!Box von AVM

Die neue „FRITZ!Box Fon WLAN 7270“ ist eine digitale Kommunikationszentrale: Denn der Router mit integriertem DSL-Modem kombiniert ADSL und modernes WLAN 11n (Draft 2.0). Zudem verfügt der Router über eine DECT-Basisstation, die den Anschluss von bis zu fünf Schnurlostelefonen erlaubt. Ebenfalls neu ist der integrierte Mediaserver, mit dem die Musik auch bei ausgeschaltetem Computer im gesamten Netzwerk hörbar ist.

Weitere Infos: www.avm.de

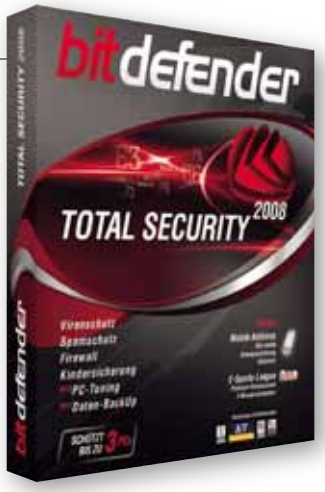
Gesamtwert: 750 Euro

10 x Software von BitDefender

„BitDefender Total Security 2008“ ist der professionelle Rundumschutz gegen Gefahren aus dem Internet – ideal für den heimischen PC oder das Home Office. Das Sicherheitspaket für drei PCs besticht durch seine komplette Ausstattung: Virenschutz, Firewall, Datensicherung, AntiSpam, AntiPhishing, PC-Tuning und Virenschutz für mobile Geräte! Der innovative „Spiele-Modus“ bietet dem PC volle Performance und Sicherheit zugleich.

Weitere Infos: www.bitdefender.de

Gesamtwert: 600 Euro



30 x Bücher von Microsoft Press

10 x PC & Internet – eine sichere Sache für die ganze Familie: Das Buch zeigt mit vielen Schritt-für-Schritt-Anleitungen, wie sich für jeden ein passender Zugang zu PC und Internet einrichten lässt.

10 x Windows Vista: Internet & E-Mail: Das Internet bietet faszinierende Möglichkeiten – dieses Buch vermittelt Ihnen praxisnah alles Wissenswerte rund ums Internet und über E-Mails.

10 x Microsoft Windows Vista – klipp & klar: Sie wollen Ihren neuen Vista-PC gleich richtig nutzen, sicher einrichten und Neues entdecken? Dann ist dieses Buch genau richtig für Sie.

Weitere Infos: www.microsoft-press.de

Gesamtwert: 300 Euro

UND SO GEHT'S

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

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

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

Teilnahmeschluss: 9. März 2008

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

Spyware entlarven

„Sie kommen in Schafskleidern, inwendig aber sind sie reißende Wölfe.“ Dieses Bibelwort passt exakt auf die neuen Superviren – ob SpySheriff, Vundo oder Zlob. In diesem Beitrag zeigen wir Ihnen, wie Sie die Hightech-Tarnung auffliegen lassen und die Schädlinge loswerden.

Auf Heft-CD

- Gmer (Security)
- Securemaker (Security)
- Spybot – Search & Destroy (Security)

Sie schützen Ihr System und aktualisieren es regelmäßig? Gut so. Sie glauben, dadurch sind Sie immun gegen Spyware und Trojaner? Gefährlicher Irrtum! Wer etwa auf einen Freeware-Virenscanner setzt, wiegt sich in falscher Sicherheit. Diese Programme sind ausgerechnet gegen die übelste Schädlingskategorie machtlos: Spyware. Aber auch viele Kaufprogramme und Spezialtools wie Spybot – Search & Destroy und Ad-Aware versagen im Kampf gegen moderne Schädlinge.

Wie also lässt sich Spyware aufspüren – und vor allem: Wie wird man sie wieder los? Wir haben es ausprobiert und im Selbstversuch die drei am weitesten verbreiteten Schädlinge auf unserem Test-PC installiert. Das erschreckende Ergebnis: Mit bekannten Standardtools lassen sie sich meistens nicht entfernen. Geschafft haben wir es schließlich doch – mit diesen Tricks und Tools.

SpySheriff Falsche Anti-Spyware restlos entfernen

Eine ganz perfide Spyware kommt daher wie der Wolf im Schafspelz: Getarnt als Spyware-Killer („Rogue Anti-Spyware“) verleitet SpySheriff seine Opfer dazu, die Schadsoftware freiwillig zu installieren. Wer darauf eingeht, bekommt den Eindringling nicht mehr los. Den dreisten Teil hebt sich das Programm bis zum Schluss auf: Bei einem vorgetäuschten Check findet der SpySheriff jede Menge Schädlinge – die gar nicht existieren. Wer die Phantom-Malware loswerden will, soll zahlen – mit Kreditkarte.

ROGUE ANTI-SPYWARE AUFSPÜREN

Den SpySheriff erkennen Sie daran, dass er Sie mit Warnhinweisen bombardiert und Sie ständig daran erinnert, jetzt die Vollversion zu kaufen. Doch das ist oft

Foto: iStockphoto

nur die Spitze des Eisbergs. Der Spion zeigt sich variabel: Mal wird nur die falsche Anti-Spyware-Komponente installiert, mal zusätzlich ein Trojaner. Nur eins ist sicher: Gegen echte Spyware unternimmt das Tool nichts!

SPYSHERIFF ENTFERNEN Überraschenderweise gibt es für den SpySheriff eine Deinstallations-Routine – in der Systemsteuerung unter „Programme hinzufügen und entfernen“. Nutzen Sie die Gelegenheit, und schicken Sie den SpySheriff in die Wüste – aber verlassen Sie sich nicht darauf. Wo sich die Malware immer einnistet, steht im Steckbrief rechts. Diese Einträge und Dateien können Sie mit dem Windows Explorer und dem Registry Editor entfernen.

AUF NUMMER SICHER GEHEN In unseren Tests ließen sich verschiedene Rogue-Anti-Spyware-Programme mit dem mitgelieferten Uninstaller entfernen. Doch in einschlägigen Foren wie dem Trojaner-Board (**www.trojaner-board.de**) berichten Hilfe Suchende immer wieder, dass sich noch mehr auf ihren Systemen eingenistet hat. Bei den dubiosen Geschäftspraktiken von SpySheriff & Co. lässt sich nicht ausschließen, dass Rogue Anti-Spyware noch andere Schädlinge eingeschleppt hat. Aus diesem Grund sollten Sie sicherheitshalber folgende Tipps für die beiden anderen Schädlinge befolgen und Ihr System mit den Tools HijackThis, Autoruns und Blacklight unter die Lupe nehmen.

Täterprofil

Name
SpySheriff

Charakteristik
Tarnt sich als Virenscanner

Alias
Adware Sheriff, SpyAxe, SpywareQuake

Aktive Prozesse
1950.exe, newdial.exe, spysheriff.exe, uninstall.exe, winstall.exe

Registry-Verstecke
HKLM\SOFTWARE\spysheriff,
HKLM\SOFTWARE\Microsoft\Windows\,
CurrentVersion\uninstall\spysheriff

Datei-Decknamen
%ProgramFiles%\spysheriff,
1950.exe, Desktop.html, newdial.exe,
spysheriff.exe, uninstall.exe,
winstall.exe,
%UserProfile%\Desktop\SpySheriff.lnk

Vundo Fiesen Hijacker löschen

Der Schädling, den wir uns als Nächstes vorknöpfen, ist mit Abstand der aggressivste. Mit dem Ziel, unseren Testrechner zu verseuchen, suchen wir auf Google nach einer gehackten Seriennummer. Denn in solchen verlockenden, aber illegalen Angeboten verstecken sich besonders häufig Hijacker und Downloader. Zwar warnt uns Google vor der möglicherweise schädlichen Webseite, doch wir ignorieren das und öffnen sie.

Dann geht alles ganz schnell: Die Seite baut sich auf, die Schadroutine wird aktiv, der PC ist verseucht. Vundo heißt der Schädling – ein Downloader. Doch das erfahren wir erst später, nachdem wir eine verdächtige Datei von 18 verschiedenen Virenscannern prüfen ließen. Nur eine Handvoll davon erkennt den Downloader. Und wie der Gattungsname schon sagt, beginnt der Eindringling sofort damit, andere Schadsoftware nachzuladen – in unserem Fall ein Plugin für den Internet Explorer, das uns mit Werbe-Popups aller Art bombardiert.

Um den Schädling zu vernichten, installieren wir die Freeware Ad-Aware 2007. Die erkennt Vundo zwar – kann den Downloader aber nicht vollständig löschen. Nach jedem Neustart ist er wieder da. Noch weniger Erfolg haben wir mit Spybot – Search & Destroy: Wir starten das Setup, können es aber nicht abschließen. Vundo killt immer wieder den Prozess und verhindert so eine Installation des Spyware-Killers. Schwereres Geschütz ist also notwendig, um der Plage Herr zu werden. →

KNOW-HOW

Gefährliche Täuschung

Hinter der scheinbar harmlosen Website verbirgt sich eines der nervigsten Schadprogramme – der SpySheriff.

Ein professionelles Logo und eine schicke Packung lassen die Malware ganz seriös erscheinen.

Hinter dem Button „Free Scan“ verbirgt sich kein kostenloser Virencheck, sondern die EXE der SpySheriff-Spyware, die Ihren Rechner infiziert.

Die Produkt-Beschreibung liest sich wie die eines echten Spyware-Killers. Wer das Programm nicht kennt, fällt leicht darauf rein.

SOFTWARE-TIPP

Diese Tools killen jede Spyware

Hat sich die Malware erst einmal festgesetzt, bekommt man sie nur mit den richtigen Tools wieder los. Diese Programme säubern Ihren PC:

HijackThis
Browser-Hijacker lassen sich mit diesem Tool identifizieren und entfernen – allerdings nur, wenn man die Stärken und Schwächen des Programms kennt.
www.hijackthis.de

Autoruns
Dieses Profitool kennt alle Registry-Verstecke, die sich als Autostart-Plattform nutzen lassen. Wenn Sie eine Malware im System vermuten, stehen die Chancen gut, dass Sie sie mit Autoruns finden und am Starten hindern.
www.sysinternals.com

Process Explorer
Um Spyware-Prozesse zu finden und zu killen, reicht das Windows-Bordmittel Taskmanager nicht. Der Process Explorer löst dieses Problem.
www.sysinternals.com

Pocket KillBox
Die Methoden der Spyware werden immer rabiater. Beenden Sie einen Prozess, startet ihn ein anderer erneut. Die KillBox macht Schluss damit.
www.killbox.net

F-Secure BlackLight
Immer öfter versteckt sich Malware mithilfe von Rootkit-Techniken. Dieses Tool von F-Secure macht die Schädlinge sichtbar – zumindest die meisten.
www.f-secure.de

Gmer
Ein Anti-Rootkit reicht für die Analyse nicht, denn nicht jedes Tool kennt alle Tricks. Als Ergänzung zu BlackLight eignet sich Gmer besonders gut.
www.gmer.net

virusscan.jotti.org
Verdächtige Dateien sollten auf jeden Fall von einem Virenscanner gecheckt werden. Jordi Bosveld bietet eine kostenlose Webseite an, die gleich mit 15 verschiedenen Virenscannern prüft.
http://virusscan.jotti.org

Täterprofil

Name
Vundo

Charakteristik
Greift Virenscanner an

Typ
Hijacker, Downloader und Trojaner

Prozesse
Zwei jedes Mal zufällig erzeugte DLLs

Registry-Verstecke
HCR\clsid\{EFCB1D95-FFF6-47BB-B6C9-61A523F04322},
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

Festplatten-Versteck
C:\Windows\System32\

SCHADSOFTWARE ERKENNEN Solange auch nur ein Prozess der Schadsoftware aktiv ist, bekommen Sie sie nicht mehr vom System. Deshalb müssen Sie zuerst die Malware und alle ihre Verstecke identifizieren. Installieren Sie zu diesem Zweck das Tool Autoruns (kostenloser Download unter **www.sysinternals.com**).

Die Freeware erledigt im Prinzip den gleichen Job wie das unter Spyware-Jägern beliebte Programm HijackThis. Im Gegensatz dazu listet es jedoch sämtliche Autostart-Einträge in der Registry. Denn anders als noch vor einigen Jahren trägt sich die Malware nicht mehr nur unter „Run“ oder „RunOnce“ ein. Der Eindringling Vundo beispielsweise nistet sich gleich noch an drei anderen Stellen ein.

Um diese zu lokalisieren, öffnen Sie Autoruns und setzen als Erstes je ein Häkchen bei „Verify Code Signatures“ und „Hide Microsoft Entries“. Hintergrund: Jede ausführbare Datei kann vom Ersteller mit einem Namen und einer digitalen Signatur versehen werden. Bei jeder Original-Microsoft-Datei ist das zum Beispiel der Fall. Mit den genannten Einstellungen filtern Sie diese Dateien heraus und sparen sich eine Menge Recherche-Arbeit.

Die restlichen Dateien müssen Sie manuell verifizieren. Auch dabei hilft Autoruns. Wählen Sie einen Eintrag mit der rechten Maustaste aus, und klicken Sie auf „Search online ...“. Daraufhin wird der Dateiname mit Microsofts Suchmaschine Live.com gesucht. In einigen Fällen lassen sich auf diese Weise die Dateien von bekannten Schädlingen identifizieren. Übrig bleibt eine Liste von suspekten Dateien und Registry-Einträgen, die Sie löschen sollten.

SCHÄDLINGE ABSCHALTEN Allerdings ist Vundo so aggressiv, dass es nicht ausreicht, die Registry-Einträge zu entfernen. Denn die aktiven Komponenten des Eindringlings restaurieren diese Einträge wieder. An dieser Stelle hilft jedoch ein Trick: Laden Sie den Process Explorer von **www.sysinternals.com** herunter, und starten Sie das Tool. Nach einem kurzen Scan zeigt es sämtliche aktiven Prozesse an. Der Trick besteht nun darin, die Hijacker-Dateien nicht aus dem Speicher zu löschen, sondern erst einmal nur zu deaktivieren. Klicken Sie dazu mit der rechten Maustaste auf den verdächtigen Prozess, und wählen Sie „Suspend“ aus. Damit lähmen Sie den Prozess lediglich – und die Prüfroutine der anderen Hijacker-Prozesse merkt davon nichts. Jetzt haben Sie es fast geschafft.

HIJACKER LÖSCHEN Ist der Angreifer dank des Process Explorer lahmgelegt, lässt er sich bequem entfernen. Notieren Sie sich zuerst Namen und Pfade all jener Dateien, die Sie dem Eindringling zuordnen konnten. Beenden Sie anschließend mit dem Process Explorer per „Kill“-Befehl alle Prozesse, die Sie zuvor mit dem „Suspend“-Befehl deaktiviert haben.

Als Nächstes löschen Sie mit Autoruns sämtliche Einträge, die Sie identifizieren konnten. Klicken Sie dazu mit der rechten Maustaste auf den verdächtigen Eintrag, und wählen Sie „Delete“. Jetzt ist die Gefahr fast gebannt. Löschen Sie im letzten Schritt noch die gefährlichen Dateien, damit diese nicht aus Versehen aufgerufen werden. Nach einem Neustart sollte Windows wieder frei von Schädlingen sein. Jetzt funktionieren auch Spybot – Search & Destroy und Ad-Aware wieder. Überprüfen Sie mit diesen Tools noch einmal, ob Sie auch wirklich nichts übersehen haben.

Zlob Gefährliche Video-Codecs sicher entfernen

Mit Versprechungen wie „Paris Hilton nackt“ und „Alle Blockbuster kostenlos“ locken Webseiten, die nur ein Ziel haben: den PC des Users zu übernehmen. Der Trick: Wer einen so beworbenen Film abspielen möchte, muss den ebenfalls beworbenen Codec installieren – und handelt sich die Malware Zlob ein.

Zu Testzwecken gehen wir auf das falsche Spiel ein und werden prompt infiziert. Angegriffen fühlen wir uns zunächst einmal nicht, denn der falsche Codec bringt sogar einen offiziellen Uninstaller mit. Doch damit lässt sich Zlob erwartungsgemäß nicht entfernen.

SCHÄDLING ENTTARNEN Einen ersten Hinweis darauf, dass etwas faul ist, geben die Netzwerk-Einstellungen. Typischerweise werden in einem Heimnetz die Name-Server von dem DHCP-Server verteilt. Der DSL-Router kümmert sich also um die Adressvergabe, und am Windows-Rechner ist diese Option eingestellt: „DNS-Serveradresse automatisch beziehen“. Der falsche Codec installiert nun einen DNS-Changer-Trojaner, welcher eigene Server aktiviert. Einmal eingestellt, kann der Betreiber des Servers jeden Schritt des Opfers im Netz nachvollziehen und sogar umlenken. Diese Modifikation wird von Tools wie Spybot – Search & Destroy erkannt und repariert. Doch die Ursache des Ganzen, das Rootkit, ist weiterhin aktiv. So bleibt nach einem Neustart alles beim Alten – also beim Schlechten.

ROOTKIT SICHTBAR MACHEN Um sich vor Gegenmaßnahmen zu schützen, greift der DNS-Changer-Trojaner zu einem besonders fiesen Trick: Jede Anfrage an das Dateisystem wird nicht direkt vom Betriebssystem beantwortet, sondern zuerst einmal von einem Rootkit manipuliert. Sicherheitsprogramme bekommen den Trojaner überhaupt nicht zu Gesicht, weil er sich ganz einfach selbst aus der Liste streicht. Und genau daran scheitern Spybot – Search & Destroy, Ad-Aware und andere Anti-Spyware. Abhilfe kann lediglich ein Anti-Rootkit-Tool schaffen – allerdings auch nicht jedes. So wird der Eindringling beispielsweise von Sysinternals' Rootkit Revealer nicht erkannt. BlackLight von F-Secure dagegen schafft das: Überprüfen Sie Ihr System mit BlackLight, so findet das Tool eine EXE-Datei, die sich aus „kd“ und drei weiteren, zufällig gewählten Buchstaben zusammensetzt.

Täterprofil

Name
Zlob

Charakteristik
Versteckt sich in Rootkits

Alias
DvdCodec, UseCodec, KeyCodec, EliteCodec, PerfectCodec, PornMagPass, QualityCodec, VCCodec, XPassword Generator, ZCodec, ZipCodec

Prozesse
kd*.exe

Registry-Versteck
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\System

Festplatten-Verstecke
C:\Windows\System32\kd*.exe,
C:\Programme\PornoPlayer*.*

Sonstiges
Verändert die Einstellungen des DNS-Servers im Netzwerk

SCHADCODE LÖSCHEN Das Programm von F-Secure bietet eine Option zum Löschen. Wählen Sie diese an, und starten Sie danach den PC sofort neu. Andernfalls ist der Trojaner noch im Speicher aktiv und kann sich – im schlimmsten Fall – selbst wiederherstellen. Nach dem Neustart sollten Sie unbedingt den Winlogon-Registry-Eintrag (siehe Täterprofil oben) entfernen. Öffnen Sie dazu Autoruns und anschließend die Registerkarte „Logon“. Dort finden Sie den Eintrag, den Sie per Rechtsklick und „Delete“ löschen sollten. Ansonsten kann es passieren, dass eine gleichnamige Datei aus dem „System32“-Verzeichnis beim nächsten Start mitgeladen wird.

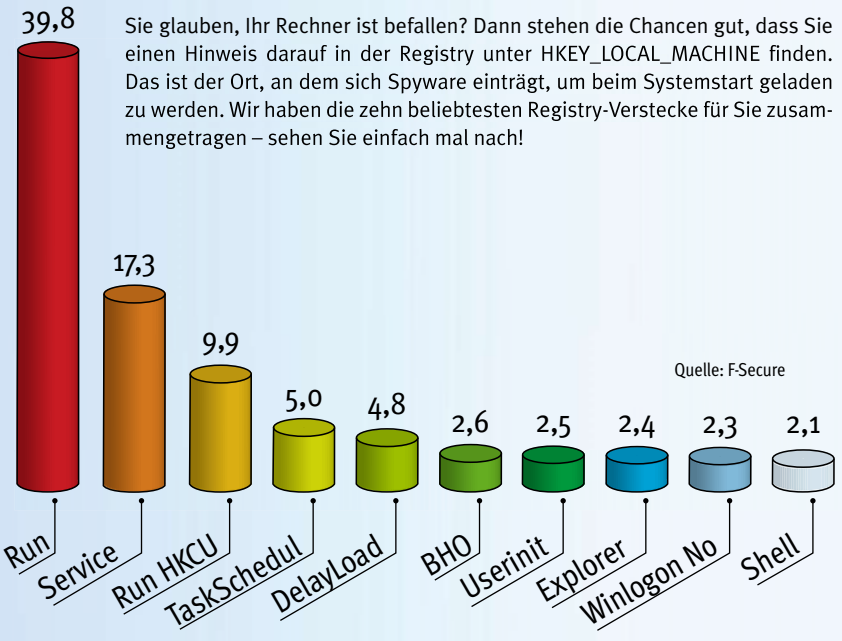
Etwaige Malware-Reste lassen sich dann mit Spybot – Search & Destroy oder Ad-Aware entfernen – und damit hat der Spuk dann wirklich ein Ende!

Valentin Pletzer

KNOW-HOW

Spyware-Verstecke in der Registry

Sie glauben, Ihr Rechner ist befallen? Dann stehen die Chancen gut, dass Sie einen Hinweis darauf in der Registry unter HKEY_LOCAL_MACHINE finden. Das ist der Ort, an dem sich Spyware einträgt, um beim Systemstart geladen zu werden. Wir haben die zehn beliebtesten Registry-Verstecke für Sie zusammengetragen – sehen Sie einfach mal nach!



Quelle: F-Secure

Gute Tools – böse Tools

Sie sind oft die letzte Rettung bei verlorenen Kennwörtern oder Angriffen aus dem Web – und gleichzeitig Hacker-Werkzeuge: Tools, die nun verboten sind, obwohl es ohne sie keine Sicherheit gibt.

Wenn alles verloren scheint, muss man den Teufel mit dem Beelzebub austreiben – etwa wenn Sie das Passwort zu Ihrem Mailaccount oder einem verschlüsselten Dokument vergessen haben: Dann hilft im Zweifelsfall nur noch ein Hackertool. Denn während die Internet-Mafia die Programme nutzt, um in PC-Systeme einzubrechen und Ihnen das Geld aus der Tasche zu ziehen, haben sie auch eine nützliche Seite. Die guten bösen Tools knacken, öffnen, kopieren, anonymisieren – kurz, sie machen Ihnen das Leben leichter. Wer sie nutzt, bewegt sich jedoch am Rand der Legalität. Denn der Gesetzgeber sagt: Schluss damit, diese Software ist verboten! CHIP stellt drei Arten dieser legalen und illegalen Tools vor.

GUTE TOOLS Diese Programme können Sie bedenkenlos nutzen.

BÖSE TOOLS Ihr Erwerb und Einsatz ist nach deutschem Recht illegal. Also: Hände weg!

GUTE & BÖSE TOOLS Software, die User ebenso wie Hacker unterstützt.

Sicherheit Das Märchen vom sicheren Passwort

Hundertprozentig sicher ist nichts – auch kein Passwort. Das heißt aber auch, dass Ihnen die guten bösen Tools helfen können, ein Kennwort wiederzufinden oder Ihr System auf Lücken zu checken.

Office Password Recovery

System: Win 98, 2000, Me, XP, Vista
Info: www.elcomsoft.com

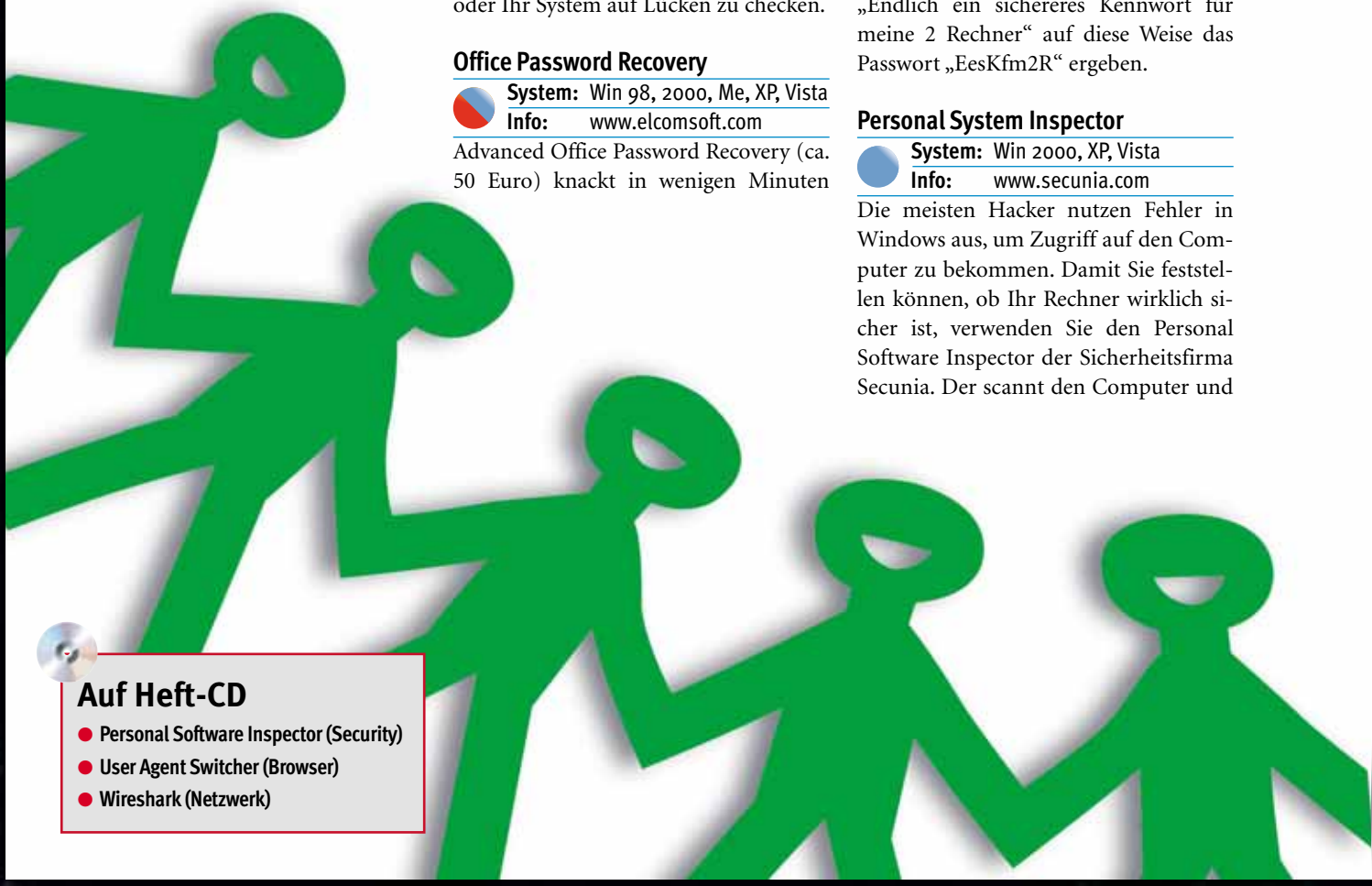
Advanced Office Password Recovery (ca. 50 Euro) knackt in wenigen Minuten verschlüsselte Office-Dokumente. Dabei versucht es erst einmal, mit einem umfangreichen Wörterbuch zum Erfolg zu kommen. Anschließend setzt das Programm Brute Force ein, probiert also alle möglichen Buchstaben-Zahlen-Kombinationen. Je nach Passwortstärke und Rechenleistung kann das mehrere Tage bis Monate dauern.

TIPP Schützen Sie sich vor Passwortknackern durch ein besonders sicheres Kennwort mit mindestens acht Stellen, Buchstaben, Zahlen und Sonderzeichen. Um es sich besser merken zu können, verwenden Sie am besten die Anfangsbuchstaben eines gut erinnerbaren Satzes. So würde beispielsweise der Satz „Endlich ein sichereres Kennwort für meine 2 Rechner“ auf diese Weise das Passwort „EesKfm2R“ ergeben.

Personal System Inspector

System: Win 2000, XP, Vista
Info: www.secunia.com

Die meisten Hacker nutzen Fehler in Windows aus, um Zugriff auf den Computer zu bekommen. Damit Sie feststellen können, ob Ihr Rechner wirklich sicher ist, verwenden Sie den Personal Software Inspector der Sicherheitsfirma Secunia. Der scannt den Computer und



Auf Heft-CD

- Personal Software Inspector (Security)
- User Agent Switcher (Browser)
- Wireshark (Netzwerk)

prüft anhand einer Anwendungs-Datenbank mit mehr als 4200 Einträgen, ob eine Hacker-anfällige Software installiert ist. Außerdem bietet das Tool gleich Download-Links zu Updates.

TIPP Um das Programm unter Vista zu installieren, benötigen Sie Administratorrechte. Das Tool ist von Microsoft nicht zertifiziert, ignorieren Sie die entsprechende Warnmeldung von Vista.

SpyAgent

System: Win 2000, XP, Vista
Info: www.spytech-web.com

Wissen Sie wirklich, was Ihr Sprössling so alles mit dem Rechner anstellt? Mit SpyAgent (ca. 50 Euro) können Sie seine Schritte am PC verfolgen. Neben Standard-Schnüffelfeatures wie dem Speichern von Tastatur- und Mauseingaben können Sie mit dem Tool auch protokollieren, auf welchen Webseiten der Nachwuchs unterwegs ist und welche Programme er startet. Das Tool schickt Ihnen auf Wunsch per E-Mail einen Bericht ins Büro.

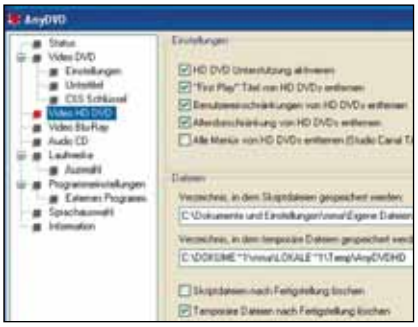
TIPP Die Stealth-Edition von SpyAgent installiert sich nach einem Doppelklick ohne Abfrage auf dem System und startet sich selbst. Dass sich die Software auf dem PC befindet, weiß nur derjenige, der sie installiert hat, denn auf dem Rechner selbst finden sich keine Spuren.

John the Ripper

System: Win 2000, XP
Info: www.openwall.com

Hacker knacken mit John the Ripper fremde Windows-Benutzerkonten, Sie bekommen mit dem gut-bösen Tool wieder Zugriff auf Ihren gesperrten Rechner. Unter Windows 98, 2000 und XP sind die User-Passwörter mit dem nicht mehr aktuellen DES-Verfahren (Data Encryption Standard) verschlüsselt. John the Ripper wird schnell damit fertig: Wer vor ein paar Jahren ein Sechs-Zeichen-Kennwort mit Groß- und Kleinschreibung entschlüsseln wollte, brauchte Jahre dafür, heute geht das in zehn Stunden. Eine Anleitung finden Sie auf **http://board.protecus.de/t12708.htm**. Allerdings: Ausgesperrte Vista-User haben ebenso das Nachsehen wie Hacker, denn für das aktuelle System hat sich Microsoft einen neuen Algorithmus ausgedacht, der bislang noch sicher ist.

TIPP Schwierige Kennwörter zu entschlüsseln dauert oftmals Monate. Wenn man dagegen mit der speziellen Version Distributed John the Ripper mehrere Rechner zusammenschließt, dauert das Knacken nur noch wenige Stunden.



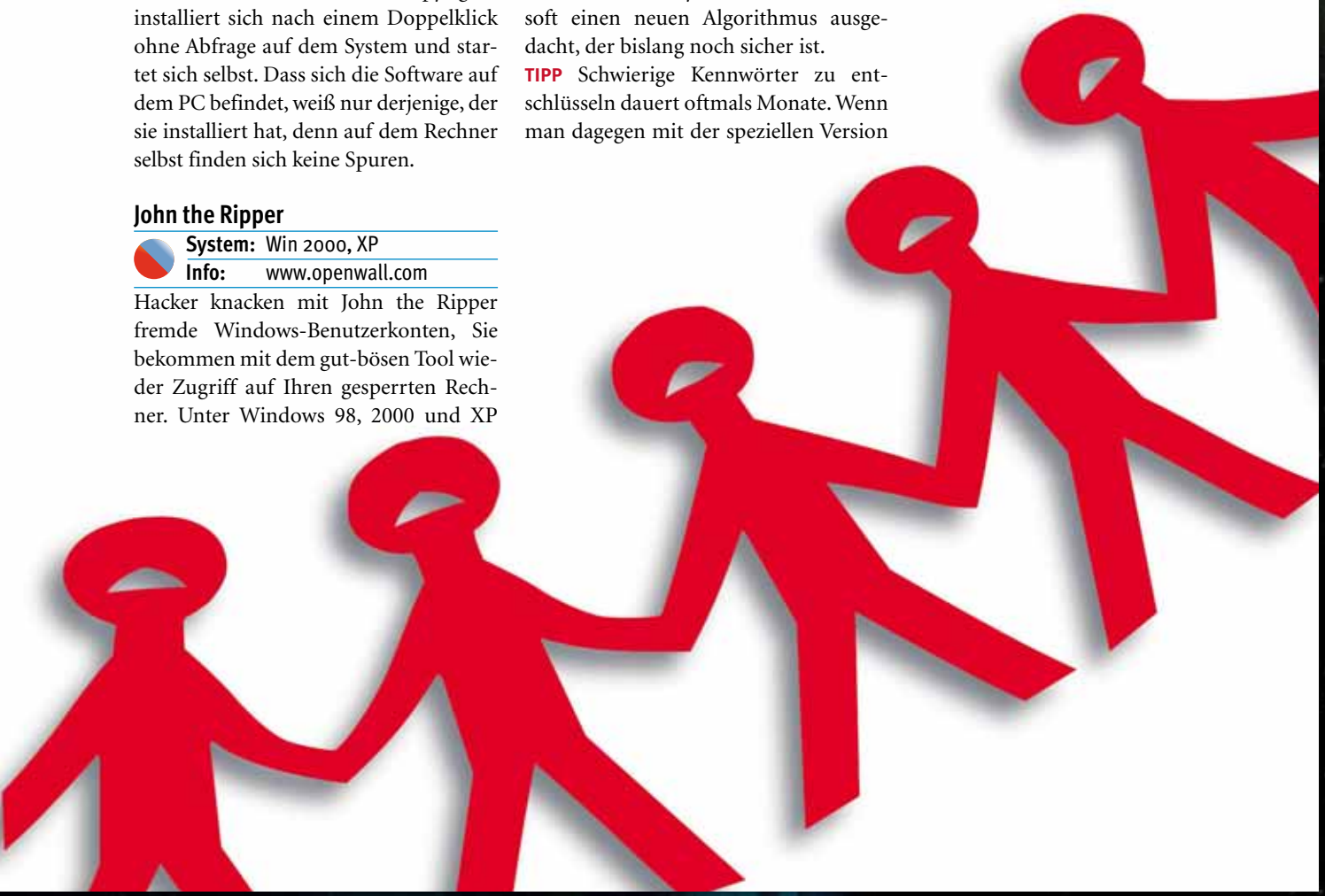
AnyDVD Das illegale Tool entfernt Sperren von DVD, HD-DVD und Blu-ray, – das Abspielen wird komfortabler.

No23live Stellen Sie ein, worüber Sie Ihre Songs streamen wollen – das Tool verteilt sie dann automatisch.

Asterisk

System: Win 98, 2000, XP
Info: nirsoft.net/utils/astlog.html

Praktisch, dass sich Outlook das Kennwort für den Mailaccount merkt und durch Pünktchen ersetzt. Dumm nur, wenn Sie sich das Passwort nicht notiert haben und es plötzlich brauchen. Keine →



Panik, Asterisk hilft. Dazu reicht der Start des Tools, das anschließend alle versteckten Passwörter protokolliert.

TIPP Bei Kennwörtern, die im Internet Explorer gespeichert sind, brauchen Sie das Zusatzprogramm AsterWin IE.

Multimedia Die Feinde von DRM und Kopierschutz

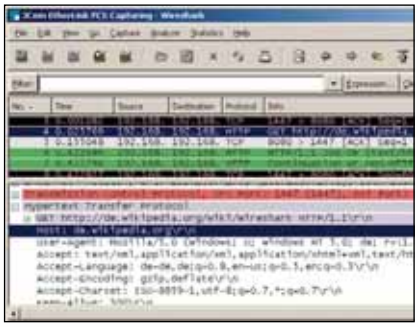
Multimedia-Inhalte verkauft kaum jemand mehr ohne Kopierschutz. Manchmal nervt der aber nicht nur, sondern bringt auch Ihr System zum Absturz. Hacker-Tools könnten helfen – wenn nicht viele davon verboten wären.

AnyDVD

System: Win XP, Vista
Info: ILLEGAL

Dieses Tool ist so verboten, dass wir laut einem Urteil nicht einmal den Link der Homepage angeben dürfen. Any-DVD knackt den Kopierschutz auf jeder DVD, der Kauf verstößt deshalb gegen das neue Urheberrecht. Doch das Programm bewirkt für den User auch Gutes: Es schaltet nicht nur den Regionalcode auf einer DVD aus, sondern auch jeden Kopierschutz. Besonders wichtig ist das bei X-Protect, denn der Schutz kann so heftig sein, dass Sie selbst eine legal erworbene Scheibe nicht abspielen können. DVDs mit dem Kopierschutz Flux erscheinen seit Neuestem vermehrt, darunter beispielsweise „Apocalypto“.

Miro Im Web-TV-Tool stehen mehr als 2000 Sender zur Verfügung. Sie können auch eigene Kanäle anlegen.



Wireshark Das Schnüffel-Tool zeigt den Inhalt von Netzwerkverbindungen an – und damit auch übermittelte Kennwörter.

TIPP Nutzern der neuen HD-Formate kann AnyDVD das Leben richtig erleichtern, denn das Tool schaltet den Kopierschutz auf HD-DVD und Blu-ray aus. Das bedeutet: Anwender brauchen nur ein preiswertes Leselaufwerk und können sich das Geld für neue HD-Komponenten wie Grafikkarte oder Monitor sparen.

FairUse4WM

System: Windows XP, Vista
Info: ILLEGAL

Nach „viodentia“, dem Programmierer dieses Tools, ließ Microsoft sogar polizeilich fahnden – kein Wunder, Fair Use4WM knackt das Microsoft-DRM, mit dem viele Musikdienste ihre Lieder schützen. Allerdings fördert das Tool nicht den Datenklau: Kunden müssen einen Song und damit die notwendige Lizenz kaufen, um ihn vom DRM zu befreien.

Ein anderer Hacker hat die Weiterentwicklung des Tools übernommen und eine Version veröffentlicht, die alle bisherigen Gegenmaßnahmen Microsofts aushebelt. Damit läuft FairUse4WM auch auf Vista und mit dem Media Player 11.

TIPP Für Gegenmaßnahmen benutzt Microsoft die Windows-Updates für den Media Player. Daher kursiert auch eine Anleitung im Netz, wie der Anwender vom Media Player 11 auf die Version 10 downgraden kann – denn mit dem alten Player läuft FairUse4WM immer.

No23live

System: Windows 98, 2000, Me, XP
Info: www.no23.de

Die Musikindustrie achtet darauf, dass ihr Kopierschutz intakt bleibt. Aber das

PROFI-TIPP

China-Connection für kostenlose Blockbuster und Bundesliga

Sie wollen Premiere nicht abonnieren und trotzdem die Live-Übertragung des Bayern-Spiels sehen? Dann zappen Sie doch einmal per Streaming-Freeware zu chinesischen TV-Kanälen. Die senden auch deutsche Sportevents rund um die Uhr ins Web.

Fußball live und gratis findet im deutschen Fernsehen nur noch selten statt. Kein Wunder bei immer teureren Senderechten. Wie schön, dass CCTV-5, der größte Sportsender Chinas, Livespiele von der italienischen Serie A bis zur deutschen Bundesliga überträgt, und zwar auch ins Web.

Mit kostenlosen Streaming-Clients wie PPLive oder SopCast lassen sich Sender wie CCTV oder der amerikanische Sportkanal ESPN am PC empfangen. Sie verteilen die Streams mit der BitTorrent-Technologie. Damit entfallen die Kosten für zentrale Server, denn jeder Zuschauer fungiert gleichzeitig als Verteiler. Als Videoformat dient in der Regel Microsofts ASF.

Programme wie Sopcast oder PPLive bieten mehr als fünfzig Sender aus aller Herren Länder an – vom liberalen Australien bis hin zum islamistisch ausgerichteten Malaysia – und außerdem Raubkopien von Kinohits.

Die goldene Zeit der Piratensender geht aber wohl bald zu Ende: Inzwischen hat der Sender CCTV-5 für alle PPLive-Zuschauer die Sportausstrahlung außerhalb Chinas gesperrt. Dagegen hilft nur eines: über einen chinesischen Proxyserver ins Internet zu gehen. Ausführliche Tipps und Anleitungen, wie das Ganze funktioniert, finden Sie in Spezialforen, beispielsweise unter **www.myp2p.eu**.

PPLIVE Mit dem Streaming-Client empfangen Sie gratis chinesische TV-Sender übers Internet – auch Bundesliga live.

Zuhören über das Netz ist nicht verboten und umgeht ebenso wie das Aufzeichnen von Audiostreams jegliche Restriktionen. No23live macht genau das: Der Player schickt den Audiostream über das Netz an andere Zuhörer, die den empfangenen Stream auch gleich mitschneiden können. Auf der Heft-CD finden Sie zusätzlich den No23 Recorder, der abgespielte Audiostreams auf dem heimischen PC aufzeichnet.

TIPP No23 unterstützt auch VST-Plugins, um die Streaming-Qualität zu verbessern. Geben Sie in den Einstellungen einfach den Ordner an, in dem die VST-Plugins liegen.

Miro

System: Windows XP, Vista
Info: www.getmiro.de

Von YouTube, Google Video bis zur BBC gibt es freie Videoclips im Internet, aber verstreut. Miro ändert das. Der Open-Source-Player sucht in verschiedenen Videodiensten, lädt dort Filme herunter und speichert sie – dieses Feature fehlt beispielsweise auf der Website von YouTube. Das Suchergebnis können Sie als eigenen Kanal archivieren. Mittlerweile finden sich im Miro Guide mehr als 7000 Kanäle – einige in HD. Darüber hinaus spielt die Software aber auch Filme ab, die schon auf der Festplatte liegen, und lässt sich außerdem als Media-Player-Ersatz nutzen.

TIPP Wenn Sie auf „Library“ gehen, zeigt Ihnen Miro alle Videos an, die Sie zuletzt angesehen haben. Klicken Sie dann – etwa bei einem YouTube-Video – rechts auf „Details“, und aktivieren Sie danach „Permalink“, öffnet Miro die entsprechende YouTube-Site.

QT Lite

System: Win 2000, XP, Vista
Info: www.codecguide.com

Viele Clips im Internet – beispielsweise Filmtrailer – liegen im MOV-Format von Apple vor. Das kann unter Windows eigentlich nur QuickTime abspielen. Doch nicht jeder will diesen Player von Apple installieren, zumal er für andere Formate wie etwa MPEG nicht sonderlich gut taugt. Als Player für MOV-Files empfiehlt sich der Media Player Classic, die Zusammenarbeit mit QT Lite klappt einwandfrei.

TIPP QT Lite hat ein Download-Tool integriert, das bei einem Klick auf einen Streaming-Link dem User die Wahl lässt, ob er das Video sofort anschauen oder zunächst auf der Festplatte speichern möchte.

KNOW-HOW

Diese Software bringt Sie in den Knast

Geht es nach der Bundesregierung, dürfen Sie viele der in diesem Artikel vorgestellten Programme nicht mehr einsetzen – darunter auch Tools, mit denen Sie Ihr Netzwerk auf Lücken prüfen. Das freut die international agierenden Hacker.

So sieht das Gesetz aus Die Strafvorschriften zur „Bekämpfung der Computerkriminalität“ stellen ab sofort das Programmieren, Überlassen, Verbreiten oder Beschaffen von „Computer-Sicherheitswerkzeugen“ unter Strafe. Der Effekt ist fatal: Denn Werkzeuge wie Portscanner helfen nicht nur Hackern, sondern auch Administratoren beim Erkennen von Sicherheitslücken.

Um diese Tools geht es Betroffen sind vor allem Tools zur Netzwerkanalyse wie etwa Wireshark oder Portscanner–Programme. Doch ebendiese Softwarewerkzeuge benötigen Administratoren und Sicherheitsexperten bei ihrer täglichen Arbeit. Im Klartext heißt das: Hacker können ab sofort ungestört agieren. User, die sich vor ihnen schützen wollen, werden kriminalisiert.

Die Folgen Zwar empfiehlt der Bundesrechtsausschuss den Gerichten, nur solche Personen zu verurteilen, die Analysetools für kriminelle Machenschaften nutzen. Wer darunter fällt, ist allerdings Auslegungssache der Gerichte. Das haben auch die Experten erkannt, die die Regierung bei der Formulierung des Gesetzes beraten haben, und vor diesem Problem gewarnt. Die Internetwirtschaft und der Bundesrat haben die Gesetzesänderung ebenfalls scharf kritisiert. Andy Müller-Maguhn, Sprecher des Chaos Computer Clubs: „Industrie und Bürgern wird systematisch die Möglichkeit genommen, ihre Systeme adäquat auf Sicherheit zu überprüfen. Dieses Verbot gefährdet die Sicherheit des IT-Standorts Deutschland.“

Netzwerk Schnüffeltools finden WLANs und Passwörter

Eigentlich sollte jede Internetverbindung mittlerweile verschlüsselt sein, denn mit speziellen Schnüffeltools können Sie den Standard-Netzverkehr ganz problemlos abhören. Das ist ein großes Sicherheitsrisiko, denn im Datenstrom finden sich in vielen Fällen Kennwörter von Mailaccounts im Klartext. Ähnlich verhält es sich mit WLAN-Kennwörtern. Deshalb reicht schon ein bisschen Lauschen, um den WEP- oder WPA-Key herauszubekommen.

Wireshark

System: Win 2000, XP, Vista
Info: www.wireshark.org

Das Tool Wireshark analysiert den Netzwerkverkehr und zeigt ihn in Echtzeit an. Dabei unterstützt das Programm 472 verschiedene Protokolle, darunter beispielsweise Virtual LAN oder das neue IPv6 von Vista.

Wer seine E-Mails über eine normale, unverschlüsselte Webverbindung abfragt, findet die Zugriffskennwörter anschließend im Klartext im Wireshark-Log wieder. Auch Anmelde-Informationen und Webseiten-Aufrufe kann der User mit Wireshark aus dem Datenverkehr auslesen.

TIPP Da das Programm den Netzwerktraffic ungefiltert ausgibt, ist es für Laien schwierig, die richtigen Informationen zu finden. Eine Anleitung finden Sie auf **www.easy-network.de/ethereal.html**.

Network Share Browser

System: Win 98, 2000, XP
Info: www.bysoft.com

Ihr PC verteilt Daten, ohne dass Sie etwas davon mitbekommen! Neben den Standardfreigaben der Systemlaufwerke, die von Windows stammen, gibt es meist noch Netzwerkfreigaben (Shares), die Sie oder andere Benutzer auf dem PC angelegt haben und die schlicht in Vergessenheit geraten sind. Das kann zu einem ernsten Sicherheitsproblem werden. Schließen Sie daher alle Freigaben, die Sie nicht benötigen. Dabei hilft Ihnen das Tool Network Share Browser. Das Programm listet die Shares auf Ihrem Rechner übersichtlich auf. →

TIPP Wenn Sie Freigaben anlegen wollen, die das Programm nicht findet, setzen Sie ein $-Zeichen hinter den Freigabenamen. Wollen Sie nun mit einem anderen Computer auf diese Ressource zugreifen, müssen Sie zwar den Namen per Hand eingeben, dafür bleibt die Freigabe unsichtbar.

Wireless Key View

System: Win 2000, XP
Info: http://nirsoft.net

Das hat vermutlich fast jeder schon erlebt: Nach einem Systemabsturz haben Sie Ihr Notebook neu aufgesetzt und wollen es nun mit Ihrem WLAN verbinden. Kein Problem – wenn Sie das Kennwort noch wüssten. Das Einzige, was an dieser Stelle in der Regel noch hilft: den Router zurücksetzen, sämtliche Daten umständlich neu eingeben – und erst nach Stunden wieder lossurfen.

Doch es geht auch anders: Mit Wireless Key View können Sie das WLAN-Kennwort auslesen. Alles, was Sie brauchen, ist Ihr Notebook und die Software. Das funktioniert sogar mit den recht sicheren WPA-Schlüsseln.

TIPP Die aktuellen WPA2-Keys mit AES-Verschlüsselung kann auch Wireless Key View nicht ausspionieren. Um diese Keys nutzen und sich dadurch besser vor Hackerangriffen schützen zu können, spielen Sie einfach gemäß den Angaben in der Bedienungsanleitung Ihres Routers die aktuelle Firmware auf. Das Kennwort dürfen Sie dann allerdings nicht mehr vergessen, denn sonst kommen Sie um einen Reset des Routers und ein aufwendiges Neuaufsetzen nicht mehr herum.

Wlandscape

System: Win 98, 2000, XP
Info: www.wlandscape.net

Die im Umkreis verfügbaren WLAN-Netze anzeigen, das kann sogar Windows von Haus aus. Das Programm Wlandscape geht an dieser Stelle noch einen Schritt weiter und bindet die Informationen in eine Straßenkarte ein. Dabei sucht das Tool nicht nur nach WLANs, sondern errechnet anhand der Signalstärke auch deren Standort. Anschließend sehen Sie in der Karte die WLANs in der Umgebung – samt deren Verschlüsselungsmethode.

TIPP Wenn Sie die Ortsdaten nicht manuell eingeben wollen, können Sie einen GPS-Empfänger mit Wlandscape verbinden. Das Tool zeigt dann Ihren Standort auf der Karte sowie die verfügbaren Funknetze mit ihren Standorten.

Online Die verbotenen Früchte des Internets kosten

Gute Surfer kommen in den Himmel und die bösen … – der Rest ist bekannt. Dass clevere User wirklich überallhin kommen, ohne dabei gesehen zu werden, dafür sorgen die passenden Tools.

Firefox, User Agent Switcher

System: Win 98, Me, NT, 2000, XP, Vista
Info: www.mozilla.com

Nichts zahlen und dennoch auf kostenpflichtigen Premium-Seiten surfen? Das ist zwar nicht die feine Art, geht unter Umständen aber ganz einfach: Man muss seinen Browser nur als Googlebot tarnen, denn der kommt überallhin.

Bezahlseiten lassen Googles Suchroboter durch, denn er soll sie für Trefferlisten indizieren. Für Firefox lässt sich dafür ein Plugin installieren, das ihn als einen anderen Browser bei einer Website anmeldet: den User Agent Switcher.

Gehen Sie in die „Options“ des Plugins und legen Sie unter „User agents | add“ ein neues Profil an. Schreiben Sie dort unter „User Agent“ folgende Zeile: „Googlebot/2.1 (+http://www.google.com/bot.html)“. Nun können Sie unter „Extras | User Agent Switcher“ den „Googlebot“ auswählen und auf bisher unzugänglichen Seiten surfen.

Allerdings klappt das nur, wenn der Webmaster die Site nicht sorgfältig programmiert hat. Denn über die IP-Adresse kann er schnell herausfinden, dass es sich nicht um den Googlebot handelt.

TIPP Den Googlebot als User Agent einzustellen sorgt auch für sicheres Surfen auf verseuchten Websites. Denn diese verstecken oft gefährliche JavaScripts vor dem Googlebot, damit die Site in den Augen von Google harmlos erscheint und in den Suchlisten auftaucht.

PeerGuardian

System: Win 98, 2000, XP
Info: www.phoenixlabs.org

Wenn Sie ins Internet gehen, verdienen andere Geld damit, Ihr Surfverhalten auszuspionieren. Harmlos ist das Ganze, wenn dabei lediglich das Kundenprofil verkauft wird. Kritischer wird die Angelegenheit dagegen, wenn dahinter die Musikindustrie steht, die ganz genau wissen will, was Sie so alles aus Tauschbörsen herunterladen. Das Tool PeerGuardian agiert wie eine Firewall und blockt anhand von ständig aktualisierten Listen diese IP-Anfragen ab. Aber auch wenn Sie mit eMule oder BitTorrent nichts am Hut haben, macht sich PeerGuardian nützlich, weil das Tool Ad- und Spyware abfängt. Wichtig bei PeerGuardian: Die Blocklisten müssen immer aktuell sein. Daher können Sie auch andere Listen importieren, etwa die der Community bluetack (**www.bluetack.co.uk**). Deren Tool Blocklist Manager kann Listen in das Format von PeerGuardian konvertieren.

TIPP Im Forum von PeerGuardian (**http://forum.phoenixlabs.org**) finden Sie seit Kurzem auch eine Vista-Version.

Cryptload

System: Win 98, 2000, XP
Info: www.cryptload.info

Websites zum Hosten von Dateien mausern sich immer mehr zum neuen Verteilsystem für Filme, Bilder und Songs. Aber was da alles auf Rapidshare, Megaupload & Co. gehostet wird, ist selten legal. Erfährt der Betreiber der Hostsite davon, dass über ihn Raubkopien vertrieben werden, sperrt er einfach den Zugang zum entsprechenden Konto und löscht die Daten.

Aus diesem Grund verschlüsseln Uploader zunehmend die Zugangslinks. Dazu benötigt der Sauger ein Tool wie Cryptload, das mit einem solchen Link die gehosteten Dateien downloaden kann. Zusätzlich bietet das Tool auch Features, mit denen der zahlende Premium-Kunde von Rapidshare Dateien schneller herunterlädt.

TIPP Sie können mit Cryptload auch Seiten nutzen, die vor dem Download das Eingeben von Zahlenkombinationen von einem JPEG-Bild verlangen – als Schutzfunktion vor dem massenhaften Download per Software-Grabber. Cryptload hat eine OCR-Schnittstelle integriert und ermittelt automatisch die verlangte Zahlenkombination.

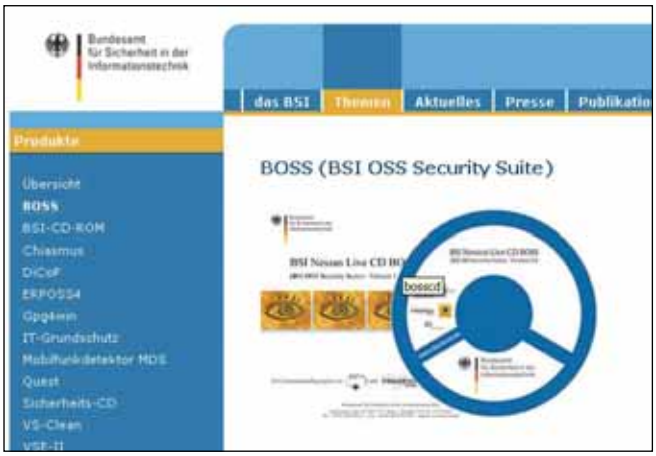
Markus Mandau, Fabian von Keudell

BOSS-CD: Staat liefert Hacker-Tools frei Haus

Mit dem Hacker-Paragrafen will der Staat die Verbreitung gefährlicher Tools unterbinden. Gleichzeitig verteilt das BSI selbst einige zwielichtige Programme. So schützen Sie sich.

Sicherheitslücken", so bemerkt das Bundesamt für Sicherheit in der Informationstechnik (BSI) ganz richtig, „bergen auch für den privaten Anwender Gefahren." Doch diese rechtzeitig zu entdecken ist kein leichter Job. Die vom BSI herausgegebene Sicherheits-CD BOSS (**www.bsi.de/produkte/boss**) enthält einige Tools, die dabei helfen sollen. Das Problem: Die Programme unterstützen nicht nur Administratoren beim Absichern ihrer Systeme, sondern auch Hacker beim Eindringen.

CHIP hat die gefährlichsten Tools analysiert und gibt Tipps, wie Sie sich vor Ihnen schützen können.



Stoff für Hacker
Auf der Homepage des Bundesamts für Sicherheit in der Informationstechnik (BSI) gibt es spannende Downloads zu entdecken.

John the Ripper

Das umstrittenste Tool auf der BOSS-CD heißt John the Ripper. Ursprünglich für Linux/Unix-Passwörter entwickelt, knackt es auch Windows-Kennwörter per Brute-Force-Attacke.

Gegenmaßnahmen: Zum Glück können Sie sich ganz einfach schützen. Da John the Ripper die verschlüsselten Passwörter von Ihrer Festplatte braucht, reicht es, wenn Sie niemanden an Ihren PC lassen.

Nessus

Die gefährlichsten Sicherheitslücken sind die, die Ihren PC über das Netzwerk zugänglich machen. Der Scanner Nessus enthält zwar keinen Schadcode, kann jedoch Sicherheitslücken vor einem Angriff ausspähen.

Gegenmaßnahmen: Am besten schützen Sie sich mit einer Firewall – egal welcher Art. Die Hauptsache ist, dass Ihr Rechner keine offenen Ports aufweist, die über das Netzwerk erreichbar sind. Denn anhand der Portnummer und der Antwort, die diese Ports geben, kann Nessus feststellen, welche Software installiert ist und ob sie eine Lücke hat.

Tiger

Die Security Suite des BSI zielt nicht nur auf Windows ab. Auch Linux-Systeme müssen sich in Acht nehmen. Das Tool Tiger beispielsweise überprüft Linux-Systeme auf Schwachstellen.

Gegenmaßnahmen: Genau wie bei Nessus eignet sich auch an dieser Stelle eine Firewall als Schutz vor dem Check. Außerdem sollten stets auch die neuesten Updates installiert sein.

Ethereal

Das CD-Image, das das BSI auf seinem Webserver zum Download anbietet, enthält sogar richtiges Spionagewerkzeug. Das Programm Ethereal, das mittlerweile eigentlich unter dem Namen „Wireshark" firmiert, protokolliert sämtlichen Netzwerkverkehr und eignet sich so als Passwortspion. Meldet sich etwa ein User bei seinem Webmail-Account unter der unverschlüsselten HTTP-Adresse an, kann Ethereal das aufzeichnen und sichtbar machen.

Gegenmaßnahmen: Nutzen Sie – sooft es geht – verschlüsselte Verbindungen. Viele Webseiten, insbesondere Freemailer, bieten zum Einloggen eine HTTPS-Seite an. Wenn Sie diese nutzen, ist der Wireshark-Mitschnitt für den Angreifer nutzlos. Aber Vorsicht: Auch bei POP3-Verbindungen wird das Passwort unverschlüsselt übermittelt. Nutzen Sie deshalb besser IMAP.

Sonstige Tools

Die übrigen Tools auf der BSI-CD BOSS 2.0 sind eher informativ denn gefährlich. Bei dem Programm ClamAV etwa handelt es sich um einen kostenlosen Virenscanner, der allerdings nicht mit der kommerziellen Konkurrenz mithalten kann. Auch vor dem Linux-Tool „chkrootkit" muss sich niemand in Acht nehmen. Ganz im Gegenteil: Dieses nützliche Tool spürt Rootkits in Linux-Systemen auf. Schade nur, dass keine Alternative für Windows auf die CD gepackt wurde.

Valentin Pletzer

Vierkampf der Browser

Der Internet Explorer verliert an Boden – kein Wunder. Der CHIP-Test zeigte: Mit jedem anderen Webbrowser surfen Sie schneller, sicherer und bequemer.

Auf die Frage, welchen Browser sie nutze, geriet Bundesjustizministerin Brigitte Zypries in einem Interview kürzlich in Verlegenheit: „Browser, Browser …“, murmelte sie. „Was war noch mal ein Browser?“ Mit diesem Unwissen dürfte Frau Zypries einer Minderheit angehören, denn Browser sind nach Betriebssystemen die am häufigsten genutzte Software überhaupt.

Deshalb ist der Browser-Markt auch stets in Bewegung. Zwar nutzen immer noch knapp zwei Drittel aller Websurfer Microsofts Internet Explorer – doch vor drei Jahren waren es noch mehr als 90 Prozent. Marktanteile gewann vor allem die Open-Source-Alternative Firefox, mit der immerhin etwa jeder Vierte online geht. Seit Hersteller Opera seinen gleichnamigen – ehemals kostenpflichtigen – Webbrowser gratis anbietet und Apple seinen Browser Safari für Windows portiert hat, steigen auch deren Nutzerzahlen. Daneben gibt es weitere Alternativen, etwa K-Meleon oder den gerade wiederbelebten Urbrowser Netscape. Doch die spielen mit weniger als einem Prozent Marktanteil so gut wie keine Rolle und sind deshalb in unserem Testfeld nicht vertreten.

Die Marktanteile des Internet Explorers könnten in den kommenden Monaten weiter bröckeln. Die Konkurrenz veröffentlicht nämlich neue Versionen ihrer Browser und verspricht Innovationen ohne Ende: Noch schneller sollen die Surfprogramme werden, noch sicherer, noch bequemer zu bedienen. Wir wollten wissen, ob die neuen Browser diesen Ansprüchen gerecht werden, und haben sie in puncto Sicherheit / Privatsphäre, Funktionsumfang und Performance getestet. Herangezogen haben wir die zum Testzeitpunkt aktuellsten Releases: die Alpha 8 von Firefox 3.0 (Codename: „Gran Paradiso“), die Beta-Version von Opera 9.5 (Codename: „Kestrel“), Safari 3.0 (ebenfalls Beta) sowie den Microsoft Internet Explorer 7.0.6.

Auf Heft-CD

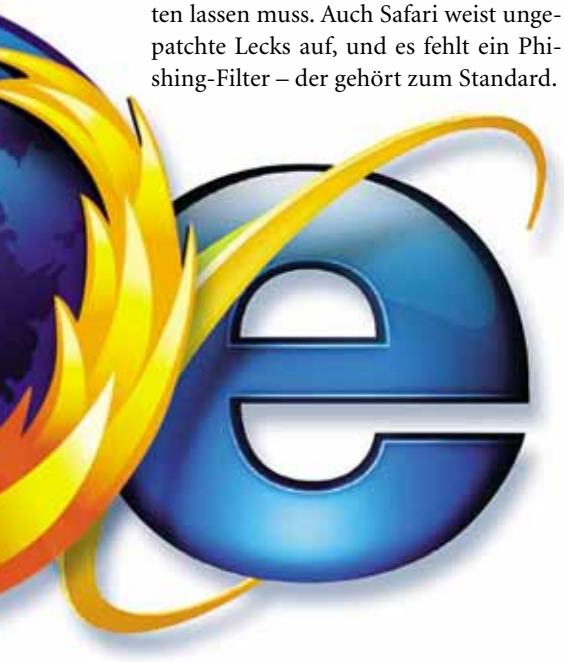
- Firefox (Browser)
- GreenBrowser (Browser)
- Opera (Browser)

Sicherheit Zu viele Lücken im Internet Explorer

Laut einer Studie von Symantec zielen etwa 80 Prozent aller Angriffe im Internet auf Webseiten oder Browser. Die Palette reicht von Phishing bis zum Ausspionieren gespeicherter Daten wie beispielsweise Passwörter. Angesichts dieser Lage erwarten wir von einem Browser, dass er die Bedrohungen abwenden oder zumindest davor warnen kann.

Am sichersten surfen Sie mit dem Testsieger Opera: Der Browser warnt vor betrügerischen Webseiten, besitzt mit Abstand das fortschrittlichste Cookie-Management, blockt Werbebanner und Popups – und merkt sich auf Wunsch alle dazu nötigen Einstellungen für jede einzelne Webseite. Außerdem ist Opera der einzige Testkandidat mit einer weißen Weste: So haben die Sicherheitsexperten des Dienstes Secunia in der aktuellen Version bisher keine einzige Sicherheitslücke festgestellt. Das gilt zwar auch für Firefox und Safari, trotzdem gefällt uns Opera einen Tick besser. Sollte nämlich doch ein Sicherheitsrisiko entdeckt werden, reagiert Opera vorbildlich, wie ein Blick in die Vergangenheit zeigt: Als einziger Hersteller patchte das norwegische Unternehmen bei der Vorgängerversion alle bekannten Schwachstellen.

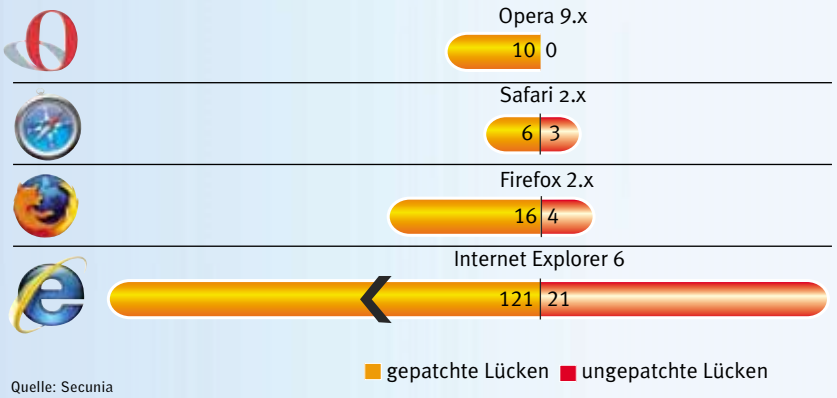
So zuverlässig arbeitet nicht einmal die Firefox-Gemeinde, die sich noch vier (unkritische) Lücken in ihrem Open-Source-Browser der Version 2.x vorhalten lassen muss. Auch Safari weist ungepatchte Lecks auf, und es fehlt ein Phishing-Filter – der gehört zum Standard.



KNOW-HOW

So sicher sind Webbrowser

Ein Blick in die Vergangenheit zeigt, welche Browser zuverlässig sind. Hersteller Opera hat als einziger alle Lücken gefixt – bei Microsoft gibt es die meisten Lecks.



Quelle: Secunia

Das schlechteste Gefühl beschleicht einen beim Surfen mit dem Internet Explorer. Der Microsoft-Browser nutzt etwa als einziger die Softwarekomponente ActiveX, über die automatisch Anwendungen im Browser ausgeführt werden können. Das Problem: ActiveX-Plugins haben sehr viele Rechte – findet ein Hacker an dieser Stelle eine Lücke, kann er meistens mühelos auf das Betriebssystem zugreifen.

Und dieses Risiko ist hoch. Denn laut dem 12. Internet Security Thread Report von Symantec lassen sich 89 Prozent der Sicherheitslücken in Browser-Plugins auf Schwachstellen in ActiveX-Komponenten zurückführen. Dagegen hilft nur das Abschalten, was Microsoft standardmäßig nicht tut.

Nur Vista-Nutzer sind leicht im Vorteil: Der Internet Explorer 7 wird im neuen Betriebssystem in einem geschützten Modus ausgeführt, der das Starten von Anwendungen nicht erlaubt. Doch allzu sicher sollten sich auch Vista-Nutzer nicht fühlen: Von den zwanzig bisher im Internet Explorer 7 gefundenen Sicherheitslecks hat Microsoft erst zwölf geschlossen.

Funktionen Dateien laden, chatten ... Opera kann alles

Erwartungsgemäß lässt kein Browser Funktionen vermissen, die heute zur Grundausstattung gehören. Verschiedene Webseiten in Tabs öffnen, Favoriten speichern und verwalten, RSS-Feeds anzeigen, integrierte Suchfunktionen – das können alle. Die Unterschiede liegen im Detail, in der Summe sind sie dann aber doch gewaltig.

Mit seiner Funktionsvielfalt deklassiert Opera die Konkurrenz. Nur ein paar Beispiele, warum wir so begeistert sind: Bei Opera surfen Sie nicht nur mit Tabs, Sie können mit den praktischen Registerkarten noch viel mehr anstellen. Sie lassen sich sortieren, in einer Vorschau anzeigen oder als Lesezeichen ablegen. Bestimmte Tab-Anordnungen können Sie als Session speichern – etwa eine fürs Büro und eine für zu Hause.

Opera ist der einzige Browser, in dem Sie für jede Webseite spezifische Einstellungen speichern können – etwa wie Cookies dieser Seite behandelt werden oder ob sie Werbung einblenden darf.

FAZIT

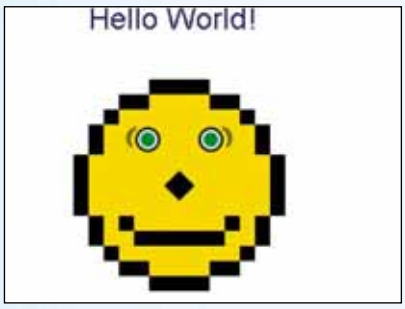
Mit diesem Test schwingt sich Opera zur Referenz auf, an der sich alle anderen Browser messen lassen müssen. In Sachen Sicherheit und Funktionsumfang ist er nicht zu schlagen, lediglich bei der Performance landet er knapp hinter Safari. Firefox lässt im Auslieferungszustand (Addons haben wir nicht berücksichtigt) ein paar Funktionen vermissen und landet daher auf Platz zwei. Microsofts Internet Explorer ist bestenfalls Durchschnitt – und abgeschlagener Letzter im Test.

→

KNOW-HOW

Der Acid2-Test

Das Internet funktioniert nach festgelegten Standards, an die sich sowohl die Programmierer von Webseiten als auch die von Browsern halten sollten. Tun sie das nicht, können HTML-Seiten falsch dargestellt werden. Ein Test für die sogenannte W3C-Konformität eines Browsers ist der Acid2-Test. Bei sauber programmierten Browsern zeigt er einen Smiley, ansonsten mehr oder weniger schlimmes Durcheinander. Dadurch kann die Lesbarkeit von Webseiten eingeschränkt werden.



Bestanden Opera, Safari und die neue Firefox-Version stellen die Testseite korrekt dar – sie sind konform zum W3C-Standard.

Nicht bestanden Statt eines Smileys zeigt der Internet Explorer 7 nur Chaos an – er erfüllt die W3C-Vorgaben nicht.

Alle Seiten lassen sich stufenlos skalieren, inklusive der Bilder – auch das ist einzigartig. Und wenn wir schon bei den exklusiven Features sind: Opera lässt sich mit Mausgesten steuern, lädt Torrent-Dateien aus dem Web und bietet einen integrierten Chat- und Mailclient. Klasse: Die neue Vorlauffunktion erkennt in einer Folge von Webseiten automatisch den Link, der zur nächsten Seite führt. Die durchdachte Druckfunktion erscheint da fast schon normal, verdient aber dennoch Erwähnung: Sie ist ebenso umfangreich wie übersichtlich, erlaubt das Skalieren der auszugebenden Seite, das Ausblenden von Hintergrundbildern, bietet eine Druckvorschau – das alles in einem einzigen Menü.

Eine solche Funktionsfülle bieten die anderen Browser bei Weitem nicht. Der Internet Explorer 7 und Safari überraschen wenig, als praktisches Detail sticht beim Apple-Browser lediglich die Snap-Back-Funktion heraus: Mit ihr gelangen Sie beim Surfen schnell zu einer markierten Ausgangsseite zurück – nützlich, wenn Sie sich Link für Link durchs Web hangeln und schnell wieder zurück zum Anfang wollen. Firefox-Nutzer können ihren Browser immerhin nach Belieben erweitern, die Plugins stehen auf der Mozilla-Webseite zu Hunderten zur Verfügung. Die Grenzen setzt das System: Die Erfahrung zeigt, dass Firefox ab zehn bis 15 Plugins deutlich langsamer wird – bisweilen auch instabil. Interessant: Trotz seiner Funktionsvielfalt bringt Opera die kleinste Installationsdatei mit. Sie ist nur 5 MByte groß, der Internet Explorer 7 kommt mit 14,1 MByte.

Performance Der schnellste Browser der Welt heißt Safari

Apple bewirbt Safari als den schnellsten Browser überhaupt. Aber ist das wichtig? Beim Surfen auf normalen HTML-Seiten kaum, die Unterschiede beim Laden und Rendern simpler Seiten liegen im Zehntelsekunden-Bereich. Bei komplexen Webservices sieht das anders aus. Den Aufbau einer Google-Maps-Seite etwa bekommt Firefox blitzschnell hin. Opera hingegen braucht dafür so lange, als wolle er die Welt neu erschaffen.

Im Test haben wir das Tempo mit dem Benchmark iBench5 überprüft. Er lässt die Browser komplexe HTML-Seiten, Cascading Style Sheets (CSS) und XML-Seiten laden sowie JavaScript ausführen – und misst die Zeit, bis alles angezeigt wird. Wirklich lädt Safari HTML-Seiten etwa doppelt so schnell wie die Konkurrenz. Das Ergebnis überrascht, denn beim Surfen wirkt er deutlich langsamer als beispielsweise Firefox. Grund: Beim Apple-Browser erscheint eine Webseite erst, wenn sie komplett geladen ist. Firefox dagegen zeigt sofort die geladenen Komponenten an und baut die Seite vor Ihren Augen auf.

Erklärungsbedürftig sind auch die Ergebnisse des Acid2-Tests (oben auf dieser Seite): Obwohl der Internet Explorer 7 den Test nicht besteht, zeigt er beim Surfen alle Webseiten richtig an. Opera dagegen, laut Acid2-Test konform mit den W3C-Standards, hat mit der Darstellung vieler Seiten Probleme – vor allem mit Web-2.0-Seiten und mit deren Ajax-Komponenten. Schuld daran ist indirekt der Internet Explorer: Da die meisten Nutzer mit ihm surfen, halten sich die Webentwickler eher an den Internet Explorer als an die W3C-Vorgaben. Weniger verwirrend sind die Messungen des Arbeitsspeicherbedarfs: Bei vielen gleichzeitig geöffneten Tabs arbeitet Opera deutlich schneller als der Internet Explorer.

Andreas Hentschel

BROWSER-TIPPS

Optimieren Sie Ihren Browser!

☑ **Internet Explorer 7: Mehr Sicherheit** Stellen Sie im Menü „Extras“ unter den „Internetoptionen“ die Sicherheitsstufe wenigstens auf „hoch“ – das verbessert die Datensicherheit. Deaktivieren Sie in den „Optionen“ auch auf jeden Fall sämtliche ActiveX-Steuerelemente.

☑ **Firefox: Plugins laden** Den Funktionsumfang von Firefox erweitern Sie mit Plugins, die die Entwickler-Community massenhaft zur Verfügung stellt (Download unter **www.mozilla.org**).

☑ **Opera: Kleine Extras nutzen** Opera kann zwar von Haus aus alles, was ein Browser können muss. Erweiterungen gibt es dennoch – als Widgets, die Sie auf dem Windows-Desktop ablegen können. Die teils nützlichen, teils witzigen Tools können Sie unter **http://widgets.opera.com** herunterladen.

☑ **Safari: Toolbar anpassen** Sie vermissen den „Startseite“-Button in der Toolbar von Safari? Passen Sie die Leiste einfach an – unter „View | Customize Toolbar“.

CHIP TESTSIEGER 01/2008

Übersicht	PLATZ 1	PLATZ 2	PLATZ 3	PLATZ 4
Produkt	Opera 9.5 Beta („Kestrel“)	Firefox 3.0 Alpha 8 („Gran Paradiso“)	Safari 3.0 Beta	Internet Explorer 7.0
Hersteller	Opera Software	Mozilla Foundation	Apple	Microsoft
Internet	www.opera.com	www.mozilla.org	www.apple.de/safari	www.microsoft.de
Gesamtwertung	94	78	63	55
	■■■■■	■■■■□	■■■□□	■■□□□
Sicherheit (45 %)	99	96	70	59
Funktionen (35 %)	100	66	45	53
Performance (20 %)	72	60	77	51
Sicherheit				
Phishing-Filter	●	●	–	●
ActiveX abgeschaltet	●	●	●	Teilweise aktiviert
Bekannte gepatchte/ungepatchte Lücken in der getesteten Version	0/0	0/0	0/0	20/8
Bekannte gepatchte/ungepatchte Lücken bei der Vorgängerversion	**10/0**	16/4	6/3	**121/21**
Werbeblocker/Popup-Blocker	●/●	●/●	–/●	–/●
Cookie-Management	Sehr detailliert für jede Webseite anpassbar	White-List für Cookies bestimmter Webseiten	Generell Cookies annehmen oder nicht	Generell Cookies annehmen oder nicht
Passwortverwaltung/Masterpasswort	●/●	●/●	●/–	●/–
Löschen privater Daten	Zwölf verschiedene Parameter wählbar	History, Cache, Cookies getrennt	„Private Browsing“-Modus speichert nichts	Alle Daten auf Knopfdruck löschbar
Funktionen				
Tabs	●	●	●	●
Tab-Verwaltung	**Sehr umfangreich**	Umfangreich	Rudimentär	Rudimentär
Vorschaufunktion für Tabs	●	–	–	●
Speichern von Sitzungen	Verschiedene Sessions speicherbar	Automatisch beim Beenden (optional)	Nur die letzte Session	–
Mehrere Startseiten einrichten	●	●	–	●
Seitenspezifische Einstellungen	Viele, etwa für Popup- und Werbeblocker	–	–	Keine
Integrierte Suche	Google voreingestellt, manuell anpassbar	Google voreingestellt, manuell anpassbar	Google voreingestellt, einzige Alternative: Yahoo	Google voreingestellt, manuell anpassbar
Favoritenverwaltung	Sehr umfangreich	Umfangreich	Umfangreich	Nur Grundfunktionen
Seitenskalierung	Alles stufenlos	Nur Textgröße	Nur Textgröße und Texteingabefenster	Stufenlos
Druckfunktion	Umfangreich und übersichtlich: an Papiergröße anpassen, Kopf- und Fußzeilen drucken, Seitenhintergrund optional drucken, Seitenränder einstellen	Umfangreich: Bilder und Hintergründe optional drucken, auf Seitengröße skalieren, Skalierung automatisch und stufenlos, inklusive Printvorschau	Passt Seiten automatisch an die Papiergröße an	An Seitenbreite anpassen, stufenlos skalierbar, Hintergrundfarben und Bilder mitdruckbar, allerdings im Einstellungsmenü (erweitert) versteckt
Rechtschreibprüfung bei Texteingabe	●	●	●	–
Anzeige RSS-Feeds	●	●	●	●
Download von Torrents	●	–	–	–
Erweiterung durch Addons	●	●	●	●
Vorlauffunktion (erkennt den Link auf die nächste Seite)	●	–	–	–
Mausgesten	●	– (nur Cursorsteuerung)	–	–
Weitere nützliche Funktionen	Mail- und Chatclient, Navigieren mit Shortcuts, Notizfunktion, Synchronisierung mehrerer Browser via Web	Automatisches Verschicken von Links via Mail, Cache-Größe skalieren	SnapBack-Funktion für schnelleres Navigieren, PDF direkt aus dem Browser anlegen	Autom. Verschicken von Links via Mail, geschützter Modus verhindert unerlaubtes Ausführen von Software (nur bei Vista)
Performance				
Belegter Arbeitsspeicher (in KByte)				
ohne Webseite	17 232 KByte	18 660 KByte	27 624 KByte	15 836 KByte
fünf geladene Webseiten	**20 724 KByte**	32 976 KByte	34 860 KByte	**40 520 KByte**
JavaScript ausführen (in Sek.) 1)	0,74 s	1,41 s	0,84 s	2,88 s
HTML-Seite aufbauen (in Sek.) 1)	**44,28 s**	38,36 s	**19,79 s**	39,17 s
Acid2-Test	Bestanden	Bestanden	Bestanden	**Nicht bestanden**

Spitzenklasse (100–90) | Oberklasse (89–75) | Mittelklasse (74–45) | Nicht empfehlenswert (44–0)

● Ja | – Nein

Wert Bester Wert | Wert Schlechtester Wert

1) Gemessen mit iBench5

Alle Wertungen in Punkten (max. 100)

1 Web-Interface aufrufen

Auf die Einstellungen Ihrer FritzBox greifen Sie am besten über Ihren Webbrowser zu. Geben Sie als Adresse „fritz.box“ ein. Sollte der Aufruf über diesen Alias nicht gelingen, öffnen Sie eine DOS-Box („Start | Ausführen | cmd“) und geben den Befehl „ipconfig /all“ ein. Haben Sie den Adressbereich Ihrer FritzBox nicht verändert, erreichen Sie die Oberfläche auch über die IP-Adresse 192.168.178.1. Schützen Sie die Einstellungen mit einem Passwort („Einstellungen | System | FRITZ!Box-Kennwort“).

2 Firmware-Update einspielen

Bringen Sie Ihre FritzBox nun auf den neuesten Stand. In den System-Einstellungen finden Sie dazu den Punkt „Firmware-Update“. Die FritzBox sucht entweder direkt über die Konfigurationsoberfläche nach einer neuen Firmware, oder Sie können über die Registerkarte „Firmware-Datei“ eine lokal gespeicherte Datei auf die FritzBox laden. Die neueste Firmware-Version finden Sie über das Serviceportal unter der Adresse **www.avm.de/de/Service/Service-Portale/index.php**.

FritzBox absichern

5 MAC-Filter aktivieren

In der Ansicht „Monitor“ sehen Sie, welche PCs an Ihrem WLAN angemeldet sind. Finden Sie einen unbekannten Computer darunter, sollten Sie Ihre Sicherheitseinstellungen überprüfen und gegebenenfalls das Passwort wechseln. Einen weiteren Schutz bietet der MAC-Adressenfilter. Wenn Sie die Option „Keine neuen WLAN-Netzwerkgeräte zulassen“ aktivieren, erlaubt die FritzBox nur noch den bereits angemeldeten PCs, die sich über ihre MAC-Adresse identifizieren, den Zugang in das Funknetz.

6 VoIP & Nachtschaltung

Um die VoIP-Funktion der FritzBox vor Missbrauch zu schützen, gehen Sie im Menü „Telefonie | Internettelefonie“ auf die Registerkarte „Internetrufnummern“. Kontrollieren Sie im Bearbeitungsmodus, ob ein Passwort für die VoIP-Rufnummer existiert. Um Strom zu sparen, können Sie in den Systemeinstellungen die „Nachtschaltung“ aktivieren. Legen Sie dabei per Checkbox auch gleich fest, dass die FritzBox das Funknetz erst abschaltet, nachdem sich der letzte Netzteilnehmer abgemeldet hat.

3 WLAN verschlüsseln

Wenn Sie in den Systemeinstellungen auf „Ansicht | Expertensicht aktivieren“ gehen, bekommen Sie unter „Einstellungen | WLAN“ Zugriff auf Ihr Funknetzwerk. Als Erstes sollten Sie im Untermenü „Sicherheit“ die WPA-Verschlüsselung aktivieren und danach im unteren Teil des Fensters „WPA+WPA2“. Versehen Sie Ihr Netzwerk anschließend mit einem sicheren Schlüssel – am besten einer längeren Kombination aus Zahlen und Buchstaben inklusive Groß- und Kleinschreibung.

4 WLAN konfigurieren

In den „Funkeinstellungen“ ändern Sie zunächst den vordefinierten Namen des Netzwerks und legen auch fest, ob Ihr Netz nach außen sichtbar sein soll oder nicht. Befinden sich in Ihrem Netzwerk mehrere Computer mit WLAN-Adapter, entscheiden Sie, ob diese miteinander kommunizieren dürfen, etwa um Dateien auszutauschen oder um Netzwerkspiele zu starten. Setzen Sie einen AVM-Stick als WLAN-Adapter ein, lässt sich dieser zur Übertragung der Zugangsdaten auf den Computer nutzen.

AVMs FritzBox gehört zu den am weitesten verbreiteten WLAN-Routern. CHIP zeigt Ihnen, wie Sie Ihre FritzBox gegen alle Gefahren von innen und außen absichern.

7 Sicher funken per VPN

Um den Datenaustausch zwischen Web und Ihrem Funknetz über ein Virtual Private Network (VPN) abzusichern, können Sie eine Laborversion (siehe Kasten rechts) nutzen. Dazu spielen Sie via „Firmware-Update“ die „VPN-Firmware“ (**www.avm.de/de/Service/Service-Portale/Service-Portal/VPN_Downloads/7170_Firmware_VPN.php?portal=VPN**) auf Ihren PC. Eine detaillierte Anleitung gibt es unter **www.avm.de/de/Service/Service-Portale/Service-Portal/index.php?portal=VPN**.

TIPP

Mehr Features aus dem Labor

Unter **www.avm.de/de/Service/Service-Portale/Service-Portal/Labor/labor.php** stehen sogenannte Laborversionen der Firmware bereit, die Ihrer FritzBox zusätzliche Features verleihen. Dazu benötigt Ihre FritzBox allerdings eine aktuelle Firmware-Version (Infos unter **www.avm.de/de/Service/Service-Portale/Service-Portal/Labor/labor_download_telefonie/labor_hinweis.php**).

Diese Features stehen bereit:

- Faxempfang und E-Mail-Weiterleitung von Fax- und Sprachnachrichten
- Sicherer Remote-Zugang über eine VPN-Verbindung
- Verbesserte Stabilität für störanfällige Anschlüsse
- Beta-Version der zukünftigen Firmware

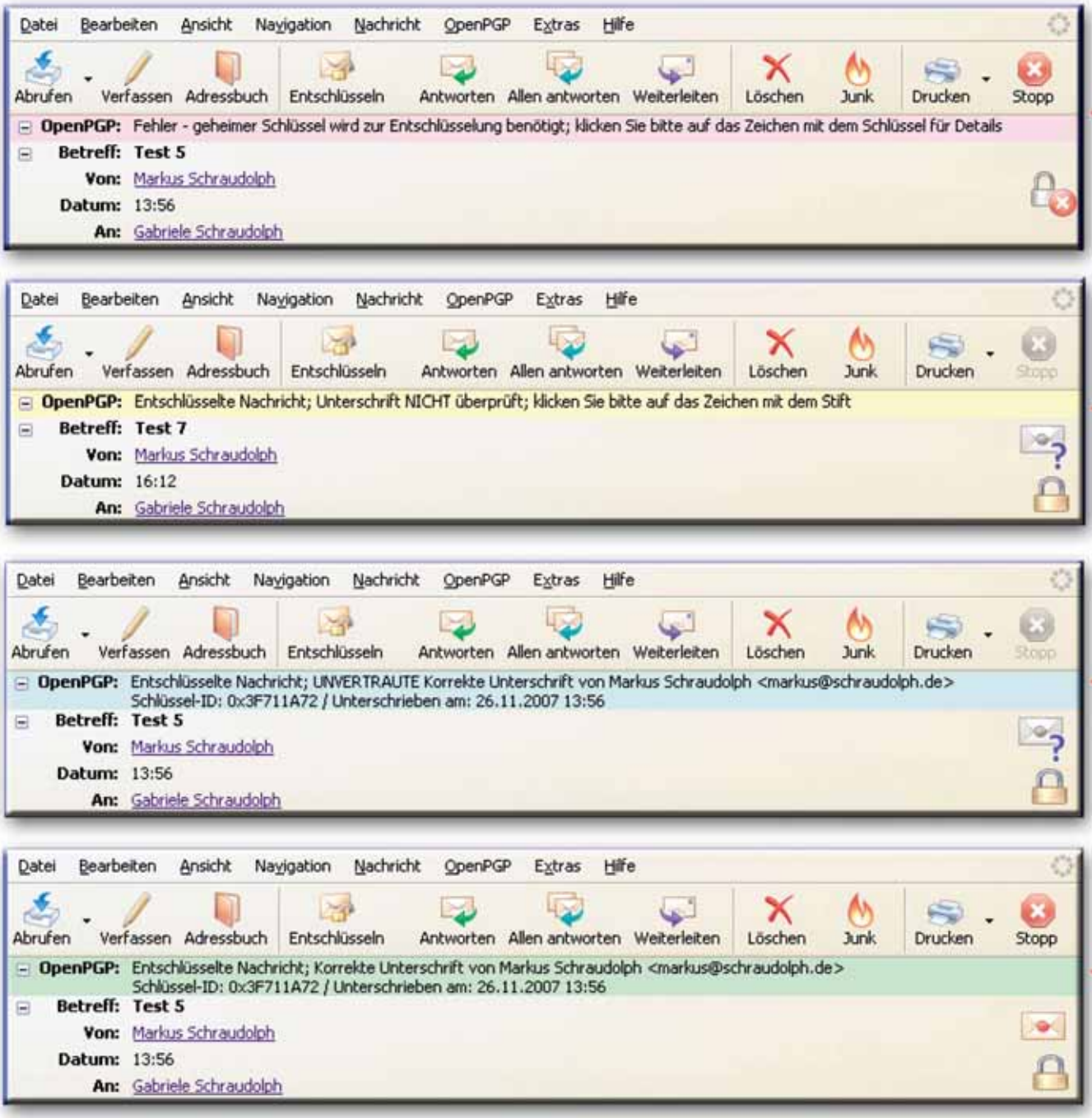
In die Beta-Version (29.04.46-9417) sind bereits zahlreiche Funktionen aus früheren Laborversionen integriert:

- Neue Benutzeroberfläche und zusätzliche Installationsassistenten
- Bis zu fünf Anrufbeantworter
- USB-Netzwerkspeicher
- Musicbox zum Streamen Ihrer Songs über das Netzwerk
- Nutzung von USB-Geräten übers Netzwerk
- WLAN-Autokanal zur Analyse Ihrer WLAN-Umgebung und Bestimmung der optimalen Übertragungsdaten

Vor der Installation sollten Sie Ihre Daten sichern.

E-Mails verschlüsseln mit GnuPGP und Enigmail

Das Briefgeheimnis existiert im Internet nicht: Alle Mitteilungen wandern stattdessen im Klartext durch die Datenkanäle. CHIP zeigt Ihnen, wie Sie sensible Mails perfekt verschlüsseln.



Auf Heft-CD

- Enigmail (Netzwerk)
- GnuPG (Netzwerk)
- Thunderbird (Netzwerk)

Rot heißt: „Unlesbar“ Die Nachricht konnte nicht entschlüsselt werden. Entweder stimmt Ihr Public Key beim Absender nicht, oder Sie haben die falsche Passphrase eingetippt.

Gelb heißt: „Aufpassen“ Die E-Mail wurde erfolgreich entschlüsselt. Allerdings konnte die Unterschrift nicht geprüft werden, weil Sie den Public Key des Absenders nicht besitzen.

Blau heißt: „Alles o.k.“ Die Nachricht ist lesbar und die Authentizität des Absenders bestätigt. Lediglich in der Schlüsselverwaltung ist die Vertrauensstufe des Partners nicht definiert.

Grün heißt: „Besser geht‘s nicht“ Sie schenken dem Absender volles Vertrauen, und seine Signierung der Nachricht hat Enigmail bestätigt.

Was bringt Ihnen eine PGP-Integration im Mailclient Thunderbird? Ein hohes Maß an Sicherheit mit minimalem Aufwand. Denn künftig versenden Sie Nachrichten und Dateien, die nur der gewünschte Empfänger entziffern kann. Dank der Signierung kann der Empfänger sicher sein, dass die Nachricht auch wirklich von Ihnen stammt. Und das Beste: Das Ganze läuft nahezu vollautomatisch.

Geteilte Schlüsselgewalt
Asymmetrie bringt Sicherheit

Einfache Verschlüsselungsverfahren arbeiten symmetrisch – beim Codieren und Decodieren einer Nachricht kommt also derselbe Schlüssel zum Einsatz. Dies macht einen gesicherten Transport des Schlüssels vom Sender zum Empfänger notwendig. Das ist unpraktisch, denn die heute üblichen Schlüssellängen machen eine Übertragung per Telefon unmöglich. Außerdem: Ein Hacker könnte dann auch an alle Schlüssel der Kommunikationspartner kommen – ein riesiges Sicherheitsloch.

Kern der verbreiteten PGP-Technik ist dagegen ein asymmetrisches Verfahren. Dabei gibt es immer zwei Schlüssel: Was der eine verschlüsselt, kann der andere in Klartext zurückverwandeln.

Jeder Schlüssel hat eine spezielle Funktion: Der „Public Key“ dient Ihren Kommunikationspartnern zum Verschlüsseln von Mitteilungen an Sie. Er wird an alle potenziellen Mailempfänger ausgegeben, ja sogar auf Internetservern veröffentlicht.

Anders der sogenannte „Private Key“: Ihn verwenden Sie, um empfangene Nachrichten zu entschlüsseln. Aufgrund der Asymmetrie des Verfahrens nützt der Public Key einem potenziellen Hacker nichts, wenn er an den Klartextinhalt Ihrer E-Mails gelangen will. Das klappt nur mit dem Private Key, den Sie nicht aus der Hand geben. Er liegt auch nicht etwa in Klartextform auf Ihrer Festplatte, sondern wird durch ein Kennwort abgesichert.

Will der Sender gegenüber dem Empfänger seine Identität nachweisen, lässt er die Nachricht „unterschreiben“. Dabei wird ein Fingerabdruck-Code der Nachricht erzeugt und per Private Key verschlüsselt. Beim Eintreffen signierter Nachrichten unternehmen Sie zweierlei: Nach dem Entschlüsseln mit Ihrem Private Key können Sie den ursprünglichen Text der Nachricht lesen. Die zweite Operation besteht in der Rückübersetzung des Fingerabdrucks mit dem Public Key des Absenders und dem Vergleich mit dem Fingerabdruck der erhaltenen Nachricht im Klartext. Stimmen die beiden Codes überein, wissen Sie, dass die Nachricht tatsächlich von diesem Absender stammt.

Automatisiert Transparente Sicherungsmethoden

Mit der richtigen Software macht die Kombination aus Verschlüsselung und digitaler Unterschrift keine Mehrarbeit. Denn die Krypto-Software erkennt die doppelte Sicherung und die Ursprungsnachricht und führt den Authentizitäts-Check durch – sofern sie die notwendigen Keys kennt. Auch beim Versenden verlangt das doppelte Einpacken nicht mehr als zwei Mausklicks.

Nachrichten, die nur digital signiert, aber nicht verschlüsselt sind, bieten Geheimniskrämern kaum Vorteile, denn jeder kann sie lesen. Immerhin weiß man dann aber sicher, dass der Absender echt ist, da ausschließlich er Zugang zum Private Key hat.

Schichtweise So spielen die Komponenten zusammen

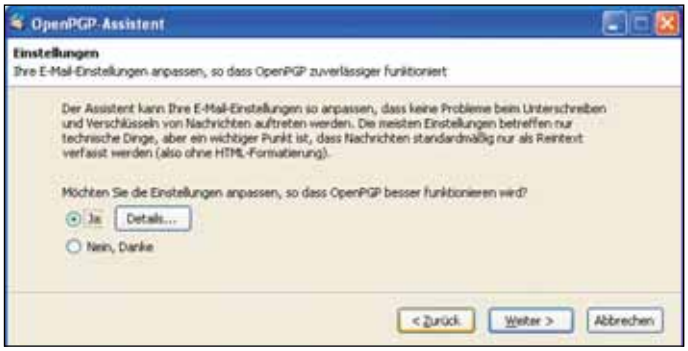
Um den beliebten Mailclient Thunderbird zum Kryptotechniker auszubauen, brauchen Sie lediglich zwei Freeware-Tools. Der Gnu Privacy Guard (GnuPG) liefert die nötigen Verschlüsselungsalgorithmen, tritt jedoch auf der Windows-Oberfläche überhaupt nicht in Erscheinung, denn er besteht nur aus verschiedenen Kommandozeilen-Programmen. Enigmail bietet die komfortable Einbettung der Verschlüsselung in Thunderbird und kümmert sich um die Kommunikation mit dem Kryptokünstler GnuPG.

Leichte Kost GnuPG und Enigmail installieren

Das Setup von GnuPG können Sie mit den Standardoptionen durchlaufen lassen. Es legt zwar Einträge im Windows-Startmenü an, die betreffen aber lediglich die Dokumentation. →

Enigmail ist als Thunderbird-Erweiterung konzipiert. Öffnen Sie also den Dialog „Extras | Add-Ons“. Dort können Sie die Installationsdatei entweder per Drag & Drop hineinziehen oder auf den „Install“-Button klicken und die Datei über „Datei | Öffnen“ suchen.

Nach dem obligatorischen Neustart von Thunderbird erkennen Sie am neuen Menüpunkt „OpenPGP“, dass die Installation geklappt hat.



Enigmail Der Einrichtungsassistent von Enigmail führt Sie beim ersten Start durch die Konfigurationsoptionen – aber nur einmal!

Schritt für Schritt Enigmail einrichten

Gehen Sie nun im Menü „OpenPGP“ auf „Schlüssel verwalten“. Beim ersten Aufruf erscheint der Assistent, der Sie durch die einzelnen Schritte der Konfiguration führt. Er erscheint allerdings nur ein einziges Mal und lässt sich auch nicht über einen besonderen Menüpunkt reaktivieren. Im Kasten unten lesen Sie, wie Sie ihn trotzdem wieder herbeizitieren.

Wählen Sie den Punkt „Alle Nachrichten verschlüsseln“ nur nach reiflicher Überlegung, denn er sperrt alle Empfänger aus, die kein Mailprogramm mit PGP-Technik besitzen. Sie können allerdings später über die „Empfängerregeln“ Ausnahmen für einzelne Empfänger festlegen. Die Option, dass Enigmail alle Thunderbird-Einstellungen anpasst, sollten Sie auf jeden Fall aktiviert lassen, denn sie sorgt für die beste Kompatibilität mit den E-Mail-Programmen Ihrer Kontakte.

Am Ende des Assistenten wird das Schlüsselpaar erzeugt. Ein spezielles Kennwort, die „Passphrase“, schützt dabei den Private Key, den sich andernfalls jeder aneignen könnte, der Zugriff auf Ihren PC hat. Die Passphrase müssen Sie bei jedem Zugriff auf den Private Key eingeben. Damit das nicht zu sehr aufhält, können Sie einen Zeitraum vorgeben, in dem das Kennwort aktiv bleibt und nicht erneut eingetippt werden muss. Die vorgegebene Zeit dafür beträgt fünf Minuten.

Das Kennwort für den Private Key muss mindestens acht Zeichen lang sein und Groß- und Kleinbuchstaben, Sonderzeichen oder Zahlen enthalten.

Nach dem Abschluss aller Einstellungen und der Anlage Ihres Schlüsselpaars bietet Ihnen Enigmail noch die Möglichkeit, ein Widerrufszertifikat zu generieren. Das ist sehr praktisch für den Fall, dass Sie später einmal einen enttarnten Schlüssel aus dem Verkehr ziehen möchten, weil damit seine Löschung beschleunigt wird.

Ernstfall: Die erste codierte Mail abschicken

Lassen Sie sich nun von einem Ihrer Kommunikationspartner seinen öffentlichen Schlüssel schicken. Benutzt er ebenfalls Enigmail, klappt das ganz einfach über die Option „OpenPGP | Meinen öffentlichen Schlüssel anhängen“ beim Verfassen einer Nachricht.

Ist die E-Mail bei Ihnen eingetroffen, können Sie über „Schlüssel des Absenders | Schlüssel importieren“ den Public Key Ihres Partners in die Schlüsselverwaltung aufnehmen.

Ihren eigenen öffentlichen Schlüssel senden Sie auf demselben Weg Ihrem Kontaktpartner zu und bitten ihn, diesen Key ebenfalls zu integrieren.

Schreiben Sie nun Ihrem Bekannten die erste Geheimnachricht. Verfassen Sie dazu eine E-Mail, und aktivieren Sie im Menü „OpenPGP“ die Optionen „Verschlüsseln“ und „Unterschreiben“. Mit den Standardoptionen von Enigmail wird Ihr Partner diese Mail scheinbar unverschlüsselt in seinem Thunderbird entdecken – denn Enigmail führt diese Aktion automatisch aus, wenn es den Public Key des Absenders vorfindet. Lediglich eine Meldung im Header und die Icons für Authentizität und Verschlüsselung weisen darauf hin, dass die Nachricht für den Rest der Welt unlesbar über das Internet gesendet wurde.

Ist die automatische Entschlüsselung ausgeschaltet, bekommt der Empfänger einen entsprechenden Button präsentiert, um die Nachricht in Klartext umzuwandeln.

Eigeninitiative Feste Regeln erleichtern den Alltag

Um von der Grundeinstellung, entweder alles oder nichts zu verschlüsseln, abzuweichen, verwenden Sie die entsprechenden Punkte des „OpenPGP“-Menüs. Statt diese Aktion für bestimmte Empfänger immer von Neuem vorzunehmen, können Sie auch feste Regeln definieren.

PROFI-TIPP

Den Enigmail-Wizard wieder herbeizaubern

Der Einrichtungsassistent von Enigmail ist sehr flüchtig. Einmal weggeklickt, verschwindet er für immer. Sie können zwar sämtliche Einstellungen auch über die normalen Programmoptionen vornehmen, aber gerade beim ersten Kontakt mit Enigmail ist der Komfort des Assistenten schon praktisch. Gut, dass Sie den Wizard notfalls erneut herbeizitieren können.

Rufen Sie dazu in Thunderbird den Menüpunkt „Extras | Einstellungen | Erweitert“ auf. Dort finden Sie in der Registerkarte „Allgemein“ den Button „Konfiguration bearbeiten“, der alle Thunderbird-Parameter listet. Tippen Sie in die Suchbox oben einfach „enigmail“ ein, klicken Sie mit der rechten Maustaste auf die Fundstelle extensions.enigmail.configuredVersion und wählen Sie „Zurücksetzen” aus. Nach dem Neustart von Thunderbird bietet der Assistent wieder seine Dienste an, sobald Sie eine Option wie die „Schlüsselverwaltung“ anwählen.

Der Dialog „Empfängerregeln“ erlaubt Ihnen, für eine bestimmte Empfängeradresse oder für ganze Domänen festzulegen, ob codiert und welcher Schlüssel verwendet werden soll.

Top Secret Fingerabdruck per Telefon abgleichen

Geht es um wirklich hoch sensible Kommunikation, etwa im Geschäftsleben, wo schlimmstenfalls Firmengeheimnisse Konkurrenten in die Hände fallen könnten, ist der einfache Austausch der öffentlichen Schlüssel mit folgendem blinden Hochsetzen der Vertrauensstufe nicht ratsam. Stattdessen sollten Sie den Schlüssel überprüfen. Dazu liefert Enigmail für jeden Schlüssel einen Fingerabdruck. Das ist eine Hexzahl, bestehend aus zehn Blöcken, die eine Checksumme für den Schlüssel darstellt.

Um den Fingerabdruck zu erhalten, gehen Sie zum „Schlüsselmanager“, klicken den gewünschten Schlüssel mit der rechten Maustaste an und wählen die Eigenschaften. Dort erscheint der Fingerabdruck im gleichnamigen Feld.

Rufen Sie danach Ihren Partner an, bitten Sie ihn, in gleicher Weise den Fingerabdruck seines öffentlichen Schlüssels anzeigen zu lassen, und gleichen Sie die Hexcodes ab. Erst danach setzen Sie den Vertrauenslevel des Schlüssels über den Kontextmenüeintrag „Besitzer-Vertrauen festlegen ...“ hoch.

Fracht an Bord: Umgang mit Dateianhängen

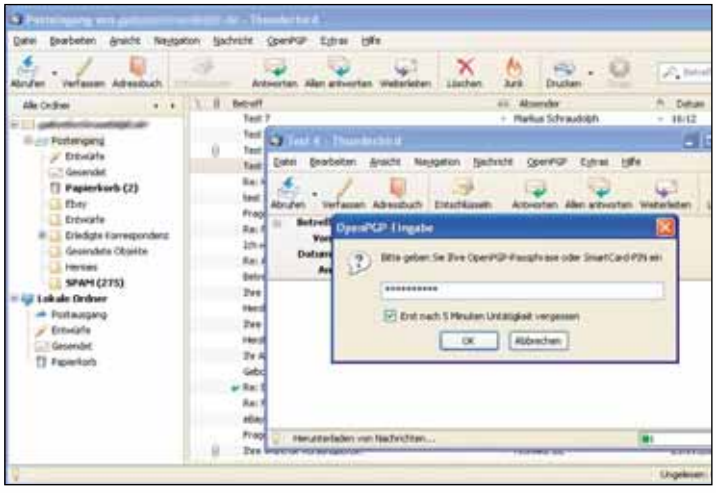
Beim Verschicken von Attachments haben Sie die Qual der Wahl, vor die Sie Enigmail beim Klick auf „Senden“ stellt. Die erste Option nimmt die Anhänge vom Verschlüsseln aus. Soll die Vertraulichkeit aber für alle Elemente der Nachricht gelten, können Sie aus zwei Optionen wählen. Die Variante „Jeden Anhang einzeln verschlüsseln …“ ist richtig, wenn Sie nicht genau wissen, mit welchem Client der Empfänger arbeitet, denn sie klappt mit jedem. Der Nachteil für den Empfänger: Mit den meisten Clients muss er jede angehängte Datei einzeln entschlüsseln. In Enigmail funktioniert das etwa über das Kontextmenü des Anhangs und die Wahl der Option „Entschlüsseln und Speichern unter…“.

Die letzte Variante „Nachricht als Ganzes verschlüsseln“ ist elegant, weil das Entschlüsseln automatisch funktioniert. Das geht auf Empfängerseite aber nur mit Pegasus, Mulberry, Seamonkey oder eben Thunderbird. Microsoft-Programme wie Outlook können die verschüsselten Anhänge nicht öffnen.

Bei Problemen GnuPGs Fehlermeldungen lesen

Weil unter der Oberfläche von Enigmail das Arbeitstier GnuPG werkelt, dringt nicht jede Warnung der Krypto-Engine bis zu Ihnen durch. Tritt ein Problem auf, etwa eine nicht entschlüsselbare Nachricht oder eine zu allgemein gehaltene Fehlermeldung, lohnt es sich, die Ausgaben von GnuPG zu betrachten.

Dazu gehen Sie im „OpenPGP“-Menü auf den Punkt „Fehlersuche | Konsole anzeigen“. Die darin enthaltenen Aufrufe der Kommandozeilen-Tools sind dabei nicht so wichtig, eher die jeweiligen Ausgaben. An dieser Stelle finden Sie etwa den Hinweis, warum eine Nachricht nicht entziffert werden konnte – weil der Schlüssel nicht passte oder weil Sie die Passphrase falsch eingetippt haben. Bei sporadischen Problemen legen Sie sich besser ein Fehlerlog an. Dazu dient der Punkt „Fehlersuche“ in den erweiterten Einstellungen des Programms.



Passphrase Ihren privaten Schlüssel schützen Sie durch ein Kennwort, damit nicht jeder Nutzer Ihres PCs Ihre geheimen Mails lesen kann.

Konkurrenzprodukt S/MIME ist nicht kompatibel zu PGP

Mit S/MIME existiert ein Standard, der wie PGP die Vertraulichkeit im Mailverkehr herstellen will. Beide Verfahren sind aber nicht kompatibel. Der Hauptunterschied besteht darin, wie die Standards mit Schlüsseln umgehen. Während bei PGP der persönliche Austausch der Public Keys vorgesehen ist, gibt es bei S/MIME Zertifizierungsserver, die einen Schlüssel, „Zertifikat“ genannt, ausgeben. Auf diese Server kann ein Mailprogramm zurückgreifen, um sich einen Schlüssel für eine empfangene Nachricht abzuholen.

Markus Schraudolph

PROFI-TIPP

Schlüssel-Backup erspart Ärger

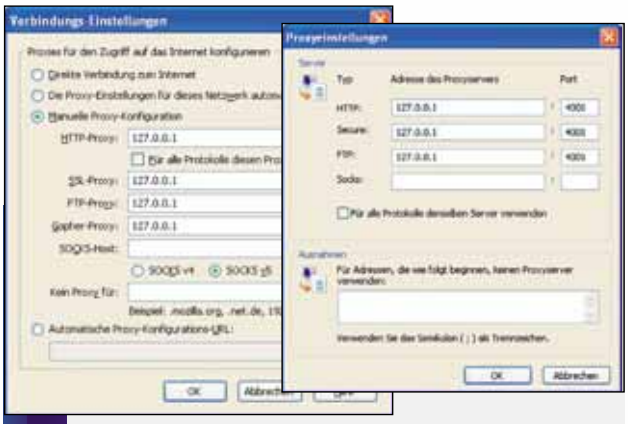
Das persönliche Schlüsselpaar aus Private und Public Key sind extrem wichtige Daten, die bei einer Neuinstallation von Windows häufig vergessen werden. Während Sie sich den Public Key jederzeit von Ihren Kommunikationspartnern holen können, ist der Private Key dann unwiderruflich verloren. Darum sollten Sie diese Schlüssel sichern; dafür reicht schon eine Diskette.

Markieren Sie dazu in der „Schlüsselverwaltung“ von GnuPG Ihren eigenen Eintrag, rufen Sie „Datei | Exportieren“ auf und legen Sie fest, dass auch der Private Key mitgesichert werden soll. Den Datenträger bewahren Sie an einem sicheren Ort auf.

Bei der Neuinstallation von Enigmail können Sie das Generieren eines Schlüsselpaars überspringen. Holen Sie sich Ihre gespeicherten Keys stattdessen über die Importoption in Enigmail zurück. Stammt die Sicherung von einem anderen PGP-Programm, tragen die Schlüssel nicht die Endung *.gpg“. Ändern Sie dann im „Datei“-Dialog den Typ auf „Alle Dateien“, um sie laden zu können.

1 JAP installieren

Für die Installation von JAP benötigen Sie neben dem Programm auch eine Laufzeitumgebung von Java ab Version 1.4. Das komplette Installationspaket bekommen Sie etwa von der Website der Universität Dresden (**http://anon.inf.tu-dresden.de/win/download.html**). Nach der Installation der Java-Laufzeitumgebung starten Sie den Client aus dem Startmenü und folgen den Anweisungen des Assistenten.



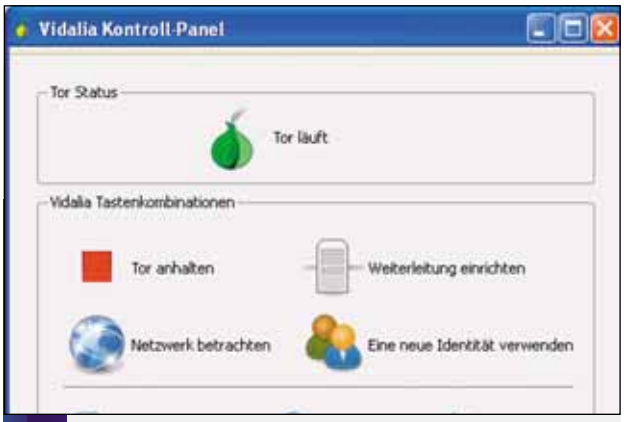
2 Internet Explorer einstellen

JAP beschränkt sich auf die Protokolle HTTP, HTTPS, FTP und Gopher. Alle anderen Anwendungen, etwa Instant Messaging oder E-Mail, lassen sich über JAP nicht verschleiern. Das Tool agiert als lokaler Proxyserver, den Sie im Browser einstellen müssen. Die Proxyserver-Adresse lautet 127.0.0.1, der entsprechende Port 4001. Öffnen Sie im Internet Explorer „Extras | Internetoptionen | Verbindungen | Einstellungen“, kreuzen Sie die Checkbox für den Proxyserver an, und geben Sie Proxyadresse und Port ein.

Surfen mit Tarnkappe

5 Wie Tor funktioniert

Beim ersten Anmelden lädt der Tor-Client eine Liste von Tor-Servern herunter. Nach dem Empfang der Daten wählt der Tor-Client eine Route aus der Tor-Serverliste. Mit dem Startserver verhandelt er die Verschlüsselung, baut eine Verbindung auf und erweitert sie um einen zusätzlichen Proxyserver auf insgesamt drei Server. Jeder Server kennt auf der Übertragungsstrecke nur seinen Vorgänger und seinen Nachfolger. Der letzte Server agiert als Exit-Knoten und stellt die Verbindung zur Zielseite her.



6 Tor installieren

Mit dem Setup installiert Tor den Tor-Client, den Privoxy-Server und die Benutzeroberfläche Vidalia. Nach der Installation nehmen Sie noch die Einstellungen in den Anwendungen vor, die über den Tor-Proxy geleitet werden sollen. Dazu gehen Sie wie bei der JAP-Installation vor und geben im Browser als Proxyserver die Adresse 127.0.0.1 und den Port 8118 ein. Die gleichen Angaben nutzen Sie auch für andere Anwendungen, beispielsweise für Ihr Messenger-Programm.

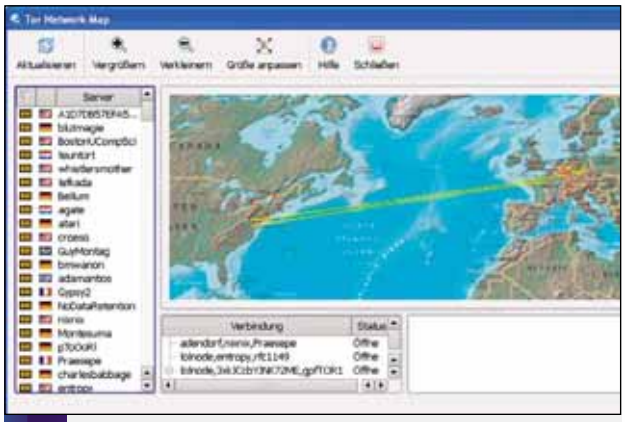
3 Firefox konfigurieren

In Firefox gehen Sie auf „Extras | Einstellungen | Erweitert | Netzwerk | Einstellungen“. Aktivieren Sie im nächsten Fenster die manuelle Proxykonfiguration, und geben Sie für alle Protokolle außer SOCKS die bekannte Proxyserver-Adresse ein. Bei beiden Browsern sollten Sie darauf achten, dass der Eintrag „localhost“ nicht als Ausnahme definiert ist. Die Firefox-Erweiterung „JAP2FF“ (**http://web.inf.tu-dresden.de/~tu462421/jap2ff/**) bietet einen Schalter zum Ein- und Ausschalten der Verschlüsselung.

4 Kostenpflichtige Anonymität

Die kostenpflichtige Version von JAP – JonDonym (**www.jondos.de/**) – garantiert, dass Ihre Anfragen über eine ganze Kette von Proxys geleitet und dabei für jeden Proxy einzeln verschlüsselt werden. Abgerechnet wird volumenbasiert und nach dem Prepaid-Modell, sodass auch an dieser Stelle keine direkte Spur zum User führen kann. Details zu den unterschiedlichen Zahlungsverfahren finden Sie unter der Adresse **www.jondos.de/de/payment**.

Tricksen Sie die staatlichen Datensammler aus! Mit den beiden Tools JAP und Tor hinterlassen Sie im Internet keine Spuren mehr – denn Ihre Anfragen laufen über anonyme Server.



7 Zusatzfunktionen nutzen

Anders als bei JAP bietet die Tor-Oberfläche einige interessante Zusatzfunktionen und erweiterte Einstellmöglichkeiten. Im Kontrollpanel sehen Sie als Erstes den Status der Anwendung – die grüne Zwiebel zeigt an, dass die Anonymisierung aktiv ist. Über Tastenkombinationen lässt sich Tor anhalten und wieder starten sowie eine Weiterleitung einrichten – damit bieten Sie über Ihren PC einen eigenen Tor-Server an. „Eine neue Identität verwenden“ ändert die Route, über die Ihre Verbindung ins Web läuft.

8 Anonymität testen

Nachdem Sie Tor oder JAP auf Ihrem PC installiert haben, sollten Sie überprüfen, ob die Anonymisierung funktioniert. Dazu können Sie etwa den Tordetektor (**http://check.torproject.org/**) einsetzen. Es gibt aber auch Webseiten, welche die an sie übermittelte IP-Adresse anzeigen, beispielsweise:

- RRDB: **www.rrdb.org/check_yourself.php?l=de**
- Gurusheaven: **www.gurusheaven.de/index_sicherheit.html**
- Leader: **www.leader.ru/secure/who.html**

Risiko Tauschbörse: Was Ihre IP-Adresse verrät

Millionen von Menschen surfen täglich im Internet, und viele glauben, sie seien dabei anonym. Fataler Irrtum: Per IP-Adresse ist jeder User identifizierbar – auch Raubkopierer und Spammer.

Glaubt man der Musikindustrie, entsteht durch Raubkopierer allein in Deutschland jährlich ein Schaden im dreistelligen Millionenbereich. Kein Wunder, dass Musiktauschbörsen verstärkt ins Visier der Ermittlungen geraten.

Wichtigstes Beweisstück der Strafverfolgung ist die IP-Adresse. Denn wie eine Telefonnummer lässt sich die Adresse einem Anschluss und damit auch einem Nutzer zuordnen. Doch nicht nur Strafverfolger interessieren sich für die IP, auch Hacker und neugierige Webmaster. CHIP zeigt Ihnen, wie eine IP-Adresse aufgebaut ist, was die IP über Sie verrät und wie Tauschbörsennutzer und Spammer enttarnt werden.

Auf Heft-CD

- Azureus (Vuze) (Netzwerk)
- NMap Portscanner (Netzwerk)
- Wireshark (Netzwerk)

IP-Adressen Aussehen und Verteilung im Internet

IP-Adressen gehören zum Alltag im Internet. Doch für viele ist die IP nicht mehr als ein abstrakter Begriff.

Dabei ist sie allgegenwärtig. Denn hinter jeder Verbindung steckt auch eine IP-Adresse – etwa wenn Sie eine Webseite aufrufen. In dem kurzen Moment zwischen dem Drücken der Return-Taste und dem Aufruf der Webseite beginnt die Kommunikation auf IP-Basis: Der Rechner schickt den Seitennamen an einen DNS-Server, und der antwortet mit einer IP-Adresse. Diese Adresse verrät dem Browser, auf welchem Webserver die Seite zu finden ist.

Doch damit nicht genug: Damit der Inhalt der Webseite überhaupt im Browser erscheinen kann, werden die Daten ebenfalls an eine IP-Adresse geschickt –

Foto: N. Schäffler

die des Rechners. Jedes Gerät im Internet besitzt also eine IP-Adresse, die sich aber auch ändern kann.

Provider unterscheiden üblicherweise zwischen zwei Typen: Da wären zum einen die festen IP-Adressen. „Fest“ bedeutet, dass die Adresse über einen längeren Zeitraum gleich bleibt. Solche Adressen werden in der Regel an Server und Router vergeben. Ein typisches Beispiel für einen Router mit fester IP-Adresse ist ein Firmennetzwerk. Jeder Mitarbeiter, der ins Internet geht, tut dies über den Router, der mit dem Provider verbunden ist. Folge: Jeder Mitarbeiter hinterlässt auf jeder Webseite dieselbe IP-Adresse.

Ganz anders verhält es sich beim zweiten Adresstyp, der dynamischen IP-Adresse. Da die Zahl der verfügbaren IP-Adressen begrenzt ist, bekommt jeder Provider einen Pool mit Adressen, mit dem er auskommen muss. In vielen Fällen reicht dieser Pool nicht aus, um jedem Kunden eine eigene IP-Adresse zu geben. Zwar besteht eine IP aus viermal drei Ziffern – das sind rein rechnerisch 4,3 Milliarden Adressen –, doch zahlreiche Regeln und Ausnahmen schränken den nutzbaren Zahlenraum ein. So verbleiben am Ende nur einige Millionen Adressen, die sich sämtliche Internetprovider weltweit teilen müssen.

Die Folge: Die IP ist einem Anschluss nur zugeordnet, solange der die Verbindung mit dem Provider aufrechterhält. Anschließend wird sie wieder freigegeben, und der nächste Kunde bekommt diese IP-Adresse. Trotzdem lässt sich eine IP-Adresse eindeutig einem bestimmten Anschluss zuordnen. Denn in Deutschland ist aufgrund des Vorratsdatenspeicherungsgesetzes jeder Provider verpflichtet, Protokoll zu führen. Gespeichert werden die Uhrzeit und die Kundennummer des Nutzers – sechs Monate lang. Für die Musikindustrie ist das ein wahres Geschenk: So lassen sich Tauschbörsennutzer auch noch Wochen später identifizieren.

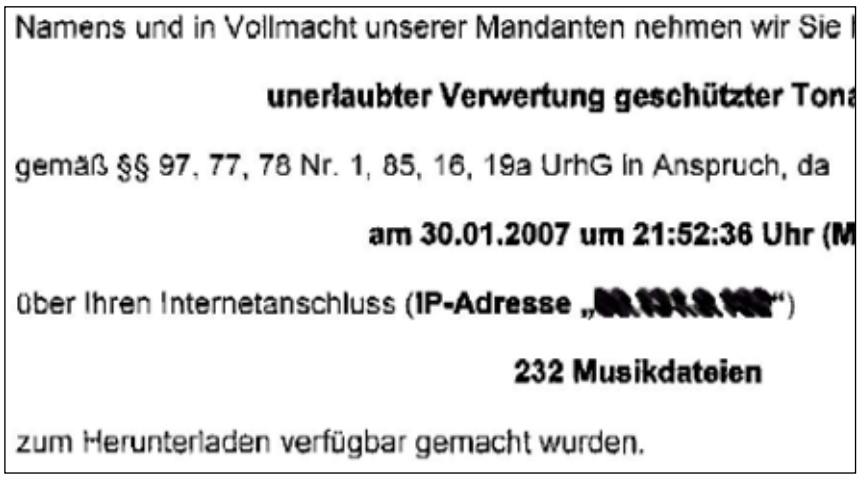
P2P Was BearShare und BitTorrent über Sie verraten

Noch gilt der Download von Raubkopien von einer Webseite als rechtliche Grauzone. Denn wer nicht selber Raubkopien verteilt, kann für den Vertrieb nicht belangt werden. In solchen Fällen konzentrieren sich die Rechteinhaber deshalb auf den Betreiber der Download-Webseite.

Ganz anders verhält es sich beim Filesharing. Denn an dieser Stelle ist jeder Teilnehmer der sogenannten Peer-to-Peer-Netzwerke (P2P) Empfänger und Sender zugleich. Für die Musik- und Filmindustrie ist das ein echtes Problem. Denn wenn ein illegales Angebot aus dem Netz verschwinden soll, reicht es nicht mehr, nur einen Server abzuschalten. Vielmehr muss jeder Teilnehmer, der eine Raubkopie besitzt, seinen Rechner vom Netz nehmen, damit das Angebot verschwindet.

Aus diesem Grund beauftragt die Industrie Firmen, die sich darauf spezialisiert haben, Filesharing-Nutzer ausfindig zu machen. Und im Prinzip ist das eine sehr leichte Aufgabe.

Denn um an die IP-Adressen der Nutzer zu kommen, müssen sich die Ermittler nur in die zumeist offenen Netzwerke einklinken und die Adressen auslesen. Besonders einfach ist das bei Programmen wie Emule, BearShare und Limewire, die das Gnutella-Protokoll verwenden. Denn im Gegensatz zu anderen P2P-Protokollen wie BitTorrent lassen sich bei Gnutella Suchanfragen in das Filesharing-Netz schicken. Der Ermittler braucht nur den Namen eines urheberrechtlich geschützten Songs einzugeben und erhält eine Liste aller IP-Adressen, die diesen Song illegalerweise anbieten. Zudem kann er eine IP-Adresse eingeben und erfährt, welche Dateien dort zum Download angeboten werden. →


Namens und in Vollmacht unserer Mandanten nehmen wir Sie I

unerlaubter Verwertung geschützter Tona

gemäß §§ 97, 77, 78 Nr. 1, 85, 16, 19a UrhG in Anspruch, da

am 30.01.2007 um 21:52:36 Uhr (M

über Ihren Internetanschluss (**IP-Adresse „[redacted]“**)

232 Musikdateien

zum Herunterladen verfügbar gemacht wurden.

Erwischt Zuerst lässt die Musikindustrie den Täter ausfindig machen, danach bekommt der Tauschbörsenteilnehmer eine Anzeige zugestellt – wie in diesem Fall.

PROFI-TIPP

Ein- und ausgehende IP-Adressen checken

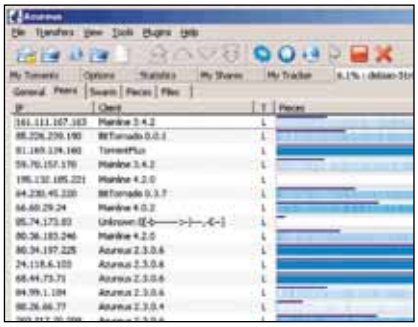
Sowohl unter Linux als auch unter Windows lässt sich mit relativ einfachen Mitteln herausfinden, mit welchen IP-Adressen Ihr PC gerade kommuniziert.

Netstat Das am schnellsten verfügbare Tool ist die On-Board-Software „netstat“. Öffnen Sie die Kommandozeile, und geben Sie den Befehl „netstat -na“ ein. Mit dem Parameter „-n“ verhindern Sie, dass das Tool versucht, aus jeder IP-Adresse einen DNS-Namen zu machen – und der Aufruf deshalb quälend langsam wird. Der Parameter „-a“ sagt dem Tool, dass Sie sämtliche Verbindungen sehen möchten. Andernfalls zeigt das Tool lediglich die Verbindungen Ihres Benutzerkontos an und nicht auch die vom System gestarteten.

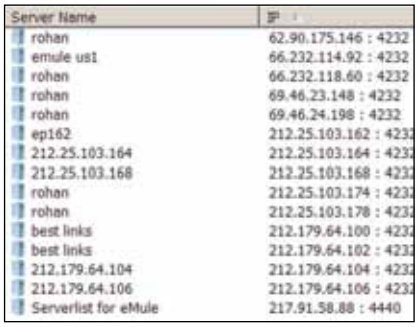
TCPView Wesentlich komfortabler als „netstat“ ist dieses Tool von Sysinternals. Dank einer grafischen Oberfläche sowie einiger guter Features finden Sie mit TCPView im Handumdrehen nicht nur heraus, mit welchen IP-Adressen Ihr Rechner gerade in Verbindung steht, sondern auch, welche Anwendung diese Verbindung geöffnet hat. So lassen sich sogar Trojaner enttarnen, die im Augenblick mit dem Hacker kommunizieren.

Mit den gesammelten Informationen und der genauen Uhrzeit ist es dann kein Problem mehr, den Nutzer der Tauschbörse ausfindig zu machen. Gibt man die IP-Adresse etwa auf einer Seite wie **www.dnsstuff.com** ein und führt einen sogenannten WHOIS-Lookup durch, erfährt man im Handumdrehen, zu welchem Providerpool die IP-Adresse gehört – inklusive Ansprechpartner, Telefonnummer und E-Mail-Adresse. Der Provider wiederum kann aufgrund der Vorratsdatenspeicherung die IP-Adresse anhand der Uhrzeit problemlos einem Kunden zuordnen.

Das funktioniert zwar nicht nur bei Gnutella, doch BitTorrent etwa erschwert die Ermittlungen ungemein. Grund: BitTorrent ist zwar auch ein offenes Filesharing-Protokoll, es lässt sich aber nicht durchsuchen. Ein Beispiel: Um ein Musikalbum per BitTorrent herunterzuladen, ist zunächst eine Torrent-Datei erforderlich. Die finden die Tauschbörsennutzer in der Regel auf einer offenen Webseite wie ThePirateBay. Wird die Torrent-Datei nur einem kleinen, exklusiven Kreis zugänglich gemacht, so endet an dieser Stelle das Glück der Ermittler. Doch selbst wenn die Torrent-Datei zugänglich ist, hilft das nicht viel. Denn sie enthält nur die Dateinamen aus dem Musikalbum und die IP-Adresse eines sogenannten Trackers. Der Tracker ist zwar zentraler Bestandteil von BitTorrent, er bietet aber selbst keine Downloads an. Vielmehr führt der Tracker nur eine große Liste aller IP-Adressen der aktiven Teilnehmer. Die Teilnehmer selbst teilt der Tracker in kleine Gruppen auf. Das soll verhindern, dass alle Teilnehmer miteinander kommunizieren müssen und dadurch ein unnötiger Verwaltungsaufwand entsteht. Wer sich also an einem Torrent beteiligt, bekommt eigentlich niemals sämtliche IPs zu Gesicht – es sei denn, es handelt sich nur um wenige Teilnehmer.



BitTorrent Der Azureus-Client gibt bereitwillig Auskunft darüber, welche IP-Adressen die Tauschpartner haben.



Tauschserver Auch die Teilnehmer des Emule-Netzwerks müssen fürchten, über ihre IP-Adresse identifiziert zu werden.

Oberstes Ziel der Musikindustrie ist es deshalb, die Tracker und Torrent-Webserver aus dem Internet zu nehmen. Das gestaltet sich aber zumeist recht schwierig, da manche Länder die Tracker nicht gesetzlich verbieten können. Da auch BitTorrent nicht anonym ist, müssen die Teilnehmer jedoch damit rechnen, entdeckt und verfolgt zu werden.

Spam So finden Sie den Absender einer E-Mail

IP-Adressen sind nicht nur ein Mittel, um Raubkopierern auf die Spur zu kommen, sondern sie können auch dabei helfen, den Absender einer E-Mail zu ermitteln. Das ist besonders für die Jagd nach einem Spammer interessant. Hilfreich ist dabei die Tatsache, dass jede E-Mail Informationen darüber enthält, welche Stationen sie durchlaufen hat und unter welcher IP-Adresse sie ihren Ursprung hat. Doch Vorsicht: Wie wir im Folgenden zeigen, lassen sich sehr viele Einträge fälschen – und so kann es recht schwierig werden, den wahren Urheber zu identifizieren.

Dreh- und Angelpunkt bei der Jagd nach einem Spammer sind die sogenannten Internet-Kopfzeilen (E-Mail-Header). Um an die heranzukommen, klicken Benutzer von Outlook mit der rechten Maustaste auf die E-Mail und anschließend auf „Nachrichtenoptionen“. Die Vorgehensweise bei anderen E-Mail-Clients können Sie unter der Adresse **http://th-h.de/faq/headerfaq.php#mailreader** finden.

Der E-Mail-Header besteht zwar lediglich aus Text, er enthält allerdings erschreckend viele Einträge – von denen die meisten für die Spammer-Jagd nur sehr am Rande interessant sind. So gibt jedes E-Mail-Programm zunächst einmal seine Identität preis. Diese Information finden Sie im E-Mail-Header unter dem Eintrag „User-Agent“ einsehbar. Die Einträge „Mime-Version“, „Content-Type“ und „Content-Transfer-Encoding“ können Sie ebenfalls ignorieren. Sie geben lediglich Auskunft über die Codierung des E-Mail-Texts.

Der erste scheinbar wichtige Eintrag einer Spammail lautet „Return-Path“. Doch auch diesen Eintrag können Sie getrost ignorieren. In der Regel fälscht nämlich ein Spammer auch diese vermeintliche Absenderadresse. Würden Sie im E-Mail-Programm auf „Antwor-

Info-Service Was die IP-Adresse oder auch der Domainname alles verrät, bekommt man eindrucksvoll unter **www.dnsstuff.com** gezeigt.

ten“ klicken, wäre das der Empfänger Ihrer Antwortmail. Besonders offensichtlich wird diese Fälschung, wenn unter „Return-Path“ Ihre eigene Adresse erscheint. Vergleichen Sie den „Return-Path“ mit der „Message-Id“. Diese ID ähnelt einer Trackingnummer der Post und setzt sich laut einer Regel aus einer einmaligen Zeichenkette und dem Absende-Server zusammen. Die „Message-Id“ könnte also etwa „SAHDRQ@hotmail.com“ lauten. Ist die vermeintliche Absende-Adresse jedoch eine Nachricht von „@yahoo.com“, wird an dieser Stelle ebenfalls der Betrugsversuch klar.

Die ersten vernünftigen Informationen bekommen Sie von den „Received“-Einträgen. An dieser Stelle können Sie nachlesen, welche Stationen die Mail durchlaufen hat. Ähnlich wie bei einem Blog ist der unterste Eintrag der älteste. Lesen sollten Sie die Einträge trotzdem von oben nach unten, da Ihr E-Mail-Server (also der oberste Eintrag) auf jeden Fall vertrauenswürdig ist. Jeder Eintrag entspricht dem Muster „Received: from X by Y with Z“. Die Absende-IP-Adresse lautet also X und wurde von Y in Empfang genommen. Zur Übertragung wurde das E-Mail-Protokoll Z verwendet. Da jeder E-Mail-Server seinen eigenen Stil hat, sind zwar alle Einträge nach demselben Muster aufgebaut, sehen aber ansonsten vollkommen unterschiedlich aus. Lassen Sie sich davon bei Ihrer Recherche nicht abschrecken.

Das erste „by“ im ersten Eintrag verrät Ihnen die Adresse Ihres E-Mail-Servers, der erste „from“-Eintrag den letzten Sender. Bei dem zweiten „Received“ sollte der letzte Sender (from) dem zweiten „by“-Eintrag entsprechen. Doch bereits an dieser Stelle kann es abweichende Angaben geben. Die harmlose Ursache dafür wäre, dass der Server mehrere Adressen besitzt. Sollten sich die beiden Adressen allerdings nicht auf denselben Server zurückführen lassen, so ist der Punkt erreicht, an dem Sie sich an den Betreiber des nächsten Knotens wenden müssen. Er muss nun über seine Serverprotokolle herausfinden, von welcher IP-Adresse die Spam-E-Mail verschickt worden ist.

Sollten Sie eine IP-Adresse als Absender identifizieren können, ermitteln Sie am besten über eine Webseite wie **www.dnsstuff.com** mit einer WHOIS-Abfrage, zu welchem Provider diese IP-Adresse gehört. Dort finden Sie auch eine E-Mail-Adresse, an die Sie sich wenden können. Schildern Sie Ihr Problem, und fügen Sie auch die Internetkopfzeilen in die E-Mail ein. Mit etwas Glück kann der Provider dann den Verantwortlichen ausfindig machen und das Problem lösen. Erwarten Sie allerdings nicht zu viel. Denn mittlerweile sind viele Versender von Spammails selber ein Opfer – nämlich das eines Botnetzwerks.

Bots sind Rechner, die von einem Hacker kontrolliert und beispielsweise als E-Mail-Server missbraucht werden. Je mehr Bot-PCs ein Hacker unter seiner Kontrolle hat, umso mehr Spam kann er in kürzester Zeit versenden.

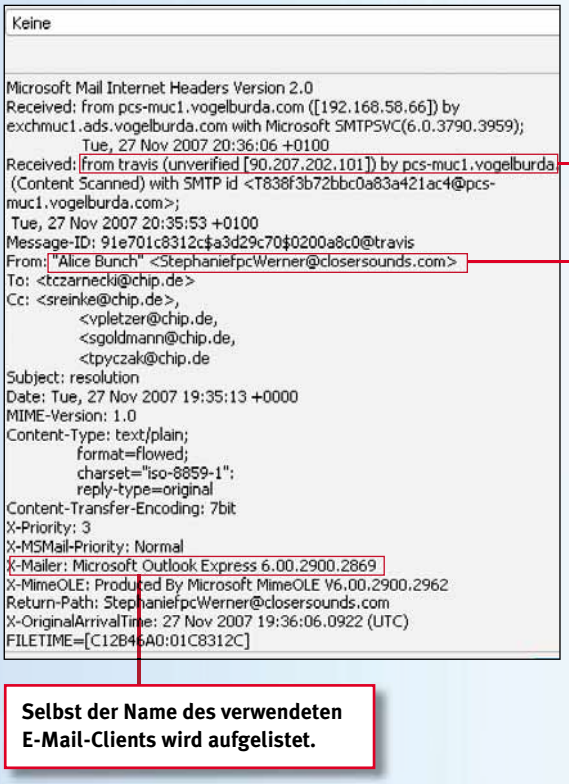
Da die Rechner eines Botnetzwerks zumeist kein Protokoll darüber führen, wann mit welcher IP-Adresse eine Verbindung aufgebaut wurde, endet dort die Spur, und der wahre Täter bleibt anonym. Einzige verbleibende Chance: Beobachtet man mit Tools wie Wireshark die ein- und ausgehenden Verbindungen der Botkommunikation, findet man vielleicht die IP-Adresse der Steuerzentrale des Botnetzwerks und kann den Spammern das Handwerk legen.

Valentin Pletzer

KNOW-HOW

Spurensicherung in der Spammail

Jeder Spammer hinterlässt Spuren, die Sie auslesen können. Der Header, der in jeder Nachricht zu finden ist, dokumentiert den Weg der E-Mail vom Absender bis zum Empfänger. Welche Server wurden verwendet? In welcher Zeitzone stehen sie? Welche Software wurde verwendet? All das hilft, den Übeltäter zu identifizieren.



WEB-LINKS

Der Blick über den Tellerrand lohnt. Die Microsoft-Suchmaschine identifiziert über den Befehl „IP:“ sämtliche Domains, die auf dem Server der angehängten IP-Adresse zu finden sind.
www.live.com

Über Meldebehörden lässt sich der verantwortliche IP-Provider identifizieren.
www.ripe.net, www.iana.net, www.apnic.net, www.lacnic.net

Sicher surfen am Hotspot

Wer Hotspots als Internetzugang nutzt, sollte zuvor einige Sicherheitsmaßnahmen treffen. CHIP zeigt Ihnen, was Sie beim Surfen im öffentlichen Raum beachten sollten.

Fast in jeder Stadt, in Cafés, der Universität oder in anderen öffentlichen Einrichtungen gibt es heute WLAN-Hotspots, mit deren Hilfe Sie sich ins Internet einwählen können. Grundsätzlich stellen diese Hotspots allerdings ein erhebliches Sicherheitsproblem dar. CHIP zeigt Ihnen, in diesem Beitrag, welche Maßnahmen Sie unbedingt treffen sollten, damit Sie auch unterwegs entspannt surfen können.

Auf den richtigen Hotspot achten Bei der Verbindung mit einem WLAN sollten Sie genau aufpassen, dass Sie auch den richtigen Hotspot auswählen.

Maßnahme 1 Beim Provider nachfragen

Es klingt unspektakulär, doch einfaches Nachfragen beim Provider ist oftmals der schnellste und einfachste Weg, um festzustellen, wie sicher ein öffentlicher Hotspot tatsächlich ist. Im Idealfall sollte als Verschlüsselung zumindest WPA2 oder Ipsec zum Einsatz kommen.

Zudem sollte der Hotspot unter keinen Umständen mit einem LAN verbunden sein, da dies ein zusätzliches Sicherheitsrisiko darstellt. Wenn überhaupt, sollte eine solche Anbindung nur über einen gesicherten Gateway existieren.

Wichtig ist auch, dass Inter-Client-Connections auf keinen Fall möglich sind. Authentifizierungen sollten ausschließlich verschlüsselt erfolgen. Wenn ein Provider dazu die Auskunft verweigert, sollten Sie von diesem Hotspot besser die Finger lassen.

Maßnahme 2 Benutzerkonto mit eingeschränkten Rechten

Moderne Betriebssysteme erlauben es, den Nutzern eines Rechners unterschiedliche Rechte zuzuweisen. Wenn Sie sich an einem öffentlichen WLAN-Hotspot anmelden möchten, sollten Sie sich auf keinen Fall als Administrator in Ihrem System eingeloggt haben.

Im Idealfall verwenden Sie ein Benutzerkonto mit stark eingeschränkten Rechten. Der potenzielle Schaden bei unerlaubten Zugriffen auf Ihr System fällt auf diese Weise deutlich geringer aus. Grundsätzlich gilt dieser Grundsatz auf allen Betriebssystemen – ob Sie auf Ihrem Notebook nun Windows oder Linux installiert haben.

Maßnahme 3 Freigaben deaktivieren

Die Datei- und Verzeichnisfreigabe Ihres Notebooks unter Windows sollten Sie bei der Nutzung eines WLAN-Hotspots am besten komplett deaktivieren, damit kein Unbefugter auf die Daten Ihrer Festplatte oder anderer Laufwerke wie USB-Sticks zugreifen kann.

Sollten Sie dennoch mal eine einzelne Freigabe benötigen, achten Sie darauf, dass Sie auch wirklich nur ein einzelnes Verzeichnis und nicht ein ganzes Laufwerk freigeben. Die Freigaben sollten Sie auf jeden Fall mit einem Passwort schützen. Die Anzeige von freigegebenen Verzeichnissen schalten Sie ab, damit sie von Fremden nicht allzu schnell entdeckt werden können.

In keinem Fall sollten Sie Verzeichnisse freigeben, in denen neben den benötigten Inhalten weitere wichtige Unterlagen zu finden sind. Kopieren Sie in diesem Fall die benötigten Daten lieber in ein eigenes Verzeichnis, und geben Sie es frei. Grundsätzlich gilt: Passwörter, Bankdaten oder gar PIN- und TAN-Nummern haben nichts auf der Festplatte eines Computers zu suchen – nicht zu Hause und schon gar nicht auf einem Notebook.

Maßnahme 4 Daten nur verschlüsselt übertragen

Bei öffentlichen Hotspots sollten Sie darauf achten, die Daten nur verschlüsselt zu übertragen. Allerdings machen sich längst nicht alle Anbieter öffentlicher Hotspots die Mühe, den Internetzugang entsprechend abzusichern. Auf unverschlüsselte WLAN-Zugänge sollten Sie aus Gründen der Sicherheit lieber vollkommen verzichten.

In der Regel kommen in Funknetzwerken drei verschiedene Verschlüsselungsmechanismen zum Einsatz. Die älteste, als WEP bekannte Verschlüsselung ist mittlerweile alles andere als sicher und sollte aus diesem Grund ebenfalls gemieden werden.

Besser sind die beiden neueren Verschlüsselungsstandards WPA und WPA2. Letzterer bietet mithilfe des symmetrischen Kryptographiesystems AES (Advanced Encryption Standard) optimalen Schutz, da dabei Schlüssellängen von bis zu 256 Zeichen zum Einsatz kommen.

Möchten Sie mit Ihrem Notebook via Hotspot eine Verbindung zu einem Firmen- oder Ihrem Heimnetzwerk aufbauen, sollten Sie dies nur unter spezi-

ellen Sicherheitsvorkehrungen tun. Am besten nehmen Sie über einen VPN-Tunnel Verbindung auf. Stellt das Zielnetzwerk eine solche Zugangsmöglichkeit zur Verfügung, benötigen Sie auf Ihrem Notebook lediglich einen einfachen VPN-Client, mit dessen Hilfe Sie die VPN-Technik nutzen können. Sowohl beim Firmen- als auch beim Heimnetzwerk muss der Client für das Zielnetzwerk konfiguriert werden.

Die Übertragung via VPN erfolgt verschlüsselt. Einige Hotspot-Anbieter wie T-Mobile sind mittlerweile dazu übergangen, VPN-Tunnel auch für den Internetzugang selbst zu verwenden. Die Nutzdaten werden während der WLAN-Übertragung als Datenpaket verpackt und via Ipsec verschlüsselt. Erst außerhalb des WLANs erfolgt dann wieder eine entsprechende Umwandlung. T-Mobile bietet für diesen Zweck einen kostenlosen Hotspot-Client an.

Maßnahme 5 Mit dem richtigen Hotspot verbinden

Schon bei der Einrichtung einer WLAN-Verbindung sollten Sie darauf achten, dass Sie sich auch mit dem richtigen Hotspot verbinden. Eine beliebte Technik von Datendieben besteht im Aufbau sogenannter Hotspot-Fakes. Dabei richten die Schnüffler in der Nähe des offiziellen WLAN-Hotspots, mit dem Sie sich verbinden wollen, ganz ähnlich geartete WLAN-Zugangspunkte ein. Sollten Sie sich einmal nicht sicher sein, ob das erreichbare WLAN wirklich seriös ist, dann verzichten Sie lieber auf einen Verbindungsaufbau.

Keine Automatik Die Option des automatischen Verbindungsaufbaus mit einem verfügbaren WLAN sollten Sie abschalten.

Maßnahme 6 WLAN nach dem Surfen abschalten

Benötigen Sie den Internetzugriff via WLAN nicht mehr, sollten Sie die WLAN-Unterstützung sofort deaktivieren. Auf diese Weise stellen Sie sicher, dass keine weiteren Angriffsmöglichkeiten mehr existieren.

Aus diesem Grund sollten Sie auch die automatische Verbindung für den Zugang zu WLAN-Netzwerken in Ihren Netzwerk-Einstellungen abschalten, denn eine WLAN-Verbindung sollten Sie prinzipiell nur manuell aufbauen. Ein automatischer Verbindungsaufbau ist zwar sehr komfortabel, aber nur durch die eigenhändige Bestätigung des Verbindungsaufbaus können Sie wirklich wissen, wann Sie sich mit welchem WLAN verbinden.

Maßnahme 7 Windows immer aktuell halten

Wenn Sie mit Ihrem Notebook häufig an Hotspots ins Internet gehen, ist es unerlässlich, dass Sie Windows und Ihre Applikationen mit regelmäßigen Updates auf dem neuesten Stand halten. Das gilt nicht nur für Windows – auch Ihren Virenscanner, die Anti-Spyware, Ihren Webbrowser und Ihren E-Mail-Client sollten Sie stets up to date halten. Nur so ist ein optimaler Schutz Ihres Notebooks möglich.

Grundsätzlich sollten Sie darauf achten, auf dem User-Account, den Sie für den Webzugriff via Hotspot verwenden, nur die Software zu installieren, die Sie auch wirklich benötigen. Dazu zählen etwa Firewall, Virenscanner und Anti-Spyware. Zusätzliche Dienste, die Sie nicht benötigen – insbesondere solche zur Fernwartung oder für den Remote-Zugriff –, sollten Sie auf Ihrem Notebook unbedingt deaktivieren.

Gut verschlüsselt Abseits eines VPN-Tunnels ist WPA2/AES die sicherste Verschlüsselungsmethode in einem WLAN.

Maßnahme 8 Datendieben das Leben schwer machen

Viele Nutzer öffentlicher Hotspots denken überhaupt nicht daran, dass die größte Gefahr für die Sicherheit ihres Systems vom eigenen Verhalten ausgeht.

Dass man sein Notebook niemals unbeaufsichtigt stehen lässt, versteht sich eigentlich von selbst – zumal dies auch das Diebstahlrisiko drastisch erhöhen würde. Hinzu kommt die Gefahr, dass Sie bei der Eingabe von Passwörtern beobachtet werden. Achten Sie also darauf, dass Sie Ihr Notebook am Hotspot möglichst unbeobachtet bedienen können.

Wichtig ist auch, dass Unbefugte möglichst nicht den Bildschirminhalt mitlesen können. Dabei sind beispielsweise Display-Folien ziemlich hilfreich. Sie machen es unmöglich, seitlich auf den Bildschirm zu blicken. Damit können Sie dann auch im Zug in aller Ruhe Ihre Firmenunterlagen durchsehen, ohne sich dabei Sorgen machen zu müssen, ob Ihr Sitznachbar die vertraulichen Texte vielleicht mitliest.

Michael Mielewczik

KNOW-HOW

Onlinebanking: Am Hotspot sehr riskant

Viele Hotspot-Nutzer fragen sich, ob sie nicht auch noch schnell ihrem Onlinekonto einen Besuch abstatten können. Besser nicht, denn ein Hotspot ist nicht der richtige Platz für finanzielle Transaktionen – ob Sie ihn nun für sicher halten oder nicht. Gerade die Eingabe von PIN- und TAN-Nummern in der Öffentlichkeit ist sehr gefährlich, und Sie sollten immer damit rechnen, dass Sie an einem Hotspot bei solchen Aktionen beobachtet werden. Vielfach wird im Zusammenhang mit Onlinebanking oder Onlineshopping bei Webseiten nach dem HTTPS-Standard auch auf die zusätzliche Sicherheit durch SSL-Verschlüsselungen mithilfe von Zertifikaten verwiesen. Gerade in einem öffentlichen Funknetzwerk sollten Sie sich jedoch darauf allein niemals verlassen.

Vorsicht, Ihr Handy überwacht Sie!

Für die Positionsbestimmung via Handy gibt es sehr sinnvolle Einsatzgebiete, doch manchmal dient sie schlicht der Überwachung des ahnungslosen Surfers. CHIP zeigt Ihnen, wie die Handy-Ortung technisch funktioniert, was Sie mit ihrer Hilfe dürfen und was verboten ist.

Foto: iStockphoto

Rein technisch gesehen, funktionieren die Ortungssysteme aller Anbieter ähnlich. Im Gegensatz zur GPS-Ortung bei Navigationsgeräten wird bei der Handy-Ortung jedoch nicht der genaue Standort des Handys ermittelt, sondern die Funkzelle, in der das Handy eingewählt ist. Ausgehend von der Mobilfunkzelle lässt sich dann eine räumliche Lokalisierung des Mobiltelefons vornehmen. Aus der Art der Ortung resultiert die Genauigkeit des Dienstes.

Im Einzelfall entspricht die Ortungsgenauigkeit der Größe einer Mobilfunkzelle. Im besten Fall lässt sich in großen Städten mit vielen Mobilfunkzellen der Handynutzer auf 50 bis 250 Meter genau orten. Auf dem Land – generell außerhalb großer Ortschaften – kann die Genauigkeit deutlich abnehmen. Was die Technik betrifft, ist die Handy-Ortung der GPS-Ortung also unterlegen – und auch mit den Möglichkeiten der Polizei ist diese Technik nicht zu vergleichen.

Bei der Handy-Ortung nimmt der Ortungsdienst keine direkte Verbindung zum Handy auf. Die Positionsdaten werden vielmehr über die auf dem Server des Netzbetreibers gespeicherten Einwahldaten des Handys ermittelt. Damit

Picos Intervistas Handy-Ortungsdienst gehört derzeit zu den bekanntesten Angeboten.

das funktioniert, muss das Handy eingeschaltet sein. Opfer der Überwachung kann also nur werden, wer gerade telefoniert, im Internet surft oder zumindest mit eingeschaltetem Mobiltelefon unterwegs ist.

Die Option, die letzte Einwahl in ein Mobilfunknetz zu ermitteln, ist Grundvoraussetzung, um die Handy-Ortung durchführen zu können. Nahezu sämtliche großen Netzbetreiber bieten diese Möglichkeit inzwischen an. Auch T-Mobile scheint als letzter großer Provider mittlerweile dazu bereit zu sein.

Die Ortungsdienste sind im Übrigen bei allen Anbietern auf das Inland beschränkt. Handy-Ortungen im Ausland sind nicht möglich. Ein spezielles Handy ist für die GSM-Ortungsdienste nicht erforderlich.

Wo ist mein Handy? So bekommen Sie es zurück

Ein Parade-Argument der Anbieter von Ortungsdiensten ist der plötzliche Verlust des wertvollen Mobiltelefons – ob Sie es nun irgendwo vergessen haben oder ob es Ihnen gestohlen wurde.

In einem solchen Fall bietet sich der Versuch an, das Handy mithilfe des Ortungssystems wiederzufinden – falls es eingeschaltet ist. Möglich ist das Ganze jedoch nur, wenn das Handy bereits vor dem Verlust beim Ortungsdienst registriert wurde. Vergessliche Zeitgenossen, die nicht mehr wissen, ob sie ihr Handy im Büro, zu Hause oder bei der Freundin vergessen haben, werden diese Möglichkeit durchaus zu schätzen wissen.

Rechtlich ist gegen die Ortung des eigenen Handys nichts einzuwenden. Ein gestohlenes Handys zu orten gestaltet sich in der Praxis deutlich schwieriger als die Suche nach einem vergessenen Mobiltelefon. Das liegt schon daran, dass das Handy grundsätzlich eingeschaltet sein muss, damit überhaupt die Möglichkeit einer Ortung besteht. Zudem macht der relativ große Radius der meisten Funkzellen das schnelle Wiederfinden eines gestohlenen Handys eher unwahrscheinlich – ganz abgesehen davon, dass man einem Diebstahlopfer nur davon abraten kann, sich auf eigene Faust auf die Suche nach dem gestohlenen Handy zu machen.

Unter der Webadresse **www.trackyourhandy.de** steht ein kostenloser Suchdienst für gestohlene Handys zur Verfügung. Nach der Registrierung der IMEI-Nummer – der Seriennummer jedes Handys – lässt sich ein Handy jederzeit über Trackyourhandy.de orten.

Dieser Dienst hat sogar noch mehr Pfeile im Köcher: Über Trackyourhandy.de können Sie eine Flash-SMS auf das verlorene oder gestohlene Handy schicken. Diese SMS teilt dem Finder oder Dieb des Handys mit, dass das Mobiltelefon bei Trackyourhandy.de registriert ist. Ehrliche Finder haben somit die Möglichkeit, sich direkt mit Ihnen in Verbindung zu setzen.

Die Rechtslage bei der Ortung eines gestohlenen Handys ist übrigens keineswegs eindeutig. So komisch es klingen mag: Auch der Dieb hat ein Recht auf Wahrung seiner Persönlichkeit und hat – auch wenn er sich rechtswidrig im Besitz eines Handys befindet – dieser Ortung nicht zugestimmt. Zugunsten einer Ortung lässt sich insofern nur argumentieren, als Sie über den Ortungsdienst ja ausschließlich Informationen zu Ihren eigenen Zugangsdaten erhalten. Welche Rechtsauffassung jeweils greift, wird wohl vom Einzelfall abhängen.

Interessant ist, dass auch Behörden bei Trackyourhandy.de einen speziellen Account haben, mit dessen Hilfe beispielsweise Polizeidienststellen, Fundbüros, Bundes- und Landeskriminalämter nach IMEI-Nummern suchen können beziehungsweise die Möglichkeit haben, IMEI-Nummern als gefunden einzutragen. Möglich ist dies übrigens nur, weil Trackyourhandy.de diese Anbindung in seinen Datenschutzbedingungen explizit aufführt. →

INFO

So aktivieren Sie die Handy-Ortung

Für den Zugriff auf die Daten der Handy-Ortung gibt es inzwischen eine ganze Reihe verschiedener Anbieter. Unter Privatkunden am weitesten verbreitet sind Dienste wie Trackyourkid oder Picos von Intervista. Die Anmeldung bei diesen Diensten verläuft in der Regel gleich.

Registrieren & aktivieren Über eine Webseite registrieren die Kunden ihr Handy. Das Aktivieren der Handy-Ortung erfolgt durch Bestätigen einer Freischalt-SMS. Bei einigen Netzbetreibern ist es zusätzlich nötig, über den Kundendienst eine explizite Freischaltung der Ortungsfunktionalität vorzunehmen. Diese Form der Anmeldung ist datenschutzrechtlich problematisch, da jeder, der in den Besitz eines fremden Handys kommen kann, in der Lage ist, diese Anmeldung vorzunehmen.

Nur mit Vertrag Cognid ist der einzige Anbieter, der einen schriftlichen Vertrag für die Aktivierung der Handy-Ortung verlangt – verständlich, wenn man bedenkt, dass Cognid vor allem gewerbliche Kunden wie Transportunternehmer oder Bauleiter gewinnen möchte. Die etwas engere Auslegung und genauere Differenzierung in Sachen Datenschutz fällt bei diesem Dienst positiv auf.

Unterschiedliche Kosten Der finanzielle Aufwand für die Dienstleistung der Handy-Ortung differiert je nach Anbieter. Die Tabelle auf 71 liefert Ihnen dazu einen ersten Überblick.

Wo ist der Partner? Das Handy verrät es

Manch einer wird auch auf die positiven Möglichkeiten der Handy-Ortung in Beziehungen verweisen wollen: Wenn man jederzeit weiß, wo sich der Partner gerade aufhält, wird der auch nicht fremdgehen können – oder wollen.

Per Handy-Ortung kann man seinen Partner kontinuierlich überwachen und seinen Aufenthaltsort ermitteln. Die Ortung kann an dieser Stelle schnell zu einem Ersatz für das essenzielle Vertrauen innerhalb einer Beziehung werden.

Gewiss sind auch in diesem Bereich legale und sinnvolle Einsatzmöglichkeiten denkbar. Sollte es also wirklich Ehefrauen geben, die so fürsorglich sein möchten, den Heimweg ihrer Männer von der Arbeit zu verfolgen, damit sie ihnen zu Hause pünktlich das Abendessen servieren können, so sind sie mit einem Handy-Ortungssystem tatsächlich gut bedient.

Ob ein solches Miteinander der Lebensführung bei einer gleichzeitigen Einschränkung der persönlichen Freiheit wirklich wünschenswert ist, sollte man sich allerdings gut überlegen. Wer tatsächlich glaubt, mit einem Handy-Überwachungssystem Beziehungsprobleme lösen und Eifersuchtsanfälle vermeiden zu können, der wird in der Regel enttäuscht werden.

Wer es dennoch ausprobieren möchte, sollte die Handy-Ortung allerdings nur mit expliziter Zustimmung des Partners aktivieren. Das ist schon deswegen notwendig, weil der Gesetzgeber an dieser Stelle sehr strenge Richtlinien zum Schutz der Privatsphäre vorgibt: Das heimliche Überwachen des Partners ist in jedem Fall verboten und eine Straftat – ob Sie nun Ihre Freundin oder Ihre Ehefrau heimlich überwachen möchten.

Dies gilt umso mehr, als die heimliche Aktivierung der Handy-Ortung auf einem fremden Handy ebenfalls illegal ist. Problematisch ist dabei, dass die Möglichkeit des Missbrauchs vergleichsweise hoch ist. Kann jemand – wenn auch nur kurz – auf Ihr Handy zugreifen, so kann er auch die Handy-Ortung aktivieren. In Zukunft gilt also gleich in zweierlei Hinsicht der Rat, immer gut auf das Handy achtzugeben.

WEB-TIPPS

Links zum Thema

Björn Steiger Stiftung
https://www.steiger-stiftung.de/
Cognid Handy-Ortung
www.cognid.de/newcce/pmw/Produkte/HandyOrtung
Mister-Vista
www.mister-vista.de/
Trackyourhandy
www.trackyourhandy.de/
Trackyourkid
www.trackyourkid.de/

Wo bleibt der Fahrer? Das Handy gibt Auskunft

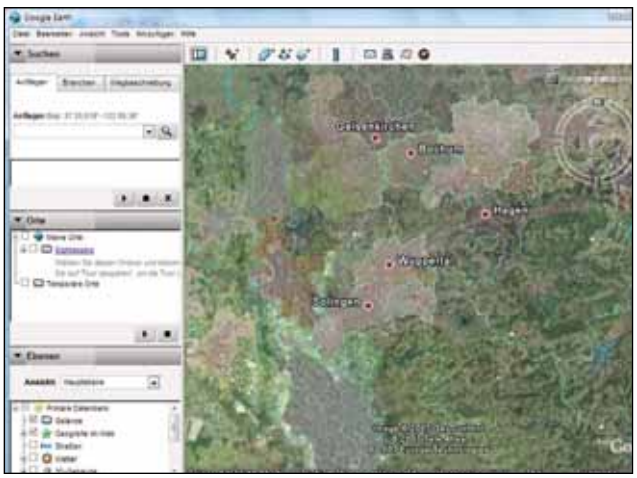
Sehr beliebt ist das Thema Handy-Ortung auch bei Arbeitgebern. Tatsächlich gibt es eine Reihe von Unternehmensbereichen, in denen man für den Wunsch nach kontinuierlichen Ortungsmöglichkeiten zumindest ein gewisses Verständnis haben kann. So ist es für ein Transportunternehmen immer interessant zu wissen, in welcher Region sich die Fahrer gerade aufhalten.

In puncto Datenschutz gelten derartige Überwachungsaktionen allerdings als äußerst bedenklich und weisen ein großes Missbrauchspotenzial durch den Arbeitgeber auf. Nicht erlaubt ist beispielsweise die Überlassung eines Firmenhandys mit aktivierter Handy-Ortung, ohne dass der Arbeitnehmer darüber informiert wird. Inwieweit man die Forderung eines Arbeitgebers nach der Verwendung eines Mobiltelefons mit aktivierter Ortungsfunktion erfüllen muss, muss jeder Arbeitnehmer im Einzelfall entscheiden. Eine Verpflichtung, dem Wunsch des Arbeitgebers zu entsprechen, gibt es jedoch nicht.

Wo ist die Unfallstelle? Das Handy weiß Bescheid

Notrufe erfolgen auch in Deutschland immer häufiger mithilfe eines Mobiltelefons. So wundert es kaum, dass auch die sich daraus ergebenden Möglichkeiten immer mehr in den Blickpunkt rücken, beispielsweise die Ortung eines Mobiltelefons bei Abgabe eines Notrufs.

Wer sein Handy bei der Björn Steiger Stiftung registriert, kann damit sicherstellen, dass die Ortung des Handys bereits während des Notrufs automatisch erfolgt. Im Falle eines schweren Unfalls kann diese Ortung für den notwendigen



Cognid Die vom Ortungsdienst Cognid ermittelten Positionsdaten lassen sich in Google Earth nutzen.

Trackyourkid Die Darstellung der Handy-Lokalisation erfolgt bei TrackyourKid wie üblich mithilfe grafischen Kartenmaterials.

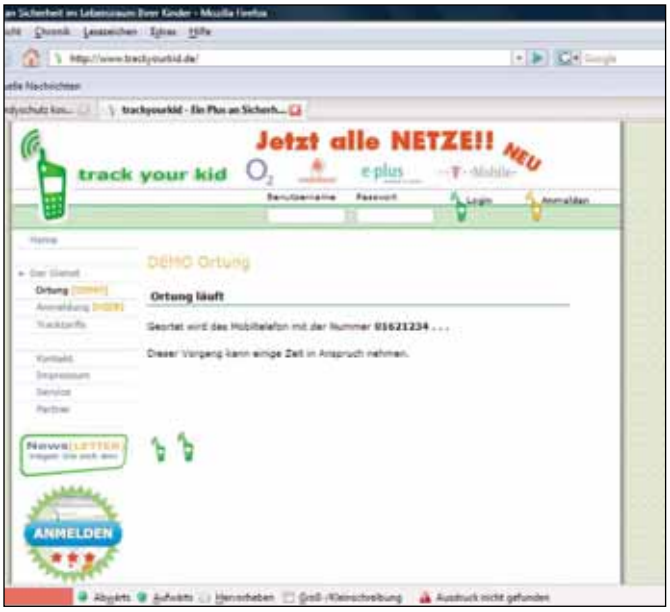
Zeitvorsprung sorgen, der für die Rettung eines Menschenlebens erforderlich ist. Und gerade für chronisch kranke Menschen, Risikosportler oder für Menschen in besonders riskanten Berufen im Außendienst dürfte die Möglichkeit der Handy-Ortung interessant sein.

Wo spielt mein Kind? Das Handy findet es raus

Auch viele Eltern finden die Option, über das Handy jederzeit Kontakt mit ihren Kindern zu halten, sehr attraktiv. Schließlich gibt ihnen der Gedanke, immer nachsehen zu können, wo sich ihre Kinder gerade aufhalten, eine gewisse Sicherheit.

In der Praxis stellt sich allerdings schnell die Frage, wie viel die Handy-Ortung bei Kindern wirklich bringt. Denn dieses System hat zweifellos auch Nachteile; schließlich werden sich nicht wenige Kinder dadurch verunsichert fühlen. Letztlich gehört auch die Entwicklung einer gewissen Eigenständigkeit zum Erwachsenwerden, und die Entscheidung für den Einsatz der Handy-Ortung sollte daher gut überlegt sein.

Auch Kinder haben ein Recht auf Privatsphäre, und Eltern sollten die Option der Handy-Ortung mit ihrem Nachwuchs besprechen und eine solche Entscheidung nicht über den Kopf der Kinder hinweg treffen. Eine einseitig gefällte Entscheidung hätte wohl schon deshalb wenig Sinn, weil das Kind das Handy einfach ausschalten könnte, wenn es gerade nicht überwacht werden will.



Dauert etwas Die Handy-Ortung über das Web-Interface von Trackyourkid kann etwas Zeit in Anspruch nehmen.

FAZIT Rein technisch gesehen, ist die Handy-Ortung eine interessante Spielerei. Wer würde nicht gern einmal auf den Spuren von James Bond wandeln? Im Einzelfall muss aber jeder selbst wissen, ob er diese Funktion einsetzen möchte. Berechtigte Bedenken in Sachen Datenschutz lassen sich jedenfalls bei fast allen möglichen Einsatzszenarien ausmachen.

Durchweg sinnvoll erscheint die Handy-Ortung lediglich im Notfall. Da Notrufe heute vorwiegend über ein Mobiltelefon abgesetzt werden, besteht damit tatsächlich die Möglichkeit, Leben zu retten.

Michael Mielewczik

INFO

Handy-Ortungsdienste im Überblick

Fünf Anbieter dominieren derzeit den Markt der Handy-Ortungsdienste. Die Preise unterscheiden sich erheblich und reichen vom kostenlosen Trackyourhandy.de bis zum teuren Premium-Paket von Trackyourkid.de.

Anbieter	Trackyourkid	Trackyourkid	Trackyour-handy	Cognid / Locate 24	Cognid / Locate 24	Mister-Vista	Intervista / personal iCOS
Internet	www.track-yourkid.de	www.track-yourkid.de	www.track-yourhandy.de	www.locate24.de	www.locate24.de	www.mister-vista.de	https://www.picosweb.de/
Vertragsmodell	Premium-Paket	Call-Paket		Tarif 1	Tarif 2	Standard	Standard
	Vertrags-bindung	Keine Vertragsbindung		Mindestens 3 Monate	Mindestens 3 Monate	–	–
Einrichtungs-gebühr	9,90 Euro	19,90 Euro	–	–	–	–	–
Jahresbeitrag	36 Euro	–	–	48 Euro	90 Euro	–	–
Vertragslaufzeit	Jederzeit kündbar	–	–	Mindestens 3 Monate	Mindestens 3 Monate	–	–
Anzahl Ortungen inklusive	20	3	1	–	–	–	–
Kosten für jede weitere Ortung	Etwa 0,35 bis 0,50 Euro	Etwa 0,75 bis 1 Euro	–	0,39 Euro	0,19 Euro	0,99 Euro	0,49 Euro
Ortbare Handys im Paket	Maximal 5	Maximal 5	1	1	1	1	1

Ihr perfekter Web-Auftritt mit Joomla

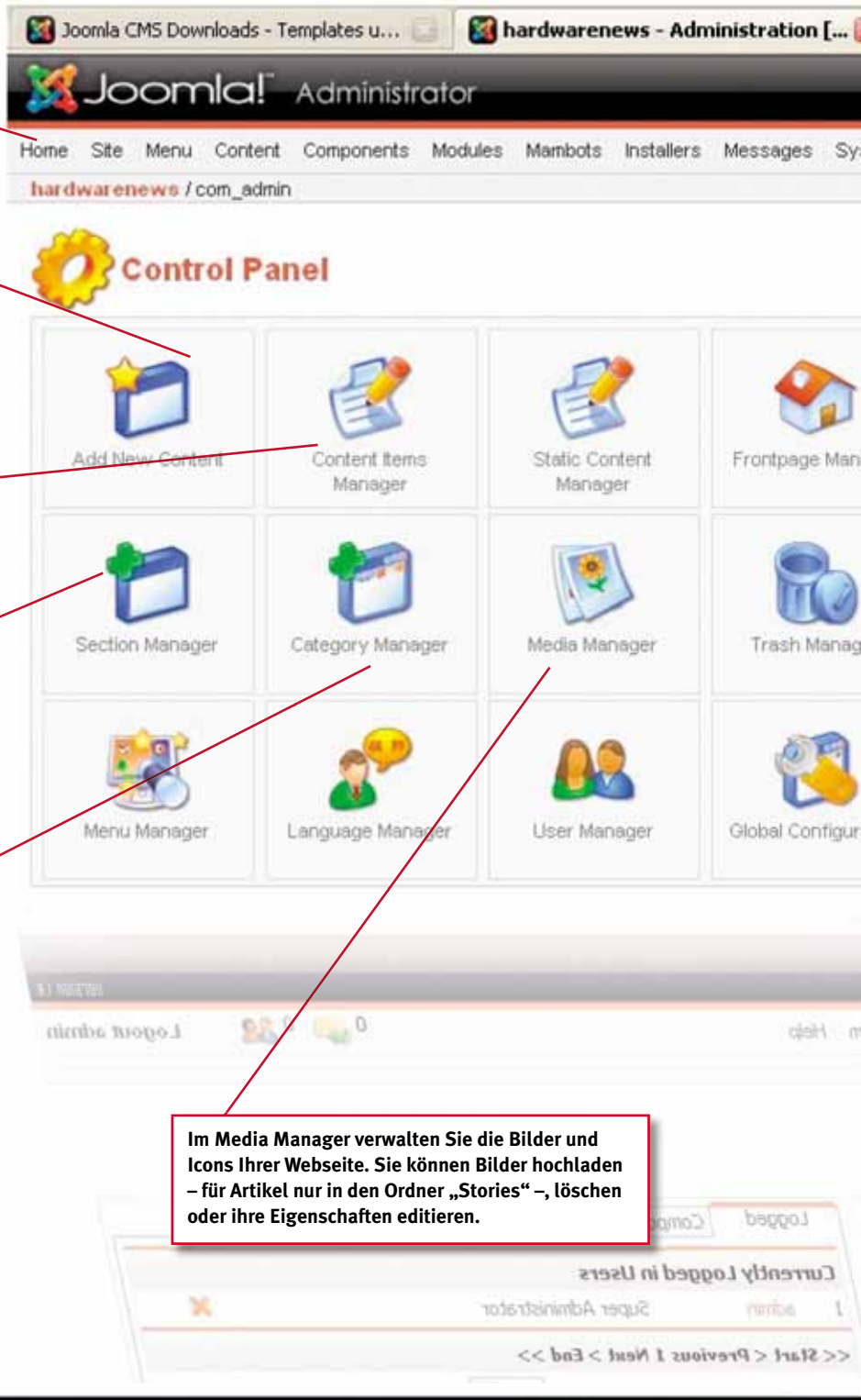
Wenn Sie sich mal verirrt haben oder schnell auf diese Seite zurückkehren wollen, genügt ein Klick auf „Home“.

Wenn Sie einen neuen Artikel eingeben wollen, startet ein Klick auf dieses Icon den Editor.

Bei einem Klick auf diesen Manager sehen Sie alle auf Ihrer Webseite gespeicherten Artikel – veröffentlichte und unveröffentlichte.

Hier geben Sie die Sektionen ein – die erste Strukturebene in Joomla.

Dieser Manager ist für die Kategorien der Sektionen zuständig – die zweite Strukturebene in Joomla.

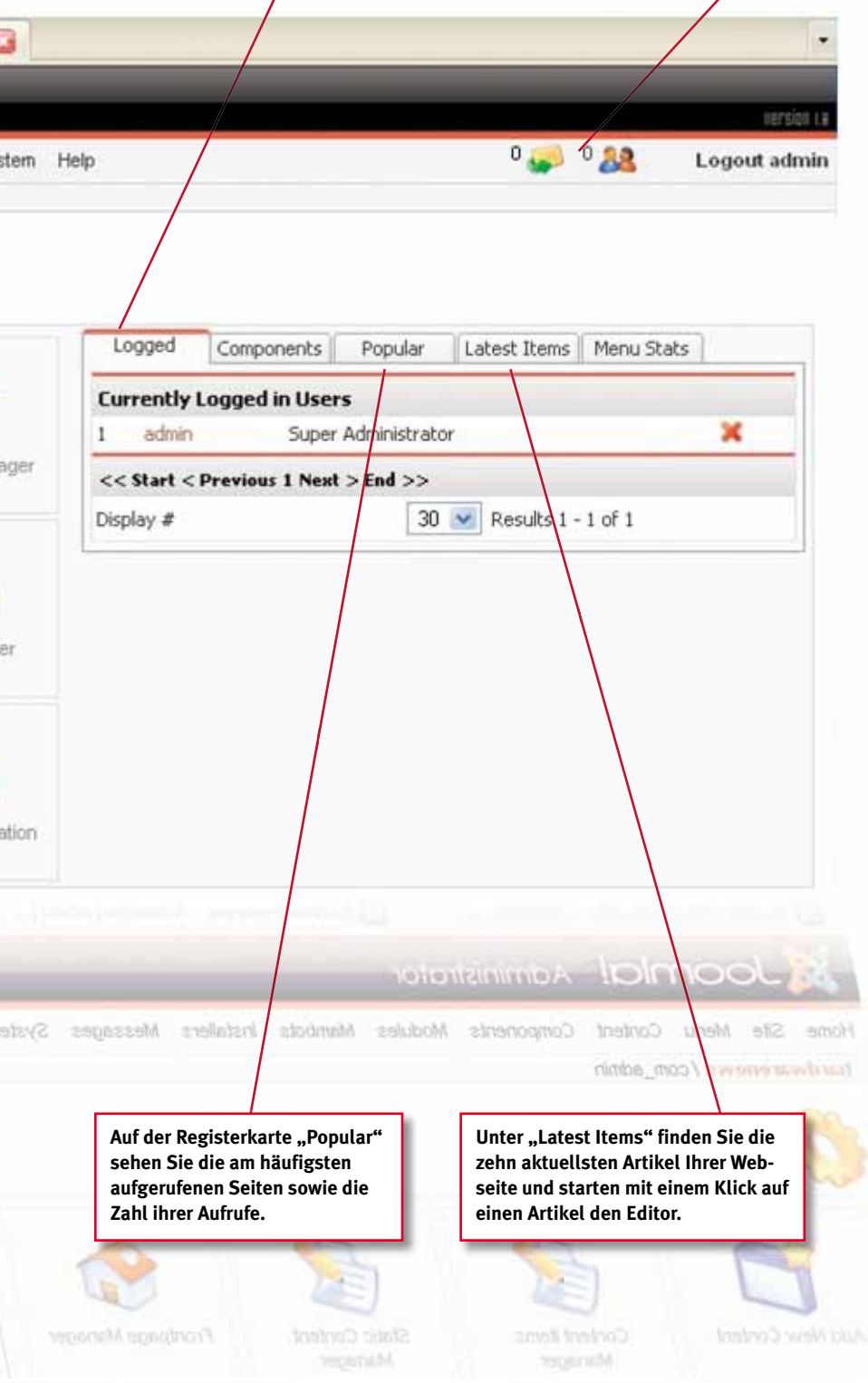


Im Media Manager verwalten Sie die Bilder und Icons Ihrer Webseite. Sie können Bilder hochladen – für Artikel nur in den Ordner „Stories“ –, löschen oder ihre Eigenschaften editieren.

Auf Heft-CD

- FileZilla (Netzwerk)
- Joomla (PHP/CMS)
- Mambo (PHP/CMS)

Mit Joomla kann wirklich jeder eine professionelle Homepage aufbauen – ohne Programmierkenntnisse oder eine Layouter-Ausbildung. So gelingt Ihr Webauftritt.



Eine Webseite zu gestalten ist heutzutage ziemlich einfach geworden. Fast alle Provider bieten Baukastenlösungen an, mit denen sich schnell eine Seite zusammenklicken lässt. Doch so richtig gut sieht keine dieser Instant-Homepages aus. Besser sind Sie da schon mit einem Content Management System (CMS) bedient.

Ein CMS ist ein Programmiersystem für Webseiten, das den Content vom Layout trennt. Sie können also den Inhalt der Webseiten in jedem möglichen Layout darstellen lassen. Diese Trennung wird durch die Speicherung der Seiteninhalte in einer Datenbank erreicht. Sobald das CMS eine Webseite anfordert, liest es die Datenbank aus und schickt die benötigten Inhalte – verpackt in HTML-Befehle – an den Browser. Der sieht dann eine normale Webseite. Das vereinfacht das Anlegen von Webseiten ungemein, denn man kümmert sich zuerst um den Inhalt der Seiten und erst anschließend um das Layout.

Joomla Homepage bauen mit einem CMS

Weitere Vorteile dieser Trennung zwischen Content und Layout: Sie können den Inhalt jederzeit ändern – er wird immer richtig dargestellt. Die Änderungen nehmen Sie zumeist in einer Word-ähnlichen Oberfläche vor. Sie können also schreiben wie bisher – ohne sich um HTML-Konventionen kümmern zu müssen. Der Aufbau einer Webseite wird damit so einfach wie das Schreiben eines Textes mit Word. Das Beste: Die meisten CMS sind Open-Source-Software und damit kostenlos.

Das CMS, mit welchem Sie garantiert am schnellsten zurechtkommen werden, heißt Joomla. Wie Sie mit Joomla in kurzer Zeit einen perfekten Webauftritt gestalten, erfahren Sie in diesem Artikel. →

1 Die Webseite planen und strukturieren

Damit die Trennung von Inhalt und Layout auch funktioniert, müssen Sie sich bei Joomla an ein paar Konventionen halten. Der Inhalt der Homepage muss nach bestimmten Kategorien geordnet sein – ansonsten kann die hinter dem CMS liegende Datenbank den Inhalt nicht speichern.

In Joomla strukturieren Sie den Inhalt in Sektionen und Kategorien, wobei eine Sektion den Kategorien übergeordnet ist. So kann beispielsweise eine Webseite die Sektion „News“ enthalten, in die alle Neuigkeiten einsortiert werden. Als Kategorien nehmen Sie dann bestimmte Themengebiete der News, bei einer Computer-Website beispielsweise „Hardware“, „Software“, „Internet“ oder „Security“. Die zugehörigen Texte geben Sie in der jeweiligen Kategorie ein. Diese Strukturierung der Inhalte hat nichts damit zu tun, wie und wo die Texte veröffentlicht werden. Wie gesagt: Joomla trennt Inhalt und Layout.

Der erste Schritt beim Entwerfen einer Webseite mit Joomla besteht also in der Strukturierung der Inhalte nach Sektionen und Kategorien. Diese Einteilung ist keine Entscheidung für die Ewigkeit. Sollten Sie später noch etwas ändern wollen, geht das problemlos. Lassen Sie sich ruhig etwas Zeit mit der Strukturierung. Es ist nicht so einfach, spontan die richtige Wahl zu treffen.

Suchen Sie bei den Inhalten nach Gemeinsamkeiten. Das sind die Sektionen. Und wenn Ihre Webseite nur zwei Sektionen aufweist, ist das auch kein Problem. Sie sollten sich stets darüber im Klaren sein, dass diese Einteilung dazu dient, die Texte später schnell wiederzufinden oder neue Texte einzusortieren.

2 Joomla installieren

Lizenzvereinbarung Akzeptieren Sie vor der Installation die Lizenzvereinbarung des XJ-Pakets.

Bei Joomla haben Sie die Wahl, das CMS zunächst auf Ihrem PC zu installieren, um Ihre Webseite in Ruhe aufzubauen, oder es gleich auf Ihrem Webspace einzurichten. Bei einer lokalen Installation ist die Homepage nicht aus dem Internet zu erreichen, und Joomla arbeitet sehr schnell. Bei einer Online-Installation können Sie die Webseite von jedem Internet-PC aus verwalten und mit Texten füllen. Allerdings hängt die Arbeitsgeschwindigkeit von Ihrer Internetverbindung und Ihrem Provider ab. So kann es bei der Online-Installation schon einmal vorkommen, dass Sie einige Sekunden warten müssen, bis Sie eine Reaktion sehen. Übrigens: Auch bei der Online-Installation können Sie einstellen, dass Ihre Webseite für andere Internetuser noch nicht sichtbar ist.

Für den Start mit Joomla empfiehlt sich die lokale Installation. Man arbeitet damit einfach schneller und unkomplizierter. Sobald alles fertig ist, können Sie die Webseite ganz einfach online stellen (siehe den Kasten auf 77).

Für die lokale Installation starten Sie das Paket XJ von der Heft-CD. Es installiert Joomla, den Datenbankserver MySQL, den Webserver Apache sowie eine Anwendung, mit der Sie Joomla per Mausklick starten können.

Im Installationsprogramm klicken Sie bei der Frage nach der Setup-Sprache einfach auf „OK“, weil die Sprache „Deutsch“ bereits ausgewählt ist. Im Setup-Assistenten klicken Sie auf „Weiter“ und akzeptieren die Lizenzvereinbarung. Im nächsten Fenster wählen Sie den Installationsordner aus; übernehmen Sie am besten die Voreinstellung. Nachdem Sie zweimal auf „Weiter“ geklickt haben, starten Sie mit „Installieren“ die Installation von Joomla.

Installationsordner An dieser Stelle können Sie den Installationsordner auswählen. Am besten übernehmen Sie den Vorschlag.

Startmenü-Eintrag Auch den Eintrag ins Startmenü können Sie bei XJ selbst bestimmen. Auch diese Vorgabe übernehmen Sie.

Nach Abschluss der Installation entscheiden Sie, ob Sie sich die Änderungen an den einzelnen XJ-Versionen ansehen möchten. Ist dies nicht der Fall, entfernen Sie das Häkchen aus der Checkbox vor „changelog.html“ und klicken auf „Fertigstellen“.

Anschließend erscheint die XJ-Startkonsole, in der Sie den Apache Webserver, den MySQL-Server sowie die drei installierten Joomla-Versionen starten können; Letztere verstecken sich unter dem Menüpunkt „Anwendung“. Nun verfügen Sie über die Joomla Version 1.0.12, eine eCommerce-Version (ein Shopsystem auf Joomla-Basis) und eine Spielwiese, auf der Sie alles ausprobieren können.

Unter dem Menüpunkt „Server“ administrieren Sie den Apache- und MySQL-Server. Normalerweise brauchen Sie an dieser Stelle nichts mehr zu ändern, XJ hat bereits ganze Arbeit geleistet. Mit einem Klick auf „Joomla! starten“ lädt Ihr Browser das Frontend – also die Webseite. Mit einem Klick auf „Admin Backend“ landen Sie bei einem Login-Bildschirm für das Backend.

Die Webseite funktioniert schon und ist noch mit einem Standardinhalt gefüllt. Sie können jedoch anhand dieses Inhalts im Backend beispielhaft nachvollziehen, wie welche Inhalte wo auf der Webseite zu sehen sein werden. Klicken Sie ruhig ein wenig auf der Webseite herum – alles funktioniert.

XJ hat Joomla 1.0.12 installiert. Die aktuelle Version ist jedoch die 1.0.13. Die sollten Sie jetzt nachinstallieren. Laden Sie den Update-Patch von der Version 1.0.12 auf die 1.0.13 herunter, entpacken Sie das Ziparchiv, und kopieren Sie den gesamten Inhalt nach C:\xampplite\htdocs\joomla\ – fertig.

Abschluss Am Ende der Installation können Sie auswählen, ob Sie die letzten Änderungen sehen oder XJ gleich starten wollen.

3 Joomla konfigurieren

Joomla-Backend Im Backend geben Sie die Inhalte ein und bestimmen den Aufbau Ihrer Homepage.

Nun machen Sie Joomla mit den wichtigsten Merkmalen Ihrer Homepage bekannt. Klicken Sie im XJ-Fenster auf „admin Backend“, und geben Sie im Login-Bildschirm als Benutzernamen „admin“ und als Passwort ebenfalls „admin“ ein. Nach einem Klick auf „Login“ befinden Sie sich im Backend.

Von dort aus steuern Sie Ihre Webseite und Joomla, geben den Content ein, definieren die Sektionen und Kategorien, wählen ein Layout aus, installieren Zusatzprogramme oder laden Bilder hoch. Um schnell auf diese Seite zu gelangen, klicken Sie ganz oben im Menü auf „Home“.

Ihre erste Aktion im Backend sollte das Ändern des Administratorpasworts sein. Klicken Sie dazu auf „User Manager“ und auf „Administrator“. Im folgenden Fenster geben Sie bei „New Password“ und „Verify Password“ Ihr neues Administratorpasswort ein. Das sollten Sie tunlichst nicht vergessen, da Sie im Augenblick ausschließlich mit diesem Passwort Zutritt ins Backend haben. Klicken Sie auf „Save“.

Anschließend gehen Sie auf „Global Configuration“. In der Registerkarte „Site“ geben Sie bei „Site Name“ den Namen Ihrer Website ein, zum Beispiel „Computernews – die neuesten und besten Nachrichten aus der IT“.

Auf der Registerkarte „Metadata“ geben Sie unter „Global Site Meta Description“ eine kurze und prägnante Beschreibung Ihrer Homepage ein. Für die Beispielseite könnte die Beschreibung lauten: „Computernews bringt die neuesten und besten Nachrichten zu Hard- und Software.“ Bei „Global Site Meta Keywords“ geben Sie Begriffe ein, die den Inhalt Ihrer Seite am treffendsten beschreiben, also etwa „Hardware, Software, Test, News, IT, Computer“.

Die übrigen Einstellungen lassen Sie zunächst unangetastet. Damit Ihre Änderungen im System gespeichert werden, müssen Sie oben auf „Save“ oder „Apply“ klicken. Ein Klick auf „Save“ schließt die aktuelle Seite, ein Klick auf „Apply“ nicht. Wenn Sie also auf der Seite weiterarbeiten wollen, klicken Sie auf „Apply“. Oben rechts finden Sie noch einen Hilfe-Button, der Ihnen einen Hilfe-Text zu der augenblicklich aktiven Seite anzeigt. Da Sie zum jetzigen Zeitpunkt keine weiteren Änderungen vornehmen wollen, klicken Sie auf „Save“.

Den Erfolg dieser Änderungen können Sie übrigens gleich sehen, wenn Sie im Hauptbildschirm auf den Menüeintrag „Site | Preview | In new Window“ klicken. Nun öffnet sich ein neues Fenster mit der Joomla-Seite und dem neuen Titel in der Browserleiste. Lassen Sie diese Seite ruhig geöffnet. Jedes Mal, wenn Sie eine Änderung in Joomla vorgenommen haben, gehen Sie auf diese Seite und drücken die [F5]-Taste oder klicken auf das „Aktualisieren“-Icon des Browsers, um die Änderungen zu sehen.

User-Verwaltung In diesem Bereich verwalten Sie die Benutzer, die sich an Ihrer Joomla-Webseite anmelden können.

→

4 Sektionen anlegen und bearbeiten

Als Nächstes legen Sie die gewünschten Sektionen und Kategorien an. Sie beginnen immer mit den Sektionen. Klicken Sie dazu zunächst auf „Section Manager“.

Unter „Section Name“ sehen Sie die bereits definierten Sektionen. Unter „Published“ können Sie sehen, ob diese Sektionen auf der Website zu sehen sind, also veröffentlicht worden sind. Momentan sind alle drei Sektionen veröffentlicht. Unveröffentlichte Sektionen sind mit einem roten Kreuz markiert. Unter „Access“ können Sie festlegen, welche Besucher diese Sektion sehen dürfen. „Public“ bedeutet an dieser Stelle so viel wie „jeder“. Bei „Registered“ sehen nur registrierte User die Sektion. Bei „Special“ können nur bestimmte User – mit dem Level „special“ – diese Sektionen zu Gesicht bekommen. Unter „#Categories“ können Sie die Anzahl der für diese Sektion definierten Kategorien sehen, unter „#Active“ alle für diese Sektion aktiven Beiträge. „#Trash“ beziffert alle Content-Einträge dieser Sektion, die in den Mülleimer befördert wurden.

Die Beispielseite hat drei Sektionen definiert: „News“, „FAQ“ und „Newsflash“. In der Sektion „FAQ“ stehen Beiträge zu häufig gestellten Fragen zur Webseite. Diese Sektion sollten wir also erhalten. Die Sektionen „News“ und „Newsflash“ enthalten beide Newsbeiträge. Aber: „Newsflash“-Beiträge kann jeder Webseitenbesucher sehen, „News“ nur registrierte User. Wenn Sie die News sehen wollen, melden Sie sich als Administrator unten links auf der Webseite an.

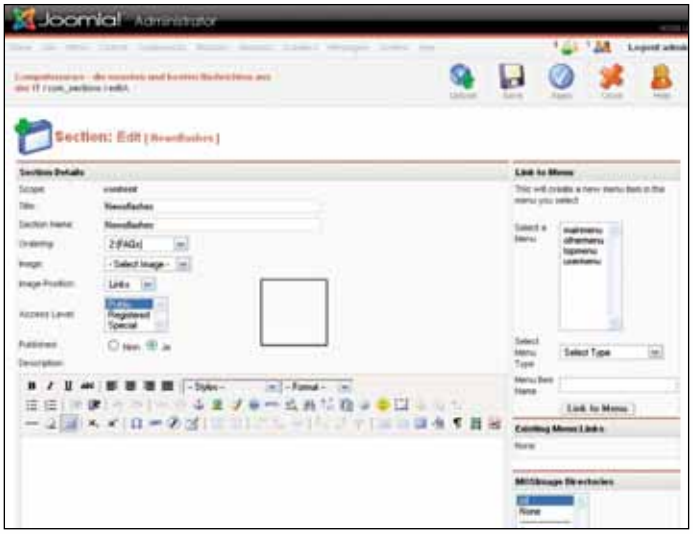
Sektionen festlegen Im „Section Manager“ verwalten Sie die erste Ordnungshierarchie von Joomla für Ihre Webseite.

Da die Beispielseite zunächst einmal recht einfach gehalten werden soll, gibt es nur News für alle. Die Sektion „News“ wird daher aus der Veröffentlichung herausgenommen. Klicken Sie auf das „Published“-Icon von „The News“. Daraufhin erscheint ein rotes Kreuz, und die Sektion ist nicht mehr auf der Webseite verfügbar. Da wir eine deutsche Seite aufbauen wollen, müssen wir „Newsflash“ noch umbenennen. Klicken Sie daher auf „Newsflashes (Newsflashes)“.

Sie landen nun im Editor von Joomla. Geben Sie bei „Title“ das Wort „Neuigkeiten“ ein. Der Title erscheint auf der Webseite als sogenannte Brotkrumenspur über dem Hauptmenü und sollte daher kurz gehalten werden. Bei „Section Name“ können Sie etwas ausführlicher werden, weil dieser Text als Sektionsüberschrift angezeigt wird. Geben Sie an dieser Stelle „Neuigkeiten aus Hard- und Software“ ein.

Da die Sektion im Hauptmenü erscheinen soll, klicken Sie im Bereich „Link to Menu“ auf „mainmenu“. Bei „Select Menu Type“ wählen Sie „Section Blog“ aus. Unter „Menu Item Name“ geben Sie den Namen an, unter dem diese Sektion im Menü auftauchen soll. Tragen Sie „Neuigkeiten“ ein, und klicken Sie auf „Link to Menu“ und auf „Save“. Diese Änderungen können Sie bereits auf der Webseite sehen – in Form des neuen Menüeintrags „Neuigkeiten“.

Da die Website auch Testberichte veröffentlichen soll, brauchen wir eine Sektion „Test“. Klicken Sie auf „New“, und Sie landen wieder im Editor. Geben Sie bei „Title“ das Wort „Tests“ ein und bei „Section Name“ die Bezeichnung „Tests von Hard- und Software“. Nach einem Klick auf „Apply“ hat sich auf der rechten Seite des Editorfensters der Bereich „Link to Menu“ geändert, und Sie können festlegen, wo diese Sektion im Menü erscheinen soll. Per Klick auf „mainmenu“ wählen wir das Hauptmenü. Bei „Select Menu Type“ wählen Sie „Section Blog“ aus. Unter „Menu Item Name“ geben Sie „Tests“ ein und klicken auf „Link to Menu“ und auf „Save“.



Sektionen einrichten Im Editor legen Sie eine neue Sektion an und bestimmen den Menüpunkt, unter dem sie auftauchen soll.

5 Kategorien anlegen oder löschen

Kategorien festlegen Im „Category Manager“ legen Sie die Kategorien der einzelnen Sektionen an und verwalten sie.

Das Anlegen von Kategorien verläuft analog. Allerdings müssen Sie noch entscheiden, welcher Sektion Sie eine Kategorie zuordnen. Zum Anlegen von Kategorien rufen Sie den „Category Manager“ aus dem Homeverzeichnis auf. Derzeit gibt es drei Kategorien. „Latest News“ ist der Sektion „News“ zugeordnet. Damit diese – wie eben festgelegt – nicht auf der Webseite sichtbar ist, sperren wir ihre Veröffentlichung mit einem Klick auf das „Published“-Icon. Die Kategorie „Newsflash“ benötigen wir nicht mehr, da unter „Neuigkeiten“ – der ursprünglichen Sektion „Newsflash“ – Meldungen über Hard- und Software veröffentlicht werden sollen. Sie wird also ebenfalls auf „Unveröffentlicht“ gesetzt.

Legen Sie nun vier Kategorien an – jeweils „Hardware“ und „Software“ in den Sektionen „Neuigkeiten“ und „Tests“. Nach einem Klick auf „New“ geben Sie im Editor bei „Category Title“ und „Category Name“ die Begriffe „Hardware“ oder „Software“ ein. Bei „Section“ wählen Sie jeweils „Tests“ oder „Neuigkeiten“ aus und klicken auf „OK“. Bei den Kategorien brauchen Sie keinen Menüeintrag zu definieren.

6 Text eingeben

Nun können Sie mit einem Klick auf „Add new Content“ bereits erste Artikel in „Tests“ und „Neuigkeiten“ veröffentlichen. Im Joomla-Editor geben Sie bei „Title“ die Überschrift ein. Wählen Sie die Sektion und die Kategorie des Artikels aus, also etwa „Neuigkeiten“ und „Hardware“. Im nächsten großen Fenster können Sie ein „Intro“ eingeben – den Vorlauftext, der in einigen Sätzen den Inhalt des Artikels zusammenfasst.

Im Fenster „Main Text“ steht dann der Beitrag selbst. Um den Text auf einer neuen Seite weiterzuführen, klicken Sie auf „Insert Page Break“. Joomla kümmert sich auch um die Nummerierung und Verlinkung der Seiten. Eine Vorschau des Artikels bekommen Sie mit einem Klick auf „Preview“ zu sehen. Wenn ein Beitrag auf der Startseite Ihrer Homepage auftauchen soll, klicken Sie im „Content Item Manager“ auf den Spalteneintrag „Front Page“. Aus dem roten Kreuz wird dann ein grüner Haken. Im „Front Page Manager“ können Sie sämtliche für die Startseite vorgesehenen Beiträge in Augenschein nehmen und verwalten.

PROFI-TIPP

So bekommen Sie Ihre Website vom lokalen PC ins Internet

Um die lokale XJ-Installation in den Webspace Ihres Providers zu transferieren, genügt es nicht, die Joomla-Installation einfach auf den Webspace zu kopieren, denn die Artikel sind in einer Datenbank gespeichert. Man muss also diese Datenbank ebenfalls in den Webspace kopieren. Dazu klicken Sie im XJ-Startfenster auf phpMyAdmin und wählen auf der linken Seite als Datenbank „joomla“ aus. Im rechten Fenster klicken Sie auf „Exportieren“.

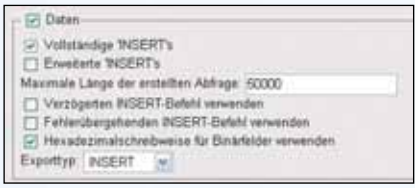
Im Kasten „Dump (Schema)“ klicken Sie auf „Alle auswählen“ und kreuzen im Kasten „Struktur“ alle Auswahlboxen an. Im Kasten „Daten“ müssen diese Haken gesetzt sein (siehe Abbildung rechts), im Kasten „Senden“ bei „Konvention merken“ und „GZip-komprimiert.

Nach zwei Mausklicks auf „OK“ wird die Datenbank unter dem Namen „joomla.sql.gz“ im Download-Verzeichnis Ihres Browsers gespeichert.

Wechseln Sie in den Admin-Bereich Ihres Webspace. Dort finden Sie ebenfalls das Programm phpMyAdmin. Legen Sie eine Datenbank mit dem Namen „Joomla“ und der Kollations-Einstellung „latin1_general_ci“ an. Klicken Sie auf „Importieren“ und „Durchsuchen“, und wählen Sie die eben gespeicherte Datenbank aus. Nach einem Klick auf „OK“ wird Ihre Joomla-Datenbank in Ihre Online-Datenbank importiert.

Rufen Sie nun mit einem Editor die Datei „configuration.php“ im Verzeichnis „C:\xampplite\htdocs\joomla\“ auf, und tragen Sie in der Zeile „$mosConfig_absolute_path = ‚C:/xampplite/htdocs/joomla‘“ statt des „C:...“ den absoluten Pfad zu Ihrer Webseite ein. Diesen Pfad erfahren Sie von Ihrem Provider. Achten Sie darauf, dass Sie am Ende keinen „/“ eintragen. Tragen Sie noch in der Zeile „$mosConfig_cachepath = ‚C:/xampplite/htdocs/joomla/cache‘;“ statt des „C:...“ den absoluten Pfad zum Cache-Verzeichnis ein. Ersetzen Sie schließlich in der Zeile „$mosConfig_live_site = ‚http://localhost:8888/joomla‘;“ „localhost...“ durch den Namen Ihrer Homepage, also etwa „www.computernews.de“. Auch hier darf kein „/“ am Ende stehen.

Laden Sie jetzt den gesamten Inhalt des Verzeichnisses „Joomla“ von „C:\xampplite/htdocs/joomla“ samt aller Unterordner per FTP in Ihren Webspace. Nun können Sie Ihre www-Adresse im Browser eingeben – und Ihre Joomla-Webseite erscheint.



Daten festlegen Setzen Sie in diesem Kasten die angezeigten Haken, und legen Sie die maximale Länge der Abfrage fest.

7 Bilder hochladen und einfügen

Bilder, die Sie in Ihre Homepage einbauen wollen, laden Sie über den Media Manager oder per FTP hoch – in der lokalen Installation von Joomla durch einfaches Kopieren des Bildes.

Den Media Manager rufen Sie über das Homeverzeichnis auf. Klicken Sie auf den Ordner „Stories“ und legen Sie einen aussagekräftigen Unterordner an, etwa „Hardware“. Dazu geben Sie bei „Create Directory“ den Begriff „Hardware“ ein und klicken auf „Create“. Nach einem Mausklick auf den neuen Ordner klicken Sie auf „Durchsuchen“ und navigieren zu dem gewünschten Bild. Markieren Sie es, und klicken Sie oben rechts auf den Button „Upload“. Das Bild wird nun in Ihren Webspace hochgeladen.

Per FTP oder bei der lokalen Installation legen Sie einen Unterordner im Ordner „Stories“ an und kopieren das gewünschte Bild in diesen Ordner.

Nun rufen Sie den Content Manager auf und klicken auf den Namen des Artikels, in dem das Bild erscheinen soll. Setzen Sie den Cursor an die richtige Stelle, und klicken Sie auf den Button „Insert image“ unterhalb des Eingabefensters. Im Text wird daraufhin in geschweiften Klammern als Platzhalter das Wort „mosimage“ eingefügt.

Bilder verwalten Im „Media Manager“ laden Sie Bilder für Ihre Webseite hoch und können sie bearbeiten, kopieren oder löschen.

Gehen Sie nun oben rechts auf die Registerkarte „Images“, und wählen Sie bei „Sub-folder“ den Ordner aus, in dem sich das Bild befindet. Klicken Sie unter „Gallery Images“ auf das Bild Ihrer Wahl und auf das obere Pfeil-Icon, sodass sein Name im Fenster „Content Images“ erscheint. Nach einem Mausklick darauf finden Sie das Bild unter „Active Image“. Unter „Image Align“ legen Sie fest, ob das Bild linksbündig, zentriert oder rechtsbündig platziert werden soll. Bei „Alt Text“ geben Sie eine Beschreibung des Bildes ein – ein wichtiger Service für Googles Suchroboter. Mit „Border“ können Sie dem Bild einen Rahmen verpassen und gleichzeitig auch seine Stärke festlegen. „Caption“ nimmt die Bildunterschrift auf, „Caption Position“ definiert die Position des Bildtextes. „Caption Align“ stellt den Bildtext linksbündig, zentriert oder rechtsbündig. Die Breite des Textrahmens legen Sie mit „Caption Width“ fest.

Nach einem Klick auf „Apply“ erscheint das Bild auf Ihrer Homepage genau an der Stelle, an der der Platzhalter „{mosimage}“ steht. Weitere Bilder veröffentlichen Sie analog: Cursor positionieren, „{mosimage}“ einfügen, Bild und Parameter wählen, „Apply“ drücken.

8 Menüs bearbeiten

Sie können jetzt bereits nach Herzenslust Texte schreiben und sie ins Joomla-System einfügen – Zeit, sich auch um die Menüstruktur Ihrer Webseite zu kümmern.

Dazu räumen wir erst einmal auf: Das Menü mit den Joomla-Einträgen etwa brauchen wir nicht. Gehen Sie auf „Menu | Menumanager“, und klicken Sie auf den Kreis vor „othermenu“ und auf „Delete“. Nach Bestätigen der Sicherheitsnachfrage ist das Menü weg.

Gehen Sie auf „Menu | mainmenu“ und setzen Sie alle nicht benötigten Menüeinträge auf „unpublished“, indem Sie auf das jeweilige Icon in der Spalte „Published“ klicken. Diese Maßnahme können Sie mit einem erneuten Klick jederzeit rückgängig machen. Wenn Sie das Menü gar nicht mehr brauchen, wählen Sie es aus und klicken auf „Trash“.

Die Reihenfolge der Menüeinträge können Sie mit den blauen Pfeiltasten oder durch die Eingabe einer Ziffer in der „Order“-Spalte festlegen. Nach Eingabe der Ziffer müssen Sie das Diskettensymbol neben „Order“ anklicken, damit Ihre Eingabe verarbeitet und die Reihenfolge aktualisiert wird.

Menüs zusammenstellen Im „Menu Manager“ legen Sie fest, welche Menüs auf Ihrer Homepage erscheinen und welche Inhalte in den Menüs zu sehen sind.

9 Untermenüs einrichten, Module & Mambots nutzen

Zum Schluss legen Sie noch für die Kategorien „Hardware“ und „Software“ einen Untermenü-Eintrag an. Nach einem Klick auf „New“ wählen Sie „Blog | Content Category“ aus, da Sie ja Kategorien einen Menüpunkt zuweisen wollen. Klicken Sie auf „Next“, geben Sie bei „Name“ den Begriff „Hardware“ ein, und wählen Sie als Kategorie „Neuigkeiten / Hardware“ aus. Dann klicken Sie auf „Neuigkeiten“, damit dieser Menüpunkt als Unterpunkt zu „Neuigkeiten“ erscheint, und speichern Ihre Eingaben mit „Save“. Ab sofort finden Sie nach einem Klick auf den Menüpunkt „Neuigkeiten“ das Untermenü „Hardware“. Nach dem gleichen Schema richten Sie die anderen drei Untermenüs ein.

Joomlas Module ausreizen Module erweitern die Funktionalität von Joomla. Im „Module Manager“ finden Sie unter „Modules | Site Modules“ zahlreiche bereits installierte Module, beispielsweise an fünfter Stelle ein Modul namens „Syndicate“. Das ist für den Kasten unten links auf der Webseite verantwortlich, mit dem Ihre Besucher einen RSS-Feed abonnieren können. Über einen Klick in der „Published“-Spalte können Sie das Modul jederzeit ausblenden. Die beiden Module „Latest News“ und „Popular“ finden Sie weiter unten. Das erste Modul stellt die neuesten, das zweite die am meisten gelesenen Beiträge dar. Ein Klick etwa auf „Latest News“ öffnet die Einstellungen für dieses Modul – die bei vielen Modulen ähnlich angelegt sind.

Unter „Title“ steht der Name des Moduls, wie er auf der Homepage zu sehen ist. Wenn Sie an dieser Stelle „Die neuesten Beiträge“ eingeben, erscheint dieser Text auf der Webseite statt „Latest News“.

Platzierung Den Modulen müssen Sie im „Module Manager“ stets bestimmte Plätze zuweisen.

Neue Funktionen Im „Module Manager“ erweitern Sie Ihre Site um bestimmte Module.

Mit „Show title“ können Sie festlegen, ob der Titel überhaupt zu sehen sein soll. Unter „Position“ legen Sie fest, wo das Modul auf der Webseite erscheint. Diese Modulpositionen bestimmt das Template, die grafische Oberfläche der Webseite. Damit Sie wissen, wo bei Ihrem Template welche Position existiert, hängen Sie doch einfach ein „?tp=1“ hinter die Webseiten-URL. Sofort bekommen Sie die verschiedenen Positionen mit Ihren Namen zu Gesicht.

Wie Sie dann sehen können, liegt die Position „user1“ links oben über dem Haupttext. Wenn Sie „Die neuesten Beiträge“ an irgendeiner anderen Stelle lesen wollen, wählen Sie sie bei den „Moduleigenschaften“ unter „Position“ aus. Mit dem Modul „Order“ bestimmen Sie die Reihenfolge, in der die Module erscheinen, wenn Sie auf einer Position mehrere Module platziert haben.

Der „Access Level“ bestimmt, ob jeder das Modul sehen soll („public“), nur registrierte Nutzer („registered“) oder nur bestimmte registrierte Benutzer („special“). „Published“ hat dieselbe Funktion wie in der Menü-Übersicht. Unter „Description“ bekommen Sie eine kurze Erläuterung, was dieses Modul überhaupt bewirkt, und mit dem Modul „Class Suffix“ können Sie per CSS-Befehl das Aussehen des Moduls beeinflussen.

Bei „Enable Cache“ geben Sie an, ob Joomla bei jedem Seitenaufruf den Inhalt des Moduls neu zusammenstellen soll oder ob er für eine gewisse Zeit gecacht wird. Das Caching beschleunigt den Aufbau der Seite. Bei einfachen und damit schnellen Modulen kann man das Caching allerdings getrost ausschalten.

Den „Module Mode“ sollte man auf der Voreinstellung „Content Items Only“ belassen. Bei „Frontpage Items“ können Sie bestimmen, ob in dem Modul auch die Artikel zu sehen sein sollen, die auf der Startseite zu sehen sind.

Mit „Count“ legen Sie fest, wie viele Beiträge gezeigt werden sollen. Und wenn es nur Artikel aus einer bestimmten Kategorie oder Sektion sein sollen, können Sie unter „Category“ oder „Section“ die jeweilige ID eintragen. Mehrere IDs trennen Sie mit einem Komma. Existiert kein Eintrag, werden alle Kategorien oder Sektionen berücksichtigt.

Im rechten Feld wählen Sie aus, auf welchen Seiten das Modul erscheinen soll. Im Beispiel sieht man die neuesten Beiträge auf der Startseite (Home) und auf der „Neuigkeiten“-Seite. Weitere Seiten können Sie mit einem Klick auf den jeweiligen Eintrag auswählen, dabei muss auch die [Strg]-Taste gedrückt sein. Wenn das Modul auf jeder Seite erscheinen soll, wählen Sie „All“.

Das Modul „Popular“ lässt sich analog bearbeiten und eindeutschen – oder ausschalten. Das Modul „Newsflash“, das oben rechts auf der Homepage erscheint, schalten Sie ebenfalls aus oder konfigurieren es neu, damit Artikel aus einer bestimmten Kategorie dort erscheinen.

Design ändern Das Aussehen Ihrer Webseite können Sie im „Template Manager“ ändern – Mausklick genügt.

→

Dazu müssen Sie in den Parametern unter „Category“ eine der vorhandenen Kategorien auswählen.

Außerdem sollten Sie noch den „Poll“-Kasten und den „Who’s Online“ von der Veröffentlichung ausnehmen. Damit wäre die rechte Spalte für neue Module frei.

Joomlas Mambots einsetzen Die Module sind nicht Ihre einzigen Helfer in Joomla. Denn da gibt es auch noch die sogenannten Mambots – kleine Programme, die in die Homepage eingebettet werden können und die eine bestimmte Funktion ausüben. So funktioniert zum Beispiel das Einbinden von Bildern über den Mambot {mosimage}. Mambots fügen einer Webseite beispielsweise eine Suchfunktion hinzu (oben rechts auf der Webseite), die Seitenumbruch-Funktion mit einer Inhaltsübersicht am Anfang oder auch einen Editor für das Backend – bei dem es sich schließlich ebenfalls um eine Joomla-Webseite handelt.

Interessant an den Mambots ist die Tatsache, dass im Internet zahllose Mambots bereitstehen, mit denen sich Websites aufrüsten lassen. Man kann etwa auch Google Maps in einen Artikel einbinden oder den Übersetzungsdienst von Google nutzen, der per Link den Artikel übersetzt.

Auch über die sogenannten Komponenten können Sie die Funktionalität von Joomla erweitern. Dabei handelt es sich ebenfalls um Programme, die aber nicht in die Webseite kopiert werden, sondern vom Backend aus arbeiten. So können Sie etwa mit Komponenten eine Backup-Möglichkeit oder eine ausgefeilte Statistikfunktion installieren.

Neue Kleider für die Homepage **Kostenlose Templates stehen zu Hunderten im Internet bereit. Sie brauchen sie nur im „Template Manager“ hochzuladen.**

Die Optik über Templates ändern Das Erscheinungsbild des Frontend bestimmen sogenannte Templates, in denen das Aussehen der Homepage definiert ist. Templates wählen Sie über den „Template Manager“ aus, welchen Sie über „Site | Template Manager | Site Template“ erreichen. Standardmäßig sind in Joomla allerdings lediglich zwei Templates installiert.

Von diesen beiden Templates ist zunächst „madeyourweb“ aktiv. Wenn Sie sich einmal ansehen möchten, wie Ihre Homepage mit dem zweiten Template aussieht, dann klicken Sie auf den Kreis vor „rhuk_solarflare_ii“ und auf „Default“. Eine Vorschau auf den neuen Look bekommen Sie übrigens, wenn Sie mit der Maus über den Namen des Templates fahren. Wenn Sie jetzt Ihre Website aufrufen, sehen Sie sie im neuen Design.

Wie Sie feststellen, beeinflusst das den Inhalt Ihrer Webseite überhaupt nicht. Aufgrund der Trennung von Inhalt und Layout können Sie jederzeit ein neues Layout für Ihre Webseite installieren, ohne Ihre bisherige Arbeit am Content zu verlieren.

Zwei Templates sind nun nicht gerade eine große Auswahl. Umso besser, dass sich Joomla-Templates auch selbst gestalten lassen – und von vielen Joomla-Nutzern im Internet zum Gratisdownload angeboten werden. So können Sie beispielsweise auf **www.joomlaos.de** mehr als 2000 Templates herunterladen. Jedes Template ist mit einem kleinen Bild vertreten. Wenn Sie mehr über ein Template wissen wollen, klicken Sie auf „Live Preview“, und schon können Sie es in seiner ganzen Pracht erleben.

Um ein neues Template zu installieren, rufen Sie das Backend und klicken auf „Installers“ und „Templates | Site“. Über „Durchsuchen“ wählen Sie das heruntergeladene Template aus. Dann klicken Sie auf „Upload File & Install“. Nun wird das Template in Ihr Joomla-System geladen, und Sie können es Ihrer Webseite zuweisen.

Module, Mambots & Komponenten installieren Die im Internet angebotenen Module, Mambots und Komponenten können Sie ebenfalls hochladen und installieren. Zu diesem Zweck klicken Sie im Backend wieder auf „Installers“ und auf „Modules“, „Mambots“ oder „Components“. Über den „Durchsuchen“-Button wählen Sie wiederum die zu installierende Funktion aus und laden sie hoch. Einige Funktionen zeigen nach der Installation in einer Art Gebrauchsanweisung, wie man das neue Feature optimal nutzen kann. Es ist empfehlenswert, sich stets an dieses Manual zu halten.

Michael Röhrs-Sperber

KNOW-HOW

Geniale Erweiterungen für Joomla

Mit Modulen, Mambots und Komponenten lässt sich Joomla optimieren.
Zunächst sollten Sie sich einen besseren Editor zulegen, etwa den „Joomla Content Editor (JCE)“. Er erleichtert das Formatieren von Text oder das Einfügen von Bildern. Der größte Vorteil gegenüber dem eingebauten TinyMCE ist jedoch die Möglichkeit, ihn mit Plugins zu erweitern. So gibt es das Plugin Advanced Link, das das interne Verlinken von Beiträgen stark vereinfacht. Für das Veröffentlichen von Bildern bietet sich die „PonyGallery“ an. Zum Aufbau einer Online-Community können Sie zur „Community Builder Suite“ greifen. Mit „Easybook“ legen Sie komfortable Gästebücher an, und mit „Docman“ installieren Sie ein Dokumentenmanagement sowie eine komfortable Download-Komponente. Mit dem „JoomlaXplorer“ verwalten Sie Ihren Webspace in einem Explorer-ähnlichen Fenster direkt im Browser. Und mit BBClone bekommen Sie einen schnellen Überblick über die Besucher Ihrer Webseite.

Foto: M. Fiorito

Angriffe auf den Server

Im Internet lauern nicht nur Gefahren für Surfer, sondern auch für Website-Betreiber. Besonders verbreitet sind derzeit XSS-Attacken gegen ungenügend geschützte Webserver.

Die bekannteste Angriffsmethode, die Programmierfehler ausnutzt, nennt sich Cross-Site Scripting oder kurz XSS. Ein geschickt maskierter Link führt den Anwender dabei auf eine vertrauenswürdig scheinende Webseite, die ihm mit JavaScript-Code auf verschiedene Art und Weise vertrauliche Daten entlockt. Mit solchen Angriffen müssen sich beileibe nicht nur die Administratoren privater Websites auseinandersetzen. Selbst große, kommerzielle Internetpräsenzen etwa von Apple, Ebay, Yahoo oder Microsoft waren bereits betroffen. Und auch deutsche Websites wurden schon Ziel solcher Attacken – darunter auch die Webseite des TÜV Süd. In der jüngsten Vergangenheit ist es Hackern zudem immer wieder gelungen, XSS-Angriffe gegen die Sites staatlicher Institutionen oder Parteien zu fahren. Im Oktober 2007 beispielsweise wurde die australische liberaldemokratische Partei Opfer einer solchen Attacke, bei der ein Bild des Premierministers mit einer veränderten Bildunterschrift versehen wurde (**www.news.com.au/story/0,23599,22562105-29277,00.html**).

Funktionsweise Wann eine XSS-Attacke möglich ist

Damit ein XSS-Angriff funktionieren kann, müssen eine oder mehrere Bedingungen erfüllt sein:

- Der Administrator der Website muss auf einen manipulierten Link des Angreifers klicken.
- Die Website muss dynamische Inhalte aufweisen und in einem Skript einen Programmierfehler enthalten.
- Im Browser des Administrators muss JavaScript aktiviert sein.
- Die Zugangsdaten zur Website werden in einem Session Cookie abgelegt.

Wenn das gegeben ist, kann der Angreifer eine Webseite beispielsweise so manipulieren, dass die Daten, die die Besucher dort in ein Formular eingeben, nicht nur an den Zielserver, sondern auch an den Server des Angreifers übertragen werden. Auf diese Weise kann er sich zum Beispiel Kreditkarten-Informationen und andere Daten beschaffen.

Die Vorbereitung auf einen solchen Angriff ist recht einfach und bedarf keiner großen Hilfsmittel. Der Angreifer ruft in einem Browser die Eingabeseite der Website auf und überträgt dabei ein kleines Skript. Es kann beispielsweise nur aus einer einzigen Zeile bestehen, mit der ein Popup-Fenster aufgerufen wird. Falls dieses Fenster dann tatsächlich erscheint, weiß der Hacker, dass diese Site eine Schwachstelle in Form eines Programmierfehlers aufweist. Und über diese Schwachstelle kann er nun die Inhalte der Site manipulieren.

Übrigens sind nicht nur dynamisch generierte Seiten anfällig für solche Attacken, sondern praktisch alle Webseiten, die Informationen an eine Datenbank übergeben. Dazu zählen beispielsweise auch Anmeldeseiten oder Formulare zum Erfassen von Daten aller Art.

Die Varianten Drei Arten von XSS-Angriffen

Man unterscheidet zwischen drei Arten von XSS-Angriffen, sie sind von 0 bis 2 nummeriert. Typ 0 ist auch als lokales Cross-Site Scripting bekannt. Angreifer, die auf diese Methode setzen, nutzen die Sicherheitslücke in einem Code-Fragment auf der Clientseite aus. Sie locken dafür das Opfer unter einem Vorwand auf eine eigens dafür manipulierte Website, die dann den benötigten JavaScript-Code ausführt. Besonders gefährdet sind von solchen Attacken ältere Versionen des Internet Explorer. Diese Browser räumen lokalen Seiten weit reichende →

Rechte ein und lassen sogar zu, dass ein Angreifer auf dem Computer des Opfers externe Programme ausführt.

Typ 1 wird als nicht-persistentes XSS bezeichnet. Der Schadcode ist dabei nicht permanent in die Webseite integriert, wo er von dem lokalen Client ausgeführt wird, sondern greift eine Schwachstelle des Webservers an. Der Angreifer nutzt dabei den Umstand aus, dass dynamisch generierte Webseiten die mittels http-get und http-post übertragenen Eingabewerte des Anwenders anpassen. Auf diese Weise schmuggelt er in die übertragenen Daten den Schadcode ein, der anschließend direkt auf dem Computer des Opfers ausgeführt wird. Ruft der Anwender die Webseite später durch die manuelle Eingabe der URL auf, funktioniert die Seite natürlich wieder ganz wie gewohnt.

Typ 2 schließlich ist die gefährlichste Variante von XSS. Bei diesen Angriffen wird der Schadcode auf dem Webserver gespeichert und bei jedem Aufruf der Anwendung erneut geladen. Wegen der permanenten Speicherung heißt diese Variante auch persistentes XSS. Hacker setzen sie gern ein, wenn sie beispielsweise über ein Gästebuch oder ein Forum Schadcode auf den Server schmuggeln können, der dort bei jedem Aufruf des Gästebuch- oder Forumbeitrags erneut zur Ausführung kommt.

Schutzmaßnahmen Daten sorgfältig verifizieren

Um sich und die Besucher Ihrer Site vor XSS-Attacken zu schützen, müssen Sie in erster Linie alle Daten, die die Webseiten an den Server schicken, genau verifizieren. Dabei gibt es zwei Vorgehensweisen: Entweder Sie definieren, welche Eingaben generell nicht zulässig sind, und filtern diese heraus, oder – und das ist der einfachere Weg – Sie geben genau an, welche Optionen es bei der Eingabe in die einzelnen Felder gibt, und lehnen alle abweichenden Einträge generell ab.

In technischer Hinsicht müssen Sie darauf achten, dass die Zeichen, die beim Ausführen von Skripten typischerweise zum Einsatz kommen, direkt in die entsprechenden Zeichenreferenzen umgewandelt werden. So sollte beispielsweise ein „<“ stets als „%3C“ übertragen werden.

Das Herausfiltern unzulässiger Benutzer-Eingaben allein genügt jedoch noch nicht als Schutz. Denn die verschiedenen Browser interpretieren die Eingaben jeweils unterschiedlich. Außerdem sind Ihnen die Hacker meist einen Schritt voraus. Das wird beispielsweise aus den einschlägigen Datenbanken zu XSS-Problemen ersichtlich. Auf der Seite der englischsprachigen Wikipedia zum Thema Cross-Site Scripting finden Sie eine Reihe von Links zu Seiten, die die möglichen Manipulationen in den einzelnen Browserversionen aufzählen. Diese Seiten bilden damit eine optimale Spielwiese für Hacker und solche, die es werden möchten.

Zusätzlich zur Filterung der übertragenen Inhalte sollten Sie auch die Session Cookies Ihres Servers schützen. Denn diese Cookies enthalten die Daten, mit denen sich der jeweilige Besucher für diese Session angemeldet hat. Haben Sie sich beispielsweise als Administrator bei einer webbasierten Anwendung angemeldet, welche mit Session Cookies arbeitet, werden Ihre Zugriffsrechte während dieser Session in einem Cookie lokal auf Ihrem Computer abgelegt. Für den Fall, dass es jetzt einem Angreifer gelingt, dieses Cookie zu kopieren, kann er von seinem PC aus ebenfalls mit Administratorrechten auf den Webserver zugreifen.

Das können Sie verhindern, indem Sie das Cookie mit der IP-Adresse des anfragenden Computers verknüpfen. Allerdings funktioniert dies nur, wenn sich Administrator und Angreifer nicht hinter einer Firewall mit NAT (Network Address Translation) befinden. Denn diese Konstruktion meldet für jeden Rechner im lokalen Netzwerk die gleiche IP-Adresse an die Webanwendung. Falls der Angreifer im gleichen LAN sitzt wie Sie, bekommt sein Session Cookie auch die gleiche IP-Adresse zugewiesen.

Schließlich können Sie als Entwickler einer Webanwendung auf der Clientseite auch komplett auf JavaScript verzichten. In diesem Fall können die Besucher Ihrer Website in Ihrer Browserkonfiguration die Ausführung von Skripten generell unterbinden und laufen damit auch nicht Gefahr, einer XSS-Attacke ausgesetzt zu werden.

Test auf Schwachstellen Acunetix erlaubt umfassende Tests auf Probleme im Zusammenhang mit Cross-Site Scripting.

Rundum-sorglos-Paket Nessus bietet Plugins zum Überprüfen von Schwachstellen in den Bereichen XSS, SQL und CGI.

Erfolgreicher Angriff Einige Websites bieten Datenbanken mit Beispielen für erfolgreiche XSS-Attacken an und zeigen auf, welche Browser dafür anfällig sind.

Schwachstellen finden
Scanner einsetzen

Die im letzten Abschnitt genannten Tipps können jedoch nur das Schlimmste verhindern. Eine grundlegend sichere Website bekommen Sie damit nicht. Um diesem Ziel ein Stück näher zu kommen, sollten Sie einen Scanner einsetzen, der Ihren Webauftritt auf mögliche Einfallstore untersucht.

Es gibt eine ganze Reihe leistungsfähiger Produkte dieser Art. Die meisten werden von den Herstellern kostenlos zur Verfügung gestellt. Das gilt beispielsweise auch für den Netzwerkscanner Nessus, der nach Installation eines Plugins auch XSS-Schwächen findet (**www.nessus.org/plugins/index.php?view=all&family=CGI+abuses+%3A+XSS**).

Eine Alternative zu Nessus ist die kostenlose Version des Web Vulnerability Scanner von Acunetix (**www.acunetix.de/cross-site-scripting/scanner.htm**). Bevor Sie sich das Programm aus dem Internet kopieren können, müssen Sie sich online registrieren. Kurz danach bekommen Sie per E-Mail den Download-Link zugeschickt. Laden Sie die ungefähr 8 MByte große Installationsdatei herunter, und folgen Sie beim Setup den Anweisungen des integrierten Assistenten.

Anschließend müssen Sie die Untersuchung Ihrer Website zunächst vorbereiten, auch dabei hilft Ihnen ein Assistent. Geben Sie im ersten Fenster unter „Scan single website“ die URL Ihrer Internetpräsenz an, und aktivieren Sie im nächsten Fenster als Ziel für die Angriffe alle Technologien, die Sie auf Ihrer Website einsetzen. Falls Sie sich nicht sicher sind, welche das sind, markieren Sie einfach alle Optionen. Die Einstellungen zum Test der Site („Crawling Options“) können Sie auf den voreingestellten Werten belassen. Wählen Sie abschließend unter „Scan Options“ noch aus, ob der Scanner eine schnelle oder eher eine intensive Prüfung durchführen soll, und aktivieren Sie auch die zusätzlichen Prüfungen, die auf dieser Seite aufgelistet werden. Anschließend können Sie mit dem Test der Site beginnen.

Als Ergebnis liefert Ihnen der Scanner eine Auswertung, wie bedroht die Site ist und wie viele Alarmmeldungen, eingeteilt in vier Levels, bei der Überprüfung ausgelöst wurden. Mit diesen Angaben können Sie nun Ihre Anwendungen und Webseiten in Hinblick auf die Sicherheit optimieren.

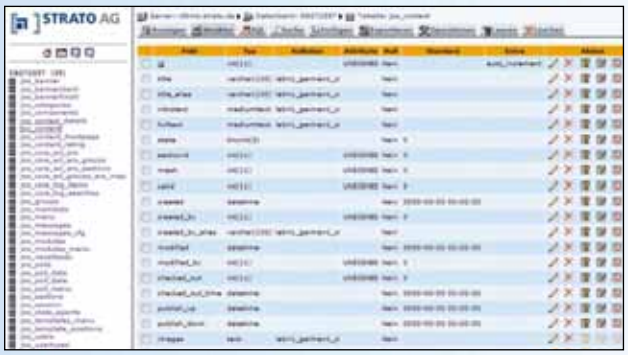
SQL-DATENBANKEN

Noch mehr Gefahrenherde für Server

Leider birgt nicht nur die Ausführung von JavaScript-Code Risiken in sich – auch eine SQL-Datenbank, die in direkter Verbindung mit einer webbasierten Anwendung steht, kann ein Einfallstor für Hacker sein. Falls die Benutzerangaben, die in die Datenbank geschrieben werden, nicht genauestens überprüft werden, lässt sich über eine SQL Injection die Kontrolle über den Datenbankserver erlangen.

Das Vorgehen eines Angreifers ist dabei ähnlich wie bei einer XSS-Attacke. Anstelle des korrekten Übergabeparameters schickt der Hacker eine oder mehrere Zeilen Code an die Datenbank. Unter bestimmten Umständen können sie dort zur Ausführung kommen und beispielsweise einen Befehl über die Kommandozeile ausführen oder Daten aus der Datenbank ausspähen. Das Ergebnis wird dann zusammen mit den ursprünglichen Daten der Anwendung ausgegeben. So kann beispielsweise parallel zur Anfrage nach einem Produkt auch die Liste der registrierten Serverbenutzer abgefragt werden – dazu benötigt der Angreifer lediglich ein wenig SQL-Wissen und ein paar Informationen über den Aufbau der Datenbank. Falls die Entwickler der Webanwendung nicht dafür gesorgt haben, dass die Benutzereingaben verifiziert und Metazeichen wie das Semikolon maskiert werden, steht der Ausführung nahezu beliebiger Befehle nichts im Wege.

Um dem vorzubeugen, sollten Sie nicht nur Ihre Eingabemasken und Datenbanken verifizieren, sondern die Anwendung in regelmäßigen Abständen mit einem Scanner wie Nessus überprüfen.



SQL Injection Auch Datenbanken sind anfällig für Hackerangriffe, weshalb Besucher-Eingaben sorgfältig überprüft werden sollten.

CGI-Skripte Bekannte Einfallstore

Das Common Gateway Interface – kurz CGI – ist zwar bereits ein wenig in die Jahre gekommen. Trotzdem sind noch zahlreiche CGI-Skripte im Einsatz, die den Datenaustausch zwischen einem Webserver und einer Anwendung steuern, die meist auf dem gleichen Server läuft. Bereits seit 1993 wird auf diese Weise eine Basis für interaktive und dynamische Webseiten geschaffen.

Da die Anwendung direkt auf dem Webserver läuft, ist sie besonders sicherheitskritisch. Das Programm sollte daher nur über die Zugriffsberechtigungen verfügen, die für seine Ausführung zwingend erforderlich sind. Und auch auf dem Server sollten nur solche Anwendungen und Dienste laufen, die er für den Betrieb unbedingt benötigt. Außerdem sollten Sie beim Einsatz von CGI-Skripten am besten nur solche Anwendungen einsetzen, die bereits mehrfach getestet und optimiert wurden. Es gibt sie für nahezu jede denkbare Aufgabenstellung – eine Suche mit Google fördert das gewünschte Skript sicherlich schnell zu Tage.

Vor dem Einsatz von CGI-Skripten – oder bevor Sie selber welche schreiben und einsetzen – sollten Sie sich allerdings unbedingt den Artikel über CGI-Security von Wolfgang Wiese durchlesen (**www.xwolf.de/artikel/cgisec.shtml**). Und bevor Sie Ihre Anwendung der breiten Öffentlichkeit zur Verfügung stellen, sollten Sie noch einen Sicherheitsscanner wie Nessus zurate ziehen und Ihre Skripte auf Verwundbarkeit durch die gebräuchlichsten Attacken analysieren lassen.

Andreas Hitzig

E-Mail-Formulare sichern

Kontaktformulare auf Webseiten sind ein potenzielles Sicherheitsrisiko, denn Spammer und Robots können sie leicht missbrauchen. CHIP zeigt Ihnen, wie Sie Ihre Formulare sichern.

Spamrobots sind nicht nur lästig und ein großes Ärgernis für Webseiten-Betreiber. Dummerweise sind sie oftmals auch äußerst raffiniert in der Vorgehensweise und finden in ungeschützten Kontaktformularen ein willkommenes Betätigungsfeld. In diesem Beitrag zeigen wir Ihnen, wie Sie die Formulare auf Ihrer Webseite wirkungsvoll absichern.

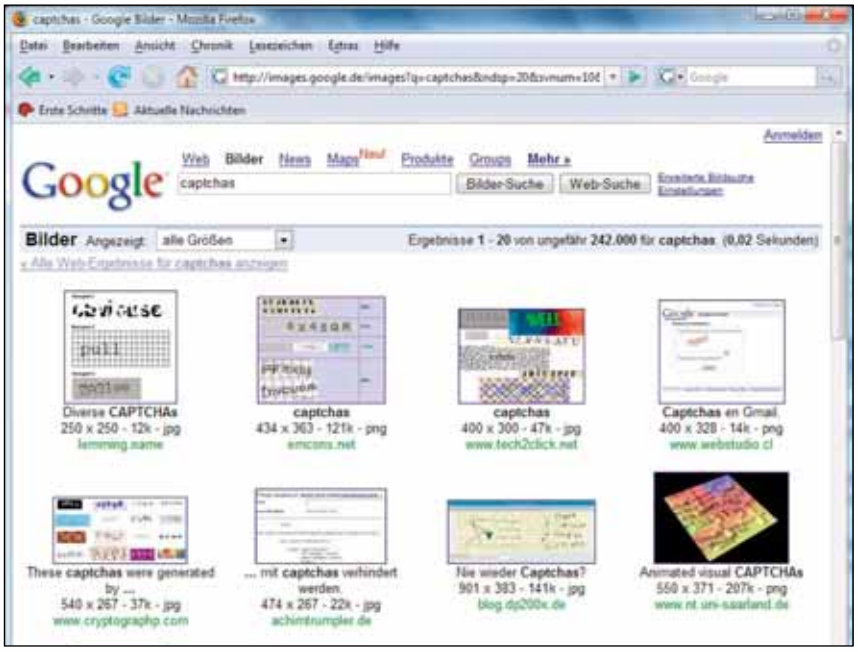
Keine E-Mail-Adressen im Klartext publizieren

Die Spambots durchsuchen das Internet ständig nach neuen E-Mail-Adressen. Dazu durchforsten sie die Homepages dieser Welt nach entsprechenden Einträgen, die dort hinterlegt sind.

Eine einfache Methode, die Bots ins Leere laufen zu lassen, besteht darin, E-Mail-Adressen auf der eigenen Homepage gar nicht erst im Plaintext-Format oder gar als echten „mailto:"-Link zu hinterlegen. Das manuelle Codieren solcher E-Mail-Adressen ist für Sie als Webseiten-Betreiber allerdings aufwendig – und die Besucher Ihrer Homepage können nicht direkt per Mausklick auf Ihre Kontaktdaten zugreifen.

Findige Entwickler haben daher zahlreiche praktische Alternativen entwickelt, mit denen Sie dieses Problem lösen können. Mithilfe von Programmen wie dem E-Mail-Protector, den Sie im Web unter der Adresse **www.jracademy.com/~jtucek/email/download.php** finden, können Sie E-Mail-Adressen effizient verschlüsseln.

Ein anderer alternativer Lösungsansatz besteht darin, Mailadressen grundsätzlich als Grafiken anzuzeigen und auf Ihrer Webseite einzubinden.



Erst mal schaun, was Google hat Der Suchbegriff „Captchas" fördert so einiges zutage – von animierten Captchas über 3-D-Reliefs bis zu komplexen Integralgleichungen.

Captcha-Codes schützen vor Spambots

Eine beliebte Methode, Formulare auf Webseiten zu schützen, ist die Implementierung sogenannter Captcha-Tests.

„Captcha" ist ein Akronym für „Completely Automated Public Tuning test to tell Computers and Humans Apart" – was so viel bedeutet wie „Vollautomatischer Test, um Rechner und Menschen auseinanderzuhalten". Die Captcha-Tests dienen also dazu, automatisch festzustellen, ob gerade ein Mensch oder ein Bot versucht, das Formular auszufüllen.

Besonders beliebt sind die bildbasierten Captcha-Tests. In einem Bild, das per Zufallsgenerator entstanden ist, wird dabei etwa ein Sicherheitscode angezeigt, den der Benutzer des Formulars eingeben muss, bevor er es abschicken kann. Solche bildbasierten Captchas existieren in unterschiedlichen Varianten und Abwandlungen. Mitunter wird beispielsweise der Versuch unternommen, durch Einfügen eines mehrfarbigen Hintergrunds den Code schwerer lesbar zu machen, oder im Bild wird statt des Codes eine einfache Rechenaufgabe gestellt, deren Lösung das Absenden des Formulars ermöglicht. Auch das Verzerren der Zeichenfolge des Codes innerhalb des Bildes ist eine beliebte Variante.

Captcha-Tests lassen sich relativ einfach in eine Homepage einbinden. Im Internet gibt es dafür zahlreiche vorgefertigte Skripte, zum Beispiel Securimage (**www.neoprogrammers.com**), Recaptcha (**www.captcha.net**) oder auch animierte Captchas (**www.animierte-captcha.de**).

Deutschsprachige Tutorials zum Implementieren von Captchas auf Ihrer Homepage finden Sie etwa unter **www.stoppt-den-spam.info/webmaster/captcha-tutorial/index.html**.

Eines sollten Sie beim Einsatz von Captchas allerdings unbedingt beachten:

Auf Heft-CD

- TinyMCE (PHP/CMS)
- WordPress (PHP/CMS)
- XAMPP (PHP/CMS)

Derartige Schutzmechanismen können die Kontaktformulare auf Ihrer Website niemals absolut abschotten. Die Captchas erschweren potenziellen Angreifern zwar ihr Vorhaben deutlich, dennoch ist es möglich – wenn auch schwieriger –, Captchas mithilfe von automatisierten Texterkennungsroutinen und Bildanalysen auszutricksen. Die Vergangenheit hat bereits mehrfach gezeigt, dass solche Methoden existieren und zum Einsatz kommen. Dennoch sind Captchas eine effiziente Methode, um Massenangriffe abzuwehren.

Gleichzeitig sollten Sie daran denken, dass besonders schwer lesbare Bildcodes automatisierte Angriffe zwar noch unwahrscheinlicher machen, dass gleichzeitig aber die Besucher Ihrer Homepage mit diesen Codes größere Schwierigkeiten haben könnten – sodass sie unter Umständen Ihre Webseite nicht mehr ansteuern werden.

Bilder sind übrigens nicht die einzige Möglichkeit, Captchas zu generieren: Auch automatisch erzeugte Audiodateien lassen sich dazu nutzen.

Formulare mit Weiterleitungs- und Prüffunktion

Zu den typischen Vorgaben eines Webformulars gehört, dass der User auch eine Antwort-Mailadresse angeben muss. Kopien der formulierten Nachricht lassen sich dann direkt an diese Adresse weiterleiten. Zudem sollte die Nachricht auch automatisch an den Mailadministrator weitergeleitet werden, damit dem sofort auffällt, wenn das System massenhaft missbraucht wird.

Abhängig vom Formular haben Sie zudem die Möglichkeit, die neuen Einträge zu überprüfen. Sinnvoll ist es beispielsweise sicherzustellen, dass in der Mailadresse kein korrumpierter Header mit zusätzlichen E-Mail-Adressen angelegt wurde. In Ihrem Kontaktformular können Sie auch einen Filter für unerwünschte Texteingaben einrichten.

Zieladresse vor Änderungen schützen

Im Kontaktformular auf Ihrer Homepage sollten Sie die E-Mail-Adresse möglichst vorgeben, sodass sie sich nicht durch das Ändern eines Werts eines Feldeintrags ändern lässt. Damit ist der Missbrauch der Mailadresse für Spamzwecke weitestgehend ausgeschlossen. Problematischer ist die Möglichkeit des automatischen Sendens der Kontaktmail an die Absender-Mailadresse. Dies ist ein potenzielles Schlupfloch für Spammer. Die Option des Weiterleitens der Kopie sollte der User aus diesem Grund manuell bestätigen – oder es sollte eine gute Plausibilitätsprüfung stattfinden.

KNOW-HOW

Captcha-Elemente festlegen

Grafische Captchas werden durch ein Skript im Webformular in die Seite eingebunden. Durch die Eingabe spezifischer Parameter sorgen Sie für das automatische Anlegen der Grafik für ein Captcha. Im Folgenden sind einige typische Elemente gelistet, die zum Anlegen eines Captchas nötig sind:

- Hintergrundbild für das Captcha
- Innenabstand des Bildes zum Captcha-Rand
- Hintergrundfarbe
- Anzahl der zu generierenden Zeichen
- Schriftart, die für das Anlegen des Captchas genutzt werden soll
- Schriftgröße
- Schriftfarbe

Spammende IP-Adressen abblocken

Das manuelle Blocken von IP-Adressen, von denen ein Angriff auf ein Kontaktformular stattgefunden hat, ist naturgemäß erst nach einem Angriff möglich. Darüber hinaus operieren die Spambots in den meisten Fällen nicht von einzelnen IP-Adressen aus, sondern nutzen zahlreiche gekaperte Rechner. Deshalb ist es in der Regel unmöglich, bestimmte IP-Adressen präventiv zu blocken.

Ist Ihnen allerdings eine solche IP-Adresse bekannt geworden, können Sie sie gezielt aussperren. Wirklich sinnvoll ist an dieser Stelle allerdings eher ein Test, bei dem überprüft wird, ob von einer einzelnen Stelle aus massenhafte Connects erfolgen, die besser geblockt werden sollen.

Das Bearbeiten der Datei robots.txt ist keine Lösung, um Spambots auszusperren, weil diese die darin enthaltenen Anweisungen in den meisten Fällen ignorieren (mehr zur robots.txt lesen Sie ab 90). Einige Spambots gehen auf der Suche nach verwertbaren E-Mail-Adressen allerdings noch dreister vor und benutzen gezielt die ausgeschlossenen Inhalte in der Datei robots.txt, um genau diese akribisch zu untersuchen. Dieses Verhalten können Sie sich wiederum zunutze machen, indem Sie dort einen Honeypot anlegen, um die Spambots anzulocken. Wird auf diesen Honeypot zugegriffen, können Sie die IP-Adresse blocken.

FAZIT: E-Mail-und Kontaktformulare auf Webseiten absolut wasserdicht zu schützen ist nahezu unmöglich. Doch bereits einfache Schutzmaßnahmen können das Missbrauchspotenzial ganz erheblich reduzieren.

Michael Mielewczik

Captcha-Skripte Im Internet finden Sie unzählige vorgefertigte Skripte, mit denen Sie Captchas in Ihre Webseite einbauen können.

So schützen Sie Ihren Weblog

Ein eigenes Web-Tagebuch ist heute schnell eingerichtet. Doch nur wenige Blogger wissen, dass sie sich durch die Veröffentlichung persönlicher Informationen in große Gefahr begeben. So schützen Sie sich vor Cyber-Stalkern.

Auf Heft-CD

- Gallery Constructor (PHP/CMS)
- WordPress (PHP/CMS)
- XAMPP (PHP/CMS)

Ursprünglich wurde der Begriff „Stalking“ nur im Zusammenhang mit Prominenten und ihren allzu aufdringlichen Fans gebraucht. Inzwischen tritt diese Form der Belästigung auch im Bereich der Weblogs massiv auf und entwickelt sich zu einer Form sozialer Gewalt. Grund: Die Hemmschwelle, jemanden im Web zu bedrohen, ist niedrig, denn der Stalker sieht sich nicht mit seinem Opfer konfrontiert.

Cyber-Stalking Wie der Psychoterror aussieht

Ein Blog ist ein Ort, an dem man spontan seine Gedanken, Gefühle, kleinen Geheimnisse oder Hoffnungen veröffentlichen kann. Dieses Online-Tagebuch ist jedoch in den meisten Fällen offen für jeden – zum Lesen, zum Kommentieren und zum Stalken.

Psychische Gewalt per Mausklick verbreiten überwiegend verlassene Partner oder verärgerte Nachbarn und Kollegen. Dazu werden einfach Adressen, Namen, Telefonnummern und E-Mail-Kontakte anonym auf einschlägigen Seiten im Internet veröffentlicht. Dazu kommt noch ein eindeutiger Text oder ein gefälschtes Foto – und schon kann man sicher sein, dass das Opfer sich einem wahren Psychoterror ausgesetzt sieht.

Oftmals schalten die Täter auch gefakte Kontaktanzeigen oder bestellen im Namen der Opfer Waren. Private Blogs werden von den Cyber-Stalkern gern mit obszönen Beiträgen zugemüllt und die Opfer mit E-Mails oder SMS-Nachrichten bedroht. Auf sogenannten Hass-Seiten erscheinen intime Informationen und im schlimmsten Fall sogar Morddrohungen.

Nicht selten gelingt es Blogstalkern sogar, Trojanische Pferde oder andere Schadprogramme auf dem PC ihrer Opfer zu installieren. Damit manipulieren sie Daten oder lesen private E-Mails beziehungsweise vertrauliche Geschäftspost – eine grauenhafte Vorstellung.

So wehren Sie sich Täter ermitteln und anzeigen

Am einfachsten ist es, im eigenen Weblog mit Blogstalkern fertig zu werden. Wenn Ihr Blog für alle offen ist, sollten Sie fremde Beiträge genau prüfen. Bleibt ein Beitrag unter dem üblichen Niveau, werden darin andere Personen beleidigt, oder ist es einfach nur Werbemüll, löschen Sie ihn. Im Wiederholungsfall entziehen Sie dem Autor die Schreiberlaubnis. In den meisten Fällen ist das Problem damit gelöst.

Die Strafverfolgung einer Beleidigung oder Verleumdung in deutschen Foren ist sehr aufwendig. Dennoch gibt es Mittel und Wege, sich gegen Stalking in Fo-

INFO

Blogs, Mailinglisten und Foren zum Thema Cyber-Stalking

Name	Angebot	Adresse	Inhalt
Cyberstalking.at	Infoseiten	www.cyberstalking.at	Belästigungen im Internet und was man dagegen tun kann
CyberStalking.de	Infoseiten, Forum	http://forum.cyberstalking.de	Diskussionsforum, Hilfen
Deutsche Stalking-Opferhilfe (DSOH)	Infoseiten	www.deutsche-stalkingopferhilfe.de	Opferberatung, Tipps gegen Stalking
Fairness Stiftung	Infoseiten	www.fairness-stiftung.de/Stalking.htm	Hinweise, Tipps & Adressen zum Thema Stalking
Jörg Kruses Web	Infoseiten und Forum	www.joergkrusesweb.de/internet/sicherheit	Sicherheit im Internet
Liebeswahn.de	Infoseiten	www.liebeswahn.de	Rat & Tat für Stalking-Opfer
Stalkingforum.de	Forum	www.stalkingforum.de (nur noch Archiv), www.stalking-forum.de (im Aufbau)	Rat & Tat bei Cyber-Stalking
Stalkingpraxis	Infoseiten	www.stalkingpraxis.de	Hinweise rund um das Stalken
Weißer Ring	Infoseiten	www.weisser-ring.de	Hilfe für Opfer krimineller Handlungen

ren zu wehren. Wer Opfer einer solchen Attacke wird, sollte sich sofort an den Forenbetreiber wenden und die Löschung dieser Beiträge verlangen. Häufig führt bereits dieser Schritt zum Erfolg.

Reagiert der Betreiber dagegen nicht, bleibt Ihnen nur der Weg, Anzeige zu erstatten. Gleichzeitig sollten Sie jede weitere Aktion oder Kontaktaufnahme des Stalkers dokumentieren. Da die Verbindungsdaten drei Monate gespeichert werden, besteht die Möglichkeit, den Täter über seine IP-Adresse und den Browser zu überführen.

Finden Stalking-Attacken in deutschen Foren statt, steht auch der Forenbetreiber in der Verantwortung und kann für die Attacken haftbar gemacht werden. Die Provider können außerdem gezwungen werden, IP- und E-Mail-Adressen herauszugeben.

Allerdings: Je besser sich ein Cyber-Stalker mit den technischen Gegebenheiten im Internet auskennt, desto schwieriger wird es, ihn zu erwischen. Aussichtslos wird die Angelegenheit, wenn der Stalker in Blogs oder Foren schreibt, die in der Karibik oder in anderen exotischen Staaten gehostet sind. Mit dem deutschen Rechtssystem ist an dieser Stelle nicht viel auszurichten.

So schützen Sie sich Zehn Tipps für Blogger

Aus dem „Goldfischteich" Internet ist ein „Haifischbecken" geworden. Deshalb sollten Sie unbedingt Ihre Privatsphäre schützen. Blogger erleichtern sich das Leben enorm, wenn sie die folgenden zehn Tipps beachten:

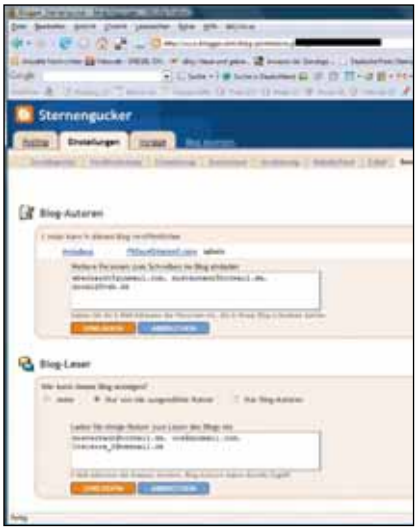
1. Sichern Sie Ihr Blog mit einem Passwort, und teilen Sie dieses niemandem (ohne Ausnahme!) mit. Geben Sie in Ihrem Blog nur ausgewählten Lesern die Möglichkeit, Kommentare oder Beiträge zu schreiben oder Bilder hochzuladen. Verstöße gegen die Blogordnung ahnden Sie mit dem Entzug der Schreiberlaubnis. Setzen Sie eine eigene Blogsoftware ein, und halten Sie diese immer aktuell.

2. Veröffentlichen Sie keine persönlichen Informationen wie Wohnort, Telefonnummer, Schule/Universität oder Mailadresse. Jede noch so kleine Information ist ein Mosaiksteinchen für das Gesamtbild Ihrer Privatsphäre.

3. Füllen Sie ein persönliches Profil niemals vollständig aus. Das sind Informationen, die Stalker besonders gern verwenden. Wählen Sie einen geschlechtsneutralen Benutzernamen.

4. Publizieren Sie nie persönliche Informationen über Freunde oder Bekannte.

5. Lesen Sie jedes Posting genau durch, bevor Sie es veröffentlichen. Streichen Sie alle Stellen, die Rückschlüsse auf Ihr persönliches Umfeld zulassen. Auch Texte, die möglicherweise für Freunde oder Bekannte gefährlich werden können, sollten Sie streichen.



Hausrecht Im eigenen Blog bestimmen Sie, wer dort einen Beitrag oder Kommentar veröffentlichen darf und wer nicht.

6. Veröffentlichen Sie keine persönlichen Fotos in Ihrem Blog.

7. Lassen Sie Ihren Computer nicht ungesichert zurück, während Sie einen Blogartikel schreiben. Andernfalls könnte jemand anderes in Ihrem Namen einen Beitrag verfassen.

8. Werden Sie in einem Forum oder Blog beleidigt oder verleumdet, melden Sie den Vorfall sofort dem Betreiber, und verlangen Sie die Entfernung der Texte oder Bilder. Dokumentieren Sie den Vorfall (Screenshots, Downloads, Ausdrucke etc.), und ziehen Sie rechtliche Schritte in Betracht. Nehmen Sie Kontakt zu einschlägigen Foren, Vereinen oder Selbsthilfegruppen auf.

9. Verbreiten Sie in Ihrem Blog keine Gerüchte, und treten Sie anderen Personen nicht zu nahe.

10. Sind Sie Opfer eines Stalkers geworden, teilen Sie ihm am besten schriftlich und unter Zeugen mit, dass Sie keinen weiteren Kontakt wünschen.

Cyber-Stalker gibt es überall, und oft sind ihre Aktionen nur die Vorstufe zu realen Belästigungen. In Foren, Chats und Organisationen wie dem Weißen Ring erhalten Betroffene Informationen und Unterstützung. Ein besonders reger Erfahrungsaustausch findet auf der Website der Deutschen Stalking-Opferhilfe (DSOH) statt, in der „Selbsthilfegruppe gegen Stalking".

Peter Klau

GLOSSAR

Was Sie über Weblogs wissen sollten

Blog Persönliches Tagebuch, das im Internet veröffentlicht wird. Ein Blog kann aus Nachrichten zu beliebigen Themen und Kommentaren dazu bestehen, aber auch Einträge in Gästebücher, die gern mit Blogspam belegt werden, zählen dazu.

Blogspam Eine Praxis, bei der wahllos Einträge in öffentlichen Blogs, die auch einen Link zu einer Webseite enthalten, manuell oder automatisch mithilfe von Skripten vorgenommen werden.

Blogosphäre (engl. „blogosphere") Die Gesamtheit der Weblogs und ihrer Verbindungen.

Blogroll Eine Liste mit Links zu anderen Weblogs, die die Redaktion oder der Autor des Web-Tagebuchs für besonders lesenswert halten.

Kommentarfunktion Jeder, der seine Mailadresse nennt, kann in einem öffentlichen Blog Kommentare abgeben. Nicht erlaubt sind Kommentare, die zu Werbezwecken eingesetzt werden – etwa um per Kommentar Spam-Werbebotschaften zu veröffentlichen. Selbstverständlich sind in Kommentaren auch keine Äußerungen erlaubt, die Persönlichkeitsrechte verletzen oder gegen Gesetze verstoßen.

Permalink Ein Verweis auf die ständige Internetadresse eines Weblog-Beitrags. Unter dieser Webadresse wird der gesamte Blogbeitrag inklusive aller Kommentare und Zusatzinformationen angezeigt.

Trackback Die Möglichkeit, in einem Weblog einen Hinweis auf einen Beitrag in einem anderen Web-Tagebuch zu hinterlassen.

VBlog Kunstwort aus „Video" und „Blog".

Weblogs Ein anderer Name für Blogs (Akronym aus „Web" und „Logbuch").

Security-Check für Ihre Website

Google weiß oft mehr, als Ihnen lieb sein kann, und liefert auf Nachfrage etwa Links zu vertraulichen Firmenunterlagen. Der Artikel zeigt Ihnen, wie Sie Ihren Webserver auf falsch abgelegte Dokumente testen und gespeicherte Dateien vor Suchmaschinen schützen.

Foto: A. Wiese/Düsseldorf International

Wer im Web etwas sucht, fragt Google. Denn die Suchmaschine aus dem kalifornischen Mountain View besitzt den mit Abstand größten Website-Index, bietet also die besten Chancen für eine erfolgreiche Suche. Doch dieses Wissen zapfen jeden Tag nicht nur Millionen von ehrlichen Internetnutzern an, sondern auch Hacker, die auf der Jagd sind nach geheimen Firmeninformationen. Um zu verstehen, wie Google an vertrauliche Dokumente eines Unternehmens kommt und wie Sie sich davor schützen können, müssen Sie wissen, wie Suchmaschinen arbeiten.

Die meisten Datenbank-Einträge von Suchdiensten wie Google, Microsoft Live Search und Yahoo Search stammen von Spidern oder Crawlern. Dabei handelt es sich um Programme, die automatisch Websites durchsuchen und die gefundenen Informationen in die Datenbank der Suchmaschine aufnehmen. Zu erkennen ist der Besuch eines solchen Crawlers im Weblog. Der Datensammler von Google beispielsweise hinterlässt in der Logdatei Einträge, die mit der Client-Domäne „googlebot.com“ gekennzeichnet sind.

Während man seine Website bei den früheren Webkatalogen anmelden musste, damit der Inhalt indexiert wurde, ist das heute nicht mehr erforderlich. Es genügt, wenn von einer anderen Internet-

präsenz auf die Site verlinkt wird. Denn die Crawler beginnen bei einer Site und arbeiten sich dann Link für Link weiter vor. Alle Webseiten, auf die sie auf diese Weise stoßen, werden automatisch in die zentrale Datenbank aufgenommen. Das ist auch der Grund dafür, warum man über Google so viele Dokumente finden kann, die nicht für das Auge der Öffentlichkeit bestimmt sind, sondern lediglich für den internen Gebrauch im Unternehmen – es genügt, wenn die Dateien aus Versehen auf dem falschen Laufwerk oder Server abgelegt werden. In vielen Fällen kommt noch ein falsch konfigurierter Proxyserver hinzu, über den die Suchmaschine zusätzlich auch auf die internen Daten des Unternehmensintranets zugreifen kann. Dann lässt sich bald das gesamte Wissen der Firma im Internet nachlesen.

In einem ersten Schritt sollten Sie daher überprüfen, welche Informationen Google über Sie, Ihre Website und eventuell auch über Ihre Firma gespeichert hat. Dazu müssen Sie der Suchmaschine einfach in der richtigen Sprache die richtigen Fragen stellen.

Die Befehle Wie Sie Google Fragen stellen

Um die Fähigkeiten von Google voll ausnutzen zu können, müssen Sie eine Reihe spezieller Befehle beherrschen. Dabei handelt es sich um die reguläre Suchsyntax von Google, die Sie direkt in das Suchfenster auf **www.google.de** eingeben können.

- **FILETYPE** Interessante Informationen sind meist nicht auf HTML-Seiten zu finden – die Website-Betreiber achten üblicherweise darauf, dass sie dort keine vertraulichen Daten veröffentlichen. Auf vielen Webservern lagern jedoch versehentlich auch die Dokumente von Büroprogrammen wie Word oder Excel, die Google dann gnadenlos auswertet und die Inhalte in seine Datenbank aufnimmt. Und mit etwas Glück – beziehungsweise Pech, aus Sicht des Website-Besitzers – enthalten diese Dateien Informationen, die das Unternehmen lieber geheim gehalten hätte. Um gezielt nach Files mit Endungen wie .doc, .xls, .ppt oder auch .pdf zu suchen, verwenden Sie den Befehl „filetype“.
- **INTITLE, ALLINTITLE** Falls Sie vermuten, dass der gesuchte Begriff im Titel einer Webseite zu finden ist, verwenden Sie den Befehl „intitle“. Suchen Sie nach mehreren Wörtern, die nebeneinander im Titel stehen sollen, greifen Sie am besten zu „allintitle“. Der Suchstring sieht dann beispielsweise wie folgt aus: „allintitle: Deutschland, Weltmeister, Fußball“. Er findet alle Seiten, bei denen die Begriffe „Deutschland“, „Weltmeister“ und „Fußball“ gleichzeitig im Titel vorkommen – das waren zum Zeitpunkt der Suche im Übrigen mehr als 700.
- **ALLINTEXT** Einen vergleichbaren Befehl wie „allintitle“ gibt es mit „allintext“ für die Suche im Text einer Seite. Er berücksichtigt jedoch nicht die vorhandenen Links und die Titel der Seiten.
- **INURL, ALLINURL** Um den Suchbegriff in den URLs der gespeicherten Websites zu finden, verwenden Sie die Befehle „inurl“ für ein einziges Wort oder „allinurl“ für eine Kombination aus mehreren Begriffen. Mit „allinurl: Urlaub, Schweden“ finden Sie beispielsweise alle Seiten, in deren Adresse die Begriffe „Urlaub“ und „Schweden“ vorkommen.
- **INANCHOR** Jedes Bild auf einer Website kann über HTML und das Anchor-Tag einen beschreibenden Text erhalten. Um in diesen Texten zu suchen, tippen Sie das Kommando „inanchor“ ein.
- **SITE** Wenn Sie nur eine bestimmte Website nach einem Begriff durchforsten wollen, geben Sie den Befehl „site“ ein. Beispiel: Die Beschreibungen der aktuellen CHIP-Sonderhefte auf **www.chip.de** erhalten Sie durch die Eingabe von „Sonderhefte site:www.chip.de“.
- **LINK** Wenn Sie herausfinden wollen, von wo auf Ihre Website verlinkt wird, setzen Sie den Befehl „link“ ein. Mit „link:www.chip.de“ beispielsweise finden Sie alle Sites, die auf die Homepage von CHIP verweisen.

Weitere Infos Google-Syntax perfekt beherrschen

Die genannten Kommandos können Ihnen dabei helfen, Schwachstellen im Sicherheitssystem Ihrer Website zu finden. Der Befehlsumfang von Google ist jedoch noch größer. Eine komplette Liste inklusive Erklärungen finden Sie beispielsweise bei Google Guide unter **www.googleguide.com/advanced_operators_reference.html**.

Eine umfangreiche Website zum Thema Hacken mit Google hat Johnny Long zusammengestellt (**http://johnny.ihackstuff.com/ghdb.php**). Er ist Mitautor des Buchs „Google Hacking“ und hat Beispiele dafür gesammelt, was sich mit Google alles im Netz finden lässt – selbst Benutzernamen und Passwörter kann man mit der Suchmaschine aufspüren.

Übrigens: Da die Anfragen mit den genannten Befehlen vergleichsweise zeitintensiv sind, hat Google die Verwendung eingeschränkt. Sie können daher pro Suchanfrage nur eines dieser Kommandos verwenden, die Befehle lassen sich nicht miteinander kombinieren.

Website-Analyse Noch mehr Tools und Hilfen

Ein guter Ausgangspunkt für die Suche versehentlich freigegebener, vertraulicher Informationen auf Ihrer Website ist der Befehl „site“. Er liefert Ihnen einen ersten Überblick, welche der einzelnen Seiten Ihres Webauftritts überhaupt von Google indiziert wurden. →

Gästebuch In der Logdatei Ihres Webservers können Sie erkennen, ob und wann die verschiedenen Crawler zu Besuch waren.

Das weitere Vorgehen erläutern wir anhand der URL **www.meineseite.de**: Abhängig von der Größe der Webpräsenz und der Anzahl der Einzelseiten kann die Ergebnisliste der Abfrage „site: www.meineseite.de“ sehr umfangreich ausfallen. Die Suche nach sicherheitskritischen Informationen gestaltet sich dann recht schwierig.

Doch es existieren Tools, die Sie bei der Analyse unterstützen. Für Linux-Anwender empfiehlt sich beispielsweise die Software Gooscan (**http://johnny.ihackstuff.com/downloads/task,doc_download/gid,28/**). Bei Windows sieht die Lage leider deutlich schlechter aus. Das Tool Site Digger wird nicht mehr weiterentwickelt. Und die letzte Version, die noch über einige Websites vertrieben wird, setzt einen API-Lizenzschlüssel von Google voraus. Ein solcher Schlüssel wird jedoch bereits seit 2006 nicht mehr vergeben.

Trotzdem gibt es Möglichkeiten, die Google-Abfragen automatisiert durchzuführen. Der Sicherheits-Dienstleister Sensepost (**www.sensepost.com**) bietet mit Wikto eine Software an, die einen eigenen Proxyserver für Google-Lizenzschlüssel zur Verfügung stellt. Das Programm nutzt die bereits erwähnte Datenbank von Johnny Long, um nach Informationen zu suchen. Damit können Sie für Ihre Website auf Knopfdruck alle Abfragen starten, die auch zum Aufbau dieser Datenbank geführt haben.

Falls Sie keinen Schlüssel für die Google-API besitzen, können Sie auch den Proxyserver Aura von Sensepost verwenden. Nach der Installation des Proxys leiten Sie dort die Adresse von localhost (127.0.0.1) auf http://api.google.com um. Das geschieht ganz einfach durch einen Eintrag in der Datei hosts, die Sie im Windows-Verzeichnis auf Ihrer Festplatte im Ordner \system32\drivers\etc“ finden. Vergessen Sie jedoch nicht, nach dem Einsatz von Wikto den Schlüssel wieder umzuändern.

Löcher stopfen Dokumente verschieben und löschen

Sobald Sie Ihre Website auf die beschriebene Weise überprüft haben, können Sie mit dem Bereinigen der Daten beginnen. Falls Google auf Ihrer Site Files indiziert hat, die nicht für die Öffentlichkeit bestimmt sind, sollten Sie sie von Ihrem Webserver entfernen, damit die Links ins Leere laufen.

Außerdem bietet Google ein Tool an, mit dem Sie versehentlich in den Cache der Suchmaschine geratene Seiten manuell entfernen können. Sie finden es auf der Google-Site bei den Informationen für Website-Administratoren (**www.google.de/support/webmasters/bin/answer.py?answer=35301&topic=8459**). Damit Sie Ihre Website nicht immer aufs Neue überprüfen müssen, sollten Sie zum Schluss noch eine Reihe von Sicherheitsmaßnahmen treffen.

Server-Rollen Welche Infos auf welchen Server?

Wenn Sie für Ihr Unternehmen einen eigenen Webserver betreiben, dann sollten Sie seine Rolle klar definieren. Während ein Internetserver seine Informationen potenziell einer unbeschränkten Anzahl von Anwendern im World Wide Web anbietet, besitzt ein Intra- oder Extranetserver lediglich einen limitierten, namentlich bekannten Benutzerkreis. Im Allgemeinen ist es das Ziel, dass Google die Inhalte des Internetservers indiziert, während die Daten auf dem Intranetserver vor der Suchmaschine verborgen bleiben sollen. Um diese Trennung zu realisieren, sollten Sie die Daten streng nach Inhalten geordnet auf physikalisch getrennte Rechner verteilen. Auf keinen Fall dürfen Sie zudem aus dem Internet in die geschlossenen Bereiche verlinken.

Sensible Firmendaten beispielsweise zu den Geschäftszielen dürfen auf keinem dieser beiden Computer gespeichert werden. Denn bereits eine kleine Fehlkonfiguration des unternehmenseigenen Proxyservers kann die Dateien für Google – und damit für die gesamte Welt – sichtbar machen.

Sicherheit Den Webserver vor Angriffen schützen

Wie sich Johnny Longs Datenbank entnehmen lässt, zielen viele Google-Abfragen darauf ab, mehr über einen bestimmten Webserver und die darauf installierten Programme zu erfahren. Sobald der Hacker diese Informationen gefunden hat, kann er die bereits bekannten Sicherheitslücken der Software

Indizierung aufheben Sie können eine Datei oder Website manuell mit den Webmaster-Tools aus dem Google-Index entfernen.

ausnutzen, um sich Zugriff auf den Server zu verschaffen. Dabei profitiert er davon, dass viele Firmen die von den Softwareherstellern bereitgestellten Sicherheitspatches erst mit einiger Verzögerung installieren. Dagegen hilft nur eins: jeden sicherheitskritischen Upgrade sofort einzuspielen.

Natürlich müssen Sie auch bei der Konfiguration des Servers äußerst vorsichtig vorgehen. So ist beispielsweise bei vielen Installationen der Verzeichnisdienst aktiv. Falls dann auf dem Server die Datei index.htm fehlt, landet ein Besucher direkt in der Verzeichnisstruktur und kann lediglich noch durch die Zugriffsrechte daran gehindert werden, die vorhandenen Dateien nach Lust und Laune zu durchstöbern.

Beim Apache-Server deaktivieren Sie den Verzeichnisdienst mit dem Eintrag „Options Indexes FollowSymLinks MultiViews“ in der Datei httpd.conf. Auch bei einem Webhoster können Sie die Funktion normalerweise abschalten. Wie das geht, verrät ein Blick in die FAQs. Notfalls hilft auch eine E-Mail an die Service-Abteilung.

Robots.txt Google muss draußen bleiben

Die Absicherung des Webservers ist allerdings nur der erste Schritt. Als Nächstes steht an, den Webauftritt so weit zu optimieren, dass Google tatsächlich nur noch auf die von Ihnen freigegebenen Seiten zugreifen kann.

Dazu sind gleich mehrere Maßnahmen erforderlich. Als Erstes passen Sie die Datei robots.txt an. Sie regelt, ob und

wie ein Spider oder Crawler Ihre Web-Seiten indizieren darf. Sie legen dieses File im Rootverzeichnis Ihrer Site ab. Achten Sie bei der Definition der Lese- und Schreibrechte auf die Datei darauf, dass der Webserver den Inhalt lesen und auswerten kann.

Gleichzeitig müssen Sie jedoch verhindern, dass ein Crawler Robots.txt indiziert, wodurch der Inhalt später in der Trefferliste von Google auftauchen würde. Dadurch könnten Hacker die Verzeichnisstruktur Ihrer Webpräsenz ermitteln. Damit die Suchmaschinen die robots.txt zwar auslesen, aber nicht in ihre Datenbank aufnehmen, müssen Sie eine entsprechende Regel definieren.

Der genaue Aufbau der Datei und die erlaubten Befehle sind bereits seit 1994 standardisiert. Eine detaillierte Beschreibung finden Sie unter **www.robotstxt.org** oder in einer SelfHTML-Dokumentation (**www.validome.org/doc/HTML_ge/diverses/robots.htm**). Die interne Organisation des Files erfolgt über einige Schlüsselbegriffe:

- **User-agent** gibt an, für welche Crawler die folgenden Befehle gelten sollen.
- **Disallow** schließt ein Verzeichnis, eine Datei oder auch die ganze Seite aus.
- **Allow** erlaubt dem Crawler den Zugriff auf ein bestimmtes Objekt.

Eine robots.txt sieht beispielsweise folgendermaßen aus:

```
# robots.txt zu
http://www.meineseite.de/
User-agent: Googlebot
Disallow: /cms/news/
User-agent: *
Disallow: /neuepraesenz/
Disallow: /tmp/
```

Die erste Befehlssequenz verbietet dem Googlebot die Indizierung des Verzeichnisses /cms/news. Die drei nächsten Zeilen untersagen zusätzlich allen Crawlern den Zugriff auf die Ordner /neuepraesenz und /tmp. Wie Sie sehen, lässt sich ein Verbot oder Gebot auf bestimmte Crawler beschränken oder durch Setzen des Sterns „*“ allgemein gültig machen. Das ist auch schon alles. Ansonsten müssen Sie nur noch wissen, dass alles, was rechts des Zeichens „#“ steht, als Kommentar gilt und von den Crawlern ignoriert wird.

Um also sämtliche Crawler und Spider von einer Website auszusperren, legen Sie eine robots.txt mit diesen beiden Zeilen an:

```
User-agent: *
Disallow: *
```

Falls Sie den Inhalt der robots.txt nicht selber tippen, sondern lieber zusammenklicken wollen, lohnt sich ein Blick auf die PHP-Anwendung robots.txt-Generator auf der Website von Searchcode.de (**www.searchcode.de/robotstxt.php**). Vor allem dann, wenn Sie einige Verzeichnisse lediglich für bestimmte Suchmaschinen zugänglich machen wollen, ist diese Methode schneller als das manuelle Eintippen der Befehlszeilen.

Beim Programm von Searchcode.de stellen Sie die Anweisungen an die Suchmaschinenbots über Auswahlmenüs ein und komponieren so über Dropdown-Listen, Checkboxen und Radio-Buttons Ihre eigene robots.txt. Zum Schluss kopieren Sie das Ergebnis in eine Textdatei, speichern sie unter dem Namen robots.txt und übertragen sie per FTP vom lokalen PC auf Ihren Webserver.

Klicken statt texten
Auf der Seite von Searchcode.de können Sie mit wenigen Klicks Ihre eigene robots.txt zusammenstellen.

Index verhindern Befehle für den HTML-Code

Ob Ihre Webseite indiziert wird oder nicht, können Sie auch über den HTML-Header einstellen. Ob die Crawler der Suchmaschinen die Seite auswerten dürfen, hängt von der Einstellung des Metatags „Robots“ ab. Sie setzen ihn genauso ein wie einen beschreibenden Metatag. Die wichtigsten Optionen heißen dabei NOARCHIVE, NOINDEX, NOFOLLOW und NOSNIPPET.

Wenn sich beispielsweise der Inhalt Ihrer HTML-Seiten häufig ändert – etwa bei einer Newsseite –, dann sollten Sie sich überlegen, sie zumindest aus dem Google-Cache herauszunehmen. Denn oft ist eine Nachricht längst überholt, taucht jedoch immer noch im Cache auf. Eine elegante Lösung für solch einen Fall ist die Indizierung mit der Option „NOARCHIVE“. Damit lassen Sie zwar eine Indizierung zu, verhindern jedoch die Übernahme der Seiteninhalte in den Cache. Der Metatag sieht dann wie folgt aus: <META NAME=“ROBOTS“ CONTENT=“NOARCHIVE“>.

Für den Fall, dass Sie die Crawler komplett von einer Seite aussperren wollen, hilft Ihnen die Kombination aus „NOFOLLOW“ und „NOINDEX“ weiter: <META NAME=“ROBOTS“ CONTENT=“NOINDEX, NOFOLLOW“>. Falls zwar die Seite durchsucht werden soll, nicht jedoch die damit verlinkten Inhalte, lassen Sie einfach den Zusatz „NOINDEX“ weg.

Google bietet in seinen Ergebnislisten jeweils eine kurze Zusammenfassung der Seiteninhalte oder zeigt die beschreibenden Metatags an. Insbesondere bei kostenpflichtigen Inhalten ist das jedoch oftmals nicht erwünscht. Die Indizierung dieser Tags und damit auch die Detailanzeige in der Ergebnisliste schalten Sie mit dem Zusatz „NOSNIPPET“ ein: <META NAME=“ROBOTS“ CONTENT=“NOSNIPPET“>.

Die beschriebenen Tags gelten für alle Crawler. Sie können sie jedoch auch auf bestimmte Suchmaschinen beschränken. Ersetzen Sie dazu den Begriff „ROBOTS“ durch den Namen des Crawlers, also beispielsweise „GOOGLEBOT“ für den Dienst von Google. Anschließend wird der Metatag von den anderen Suchmaschinen ignoriert.

Andreas Hitzig

Hosting-Tarife für Einsteiger & Profis

Die Auswahl an Webhostern in Deutschland ist riesig. CHIP hat für Sie den Markt analysiert und zeigt Ihnen, worauf Sie bei der Auswahl des Providers achten sollten.

Die letzten Wochen waren von den Werbekampagnen der großen Webhoster Strato und 1&1 geprägt, die sich mit neuen Tarifen massiv Konkurrenz machen. Ein Blick unter die Oberfläche zeigt jedoch, dass die Großen nicht immer die besten Tarife bieten und gerade bei den Folgekosten gar nicht mehr so günstig sind.

CHIP hat sich für Sie die Tarife der wichtigsten deutschen Webhoster angesehen – für Einsteiger, Fortgeschrittene und Profis. Ab 95 finden Sie eine große Übersichtstabelle, die Ihnen hilft, den für Ihre Zwecke besten Provider für Ihre Website zu finden. Die Anbieter von kostenlosem Webspace haben wir ebenfalls berücksichtigt (siehe Kasten auf 93).

1&1 Gleich vier Pakete hält 1&1 für Einsteiger bereit. CHIP empfiehlt Homepage-Neulingen das Paket „Homepage Basic“.

Web-Baukästen Hosting für Einsteiger

Am Anfang entscheidet vor allem das richtige Handwerkszeug – denn stundenlang über Büchern zu brüten und in die Tiefen von HTML und JavaScript einzusteigen schreckt viele beim Aufbau eines eigenen Zuhauses im Internet ab. Die großen Provider haben darauf reagiert und bieten den Kunden sogenannte Homepage-Baukästen an. Bei diesen Programmen handelt es sich um sehr vereinfachte Content-Management-Systeme: Sie wählen aus einer Reihe von Vorlagen die ansprechendste aus, entscheiden sich für die passenden Bilder und Farben und geben danach gleich die ersten Texte ein. Dank dieser Hilfestellung stehen Ihre ersten eigenen Webseiten in kürzester Zeit online.

Allerdings lassen sich die Baukastensysteme nur sehr eingeschränkt individuell anpassen, weshalb sie mehr eine Basis für die ersten Versuche im Webdesign sind. Die besten Angebote in diesem Zusammenhang bieten Strato und 1&1, aber auch Goneo kann mit seinen clickStart Pages mithalten.

Besonders die Pakete von Strato und 1&1 zeichneten sich in der Vergangenheit durch interessante, kostenlose Software-Zugaben aus, etwa kommerzielle Programme zum Gestalten von HTML-Seiten und Bearbeiten von Grafiken. Inzwischen ist das Angebot an leistungsfähiger Freeware und Open-Source-Anwendungen jedoch so groß geworden, dass dieses Kaufargument etwas in den Hintergrund gerückt ist. So bietet beispielsweise das Open-Source-Grafikprogramm Gimp jede Menge interessante und professionelle Funktionen für das Bearbeiten von Bildern.

Strato liefert in den vorgestellten Paketen noch Adobe GoLive 9 und Photoshop Elements 5 mit, 1&1 hat seine Pakete vor allem für Einsteiger deutlich abgespeckt.

Ein weiterer wichtiger Aspekt bei der Auswahl des Webhosters ist das Angebot in Sachen E-Mail – und damit verbunden die grafische Oberfläche zum Schreiben und Lesen der Mails von unterwegs. Eine Umleitung auf einen Account bei GMX, web.de oder Google Mail ist zwar meistens möglich, beim Antworten geht jedoch die eigene E-Mail-Adresse meinname@meinedomain.de verloren.

Die meisten Webhoster haben inzwischen auf die Wünsche der Kunden reagiert und liefern in ihren Paketen einen Webclient für E-Mails mit.

Strato Gerade für Einsteiger sind die PowerWeb-Pakete von Strato ideal für einen schnellen Start.

Mit den Einsteigerpaketen kommen die Website-Neulinge schon ganz schön weit, denn nur die wenigsten starten nach kurzer Zeit bereits eigene Datenbank- und PHP-Entwicklungen. Trotz allem sollten Sie – falls Sie dies in Betracht ziehen – darauf achten, dass der Webhoster Ihrer Wahl auch in diesem Segment mit entsprechenden Features aufwarten kann, damit Sie nicht schon nach ein, zwei Jahren mit Ihrer kompletten Webpräsenz umziehen müssen.

In diesem Zusammenhang sollten Sie auch auf die Laufzeiten der Pakete und die Folgekosten für die Zeit nach dem Aktions-Sonderangebot achten. Bei einer Reihe von „Null-Euro-Tarifen“ müssen Sie nach Ablauf der Gratismonate mit hohen Preisen und einer Laufzeit von 24 Monaten rechnen. Wichtig ist auch die Kündigungsfrist, die in der Regel drei Monate beträgt; lassen Sie sie verstreichen, verlängert sich der Vertrag automatisch um ein weiteres Jahr.

Als Einsteiger sollten Sie auch einen Blick auf die Supportkosten werfen – oft genug funktioniert am Anfang nicht alles so, wie es soll, und ein günstiger telefonischer Support bei Problemen hält die Telefonrechnung klein.

CGI-Skripte & mehr Hosting für Fortgeschrittene

Sind Sie bereits stolzer Besitzer einer eigenen Homepage, die allerdings mittlerweile an ihre Leistungsgrenzen stößt, wird Ihr Hauptaugenmerk in Zukunft auf der funktionalen Erweiterung Ihrer Website liegen.

Auch auf diesen Umstand haben zahlreiche Webhoster reagiert: Bereits seit vielen Jahren halten die meisten Provider für diese Zielgruppe vordefinierte CGI-Skripte mit fertigen Funktionalitäten bereit, die Sie mit wenigen Programmzeilen ganz einfach in Ihre Seiten integrieren können. Vom eigenen Gästebuch, Forum oder Weblog sind Sie dann meistens nur noch einen Copy & Paste-Schritt entfernt.

Auch neue Technologien bleiben nicht außen vor – mit gutem Beispiel gehen etwa die Anbieter Strato, 1&1 und 1blu voran und liefern AJAX-Anwendungen zur einfachen Integration mit.

Schwierig ist es erfahrungsgemäß auch, die Homepage aktuell zu halten und den Besuchern immer wieder frische News zu bieten. Eine interessante Unterstützung bei dieser Aufgabe sind die Content-Module von 1&1 – dabei wählen Sie aus einer Sammlung von News die für Ihre Seite passenden aus und lassen sie darstellen. Die Nachrichten werden von 1&1 ständig aktualisiert, sodass Sie Ihren Besuchern immer die neuesten Informationen aus Sport, Politik und der Welt des Showbiz liefern können.

Bei steigender Seitenanzahl Ihrer Homepage sollte auch der Besucherstrom mitwachsen, denn Ihre Website soll schließlich der Außenwelt einige Informationen über Sie oder das Thema, das Sie präsentieren, bieten. Achten Sie bei den Statistiken zu Ihrer Homepage darauf, dass Ihnen der Provider nicht nur die Logdateien zur Verfügung stellt, sondern auch eine grafische Auswertung bietet. Damit sehen Sie gleich online, wie der Traffic auf Ihrer Website über einen bestimmten Zeitraum hinweg ausgefallen ist, ob sie bereits im Fokus der Suchmaschinen steht und welche Informationen bei den Besuchern auf besonderes Interesse gestoßen sind.

Planen Sie den Verkauf eigener Produkte, bietet sich dazu ein vorkonfigurierter Onlineshop an. Viele kleinere Webhoster haben in ihre Pakete die Open-Source-Software OS Commerce integriert, die zwar ein wenig Konfigurationsaufwand erfordert, vom Leistungsumfang her den kommerziellen Shoppaketen aber nur wenig nachsteht.

Strato hatte noch vor etwas mehr als einem Jahr einen Onlineshop in seine Webhosting-Paketen integriert, bietet diesen nun aber als gesondertes Angebot an. Das bringt zwar mehr Flexibilität, verursacht aber auch zusätzliche Kosten. Bei 1&1 bekommen Sie nur einen kleinen Onlineshop mit maximal zehn Artikeln – was lediglich für den Test ausreicht, ob die angebotenen Waren auch ihre Zielgruppe finden.

Sollten Sie also den Aufbau eines größeren Webshops planen, müssen Sie ent- →

INFO

Kostenloser Webspace

Neben den kommerziellen Angeboten hat CHIP auch eine Reihe kostenloser Webhoster für Sie zusammengestellt. Wir haben solche Provider in die Auswahl aufgenommen, die ihr Angebot zeitnah zur Verfügung gestellt haben und eine Datenbank sowie Unterstützung für PHP oder ASP bieten.

Elusive Webspace
PHP-fähiger Webspace mit einer MySQL-Datenbank, unbegrenztem Webspace und Traffic (**www.elusive-hosting.de**)

Ja-Nee.de
PHP-fähiger Webspace mit einer MySQL-Datenbank, 150 MByte kostenlosem Webspace sowie 20 GByte Traffic inklusive (**www.ja-nee.de**)

oHost
PHP-fähiger Webspace mit einer MySQL-Datenbank, 2500 MByte Webspace und unbegrenztem Traffic (**www.ohost.de**)

Pytal
PHP-fähiger Webspace mit einer MySQL-Datenbank, unbegrenztem Webspace und Traffic (**www.pytal.de**)

Uttx.net
Einziges Angebot mit fünf MySQL-Datenbanken, PHP-Unterstützung und 200 MByte Speicherplatz (**www.uttx.net**)

Goneo Der Provider hat sein Angebot schrittweise ausgebaut und bietet nun auch Einsteigern interessante Pakete an.

1blu Provider wie 1blu befriedigen die wachsende Nachfrage nach Shoplösungen mit eigenständigen Angeboten.

weder zu den kostenpflichtigen Zusatzprodukten greifen, die dann auch die Kaufabwicklung per Kreditkarte bieten, oder einiges an Zeit investieren und sich mit kostenlosen Anwendungen wie OS Commerce Ihren eigenen virtuellen Laden aufbauen. 1blu liefert immerhin die Basic-Version des GS ShopBuilder mit – sogar schon im „Homepage"-Paket für Einsteiger.

PHP & MySQL Hosting für Profis

In der abschließenden Rubrik dieser Marktübersicht hat CHIP besonderen Wert darauf gelegt, dass Sie Ihre Webpräsenz flexibel erweitern können. Dazu dient die Unterstützung von PHP ebenso wie die Integration von MySQL-Datenbanken in das Hostingpaket.

Je nach Angebot und erwartetem Besucherstrom kann der Traffic recht schnell beachtliche Zusatzkosten verursachen. Deswegen sollten Sie darauf achten, dass Sie mit Ihrem Tarif entweder eine hohe Freimenge an zu übertragenden Daten bekommen oder der Anbieter von vornherein unlimitierten Datentransfer ohne Mehrkosten zusichert.

Gerade bei beliebten privaten, aber auch bei kommerziellen Websites spielt das Thema Verfügbarkeit der Site – und ebenso die Verfügbarkeit des Supports bei Problemen – eine wichtige Rolle. Ob zu später Stunde oder am Wochenende, Ihr Webhoster sollte jederzeit in der Lage sein, technische Probleme schnell zu lösen. Achten Sie in diesem Zusammenhang auch darauf, dass die entsprechende Hotline kostenlos ist.

Evanzo Der Provider bietet mit rund zwölf Euro Jahresgebühr einen extrem günstigen Einstieg in den Profibereich.

Wichtig ist auch das Thema Backup – achten Sie darauf, dass der Provider Ihrer Wahl Ihre Website nicht nur mindestens alle 24 Stunden sichert, sondern darüber hinaus auch einen einfachen Weg bietet, die gesamte Webpräsenz oder auch nur einzelne Seiten oder die Datenbank wiederherzustellen.

Gerade im Bereich der Hosting-Angebote für Profis gibt es eine Vielzahl von recht preiswerten Angeboten – die Bandbreite reicht an dieser Stelle am unteren Ende von rund zwölf Euro beim Angebot von Evanzo bis hin zu rund 130 Euro bei der Domainfactory. An dieser Stelle gilt es im Einzelfall abzuwägen, wie viel Support Sie benötigen – aber auch, wie viele Gäste Sie auf Ihrer Website erwarten. Ist die Anbindung des Webhosters nicht ausreichend, ist Ihre Internetpräsenz bei starkem Besucherandrang nicht mehr erreichbar – ein typisches Bild zum Beispiel bei beliebten Foren in den Abendstunden.

Ja-Nee.de Zum Experimentieren reicht fürs Erste auch ein kostenloses Hostingangebot, etwa das von Ja-Nee.de.

FAZIT CHIP hat Ihnen in dieser Marktübersicht einige Entscheidungshilfen für die Auswahl des richtigen Webhosters an die Hand gegeben. Lassen Sie sich nicht von auf den ersten Blick kostenlosen Angeboten und riesigen Softwarepaketen blenden. Achten Sie stattdessen lieber auf die Folgekosten – auch Pakete, die nach Flexibilität aussehen wie die Dynamix-Angebote von Strato, haben im eigenen Haus günstigere Alternativen mit gleichen Leistungsmerkmalen.

Ein kleinerer Anbieter muss nicht unbedingt schlechter sein, denn dort bekommen Sie oft mehr für Ihr Geld: Der Trend geht an dieser Stelle stark zu vorinstallierten Open-Source-Anwendungen, die Sie ohne Vorkenntnisse selbst aktivieren und nutzen können. Im Bereich Content Management ebenso wie beim eigenen Webshop bieten Open-Source-Programme wie Joomla oder OS Commerce interessante Alternativen. Auf den folgenden Seiten finden Sie eine detaillierte tabellarische Übersicht der besten Tarife für Einsteiger, Fortgeschrittene und Profis der führenden deutschen Webhoster.

Wenn Sie sich noch nicht sicher sind, was Sie alles benötigen, und erst einmal ein wenig experimentieren wollen, lohnt sich ein Blick in den Infokasten „Kostenloser Webspace" auf 93. Bei diesen Angeboten müssen Sie zwar meistens auf eine eigene Domain verzichten und teilweise Werbeeinblendungen hinnehmen, dafür haben Sie genug Speicherplatz und die richtige technische Ausstattung wie PHP und MySQL-Datenbanken, um ausgiebig den Einstieg in die eigene Website vorzubereiten.

Andreas Hitzig

TARIFE DER WICHTIGSTEN WEBHOSTER

Einsteiger

Anbieter	Strato	1&1	Lycos	Evanzo	goneo	Host Europe	Server4you	Domainfactory	Hetzner	1blu
URL	www.strato.de	www.1und1.info	www.lycos.de	www.evanzo.de	www.goneo.de	www.hosteurope.de	www.server4you.de	www.df.eu	www.hetzner.de	www.1blu.de
Domain										
Paketname	PowerWeb Basic	1&1 Homepage Basic	Active	Starter S	Homepage Start	Web Pack S 2.0	Racer Go X2	MyHome S	SH 200	Homepage
Anzahl Domains (de)	3	1	1	1	2	1	2	1	1	1
Speicherplatz	500 MByte	300 MByte	1000 MByte	1 GByte	500 MByte	100 MByte	400 MByte	100 MByte	1 GByte	40 MByte
Enthaltener Traffic	50 GByte	30 GByte	10 GByte	Kein Limit	Kein Limit	25 GByte	75 GByte	Kein Limit	10 GByte	8 GByte
FTP-Zugang	●	●	●	●	●	●	●	●	●	●
Messaging										
POP3-Postfächer	100	30	100	100	100	25	100	Kein Limit	25	25
Anti-Spam	●	●	–	●	●	●	–	●	●	●
UMS	●	●	–	–	–	–	–	–	–	–
SMS/Fax	50 gratis/Monat, jede weitere SMS 0,10 €, MMS 0,30 € jedes weitere Fax 0,20 €	0,19 € je SMS	–	–	–	– / optional	–	0,10 € je SMS	–	–
Webclient	●	●	●	●	●	●	●	●	●	●
Weitere Funktionen										
Onlineshop	– [1]	–	–	●	● (OS Commerce)	–	● (OS Commerce)	–	–	GS Shop Builder Basic
CGI-Baukasten	●	●	●	Eigene Skripte nutzbar	Eigene Skripte nutzbar	●	●	●	●	–
FrontPage-Erweiterung	●	–	●	–	–	–	–	–	–	–
Weitere Funktionen	EasyVideo, 10 Seiten LivePages, 10 Seiten Mobile-Pages, Weblog, Fotoalbum	5 Seiten 1&1 Homepage-Baukasten, Blog, Fotoalbum	1Click!site, Easy WebBuilder, PHP4, PHP5, MySQL, FrontPage-Erweiterung, 50 € Google AdWords Gutschein, Toolbar Builder, Gästebuch	FlashSite Builder Light	clickStart-Anwendungen, easyPages	Webstatistik, tägliche Datensicherung, SSL-Proxy, SSI, Homepage-Baukasten	30 Seiten Homepage-Baukasten, WAP, ausführliche Statistiken, WebFTP, Blog	SSL, Backup, Statistiken, Weblog, Gästebuch, Benutzerzähler	Tägliches Backup	–
ClipArts	●	●	–	–	●	–	●	–	–	–
Enthaltene Software	Steganos Internet Security Special Edition Entry 2007, Adobe GoLive 9, Adobe PhotoShop Elements 5, diverse andere Programme	Ulead GIF Animator 5, diverse weitere Programme	–	62 vorinstallierte Open-Source- und Freeware-Programme wie Typo3, Mambo oder phpBB	Mehr als 20 vorinstallierte Open-Source- und Freeware-Programme	DokuWiki, CMS Light und andere Software	–	–	–	1blu Homepage Builder, GS Shop Builder Basic
Kosten										
Einrichtungsgebühr	14,90 €	9,60 €	–	–	4,95 €	14,99 €	–	4,95 €	9,90 €	16,90 €
Preis / Jahr	47,88 €	35,88 €	83,40 €	11,88 €	7,50 €	7,88 €	46,80 €	13,80 €	23,88 €	10,80 €
Gesamtpreis 1. Jahr	62,78 €	45,48 €	83,40 €	11,88 €	12,45 €	32,87 €	46,80 €	18,75 €	33,78 €	27,70 €
Mindestlaufzeit	6 Monate	24 Monate	12 Monate	12 Monate	12 Monate	12 Monate	12 Monate	12 Monate	30 Tage	12 Monate
Aktionsrabatt		2,99 € / Monat im 1.Jahr, 3,99 € ab dem Folgejahr	Keine Einrichtungsgebühr	–	Erste 6 Monate kostenlos	–	Alternativ die ersten 333 Tage kostenlos bei 24 Monaten Laufzeit	–	–	–

→

● = Ja – = Nein

[1] Separates Angebot Onlineshops zusätzlich buchbar

TARIFE DER WICHTIGSTEN WEBHOSTER

Fortgeschrittene

Anbieter	Strato	1&1	Lycos	Evanzo	goneo	Host Europe	Server4you	Domainfactory	Hetzner	1blu
URL	www.strato.de	www.1und1.info	www.lycos.de	www.evanzo.de	www.goneo.de	www.hosteurope.de	www.server4you.de	www.df.eu	www.hetzner.de	www.1blu.de
Domain										
Paketname	PowerWeb Basic	1&1 Homepage Perfect	Active	Starter S	Homepage Start	WebPack S 2.0	Racer Go X2	MyHome S	SH 200	Homepage Professional
Anzahl Domains (de)	3	2	1	1	2	1	2	1	1	3
Speicherplatz	500 MByte	500 MByte	1000 MByte	1 GByte	500 MByte	100 MByte	400 MByte	100 MByte	1 GByte	650 MByte
Enthaltener Traffic	50 GByte	50 GByte	10 GByte	Kein Limit	Kein Limit	25 GByte	75 GByte	Kein Limit	10 GByte	40 GByte
FTP-Zugang	●	●	●	●	●	●	●	●	●	●
Messaging										
POP3-Postfächer	100	100	100	100	100	25	100	Kein Limit	25	200
Anti-Spam	●	●	–	●	●	●	–	●	●	●
UMS	●	●	–	–	–	–	–	–	–	–
SMS/Fax	50 gratis/Monat, jede weitere SMS 0,10 €, MMS 0,30 € jedes weitere Fax 0,20 €	0,19 € je SMS	–	–	–	–	–	0,10 € je SMS	–	–
Webclient	●	●	●	●	●	●	●	●	●	●
Weitere Funktionen										
Onlineshop	– [1]	●	–	●	● (OS Commerce)	–	● (OS Commerce)	–	–	GS Shop Builder Basic
CGI-Baukasten	●	●	●	Eigene Skripte nutzbar	Eigene Skripte nutzbar	●	●	●	●	Eigene Skripte nutzbar
FrontPage-Erweiterung	●	–	●	–	–	–	–	–	–	–
Weitere Funktionen	EasyVideo, 10 Seiten LivePages, 10 Seiten MobilePages, Weblog, Fotoalbum	10 Seiten 1&1 Homepage-Baukasten	1Click!site, Easy Web Builder, PHP4, PHP5, MySQL, FrontPage-Erweiterung, 50 € Google AdWords Gutschein, Toolbar Builder, Gästebuch	FlashSite Builder Light	clickStart-Anwendungen, easyPages	Webstatistik, tägliche Datensicherung, SSL-Proxy, SSI, Homepage-Baukasten	30 Seiten Homepage-Baukasten, WAP, ausführliche Statistiken, WebFTP, Blog	SSL, Backup, Statistiken, Weblog, Gästebuch, Benutzerzähler	Tägliches Backup	PHP4, PHP5, MySQL-Datenbank, AJAX-Skripte
ClipArts	●	●	–	–	●	–	●	–	–	–
Enthaltene Software	Steganos Internet Security Special Edition Entry 2007, Adobe GoLive 9, Adobe PhotoShop Elements 5, diverse andere Programme	Macromedia Contribute 3+, Ulead GIF Animator 5, diverse weitere Programme	–	62 vorinstallierte Open-Source- und Freeware-Programme wie Typo3, Mambo oder phpBB	Mehr als 20 vorinstallierte Open-Source- und Freeware-Programme	DokuWiki, CMS Light und andere Software	–	–	–	Namo Free-Motion 2006, Namo Web Editor 2006, 1blu-HomepageBuilder, diverse vorinstallierte Open-Source-Programme
Kosten										
Einrichtungsgebühr	14,90 €	9,60 €	–	–	4,95 €	14,99 €	–	4,95 €	9,90 €	16,90 €
Preis / Jahr	47,88 €	59,88 €	83,40 €	11,88 €	7,50 €	17,88 €	46,80 €	13,80 €	23,88 €	58,80 €
Preis im 1. Jahr	62,78 €	69,48 €	83,40 €	11,88 €	12,45 €	32,87 €	46,80 €	18,75 €	33,78 €	75,70 €
Mindestlaufzeit	6 Monate	24 Monate	12 Monate	12 Monate	12 Monate	12 Monate	12 Monate	12 Monate	30 Tage	6 Monate
Aktionsrabatt		4,99 € / Monat im 1. Jahr, 6,99 € / Monat im 2. Jahr	Keine Einrichtungsgebühr	–	Erste 6 Monate kostenlos	–	Alternativ die ersten 333 Tage kostenlos bei 24 Monaten Laufzeit	–	–	–

● = Ja – = Nein

[1] Zusätzlich buchbar, nicht integriert

TARIFE DER WICHTIGSTEN WEBHOSTER

Profis

Anbieter	Strato	1&1	Lycos	Evanzo	goneo	Host Europe	Server4you	Domainfactory	Hetzner	1blu
URL	www.strato.de	www.1und1.info	www.lycos.de	www.evanzo.de	www.goneo.de	www.hosteurope.de	www.server4you.de	www.df.eu	www.hetzner.de	www.1blu.de
Domain										
Paketname	PowerWeb Basic	1&1 Homepage Business	Active	Starter S	Homepage Plus	WebPack M 2.0	Racer Pro	Managed Hosting S	SH 500	Homepage Professional
Anzahl Domains (de)	3	3	1	1	3	1	3	10	1	3
Speicherplatz	500 MByte	1000 MByte	1000 MByte	1 GByte	1000 MByte	200 MByte	1000 MByte	1 GByte	2 GByte	650 MByte
Enthaltener Traffic	50 GByte	75 GByte	10 GByte	Kein Limit	Kein Limit	50 GByte	150 GByte	100 GByte	20 GByte	40 GByte
FTP-Zugang	●	●	●	●	●	●	●	●	●	●
Messaging										
POP3-Postfächer	100	250	100	100	200	50	500	Kein Limit	50	200
Anti-Spam	●	●	–	●	●	●	–	●	●	●
UMS	●	●	–	–	–	–	–	–	–	–
SMS/Fax	50 gratis/Monat, jede weitere SMS 0,10 €, MMS 0,30 € jedes weitere Fax 0,20 €	0,19 € pro SMS	–	–	–	–	–	SMS: 0,10 € je SMS	–	–
Webclient	●	●	●	●	●	●	●	●	●	●
Weitere Funktionen										
MySQL-Datenbank	1	3	1	1	2	1	3	1	1	2
PHP4	●	●	●	●	●	●	●	●	●	●
PHP5	●	●	●	–	●	●	–	●	●	●
Perl	●	●	–	●	●	●	●	●	●	●
SSI	●	●	●	●	●	●	●	●	●	–
Web-Statistiken	●	●	●	●	●	●	●	●	●	●
Online-Shop	– [1]	●	–	● (Open Source)	● (Open Source)	–	● (OS Commerce)	● (OS Commerce)	–	GS Shop Builder Basic
CGI-Baukasten	●	●	●	–	Bedingt	●	●	●	●	Eigene Skripte einsetzbar
ClipArts	●	●	–	–	●	–	●	–	–	–
FrontPage-Erweiterung	–	●	●	–	–	–	●	–	–	–
Weitere Funktionen	EasyVideo, 10 Seiten LivePages, 10 Seiten MobilePages, Weblog, Fotoalbum	1&1 Homepage-Baukasten, 1&1 DynamicSite Creator, 1&1 Blog, 1&1 Content-Module, PDF-Website Generator, diverse Guthaben bei Werbecentern	50 € Gutschein AdSense, unbegrenzte Subdomains	FlashSite Builder Light	clickStart-Anwendungen, easyPages	Python, Ruby, TCL, WAP-MIMES, tägliche Datensicherung, Backup on the fly	WAP, Mailinglisten, Homepage-Baukasten mit 60 Seiten, Blog	Cronjobs, DB-Backup	Typo3, tägliches Backup	AJAX-Skripte
Enthaltene Software	Steganos Internet Security Special Edition Entry 2007, Adobe GoLive 9, Adobe PhotoShop Elements 5, div. andere Programme	Macromedia Contribute 3, Photoshop Elements 5, Ulead GIF Animator 5, diverse andere Programme	–	62 vorinstallierte Open-Source- und Freeware-Programme wie Typo3, Mambo oder phpBB	Mehr als 20 vorinstallierte Open-Source-und Freeware-Programme	WordPress Weblog, phpBB Forum, MySQLDumper, DokuWiki, Fotoalbum und andere Anwendungen	–	Diverse vorinstallierte Open-Source-Systeme wie Mambo, phpBB, DokuWiki	–	Namo Free-Motion 2006, Namo WebEditor 2006, 1blu-Homepage-Builder, div. vorinstallierte Open-Source-Programme
Kosten										
Einrichtungsgebühr	14,90 €	14,90 €	–	–	–	14,99 €	–	9,95 €	9,90 €	16,90 €
Preis / Jahr	47,88 €	119,88 €	83,40 €	11,88 €	14,70 €	41,88 €	106,80 €	119,40 €	59,88 €	58,80 €
Preis im 1. Jahr	62,78 €	134,78 €	83,40 €	11,88 €	14,70 €	56,87 €	106,80 €	129,35 €	69,78 €	75,70 €
Mindestlaufzeit	6 Monate	24 Monate	12 Monate	12 Monate	12 Monate	12 Monate	12 Monate	6 Monate	30 Tage	6 Monate
Aktionsrabatt	–	9,99 € / Monat im 1. Jahr, 14,99 € / Monat im2. Jahr	Keine Einrichtungsgebühr	–	Erste 6 Monate kostenlos	–	Altern. bei einer Laufzeit von 24 Monaten erste 333 Tage kostenlos	–	–	–

● = Ja – = Nein

[1] Zusätzlich buchbar, nicht integriert

Das nächste CHIP-Sonderheft

Ab 3. März

Alles über Online-Poker

Poker – speziell das Pokern im Internet – boomt weiter ohnegleichen. CHIP nimmt Sie mit in die Welt der virtuellen Spielkarten.

→ **Test: Die größten Pokerräume**
CHIP testet die größten Anbieter auf Herz und Nieren und sagt Ihnen, wo Sie am besten und sichersten zocken.

→ **Online-Poker vs. Live-Tisch**
CHIP erklärt Ihnen die wichtigsten Unterschiede und zeigt, wie Sie Ihre Gegner auch vor dem Monitor richtig taxieren.

→ **Sicher pokern im Internet**
CHIP zeigt, was die Anbieter gegen Betrügereien unternehmen und welche Zahlungssysteme wirklich sicher sind.

→ **Gewinnen ohne Risiko**
CHIP präsentiert die besten Freeroll- und Bonus-Angebote – für alle, die ohne eigenen Einsatz Geld gewinnen wollen.

Foto: iStockphoto

Impressum

Redaktionsleiter Sonderhefte: Andreas Vogelsang (verantwortlich für den Inhalt)
Redaktion: Manuel Schreiber
Freie Mitarbeiter: Isolde Durchholz, Roland Freist
Autoren dieser Ausgabe: Stephan Goldmann, Andreas Hentschel, Andreas Hitzig, Fabian von Keudell, Peter Klau, Markus Mandau, Michael Mielewczik, Michael Röhrs-Sperber, Valentin Pletzer, Markus Schraudolph
Leserservice CHIP-Sonderhefte: sonderhefte@chip.de
Grafische Gestaltung: Isabella Schillert (CvD), Steffi Schönberger (Titel, Grafikleitung)
Bildagentur/Syndication: Sabrina Stange (Projektmanagerin), Calina Amann, Tel. (089) 746 42-150, www.chipimages.de
EBV: Jürgen Bisch, Gisela Zach
Bildredaktion: Gertraud Janas-Wenger, Gabi Koller
Leitung Hardware & Testcenter: Dr. Ingo Kuss (Ltg.), Josef Reitberger (Stellv.)
Testcenter: Klaus Baasch, Werner Gaschar, Martin Jäger, Torsten Neumann
CHIP-CD/-DVD: Anja Laubstein (Ltg.); Bastian Stein (Projektmanager), Kresimir Dulić (CD-/DVD-Producer)
Verlagsleiter CHIP-Sonderhefte: Jürgen Hiller
Anzeigenleitung CHIP-Sonderhefte: Anke Huber (verantwortlich für den Anzeigenteil)
Herstellung: Dieter Eichelmann, Verlags-Herstellung, Vogel Services GmbH, D-97082 Würzburg
Verlag: CHIP Communications GmbH, Poccistraße 11, D-80336 München, Tel. (089) 746 42-0, Fax: (089) 74 60 56-0
Die Inhaber- und Beteiligungsverhältnisse lauten: Alleinige Gesellschafterin ist die CHIP Holding GmbH mit Sitz in Poccistraße 11, D-80336 München
Geschäftsführer: Dr. Jan-Gisbert Schultze, Thomas Pyczak
Anzeigenverkauf:
PLZ 0, 1, 2, 3:
Key Account Manager: Paul Schlier, Tel. (04642) 96 54 99, Fax (04642) 96 51 86
Mediaberaterin: Eyke Szopieray, Tel. (04642) 96 51 85, Fax (04642) 96 51 86
PLZ 4, 5, 6:
Key Account Manager: Hartmut Wendt, Tel. (089) 746 42-392, Fax -325,
Mediaberater: Alto Mair, Tel. (089) 746 42-197, Fax -325
PLZ 7, 8, 9:
Key Account Managerin: Katharina Dursch, Tel. (089) 746 42-116, Fax -325,
Mediaberater: Marcel Pelders, Tel. (089) 746 42-526, Fax -325
Zentrale Anzeigenverwaltung und Disposition: Linda Anders, Tel. (089) 746 42-529, Fax -300
Sabine Maurer, Tel. (089) 746 42-252, Fax -300
E-Mail: anzeigen@chip.de
Leiter Direktmarketing: Patrik Holtz
Vertrieb Einzelverkauf: Burda Medien Vertriebs GmbH, Arabellastraße 23, D-81925 München
Digitale Druckvorlagenherstellung: Vogel Services GmbH, D-97082 Würzburg
Druck: Vogel Druck und Medienservice GmbH, D-97204 Höchberg