Windows sichern

Mit den richtigen Tipps und Tools schützen Sie sich vor allen Gefahren aus dem Internet. Der Artikel zeigt, wie Sie Ihren PC säubern und Neuinfektionen verhindern.

Eine grundlegende Sicherung des PCs benötigt nicht viel: Die wichtigsten Tipps finden Sie knapp zusammengefasst im Kasten "Windows sichern: Die vier wichtigsten Tipps" auf der nächsten Seite.

Darüber hinaus zeigt Ihnen der Artikel, wie Sie Schädlinge aufspüren und beseitigen. Weitere Tipps erläutern, wie Sie Ihre Daten vor Verlust bewahren und wie Sie sicher im Internet surfen. Alle dafür nötigen Tools finden Sie auf sowie kostenlos im Internet.

Windows sichern

Wenn der PC anfängt, sich eigenartig zu verhalten, fragen sich viele Anwender, ob er vielleicht verseucht ist. Mit den folgenden Tipps finden Sie heraus, ob sich ein Schädling auf Ihrem Rechner versteckt.

Spy- und Adware jagen

Spybot Search & Destroy 1.6.2 (kostenlos, **www.safer-networking.org/de/spybotsd** und auf) eignet sich vor allem zum Aufspüren aktiver Spione. Bei der Beseitigung der erkannten Gefahren zeigt das Programm mitunter Schwächen.

So geht's: Führen Sie das Setup aus und lassen Sie am Ende sowohl Spybot Search & Destroy als auch den Hintergrundwächter Tea Timer starten. Erstellen Sie anschliessend mit einem Klick auf *Sicherung anlegen* eine Kopie der Registry.

Die Funktion *System immunisieren* bewirkt, dass Spybot zahlreiche Einträge in Ihrer Hosts-Datei vornimmt, um den PC vor schädlichen Webseiten zu schützen. Zuletzt starten Sie mit einem Klick auf *Programm benutzen* das eigentliche Hauptprogramm. Ein Klick auf *Überprüfen* führt die Suche nach Spionen auf Ihrem PC aus (Bild A). Am Ende des Scans erhalten Sie eine Zusammenfassung der gefundenen Schädlinge und Tracking-Cookies, die Sie mit *Markierte Probleme beheben* entfernen. Setzen Sie das im folgenden Abschnitt beschriebene Tool Anti-Malware 1.38 ein, wenn Spybot einen gefundenen Spion nicht entfernen kann.

Spybot Search & Destroy 1.6.2: Das Tool hat im Online-PC-Test 80 Prozent der aktiven Spionageprogramme erkannt, konnte allerdings nur 35 Prozent entfernen (Bild A).

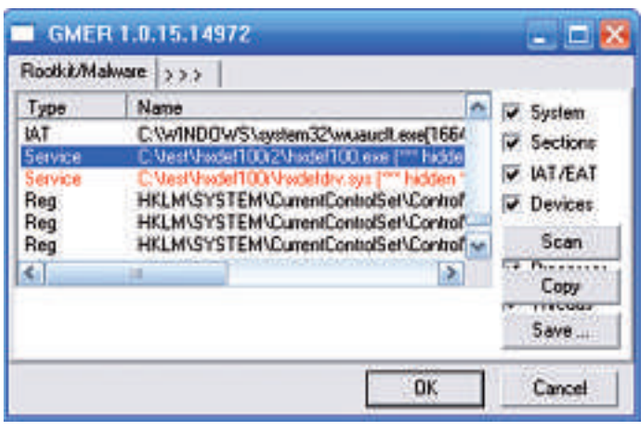
Trojaner beseitigen

Anti-Malware 1.38 (kostenlos, **www.malwarebytes.org/mbam.php** und auf) ist ein mächtiges Reinigungs-Tool, das viele Trojaner erkennt und entfernt (Bild C).

So geht's: Installieren Sie Anti-Malware und aktualisieren Sie anschliessend die Signaturen. Nur so erkennt das Tool auch die neuesten Gefahren.

Markieren Sie dann auf dem Reiter *Scanner* die Option *Vollständigen Suchlauf durchführen* und klicken Sie auf *Scan*. Es öffnet sich ein kleines Fenster, in dem Sie vor jedes zu prüfende Laufwerk ein Häkchen setzen. Mit *Scan starten* beginnen Sie mit der Suche nach Trojanern auf Ihrem PC. Bestätigen Sie das Ende des Scans mit *OK* und klicken Sie danach auf *Ergebnisse anzeigen*.

Schliessen Sie zuerst alle geöffneten Windows-Anwendungen, bevor Sie mit *Entferne Auswahl* die gefundenen Schädlinge in Qua-



Gmer 1.0.15.14972: Gefundene Rootkits markiert das Tool in Rot (Bild B).

Kompakt

- *Der Artikel zeigt, wie Sie Schädlinge finden und entfernen.*
- *Alle Sicherheitsprogramme, die Sie dafür brauchen, sind auf der Heft-DVD.*

rantäne verschieben. Es kommt sonst eventuell zu Problemen bei der Desinfektion.

Anti-Malware öffnet nach Ende des Scans automatisch den Texteditor mit einem Protokoll, welche Schädlinge gefunden und entfernt wurden. Sie finden diese Datei auch im Ordner *Logs* unterhalb des Installationsverzeichnisses von Anti-Malware.

Rootkits aufspüren

Rootkits sind besonders heimtückisch, weil sie komplett unsichtbar sind. Ein Windows-Rootkit bringt meist eigene Systemtreiber mit, die es installiert. Danach wird es im Windows-Explorer nicht mehr angezeigt. So, als wäre es gar nicht vorhanden.

Auch herkömmliche Virenscanner fallen auf diese Tricks oft herein. Nur Spezialtools wie Gmer 1.0.15.14972 (kostenlos, **www.gmer.net** und auf) kommen den heimlichen Schädlingen auf die Schliche (Bild B).

Daten verschlüsseln

Zur Grundsicherung eines Computers gehört es auch, wichtige Dateien und Dokumente zu verschlüsseln. So sind Ihre Daten sicher vor Schädlingen, Hackern und selbst vor neugierigen Arbeitskollegen, die sich an Ihrem PC zu schaffen machen.

So geht's: Mit Truecrypt 6.2a (kostenlos, **www.truecrypt.org** und auf) legen Sie verschlüsselte Container an, in die Sie die zu sichernden Daten ablegen. Nur wenn der Container in das Dateisystem Ihres Computers eingebunden ist, können Sie – oder Fremde – auf die gesicherten Daten zugreifen. Der Container sollte deswegen nach der Benutzung so schnell wie möglich wieder vom Dateisystem getrennt werden. Die Daten sind dann wieder verschlüsselt und sicher vor fremdem Zugriff.

Installieren Sie zuerst Truecrypt und öffnen Sie dann das Archiv mit der deutschen Sprachdatei, das Sie ebenfalls auf finden. Entpacken Sie den Inhalt des Archivs in den Installationsordner von Truecrypt und starten Sie das Tool neu. Die Oberfläche ist nun in Deutsch.

Legen Sie jetzt einen neuen Container mit einem Klick auf *Volume erstellen* an. Ein neues Fenster öffnet sich. Klicken Sie zwei Mal auf *Weiter* und danach auf *Datei …*, um den Namen und Speicherort Ihres Containers festzulegen. Navigieren Sie zu einem geeigneten Ordner und geben Sie den gewünschten Namen in das Feld *Dateiname* ein. Bestätigen Sie mit *Speichern* und klicken Sie danach zwei Mal auf *Weiter*. Geben Sie die gewünschte Grösse Ihres verschlüsselten Containers an. Dieser Wert sollte nicht zu klein sein, da er sich nachträglich nicht mehr verändern lässt.

Mit *Weiter* gelangen Sie zur Eingabe des Passworts. Dieses sollte auch Sonderzeichen und Zahlen enthalten. Sie dürfen das Kennwort nicht vergessen, weil Sie sonst den Zugriff auf Ihre verschlüsselten Daten verlieren.

Nachdem Sie nun erneut auf *Weiter* geklickt haben, müssen Sie den Mauszeiger etwa 30 Sekunden lang kreuz und quer über den Bildschirm bewegen. Dadurch erstellen Sie einen zufälligen Schlüssel, den das Programm zum Formatieren Ihres Containers benötigt. Klicken Sie anschliessend auf den Button *Formatieren* und bestätigen Sie mit *OK* und *Beenden*. Der Container ist nun einsatzbereit.

Klicken Sie in das grosse Feld im Hauptfenster von Truecrypt und wählen Sie so einen Laufwerkbuchstaben aus, unter dem Truecrypt den Container in das Dateisystem Ihres Computers einbindet. Wählen Sie den Container anschliessend über *Datei …* aus und aktivieren Sie ihn mit *Einbinden*. Nach der Eingabe des Passworts steht er Ihnen im Windows-Explorer wie eine normale Partition zur Verfügung.

Vergessen Sie nicht, den Container per Klick auf *Trennen* wieder zu deaktivieren, wenn Sie ihn nicht mehr benötigen.

Wichtige Daten sichern

Zum Schutz vor Gefahren aus dem Internet gehört auch die Sicherung Ihrer wichtigsten Dateien auf ein separates Medium. Sowohl bei einem Virenbefall als auch bei einem Systemfehler sind Ihre Daten dann vor Verlust geschützt. Cobian Backup 9.5.1.212 (kostenlos, **www.cobian.se/cobianbackup.htm** und auf) bietet zahllose Funktionen wie automatische Backups und sichert Dateien auf Wunsch sogar in einen FTP-Ordner im Internet.

So geht's: Installieren Sie Cobian Backup und belassen Sie bei der Frage nach dem *Installationstyp* die Auswahl auf *Windows-Dienst*. Das Programm startet dann automatisch als Windows-Dienst. ▶

Windows sichern: Die vier wichtigsten Tipps

Diese vier Massnahmen sichern Ihr Windows schnell und effektiv.

1. Virenscanner installieren
Ein aktueller Virenscanner mit Hintergrundwächter schützt vor den meisten Schädlingen (Bild D). Ein gutes Antivirenprogramm ist Avast 4.8 Home Edition (kostenlos, **www.avast.com** und auf).

2. Firewall verwenden
Installieren Sie eine Desktop-Firewall wie Online Armor Free 3.5.0.14 (kostenlos, **www.tallemu.de** und auf), wenn Sie keinen DSL-Router mit integrierter Firewall haben.

3. Software aktualisieren
Laut Secunia befindet sich auf 98 Prozent aller PCs Software mit Sicherheitslücken. Halten Sie Ihre installierten Programme deswegen mit dem Personal Software Inspector 1.5.0.0 (kostenlos, **www.secunia.com/vulnerability_scanning/personal** und auf) aktuell.

4. Windows patchen
Aktivieren Sie die automatischen Updates für Windows über *Start, Systemsteuerung, Sicherheitscenter* und klicken Sie auf *Automatische Updates*. Aktivieren Sie dort *Updates downloaden, aber Installationszeitpunkt manuell festlegen*. So erhalten Sie schnell und komfortabel alle Sicherheits-Patches.

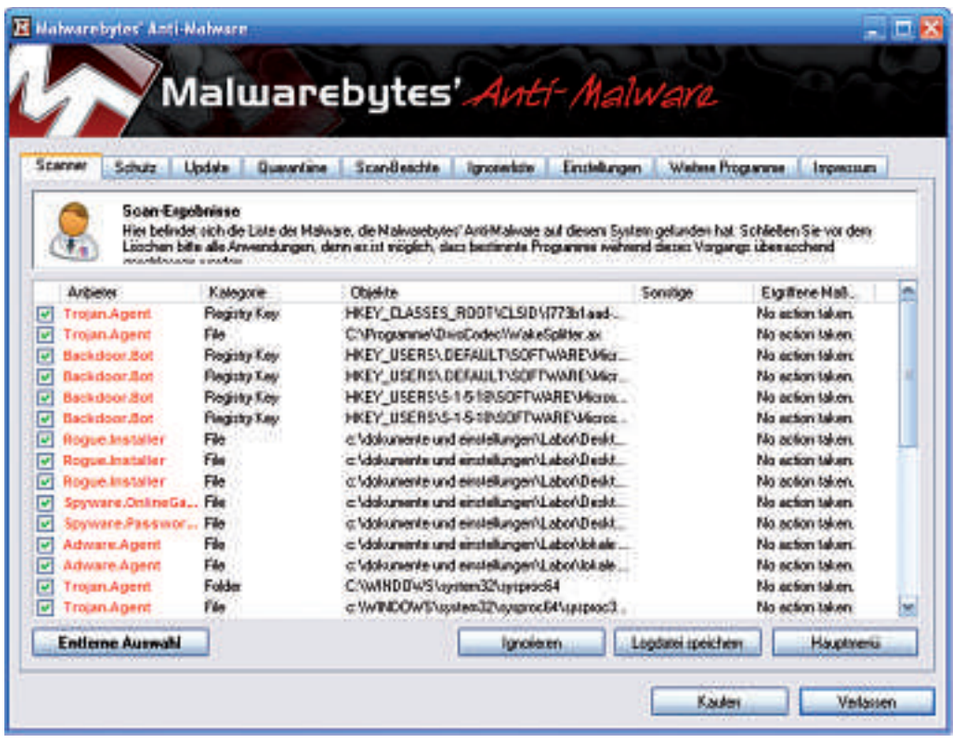
Avast 4.8 Home Edition: Der kostenlose Virenscanner hat einen Schädling entdeckt (Bild D).

Klicken Sie nach dem Setup doppelt auf das Fliegenpilz-Icon unten rechts im System-Tray, um die Bedienoberfläche zu öffnen. Legen Sie zuerst einen Backup-Auftrag mit *Sicherung, Neue Sicherung* an. Setzen Sie dann in dem neuen Fenster ein Häkchen vor *Volumeschattenkopie verwenden*. Das Programm sichert damit auch gerade geöffnete Dateien (Bild E). Stellen Sie den *Sicherungstyp* auf *Inkrementell* um, damit Cobian Backup nicht immer alle Dateien erneut komplett sichert.

Wählen Sie danach oben links *Dateien* aus und klicken Sie unter *Quelle* auf *Hinzufügen*. Wählen Sie *Verzeichnis* aus, um komplette Ordner zur Sicherung hinzuzufügen, und *Dateien*, um einzelne Dateien auszuwählen. Sobald Sie dies erledigt haben, legen Sie mit einem Klick auf *Hinzufügen* bei *Ziel* fest, wohin Ihre Daten gesichert werden sollen. Das Hinzufügen zu sichernder Dateien lässt sich auch per Drag-and-Drop aus dem Windows-Explorer heraus erledigen.

Bei *Zeitplaner* stellen Sie anschliessend ein, wann und wie oft das Backup durchgeführt werden soll. Bei *Komprimierung* legen Sie fest, ob die Dateien gepackt werden sollen. Sobald Sie mit allen Einstellungen zufrieden sind, schliessen Sie die Konfiguration mit *OK* ab. Der Backup-Auftrag taucht nun im Hauptfenster auf. Wählen Sie ihn aus und klicken Sie oben auf das Diskettensymbol. Bestätigen Sie das Info-Fenster mit *OK*, um das Backup zu starten. Sicherungsaufträge mit Zeitplan führt das Programm selbstständig zum angegebenen Zeitpunkt aus.

Prüfen Sie bei jedem neuen Auftrag, ob auch alle Daten wie vorgesehen gesichert wurden. Nichts ist ärgerlicher, als sich auf ein Backup zu verlassen, das fehlerhaft ist.



Anti-Malware 1.38: Auf einem verseuchten PC findet das Tool oft mehr als nur einen einzigen Schädling, hier zum Beispiel einen Trojaner, ein Backdoor-Tool sowie Spy- und Adware (Bild C).

Sicher im Internet

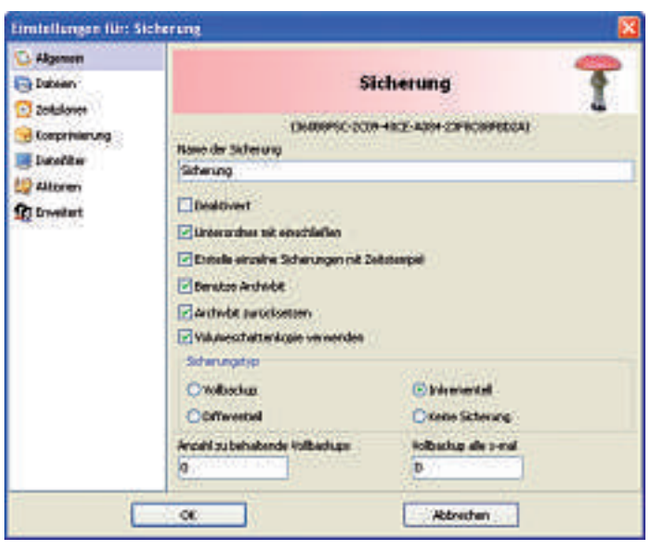
Schädlinge verbreiten sich immer häufiger direkt über den Browser. Bereits der Besuch einer vermeintlich harmlosen Webseite kann genügen, Ihren PC zu verseuchen. Mit den richtigen Tools lässt sich dies jedoch verhindern.

Drive-by-Downloads verhindern

Bereits der Besuch einer eigentlich seriösen Webseite, auf der ein manipuliertes Werbebanner zu sehen ist, kann genügen, um Ihren PC mit einem Schädling zu infizieren. Man nennt diese oft unterschätzte Gefahr Drive-by-Downloads.

Dabei nutzen die Angreifer gezielt Sicherheitslücken im Browser und in Anwendungen wie Flash oder Java aus, um gefährlichen Schadcode einzuschleusen. Dieser erste Dropper lädt dann meist weitere Schädlinge wie Trojaner und vielleicht auch ein Rootkit herunter und installiert sie.

So geht's: Die beiden Firefox-Erweiterungen Adblock Plus 1.0.2 (kostenlos, **www.adblockplus.org/de** und auf DVD) und Noscript 1.9.5 (kostenlos, **www.noscript.net** und auf DVD) schützen vor Drive-by-Downloads. Adblock Plus filtert Werbung aus, so dass ein manipuliertes Banner gar nicht mehr geladen wird. Noscript blockiert die riskante Javascript-Technik und erlaubt sie nur noch auf ausgewählten Seiten. Weiteren Schutz beim Surfen bietet der Exploit Shield 0.70 Beta (kostenlos, **www.fsecure.com/labs** und auf DVD).



Sicherung planen in Cobian Backup 9.5.1.212: Die Option *Volumeschattenkopie verwenden* bewirkt, dass das Tool auch gerade geöffnete Dateien sichert (Bild E).

Spam reduzieren

Spam-Mails sind unerwünscht zugesandte Werbenachrichten. Fast alles, womit sich Geld machen lässt, taucht auch in Spam-Mails auf. Spam kann man nicht ganz vermeiden, man kann ihn nur reduzieren.

So geht's: Thunderbird enthält einen leistungsfähigen Spamfilter. Markieren Sie jede Spam-Mail, die Sie erhalten, mit dem Mauszeiger und klicken Sie danach auf *Junk*. So trainieren Sie den Spamfilter, der mit der Zeit immer bessere Ergebnisse erzielt.

Seien Sie darüber hinaus vorsichtig, wo und wann Sie Ihre E-Mail-Adresse im Web verwenden. Spammer forsten Webseiten gezielt nach neuen Mail-Adressen ab. Ist eine Adresse erst einmal in die Fänge eines Spamversenders geraten, bekommt man sie dort praktisch nie wieder heraus. Der Artikel "Adressen auf Zeit" (Online PC Zeitung 9/2009 auf Seite 2) beschreibt, wie Sie Ihre E-Mail-Adresse vor Spammern schützen. ■

Andreas Th. Fischer