Ad- und Spyware auf Ihrem Rechner

VERSEUCHTE FREEWARE

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

Von **Arne Arnold**

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

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

Außerdem gibt's jede Menge Abzocker-Programme, die vorgeben, das System kostenlos zu schützen, in Wirklichkeit aber den Anwender dazu erpressen, eine kostenpflichtige Version zu kaufen. Dass die keinen nennenswerten Nutzen hat, erfährt der Anwender nicht. Wir berichten über den aktuellen Stand bei werbefinanzierter Freeware, Ad- und Spyware sowie allen anderen potenziell unerwünschten Modulen. Und natürlich erfahren Sie auch, wie Sie sich vor den Gefahren schützen können.

Verseuchte Freeware

Infektion erwünscht

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

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

Foto: © fotolia

fen sie sich auf 5,8 Millionen Dollar, im Jahr davor auf nur 2,4 Millionen. Den Report können Sie über **www.pcwelt.de/a3e** als PDF-Datei (55 KB) herunterladen.

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

Toolbars: Verseuchung geduldet

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

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

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

Gerade die Google-Toolbar steht aber in der Kritik von Datenschützern. Wer hier Funktionen wie Page Rank, Rechtschreibprüfung, Auto Link oder Wort-Übersetzung

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

aktiviert, erklärt sich damit einverstanden, dass sein Surfverhalten an Google übermittelt wird.

Unsere Meinung: Man kann Google zugute halten, dass der Konzern viel darüber verrät, was er speichert. Infos finden sich

„Viele Anwender fürchten Googles Datenmacht und meiden seine Toolbar“

etwa auf der Datenschutzseite zur Toolbar (über **www.pcwelt.de/3dd**) und seit November 2007 auch als Video-Channel auf Youtube (**www.youtube.com/googleprivacy**). Trotzdem schätzen viele Anwender Googles Datenmacht und -sammlung als gefährlich ein und meiden die Toolbar.

Ad- & Spyware: Unerwünscht

Die Grenze zwischen nützlicher Such-Toolbar und spionierendem Browser-Plug-in ist unscharf. Nur für Anwender, die lieber nicht verraten wollen, welche Websites sie besuchen, ist die Grenze klar: Toolbars von Suchmaschinen selbst sind meist noch akzeptabel, fast alle anderen Plug-ins mit Sucheingabe sind es nicht.

Beispiel Zango-Toolbar: Diese Toolbar kommt ebenfalls huckepack mit anderer Software. Diese wird teilweise recht aggressiv per Werbe-Pop-up angeboten, wie die Bilderserie auf Seite 82 zeigt.

Wer sich die Zango-Toolbar installiert, bekommt Pop-ups angezeigt, die laut Zango auf die Suchbegriffe des Anwenders abgestimmt sind. Zumindest macht der Hersteller kein Geheimnis aus seiner Datensammelwut. Auf der Website erklärt er potenziellen Werbekunden, wie das System funktioniert (siehe letzte Abbildung der Bilderserie Seite 82).

Badware: Je beliebter eine Freeware ist, umso interessanter ist sie für Programmierer von Werbemodulen. Und wenn die Freeware-Macher auch noch bereit sind, solche Module einzubauen, dann gibt's das Tool oft in mehreren verseuchten Versionen. Stopbadware.org, eine Organisation einer Universität und mehrerer Firmen, hat es sich zur Aufgabe gemacht, verseuchte Freeware zu finden (**www.stopbadware.org**).

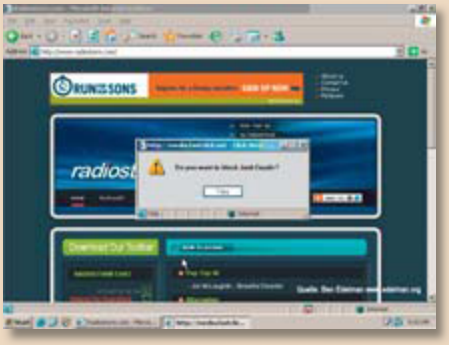
CD DVD IM ÜBERBLICK Kostenlose Schutz-Tools

Programm	Kategorie	Windows	Internet (Download)	Seite
◉ **Ad-Aware 2007 Free 7.0.2** [1) 2)]	Ad- und Spyware-Jäger	2000, XP, Vista	**www.lavasoft.de** (19 MB)	–
◉ **Antivir PE Classic 7.0** [1)]	Antiviren-Programm	2000, XP, Vista	**www.free-av.de** (17 MB)	–
◉ **McAfee Siteadvisor 2.5**	Website-Analyse	98/ME, 2000, XP, Vista	**www.siteadvisor.com** (1,7 MB)	86
Moka 5 1.0 [1) 2)]	virtueller PC	XP	**www.moka5.com** (45 MB)	87
Netcraft Toolbar 1.1 [2)]	Website-Analyse	2000, XP, Vista	**http://toolbar.netcraft.com** (3 MB)	86
◉ **Spybybot Search & Destroy 1.5.1** [1)]	Ad- und Spyware-Jäger	98/ME, 2000, XP, Vista	**www.spybot.info/de** (7 MB)	–
Windows Defender 1.5	Ad- und Spyware-Jäger	XP	**www.pcwelt.de/3d8** (5 MB)	–
◉ **WISO Internet Security** [3)]	PC-Sicherheitspaket	2000, XP, Vista	**www.buhl.de** (35 MB)	–

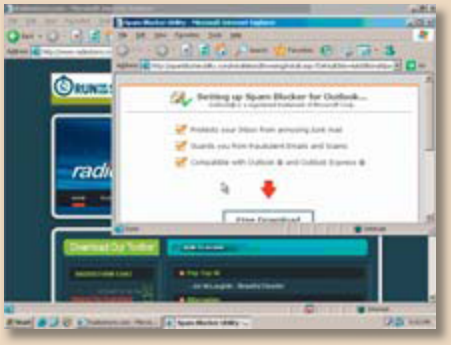
◉ auf CD/DVD und unter **www.pcwelt.de** 1) gratis für private Nutzung 2) englischsprachig 3) 180-Tage-Testversion auf CD/DVD, Vollversion 39,95 Euro

›

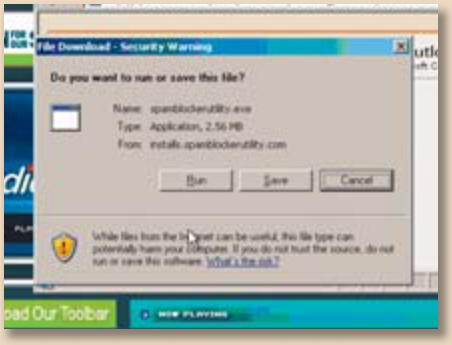
Serie 1: Neugierige Toolbar kommt huckepack mit einer Freeware



Schritt 1: Ein Werbe-Pop-up für einen Spamblocker soll zum Klicken verführen

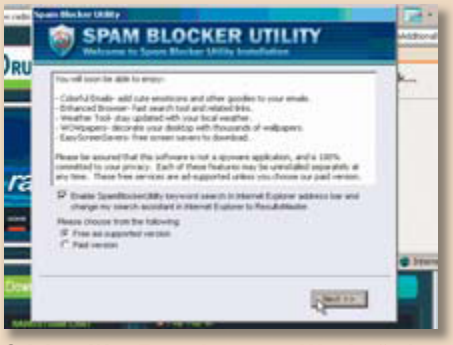


Schritt 2: Wer auf das Pop-up klickt, landet auf der Download-Site für den Spamblocker



Schritt 3: Das standardmäßige Download-Fenster des Browsers wird angezeigt

Schritt 4: Nach dem Start der Installationsdatei erscheinen sogar Lizenzbedingungen



Schritt 5: Wer „Free ad-supported Version“ mit „Next“ bestätigt, bekommt die Zango-Toolbar

Geschäftsmodell: Der Adware-Hersteller Zango erklärt hier, wie sein „Dienst“ funktioniert

Als verseucht (also Badware) gilt für die Organisation jedes Programm, das auf dem PC des Anwenders Dinge macht, die der Anwender nicht wünscht. Der Begriff Badware umfasst damit Ad- und Spyware, aber auch noch weitere nervige Programme. Die Organisation veröffentlicht eine Liste mit Programmen, die sie als Badware einstuft.

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

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

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

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

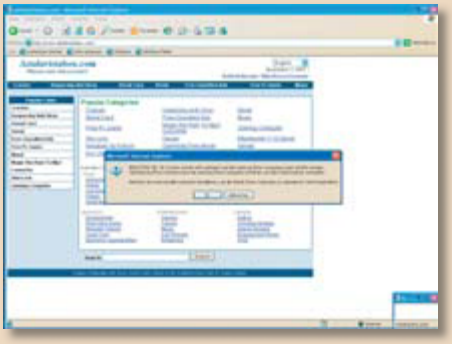
Betrugs-Software

Tuning-Software zockt Sie ab

Im Jahr 2007 tauchten extrem viele Betrugsprogramme (Crimeware) auf. Das sind Tools, die versuchen dem Anwender unter Vorspiegelung falscher Tatsachen das Geld aus der Tasche zu ziehen. Die Betrüger probieren das etwa mit vorgeblicher Tuning-Software. Wie das genau abläuft, zeigt unsere Bilderstrecke auf Seite 84.

Schritt 1: Beim Surfen erscheint ein Pop-up, das einer Windows-Systemmeldung äh-

Serie 2: Ein angebliches Gratis-Tuning-Tool erpresst zum Kauf einer Vollversion



Schritt 1: Ein Pop-up empfiehlt, das System zwecks Optimierung untersuchen zu lassen

Schritt 2: Wer geklickt hat, landet auf der Site eines vorgeblichen Optimierungs-Tools

Schritt 3: Anschließend kommt ein Pop-up, das auf ein folgendes Download-Fenster hinweist

Schritt 4: Nach dem Download gibt's einen Installer – sogar mit Geschäftsbedingungen

Schritt 5: Das Tuning-Tool findet angeblich schwere Systemfehler

Schritt 6: Wer die Fehler reparieren lassen will, landet bei einem Kaufformular

nelt. Darin wird behauptet, dass Ihr System nicht optimiert sei und sich die Leistung Ihres PCs erhöhen lasse. Es wird vorgeschlagen, kostenlos ein Tool zu installieren.

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

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

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

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

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

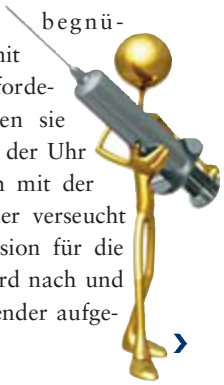
Sicherheits-Tool erpresst Sie

Die Masche mit der Tuning-Software (oben) gibt's auch mit Sicherheits-Software. Hier ist der Druck auf den Anwender sogar noch um einiges höher. Denn die angeblichen Antispyware- oder Antiviren-Programme behaupten, sie hätten schädlichen Code auf dem PC gefunden. Den Verlauf dieser Abzocke sehen Sie in der Bilderserie auf Seite 86.

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

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

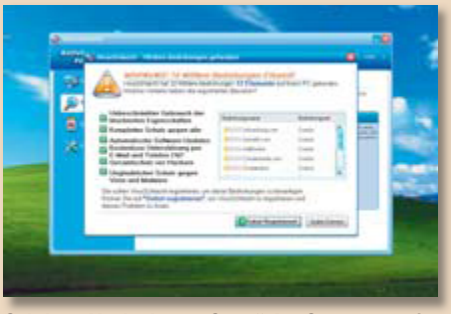
Einige der Programme begnügen sich übrigens nicht mit der einmaligen Kauf-Aufforderung. Stattdessen platzieren sie sich im Infobereich neben der Uhr und melden sich stündlich mit der Warnung, dass der Rechner verseucht und der Kauf der Vollversion für die Reinigung nötig sei. So wird nach und nach Druck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



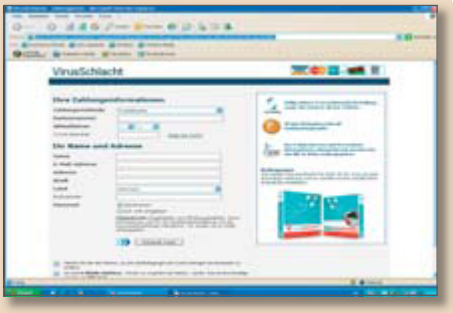
Serie 3: Eine angebliche Gratis-Antiviren-Software erpresst zum Kauf der Vollversion

Schritt 1: Ein Pop-up empfiehlt, den PC nach Viren durchsuchen zu lassen

Schritt 2: Wer geklickt hat, landet auf der Website eines vorgeblichen Antiviren-Tools



Schritt 3: Nach einem „Scan“ des Systems stuft das Tool Cookies als mittlere Bedrohung ein



Schritt 4: Wer die Bedrohung beseitigen will, muss die Vollversion kaufen – für 40 Euro

Betrug erkennen

Richtig installieren & Filter einsetzen

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

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

Betrüger oder schlechtes Programm

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

Internet: Google-Fundstellen checken

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

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

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

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

Infektion vermeiden

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

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