



# Achtung, Virenbefall

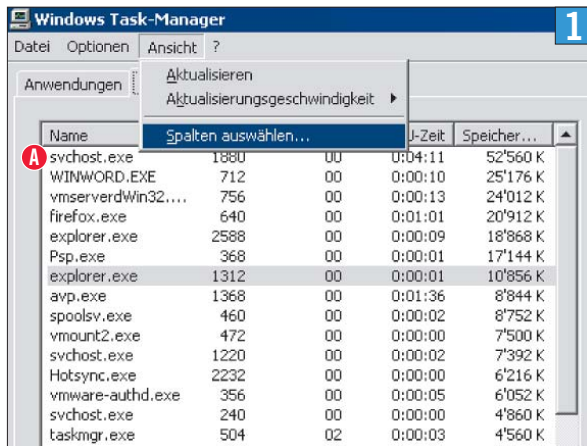
**Moderne PC-Schädlinge verstecken sich tief im System und sind für Antivirenprogramme unsichtbar. Mit folgenden Tipps bemerken Sie die Übeltäter dennoch.**

■ von Gaby Salvisberg

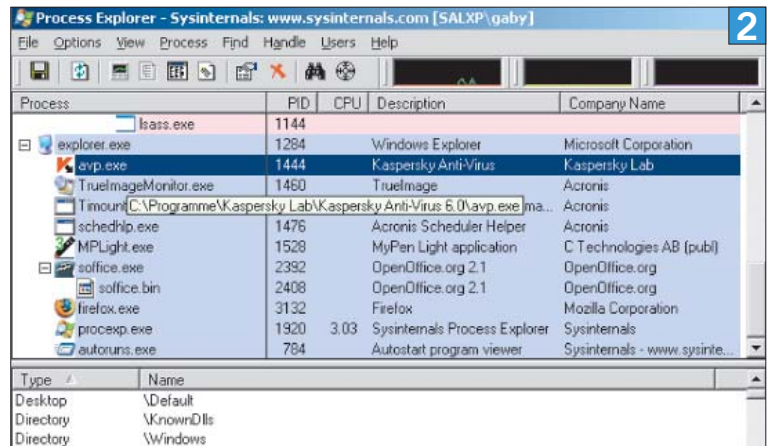
**W**enn eine Antiviren-Software einen Schädling nicht enttarnt, gibt es nur wenige deutliche Anzeichen für einen Befall. Die meisten infizierten PCs scheinen ganz normal zu funktionieren. Der Grund: Heute geht es Schädlingsprogrammierern nicht mehr um Ruhm oder Hackerehre. Sie wollen nur eines: Geld verdienen. Deshalb ist ein Befall viel schwerer zu entdecken als vor ein paar Jahren. Damals pflegten Schädlinge recht deutlich auf sich aufmerksam zu machen. Sei es durchs massenhafte Löschen bestimmter Dateien oder durchs Anzeigen seltener Meldungen.

Heutige Angreifer bringen hingegen mit ihren Übeltätern möglichst viele PCs unter ihre Kontrolle. Die infizierten Systeme spionieren sie dann aus oder missbrauchen sie für andere Zwecke, zum Beispiel für erpresserische Angriffe auf Online-Shops. Moderne Schädlinge arbeiten deshalb lieber im Verborgenen. Virenschreiber nutzen sogar spezielle Techniken wie Rootkits, um ihre virtuellen Attentäter vor Sicherheitsprogrammen zu verstecken (siehe Box «Tarnkappe für Viren», S. 32).

Oft sind es nur noch kleinste Anzeichen, die einen Hinweis auf eine Infizierung liefern. Jedes dieser Symptome kann – einzeln betrachtet –



Der Prozess A mit dem höchsten Speicherverbrauch könnte am langsamen PC schuld sein



Das gelbe Kästchen zeigt, wo die Datei liegt, die für den markierten Prozess verantwortlich ist

auch völlig andere, harmlose Ursachen haben. Der PCTipp zeigt nachfolgend die wichtigsten Verdachtsmomente auf Schädlingsbefall, mit samt den möglichen harmlosen Ursachen. Gleichzeitig erhalten Sie Tipps, wie Sie die Ursachen eingrenzen und beseitigen können. Alle benötigten Programme können Sie in einem Download-Paket bequem unter [www.pctipp.ch](http://www.pctipp.ch) mit **WEBCODE 35906** herunterladen (Info zum PCTipp-Webcode, S. 5).

## Langsamer PC

**Virus:** Ein infizierter Rechner, der Spam oder Viren verschickt, hat weniger Zeit für andere Aufgaben. Der PC wird dadurch etwas langsamer.

**Harmloser Grund:** Fast jeder Windows-PC verliert mit der Zeit an Tempo. Die Ursache: Es sammeln sich immer mehr Dateien, Programme und **Registry**-Einträge an, die das Betriebssystem verwalten muss.

**Tipp:** Finden Sie heraus, was Ihr Computer gerade treibt. Die erste Anlaufstelle dazu ist der Task-Manager. Unter Windows 2000 und Windows XP rufen Sie ihn mit der Tastenkombination **Ctrl+Shift+Esc** auf. Öffnen Sie nun das Register **PROZESSE**. Blenden Sie via **ANSICHT/SPALTEN AUSWÄHLEN** die Spalten «Name», «Prozess-ID» (PID), «CPU-Auslastung», «CPU-Zeit» und «Speicherauslastung» ein, **Screen 1**. Klicken Sie jetzt einmal oder mehrmals kurz auf den Spaltentitel «Speicherauslastung», bis der Prozess mit dem grössten Arbeitsspeicherverbrauch zuoberst steht.

Der Task-Manager alleine liefert nicht alle benötigten Informationen. So fehlt beispielsweise eine Info, wo die zum Prozess gehörende Datei liegt. Profis greifen darum gerne zum kostenlosen Process Explorer. Er ist im Download-Paket

enthalten, das Sie mit **WEBCODE 35906** herunterladen können. Der Process Explorer zeigt an, wo die Prozessdateien liegen, **Screen 2**.

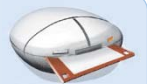
Zudem spüren Sie mit dem Programm verdächtige Prozesse einfacher auf. Suspekt sind etwa Prozesse, die aus speziell verpackten Dateien stammen. Diese werden in knalligem Lila hervorgehoben (nicht in blassem Lila wie im Bild).

Das Deuten von Prozessen ist schwierig. Schauen Sie deshalb zusätzlich nach, welche Programme beim Windows-Start überhaupt geladen werden. Damit ein Programm oder ein Prozess laufen kann, muss er zuerst ausgeführt werden und hat irgendwo im System einen Starteintrag. Dieser lässt sich mit dem kostenlosen Sysinternals-Werkzeug «Autoruns» aufspüren.

Entpacken Sie zuerst das Download-Paket und anschliessend die Datei Autoruns.zip. Doppelklicken Sie nun autoruns.exe. Wählen Sie danach **AGREE**. Jetzt listet das Werkzeug in mehreren Reitern den Inhalt sämtlicher Autostarteinträge auf, **Screen 3**. Lassen Sie sich nicht von der Menge der Einträge verwirren. Manche sind nur der Vollständigkeit halber aufgelistet, werden jedoch höchst selten von Schädlingen benutzt.

### SERVICE

## Komplettpaket

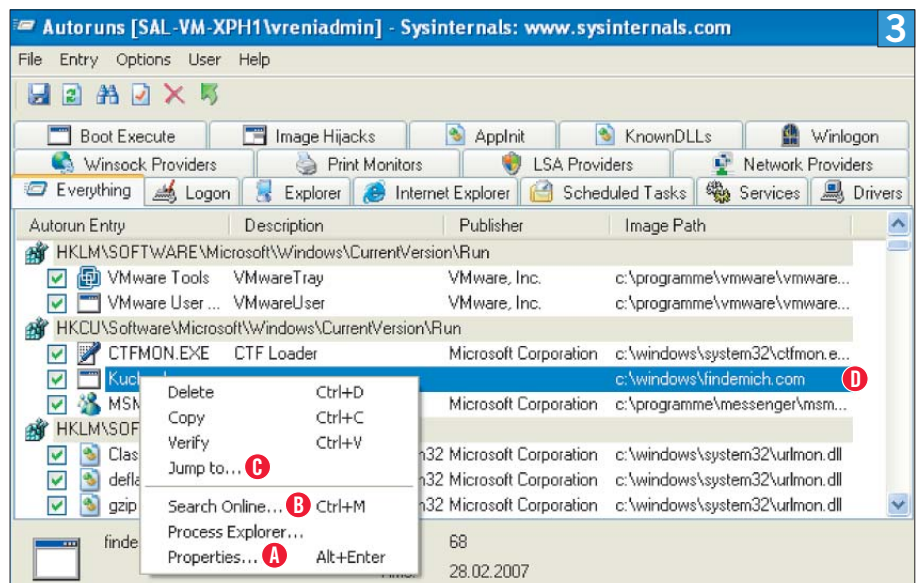


Der PCTipp bietet Ihnen alle im Artikel erwähnten Programme in einem Download-Paket an. Damit speichern Sie diese schnell und bequem auf der Festplatte.

**So gehts:** Besuchen Sie [www.pctipp.ch](http://www.pctipp.ch) und laden Sie das Komplettpaket mit **WEBCODE 35906** herunter.

Genauere Infos über einzelne Einträge bekommen Sie einerseits per Rechtsklick und via **PROPERTIES A**, andererseits über die Option **SEARCH ONLINE B**. Sehr praktisch ist auch der Menüpunkt **JUMP TO C**. Dieser öffnet den Registry-Editor mit samt dem Zweig, der den Eintrag enthält.

Können Sie einen Eintrag keiner Anwendung bzw. keinem Treiber zuordnen, finden Sie anhand der Autoruns-Informationen heraus, in welchem Ordner die Datei liegt **D**. Ob sie harmlos ist oder nicht, kann Ihnen anschliessend die Webseite [www.virustotal.com](http://www.virustotal.com) sagen. Dort wählen Sie einfach per **DURCHSUCHEN** die Datei aus und ▶

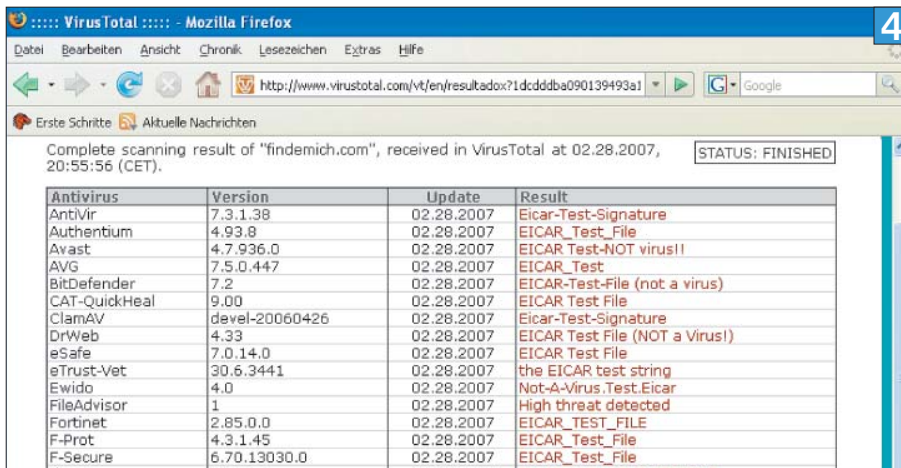


Dank Autoruns finden Sie heraus, welche Dateien automatisch von Windows gestartet werden

### FACHCHINESISCH

## Registry

Spezielle Datenbank, die von Windows verwaltet wird. Aufgrund der Registry weiss Windows beispielsweise, wie gewisse Dateitypen bearbeitet werden müssen.



Die Testdatei wird bei Virustotal.com von allen Scannern erkannt

klicken auf SEND. Sie wird nun mit 30 verschiedenen aktuellen Virensclannern geprüft. Je nach Auslastung der Webseite dauert es einige Minuten, bis die Resultate erscheinen. In unserem Beispiel haben wir eine bekannte Testdatei namens EICAR scannen lassen, die von allen Virenjägern erkannt wird, **Screen 4**. Ein solch einhelliges Resultat ist jedoch selten. Neue Schädlinge werden oft nur von einer Handvoll Antivirenprogrammen entlarvt.

**Achtung:** Setzt ein Angreifer Rootkits ein, sind die schädlichen Prozesse in den erwähnten Tools nicht sichtbar. Befolgen Sie deshalb auch die Tipps in der Box «Tarnkappe für Viren», S. 32.

## Suspekter Internetverkehr

**Virus:** Blenden Sie das Netzwerk- oder Modem-Icon in der Taskleiste ein, falls es nicht bereits angezeigt wird. Öffnen Sie dazu unter START/SYSTEMSTEUERUNG/NETZWERK- UND INTERNETVERBINDUNGEN die NETZWERKVERBINDUNGEN und rufen Sie über die rechte Maustaste die EIGENSCHAFTEN Ihrer Verbindung auf. Haken Sie «Symbol bei Verbindung im Infobereich anzeigen» an.

Es werden zwei kleine PCs in der Taskleiste eingblendet, **Screen 5**. Die blinkenden Monitore signalisieren, dass Daten verschickt oder empfangen werden. Wenn Datenverkehr stattfindet, obwohl Sie weder mailen noch surfen, könnte das ein Indiz für einen Schädling sein. Dieser unterhält sich vielleicht mit seinem Schöpfer oder schickt Viagra- und Börsen-Spam in der Welt herum.

**Harmloser Grund:** Auf den meisten PCs sind Anwendungen installiert, die ständig Netzwerk- und Internetverkehr produzieren. Da gibt es z.B. die Update-Funktionen des Virensclannern und von Windows. Auch ein Chat-Programm wie der MSN Messenger schickt und empfängt immer wieder ein paar Datenpakete, selbst wenn Sie sich mit niemandem unterhalten.



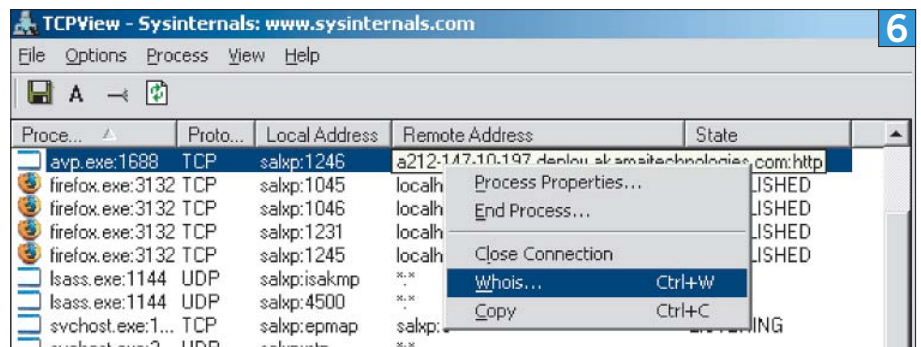
Das rot umrahmte Icon verrät, ob Daten übers Internet oder Netzwerk transferiert werden

Nicht zuletzt suchen immer mehr Anwendungen selbstständig bei den Herstellern nach Updates, so zum Beispiel der Adobe Reader oder Suns Java Runtimes.

**Tip:** Microsoft bietet ein Gratis-Tool namens TCPView an, mit dem Sie den Datenverkehr analysieren können. Auch dieses finden Sie im PCtipp-Download-Paket. Nach dem Entpacken doppelklicken Sie die Datei Tcpview.exe. Schliessen Sie alle Programme und warten Sie zwei bis drei Minuten, bis deren Verbindungen aus TCPView verschwunden sind. Was dann noch mit der Aussenwelt kommuniziert, könnte ein Schädling sein.

Prüfen Sie nur jene Dienste genauer, die auf externe Stellen verweisen, also etwa auf **→ IP-Adressen** oder auf **→ Domains**. Werden solche Verbindungen angezeigt, versuchen Sie per Rechtsklick und WHOIS herauszufinden, wem diese Adresse gehört, **Screen 6**. Häufig stösst man dabei auf das harmlose Resultat «Akamai Technologies». Das ist eine Firma, die für zahlreiche grosse Unternehmen den Internetverkehr regelt.

Bringt die Whois-Funktion keine klärenden Infos, notieren Sie sich die Domain oder die IP-Adresse. Surfen Sie zu [www.dnsstuff.com](http://www.dnsstuff.com) und scrollen Sie auf der Webseite etwas herunter. Den Domainnamen tippen Sie (ohne http:// und www.) im Bereich «Domain name tests» ins Feld «WHOIS Lookup» ein. Erscheint als Ergebnis ein wildfremder Provider aus China oder Russland, spricht vielleicht gerade ein Schädling mit seinem Programmierer.



TCPView informiert über die aktiven Netzwerk- und Internetverbindungen

Haben Sie nur eine IP-Adresse, gibt der Punkt «Reverse DNS lookup» unter «IP Tests» Aufschluss. Es ist auf jeden Fall verdächtig, wenn eine IP-Adresse auf einen normalen PC verweist, der per ADSL oder Wählmodem angeschlossen ist. Im Resultat ist dies oft an einem Zusatz wie «dsl», «client» oder «dialup» zu erkennen.

**Achtung:** Setzt ein Angreifer Rootkits ein, ist der verdächtige Internetverkehr in TCPView nicht sichtbar. Befolgen Sie deshalb auch die Tipps in der Box «Tarnkappe für Viren», S. 32.

## Dubiose Festplattentätigkeit

**Virus:** Obwohl Sie am PC nichts tun, beginnt plötzlich die Festplatte zu arbeiten. Sie sehen auch an den LEDs der Gehäusefront, dass irgendetwas im Gange ist. Wenn Sie nicht selbst auf die Platte zugreifen, dann muss es jemand oder etwas anderes sein – vielleicht ein Schädling.

**Harmloser Grund:** Es gibt mehrere harmlose Ursachen für den plötzlichen Harddisk-Eifer. Einige Anwendungen nutzen eine Arbeitspause, um bestimmte Aufgaben zu erledigen. Da wären zum Beispiel der Windows-Indexdienst oder sonstige Desktop-Suchprogramme, die neu erstellte oder veränderte Dateien in den Suchindex aufnehmen. Vielleicht ist auch der Virensclanner die Ursache, der den

### → FACHCHINESISCH

#### IP-Adresse

Computer benötigen in einem Netzwerk eine eindeutige Adresse, damit sie mit anderen PCs kommunizieren können. Die IP-Adresse besteht aus vier maximal dreistelligen Zahlen, die durch einen Punkt getrennt sind (z. B. 82.10.207.13). Die Werte liegen zwischen 0 und 255.

#### Domain

Ein typisches Beispiel einer Domain ist [www.pctipp.ch](http://www.pctipp.ch) – eine Adresse, unter der ein Rechner im Internet erreichbar ist. Domains setzen sich meist aus drei Teilen zusammen. Zuvor steht die Subdomain (z. B. www). Anschließend folgt der Domainname (pctipp). Den Abschluss bildet die sogenannte Top Level Domain. Sie bezeichnet entweder ein Land (ch steht für die Schweiz) oder eine Funktion, z. B. biz für Unternehmen.

Komplettscan der Platte lieber dann macht, wenn Sie die volle Leistung des PCs nicht benötigen. Diverse Systemwartungswerkzeuge legen ebenfalls in einer Ruhepause los, um beispielsweise die Harddisk zu defragmentieren.

**Tip:** Öffnen Sie Ihren Virens Scanner und klicken Sie sich durch die Menüs, z.B. bei Kaspersky Anti-Virus auf VIRENSUCHE. Wenn Sie einen wachsenden Fortschrittsbalken entdecken oder wenn Dateinamen rasch durchrattern, ist der Fall klar: Ihr Virens Scanner führt eine Überprüfung durch, [Screen 7](#).

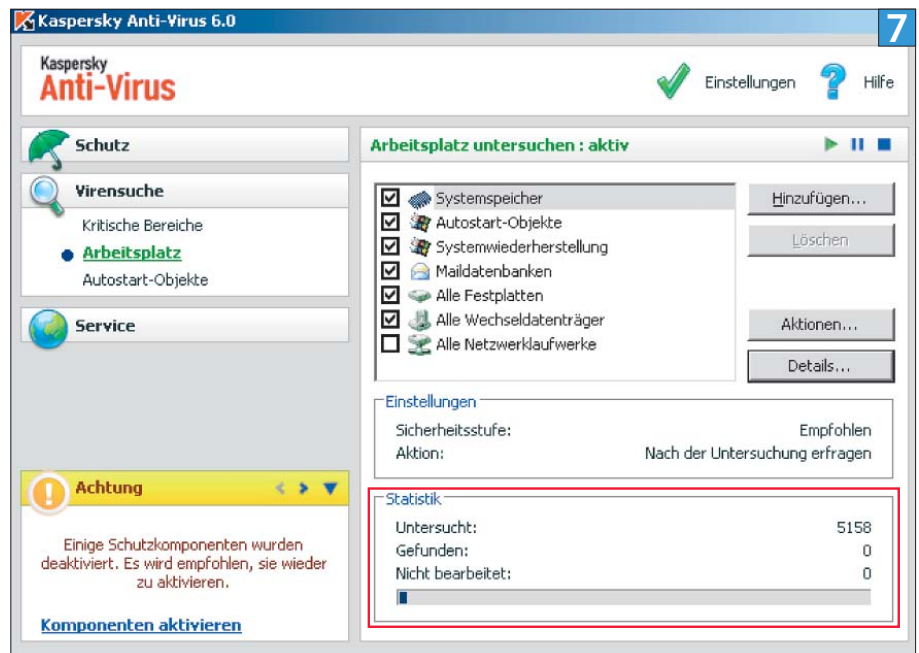
Schauen Sie ausserdem unter START/SYSTEMSTEUERUNG/LEISTUNG UND WARTUNG/GEPLANTE TASKS nach. Vielleicht ist dort eine sich wiederholende Systemaufgabe aufgeführt, z.B. das Defragmentieren der Festplatte oder ein automatisches Update, [Screen 8](#).

## Plötzliche Abstürze

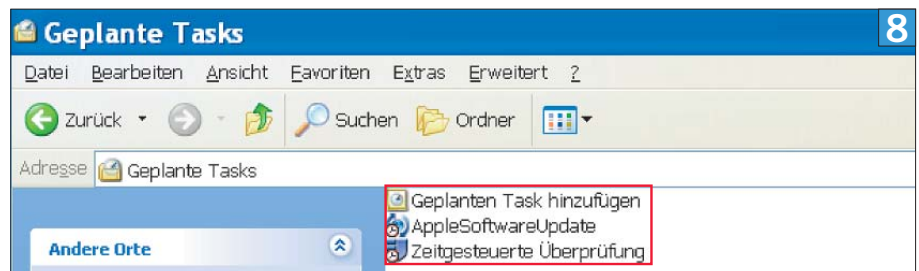
**Virus:** Ein befahrener PC stürzt häufiger ab als ein gesunder. Dahinter steckt keine Absicht des Virenautors. Ihm bleibt oft wenig Zeit, seine Schädlinge vor dem Einsatz ausgiebig zu testen. Deshalb enthalten diese meist viele Programmierfehler, die sich auf dem PC des Opfers durch Abstürze bemerkbar machen.

**Harmloser Grund:** Windows und installierte Anwendungen brauchen keine Schädlinge, um sich abzuschliessen. Dies leisten harmlose Programme ganz von selbst, indem sie falsche Systemdateien ersetzen, Treiberkonflikte verursachen oder Programmierfehler aufweisen. Selbst wenn es nicht die Software ist, die für blaue Bildschirme und rote Köpfe sorgt, kann immer noch die Hardware schuld sein. Ursachen für Abstürze sind vor allem defekte, schlecht montierte oder ungenügend gekühlte Bauteile.

**Tip:** Überlegen Sie, welche Software installiert oder durch ein Update verändert worden ist, bevor sich die Abstürze häufen. Suchen Sie bei den Herstellern dieser Programme nach Hinweisen (z.B. im Support-Forum). Wenn



Der wachsende Fortschrittsbalken zeigt an, dass der Virens Scanner gerade die Harddisk prüft



Einige Programme führen in regelmässigen Zeitabständen automatisch Wartungsarbeiten und Aktualisierungen aus

die Abstürze mit bestimmten Fehlermeldungen oder Fehlercodes einhergehen, notieren Sie diese und suchen Sie per Google danach.

Hardware-Defekte sind schwerer auszumachen. Lesen Sie hierzu den Artikel «Auf Her(t)z und Nieren» in PCTipp 7/2005, S. 42, oder unter [www.pctipp.ch](http://www.pctipp.ch) mit [WEBCODE pdf050742](#).

## Defekter Virens Scanner

**Virus:** Hat sich ein Schädling am Virens Scanner vorbeigeschleust, will er auf dem frisch infizierten PC nicht entdeckt werden. Darum legen manche Würmer und Trojaner den Virens Scanner lahm. Das kann auf mehrere Arten geschehen: Entweder schiesst ein Wurm alle typischen Antivirenprozesse ab oder er leitet jeglichen Internetverkehr zu Antivirenherstellern ins Leere. Die Folge: Der Virens Scanner funktioniert zwar noch, kann aber keine Updates mehr nachladen.

Andere Bösewichte verwenden die Holzhammermethode: Die meisten Nutzer arbeiten mit Administratorrechten. Ein installierter Schädling erhält diese Rechte auch, worauf es für ihn ein Leichtes ist, beim nächsten PC-Start einfach die Dateien des Antivirenprogramms zu löschen.

**Harmloser Grund:** Wenn ein Virens Scanner ohne erkennbaren Grund plötzlich nicht mehr starten oder updaten will, ist dies höchst verdächtig. Für die Symptome muss aber nicht zwingend ein Virus oder Wurm verantwortlich sein. Vielleicht wurde beim letzten Update eine fehlerhafte Datei übermittelt, weshalb das Programm nicht mehr funktioniert. Das ist bei den meisten dem PCTipp bekannten Virens Scannern

### HINTERGRUND

## Rootkits: Tarnkappe für Viren

Ein typischer Schädling besteht aus mindestens einer Programmdatei, aus einem Registry-Eintrag und – wenn er gestartet ist – aus einem Prozess sowie den zugehörigen Netzwerkverbindungen. Alle Elemente sind normalerweise mit den im Artikel erwähnten Werkzeugen zu entdecken, ausser die Angreifer verwenden Rootkits. Dabei handelt es sich um eine Art Tarnkappe für Schädlinge. Mit ihr verstecken Virenschreiber eines oder mehrere der vier Elemente. Die Schädlinge lassen sich dann nicht mehr im Windows-

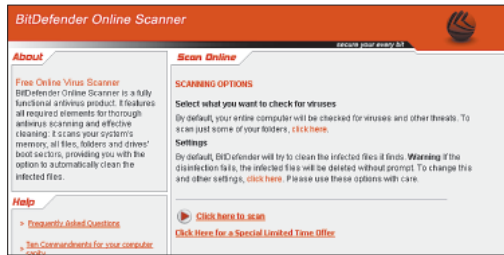
Explorer, Registry-Editor, Task-Manager oder per TCPView entdecken. Unsichtbar sind die Übeltäter aber nicht: Sogenannte Rootkit-Scanner ermöglichen es, die verborgenen Angreifer zutage zu fördern. Die finnischen Viren bekämpfer von F-Secure bieten unter [www.f-secure.com/blacklight/try\\_blacklight.html](http://www.f-secure.com/blacklight/try_blacklight.html) einen Rootkit-Scanner an. Wer F-Secure Internet Security 2006 oder 2007 besitzt, verfügt bereits über ein solches Prüf-Tool. Ein weiterer Rootkit-Scanner stammt von Gmer ([WEBCODE](#)

[35906](#)). Doppelklicken Sie zum Starten des Programms auf gmer.exe, wechseln Sie ins Register ROOTKITS und klicken Sie auf SCAN. Verborgene Elemente werden mit dem Vermerk «hidden» angezeigt. Der PCTipp empfiehlt, vor der Benutzung von Gmer die englischsprachige Seite mit den häufig gestellten Fragen zu lesen ([www.gmer.net/faq.php](http://www.gmer.net/faq.php)). Weitere Rootkit-Scanner werden von Sophos ([www.sophos.com/products/free-tools/sophos-anti-rootkit.html](http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html)) und von Microsoft ([WEBCODE 35906](#)) angeboten.

LINKS

# Mehrere Virens Scanner

Die Chance, einen Schädling zu entdecken, ist höher, wenn Sie Ihre Festplatte mit mehreren Produkten prüfen. Das hat einen einfachen Grund: Virens Scanner von unterschiedlichen Herstellern verwenden unterschiedliche Scanwerkzeuge und Virenerkennungsdatenbanken. Was das eine Antivirenprogramm nicht entdeckt, könnte von einem anderen gefunden werden. Langjährige PCTipp-Leser wissen jedoch, dass es zu Problemen führt, wenn mehr als ein Virens Scanner installiert sind. Möchten Sie eine zweite Meinung einholen, nutzen Sie deshalb besser einen der nachfolgend aufgeführten Webscanner. Schalten Sie zuerst den eigenen Virens Scanner mit einem Rechtsklick auf sein Symbol im Windows-Infobereich (in der Taskleiste unten rechts) vorübergehend aus, damit sich die beiden nicht gegenseitig behindern. Die meisten Webscanner funktionieren nur mit dem Internet Explorer, jener von Trend Micro läuft auch mit Firefox, sofern die Java Runtimes (WEBCODE 17345) installiert sind.



BitDefender: [www.bitdefender.com/scan8/ie.html](http://www.bitdefender.com/scan8/ie.html)



F-Secure: <http://support.f-secure.de/ger/home/ols.shtml>



Panda: [www.pandasoftware.com/activescan/de/activescan\\_principal.htm](http://www.pandasoftware.com/activescan/de/activescan_principal.htm)



Emsi Software: [www.emsisoft.de/de/software/ax](http://www.emsisoft.de/de/software/ax)



Kaspersky: [www.kaspersky.com/de/virusscanner](http://www.kaspersky.com/de/virusscanner)



Trend Micro: [http://de.trendmicro-europe.com/consumer/housecall/housecall\\_launch.php](http://de.trendmicro-europe.com/consumer/housecall/housecall_launch.php)

schon einmal vorgekommen. Auch ein Ausbleiben der Antiviren-Updates kann harmlose Gründe haben: Vielleicht liegt eine Störung der Internetverbindung vor oder der Update-Server des Antivirenherstellers ist überlastet.

**Tip:** Besuchen Sie auf jeden Fall das Supportforum des Antivirenherstellers, um dort nach Hinweisen auf Probleme zu suchen. Wenn Sie per Browser nicht auf seine Webseite gelangen, obwohl andere Seiten problemlos funktionieren, dann hat womöglich ein Schädling bereits Systemdateien verändert.

## Zickige Systemprogramme

**Virus:** Schädlinge würgen gerne Systemprogramme ab, die man zur Fehlersuche und -behebung verwendet. Wenn sich etwa der Task-Manager oder der Registry-Editor nach jedem Öffnen sofort wieder schliesst, ist dies ein mehr als deutliches Alarmzeichen für Schädlingsbefall.

**Harmloser Grund:** Es gibt nur wenige harmlose Ursachen für dieses Verhalten. Ein Systemadministrator kann beispielsweise den angemeldeten Benutzern das Starten solcher Programme verbieten. Dann erscheint

jedoch eine entsprechende Meldung. Eine andere Erklärung: Die Programmdateien sind aus irgendeinem Grund defekt, was mit grosser Wahrscheinlichkeit auf einen Festplattenfehler zurückzuführen wäre.

**Tip:** Führen Sie die bereits genannten Tipps aus. Prüfen Sie zusätzlich den Zustand Ihrer Festplatte. Eine Anleitung dazu finden Sie im auf S. 32 erwähnten PCTipp-Artikel «Auf Her(t)z und Nieren».

## Schädlingsbekämpfung

Deuten alle Zeichen auf einen Schädlingsbefall, muss das System gesäubert werden. Das Problem: Fast jedes aktuelle Schadprogramm lädt weitere unbekannte Dateien aus dem Internet nach. Manchmal werden auch Einstellungen verändert, die Virens Scanner nicht aufspüren. Nach Meinung von Sicherheitsexperten reicht es deshalb nicht, die Schädlinge nur zu entfernen. Das System sollte komplett neu aufgesetzt werden. Anlehnend an den Ursprung des Begriffes «Trojanisches Pferd» erklären die Experten dies mit folgender Analogie: Sie werden zwar das Holzpferd los, aber die damit eingeschleppten «Griechen» haben sich längst in der Stadt bzw. in Ihrem PC verteilt.

Auch Microsoft rät dazu, ein befahreneres System komplett neu zu installieren. Der PCTipp schliesst sich dieser Ansicht an, denn niemand kann wissen, was ein Angreifer im infizierten System bereits verändert hat. Am besten sichern Sie zuerst Ihre persönlichen Daten (Texte, Bilder, Mails, Adressen etc.) auf einen externen Datenträger wie einen USB-Stick, eine CD-ROM oder eine Festplatte. Formatieren Sie anschliessend die Systempartition und installieren Sie Windows mitsamt den von Ihnen genutzten Programmen von Grund auf neu. Eine ausführliche Anleitung zur Installation von Windows finden Sie im PCTipp 9/2004 oder unter [www.pctipp.ch](http://www.pctipp.ch) mit WEB-CODE pdf040934.

Wer sein System nicht neu installieren möchte, sollte den PC zumindest mit mehreren topaktuellen Virens Scannern prüfen. Der PCTipp ist auf ein nützliches Werkzeug namens Multi AV Scanning Tool gestossen. Es lädt auf Wunsch die Kommandozeilenversionen von vier verschiedenen Scannern herunter, mitsamt der aktuellsten Virenerkennung. Nach dem Download eines Scanners führt Multi AV eine komplette Prüfung der Festplatte durch. Das Multi-AV-Werkzeug ist nur in Englisch erhältlich, deshalb haben wir für Sie in diesem Heft auf Seite 35 eine ausführliche Anleitung bereitgestellt. Auch Multi AV erhalten Sie mit WEBCODE 35906.

# Der Klick zu noch mehr Wissen – mit Ihrem PCtipp-Abo

Sichern Sie sich jetzt die besten Tipps und Tricks rund um den PC. Zu einem unschlagbar günstigen Preis jeden Monat in Ihrem Briefkasten.

**KLICKEN SIE HIER**

## AUCH SO KÖNNEN SIE GANZ EINFACH ABONNIEREN:

Bestellen Sie Ihr Abo übers Internet [www.pctipp.ch/abo](http://www.pctipp.ch/abo). Oder füllen Sie den Talon aus und senden Sie ihn an: PCtipp-Leserservice, Postfach, CH-9026 St. Gallen, Fax +41 71 314 04 08.

- Ja, ich möchte den PCtipp kennenlernen und bestelle ein Jahresabonnement Schweiz: **12 Ausgaben plus ein Sonderheft (Wert Fr. 5.90) für nur Fr. 49.–** (statt Fr. 56.30 am Kiosk).  
Ausland: Fr. 64.– (Westeuropa, B-Post), Fr. 81.– (sonstige Länder, Luftpost) P010413
- Ich profitiere doppelt und bestelle ein **2-Jahres-Abo** für nur Fr. 86.– (statt Fr. 112.60 am Kiosk). 2-Jahres-Abo im Ausland nicht erhältlich.

Herr/Frau (Zutreffendes unterstreichen)

Vorname/Name

Firma

Strasse/Nr.

PLZ/Ort

Land



## URHEBERRECHTS-HINWEIS

Der Artikel in diesem PDF-Dokument stammt aus dem PCtipp, der grössten Schweizer Computer-Zeitschrift. Der Inhalt ist urheberrechtlich geschützt. Die Urheberrechte liegen bei der **IDG Communications AG**. Nachdruck, Verbreitung und elektronische Wiedergabe, auch auszugsweise, nur mit schriftlicher Genehmigung des Verlages.

Stand: Juni 2008

Preise für die Schweiz inkl. 2,4% MwSt.

## WAS SIE NICHT DÜRFEN:

- Sie dürfen dieses PDF-Dokument nicht für kommerzielle Zwecke einsetzen.
- Sie dürfen dieses Dokument nicht verändern.
- Sie dürfen dieses Dokument weder gedruckt noch elektronisch in grossen Mengen an Dritte verteilen.
- Sie dürfen dieses Dokument nicht selbst als Download anbieten, jedoch einen Link darauf setzen.

## WAS SIE DÜRFEN:

- Sie dürfen dieses Dokument ausdrucken und bei Bedarf an einzelne Dritte weitergeben.
- Sie dürfen dieses Dokument in elektronischer Form an einzelne Dritte weitergeben.

Dieses PDF-Dokument stellen wir Ihnen gratis zur Verfügung. Mit einem Abo des PCtipp leisten Sie einen Beitrag, der dieses Gratisangebot weiterhin ermöglicht.