

Vorbeugen ist alles, ganz besonders beim Schutz vor Trojanern, Computerviren und anderen Schadensprogrammen. Aber was tun, wenn der Ernstfall dann doch einmal eintritt? Dann sollten Sie das betroffene Windows am besten so wenig wie möglich nutzen oder – besser noch – gar nicht starten. Helfen können Ihnen dabei Tool-Sammlungen, die sich auf einem schreibgeschützten USB-Stick befinden. Oder Sie nutzen ein voll funktionsfähiges Notfall-Linux auf einer bootfähigen CD, das die nötigen Säuberungsprogramme enthält.

- Sicher ist sicher: Such- und Analyseprogramme von virenfreien Medien starten T 87/3
- Diese Tools gehören unbedingt auf Ihr Notfallmedium T 87/4
- PC-Diagnose: So gehen Sie richtig vor T 87/5
- Schädlinge aufspüren und beseitigen – Schritt 1: Microsofts Tool zum Entfernen bösartiger Software T 87/6
- Schritt 2: Rootkits aufspüren und beseitigen mit dem Blacklight Rootkit Eliminator T 87/7
- B-Probe: Überprüfen Sie Ihren PC zusätzlich mit dem RootkitRevealer T 87/9
- Positiver Rootkit-Befund – und nun? T 87/10
- Viren aufspüren und beseitigen T 87/11
- Ad- und Spyware-Programme mit Ad-Aware 2007 aufspüren und beseitigen T 87/13
- Nachtarbeiter: So überprüfen Sie Ihr System über Nacht intensiv auf Viren T 87/15
- avast! Home for Linux unter Knoppix installieren T 87/16
- Den PC mit avast! Home for Linux auf Viren untersuchen T 87/18
- B-Probe mit BitDefender Free Edition für Linux T 87/20
- Scannen per Kommandozeile T 87/21

Autor: **Christian Grugel**



Wenn sich der PC plötzlich merkwürdig verhält

Guido L. beschleicht ein ungutes Gefühl: Seit einigen Tagen reagiert sein PC ungewohnt träge auf Tastatur- und Mauseingaben. Auch die ständigen Festplattenaktivitäten und Netzwerkzugriffe sind alles andere als normal. Als schließlich noch die automatische Update-Funktion der Antiviren-Software versagt, ist er sich sicher: Ein Virus muss sich auf seinem PC eingenistet haben. Doch kann das überhaupt möglich sein? Schließlich schützt Herr L. seinen PC mit Antiviren-Software und tagesaktuellen Virensignaturen.

Heimliche Infektion – trotz Antiviren-Programm

Die Sorge von Herrn L. ist nicht unberechtigt: Trotz des Einsatzes von Antiviren-Software, dem regelmäßigen Aktualisieren der Virensignaturen und einem gut gepflegten und mit allen aktuellen Patches ausgestatteten Windows-System ist eine Infektion des Rechners mit Schad-Software nicht auszuschließen.

Antiviren-Produkte haben das Nachsehen

Grund: Selbst bei den besten Antiviren-Produkten vergehen zuweilen mehrere Stunden von der Entdeckung eines neuen Schädling bis zur Bereitstellung passender Signaturen. Die Entwicklung neuer Sicherheitstechnologien wie dem Behaviour Blocking, das Schädlinge künftig allein anhand ihres Verhaltens aufspüren soll, steckt hingegen noch in den Kinderschuhen.

Neue Viren auf Mausclick

Ein weiteres Problem: Das Kreieren neuer Viren ist heutzutage selbst für Laien kein Problem mehr – dazu genügen wenige Mausclicks. Entsprechende Viren-Baukästen sind im Internet weit verbreitet.

Ein Restrisiko bleibt immer

Last but not least gibt es de facto kein System ohne Sicherheitslücken. Diese betreffen nicht nur das Betriebssystem. Auch bei Anwendungs-Software müssen die Hersteller regelmäßig nachbessern, um bekannt gewordene Sicherheitslücken zu schließen.

Umso wichtiger sind eine aufmerksame Beobachtung des eigenen PCs und ein besonnenes Vorgehen im Verdachtsfall. Wie Sie sich in einer solchen Situation richtig verhalten, schildert Schritt für Schritt der folgende Beitrag.

Seien Sie stets aufmerksam!

Sicher ist sicher: Such- und Analyseprogramme von virenfreien Medien starten

Haben Sie den Verdacht, dass sich auf Ihrem Rechner trotz aller Sicherheitsmaßnahmen ein Schädling eingenistet haben könnte, ist den Suchergebnissen der lokal installierten Antiviren-Software im Zweifelsfalle nicht mehr zu trauen.

Blindes Vertrauen unangemessen

Viele Schädlinge sind längst so raffiniert, dass sie die installierten Antiviren-Programme nach der Infektion gezielt umgehen oder gar komplett außer Gefecht setzen.

Intelligente Schädlinge

Hat sich gar ein Rootkit eingenistet, bleiben die verräterischen Prozesse und Dateien dem Virenscanner nicht selten komplett verborgen. Beim Aufspüren von Rootkits kann bislang keine der aktuellen Antiviren-Lösungen wirklich überzeugen. Spezialisierte Rootkit-Scanner leisten hier gründlichere Arbeit.

Kaum zu entdecken: Rootkits

Im Verdachtsfall liefern letztlich nur Virenscanner, Analyseprogramme und Rootkit-Detektoren, die auf einem schreibgeschützten und virenfreien Medium residieren und ohne lokale Installation auskommen, vertrauenswürdige Ergebnisse.

Virenfreie Startumgebung nötig

An Medien kommen neben USB-Sticks mit Schreibschutz auch optische Medien, sprich CDs oder DVDs, infrage. Der Schreibschutz garantiert, dass die Analyseergebnisse der eingesetzten Programme nicht vom infizierten System manipuliert werden können.

Schreibschutz unverzichtbar

**USB-Sticks
mit Schreib-
schutz**

Die USB-Stick-Variante ist sicherlich die komfortablere Alternative. Allerdings sind entsprechende Sticks mit Schreibschutz rar. Zu den wenigen Anbietern, die USB-Sticks mit mechanischen Schreibschutzschaltern anbieten, zählen beispielsweise Buffalo und TrekStore.

**Diese Stick-
Serien sind
geeignet**

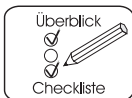
Bei Buffalo sind die Sticks der Serie „Ultra High Speed Professional Type R“ mit einem entsprechenden Schalter ausgestattet. Bei TrekStore sind es die Sticks der Serie „USB-Stick CS“.



Die Sticks der Serie „USB-Stick CS“ von TrekStore zählen zu den wenigen USB-Sticks, die mit mechanischem Schreibschutzschalter ausgestattet sind.

**Regelmäßige
Updates nötig**

Die auf einem solchen Stick gespeicherten Programme müssen natürlich von Zeit zu Zeit aktualisiert werden – eine Investition, die sich letztlich aber auszahlt.

**Diese Tools gehören unbedingt auf Ihr
Notfallmedium****Unverzichtbare
Tool-
Sammlung**

Um im Fall der Fälle gerüstet zu sein, sollten Sie die folgenden sechs kostenlosen Programme stets auf Ihrem Notfallmedium griffbereit halten. Beachten Sie, dass manche der Programme als ZIP-Archiv vorliegen und vor dem Einsatz entpackt werden müssen.

Name und Hersteller des Tools	Funktion	Download-Adresse
Tool zum Entfernen bössartiger Software (Microsoft)	Universelles Schädlingsaufspürprogramm	http://www.microsoft.com/germany/sicherheit/tools/malwareremove.mspx
Blacklight Rootkit Eliminator (F-Secure)	Rootkits aufspüren	http://www.f-secure.com/security_center
RootkitRevealer (SysInternals)	Rootkits aufspüren	http://www.microsoft.com/germany/technet/sysinternals/utilities/RootkitRevealer.mspx
Virus Cleaner (Avast)	Viren aufspüren	http://www.avast.com/eng/down_cleaner.html
Avert Stinger (McAfee)	Viren aufspüren	http://vil.nai.com/vil/Stinger/
Ad-Aware 2008 Free (Lavasoft)	Ad- und Spyware aufspüren	Top-aktuell: Seite 21. Mai gibt's Version 2008 http://www.lavasoftusa.com/products/ad_aware_free.php

PC-Diagnose: So gehen Sie richtig vor

Das A und O bei der Prüfung verdächtiger Systeme ist die richtige Wahl der Such- und Analysewerkzeuge sowie der Einsatzreihenfolge.

Eine Frage der Vorgehensweise

So macht es beispielsweise wenig Sinn, mit der Suche nach Viren zu beginnen, solange noch nicht geklärt ist, ob auf Ihrem PC möglicherweise ein Rootkit sein Unwesen treibt.

Die Einsatzreihenfolge ist entscheidend

Denn in diesem Fall wird die Antiviren-Software mit hoher Wahrscheinlichkeit nur einige der Schädlinge finden – selbst wenn der PC mit Viren geradezu verseucht ist.

Getarnte Schädlinge



Ebenso sollten Sie nicht blind den Ergebnissen eines einzelnen Programms vertrauen: Sinnvoller ist es, den Einsatz verschiedener Spürprogramme geschickt miteinander zu kombinieren, sodass sich deren spezifische Stärken und Schwächen sinnvoll ergänzen.

Verhältnismäßigkeit der Mittel

Schlussendlich bietet es sich nicht zuletzt aus Zeitgründen an, zunächst mit einer weniger intensiven, aber dafür zeitsparenden Suche zu beginnen und erst bei weiteren Verdachtsmomenten gezielt in die Tiefe zu gehen.

Risiko: Fehlalarm

Schließlich benötigt eine Suche mit maximaler Suchtiefe nicht nur mehrere Stunden, sondern erhöht auch das Risiko von Fehlalarmen.

**Schädlinge aufspüren und beseitigen – Schritt 1:
Microsofts Tool zum Entfernen bössartiger Software****Nutzen Sie das Microsoft-Tool**

Für eine erste Schnellüberprüfung Ihres Systems bietet sich Microsofts „Tool zum Entfernen bössartiger Software“ an. Das Tool hat sich bestens bewährt, um ein System in kurzer Zeit auf weitverbreitete Schädlinge hin zu überprüfen.

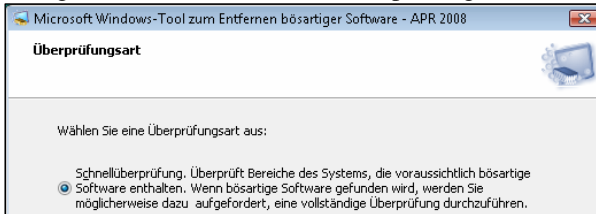
Automatische Überprüfung unzuverlässig

Sofern die automatische Update-Funktion von Windows aktiviert und Ihr PC regelmäßig mit dem Internet verbunden ist, wird das Programm zwar automatisch heruntergeladen, aber bei der automatischen Ausführung hakt es zuweilen.

Das Tool einsetzen

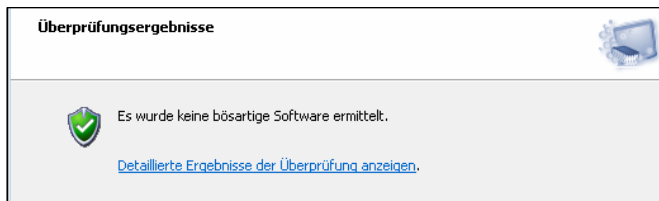
Zudem könnte ein Schädling die Funktion längst blockiert haben. Es ist daher sinnvoll, das Programm per Hand zu starten:

- Starten Sie das Tool vom schreibgeschützten Medium und wählen Sie im Programmassistenten unter „Überprüfungsart“ den Modus „Schnellüberprüfung“ aus.



Schritt für Schritt zum sauberen PC: Zu Beginn der Überprüfung bietet sich das Microsoft Tool zum Entfernen bösartiger Software an.

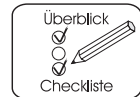
Die anschließende Überprüfung Ihres Rechners dauert im Gegensatz zur „Vollständigen Überprüfung“ keine Stunden, sondern nur wenige Minuten.



Alles sauber: Die Überprüfung hat keine verdächtigen Dateien zutage gefördert.

Tipp: Sofern Sie einen konkreten Verdacht hegen, dass sich in einem bestimmten Verzeichnis ein Schädling eingenistet haben könnte, steht Ihnen noch die „Benutzerdefinierte Überprüfung“ zur Verfügung. Die zu überprüfenden Ordner wählen Sie in diesem Fall manuell aus und können diese dann einer intensiven Prüfung unterziehen.

Schnellüberprüfung wählen



Zügige Ergebnisse

Haben Sie einen konkreten Verdacht?

Schritt 2: Rootkits aufspüren und beseitigen mit dem Blacklight Rootkit Eliminator

1. →
2. →
3.
Anleitung

1. →
2. →
3.
Anleitung

Kein Universal-Tool verfügbar

Der Blacklight Rootkit Eliminator

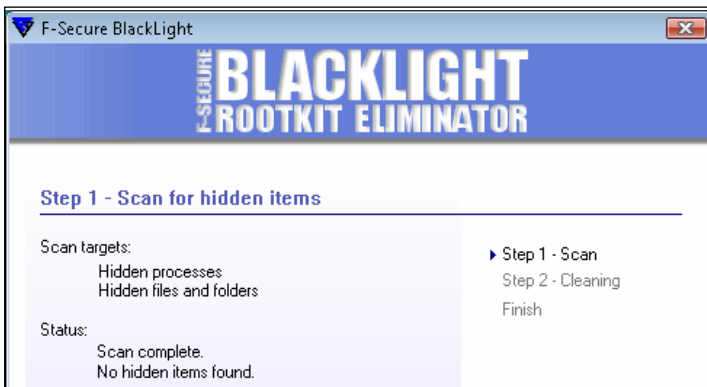
Scan durchführen

Bei der Suche nach unerwünschten Parasiten sollten Sie nach dem durchgeführten Schnelltest zu allererst sicherstellen, dass Ihr Rechner frei von Rootkits ist.

Das ist leichter gesagt als getan, denn nirgends sonst ist die Überprüfung durch mehrere Programme so dringend angeraten wie bei der Suche nach Rootkits. Nur so erhalten Sie am Ende verlässliche Ergebnisse.

Für eine erste Überprüfung des Systems auf Rootkits hat sich der „Blacklight Rootkit Eliminator“ von F-Secure bewährt. Das Tool arbeitet zügig und liefert dennoch vergleichsweise zuverlässige Ergebnisse:

- Starten Sie das Programm und klicken Sie im ersten Schritt des Assistenten auf „Scan“. Anschließend dauert es einige Minuten, bis das Ergebnis der Prüfung vorliegt.



Glück gehabt: Der Blacklight Rootkit Eliminator konnte keine Auffälligkeiten feststellen.

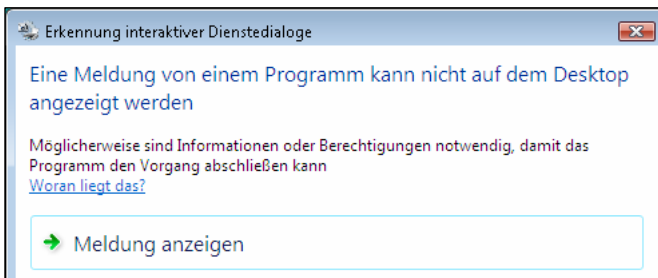
Hinweis: Sollte das Tool fündig werden, können Sie in Schritt zwei direkt die Säuberung des PCs veranlassen.

B-Probe: Überprüfen Sie Ihren PC zusätzlich mit dem RootkitRevealer

Prinzipiell leistet der „RootkitRevealer“ von SysInternals Ähnliches wie der Blacklight Rootkit Eliminator. Allerdings nutzt der RootkitRevealer noch weitere Suchtechniken, so dass eine zusätzliche Überprüfung mit dem Tool sinnvoll ist:

1. Um das Programm zu starten, führen Sie die Datei „RootkitRevealer.exe“ aus.
2. Klicken Sie auf „Scan“, um den Prüfvorgang zu starten.

Hinweis: Das Tool ist derzeit noch nicht voll Vista tauglich, so dass die Anzeige des Programmfensters zunächst mit der folgenden Fehlermeldung blockiert wird:



Vista-Animositäten: Die Anzeige des Programmfensters wird zunächst blockiert.

In diesem Fall klicken Sie auf „Meldung anzeigen“; Vista startet dann einen separaten Desktop-Prozess, in dem das RootkitRevealer-Fenster angezeigt wird.

Säuberung auf Mausclick



System ein zweites Mal überprüfen

Programm ausführen

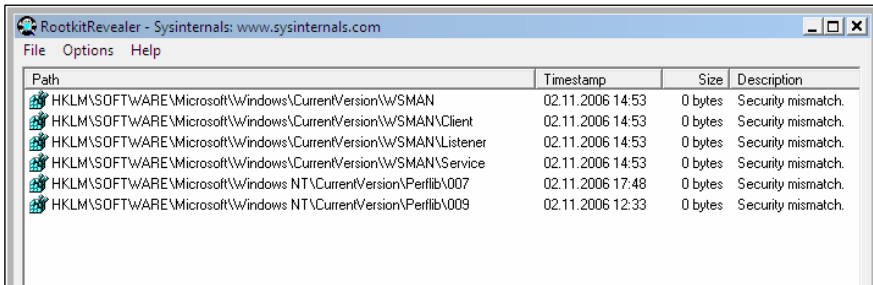
Scan starten

Programm unter Vista einsetzen

Anzeige auf separatem Desktop

**Sensibles
Spürtool**

Das Tool reagiert vergleichsweise sensibel und Fehlalarme sind nicht auszuschließen. Häufig genügt es bereits, wenn sich der Systemzustand im Laufe der Analysephase auch nur geringfügig ändert, und das Programm schlägt Alarm.



The screenshot shows the RootkitRevealer application window with the following data:

Path	Timestamp	Size	Description
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wsmn	02.11.2006 14:53	0 bytes	Security mismatch.
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wsmn\client	02.11.2006 14:53	0 bytes	Security mismatch.
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wsmn\listener	02.11.2006 14:53	0 bytes	Security mismatch.
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wsmn\service	02.11.2006 14:53	0 bytes	Security mismatch.
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\007	02.11.2006 17:48	0 bytes	Security mismatch.
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009	02.11.2006 12:33	0 bytes	Security mismatch.

Sensibles Spür-Tool: Fehlalarme wie hier bei einem frisch installierten Windows sind beim RootkitRevealer nicht auszuschließen.

**Eigeninitiative
gefragt**

Leider gibt das Tool von sich aus keine Hilfestellung bei der Klärung, ob es sich bei den angezeigten Unstimmigkeiten um begründete oder lediglich um Fehlalarme handelt. Dies gilt es im Zweifelsfall selbst zu recherchieren.

**Hier finden
Sie Antworten**

Eine erste Anlaufstelle für die Recherche ist das SysInternals-Forum, das Sie unter der Internet-Adresse „<http://forum.sysinternals.com>“ finden. Hier gilt es nach Informationen bezüglich der beanstandeten Registry-Schlüssel zu suchen oder die ausgegebenen Warnungen zwecks Risikobewertung im Forum einzustellen. Alternativ bietet sich eine Google-Suche an.

Positiver Rootkit-Befund – und nun?

Anders als der Blacklight Rootkit Eliminator bietet das SysInternal-Tool keine Möglichkeit, gefundene Rootkits einfach per Mausklick zu löschen.

**Problem:
Dateien löschen**

Sofern das Löschen verdächtiger Dateien bei laufendem Betriebssystem mit Bordmitteln nicht gelingt – bei aktiven Rootkits dürfte das die Regel sein –, bleibt Ihnen nur die Möglichkeit, ein separates Betriebssystem von CD/DVD zu booten und von diesem aus die nötigen Löschaktionen durchzuführen.

Unabhängiges Betriebssystem nötig

Dazu bietet sich beispielsweise das auf Linux basierende „Knoppix“ an. Die dafür nötigen Schritte erläutern die beiden Beiträge K 70 und D 41 in dieser Ausgabe.

Nutzen Sie Knoppix

Tipp: Da Fehlalarme nie gänzlich auszuschließen sind, empfiehlt es sich, verdächtige Dateien nicht direkt zu löschen, sondern zunächst lediglich die Dateiendungen zu ändern – beispielsweise von „.exe“ oder „.dll“ in „.test“.

Dateien umbenennen

Das genügt, um beim nächsten Systemstart das Laden beziehungsweise Ausführen der Rootkits zu verhindern, und ermöglicht dennoch in einem zweiten Schritt das schnelle Auffinden und Löschen der Dateien, sofern das System über einen längeren Zeitraum stabil läuft.

Dateien endgültig löschen

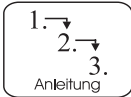
Viren aufspüren und beseitigen

Bescheinigen Ihnen die bisher eingesetzten Tools, dass Ihr PC frei von Rootkits ist, unterziehen Sie Ihr System als Nächstes einem Virenschnelltest:

Der Virenschnelltest

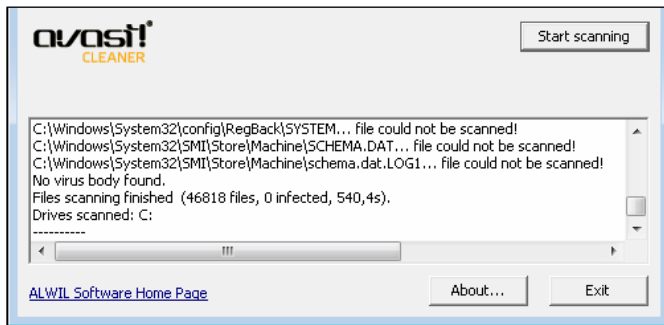
1. Starten Sie zunächst den „Virus Cleaner“ von Avast, indem Sie die Datei „aswclnr.exe“ von Ihrem Rettungsmedium ausführen.

Virus Cleaner einsetzen

**Administra-
torrechte
nötig****Scan starten**

Hinweis: Unter Vista müssen Sie das Programm explizit mit Administratorrechten ausführen. Dazu klicken Sie mit der rechten Maustaste auf die zugehörige EXE-Datei und wählen aus dem angezeigten Kontextmenü den Befehl „Als Administrator ausführen“ aus.

2. Klicken Sie anschließend auf die Schaltfläche „Start scanning“, um mit der Virensuche zu beginnen.



So weit ist alles okay: Anders als vollwertige Virenscanner überprüft der Virus Cleaner lediglich besonders gefährdete Systembereiche auf einschlägige Viren – das spart Zeit, lässt aber dennoch erste Rückschlüsse auf den Zustand des Systems zu.

**Avert Stinger
einsetzen**

Sofern die Überprüfung Ihres Systems mit dem Virus Cleaner keine Viren zutage fördert, überprüfen Sie das System anschließend mit „Avert Stinger“:

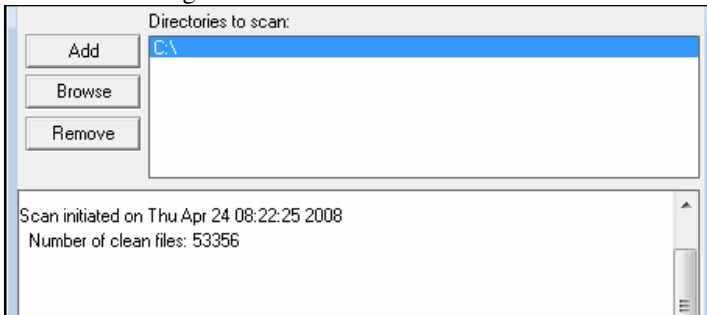
**Programm
ausführen**

1. Führen Sie von Ihrem Notfallmedium die Datei „stng380.exe“ aus.

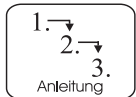
Scan starten

2. Starten Sie die Virensuche mit einem Klick auf die Schaltfläche „Scan Now“.

Hinweis: Auch Avert Stinger sollten Sie unter Vista mit Administratorrechten starten, damit das Programm auf möglichst viele Dateien Zugriff erhält.



Administratorrechte empfohlen



Glück gehabt: Der Scan lief ohne Alarmmeldung durch!

Um es nochmals in aller Deutlichkeit zu sagen: Die beiden Tools stellen keinen Ersatz für einen umfassenden Scan mit einem vollwertigen Antiviren-Programm dar, sondern dienen lediglich als „Erkundungstrupp“.

Kein Ersatz für umfassenden Scan

Fallen die Tests negativ aus, sinkt jedoch die Wahrscheinlichkeit, dass sich ein Virus eingeschlichen hat, sodass Sie einen intensiven Virencheck getrost auf die kommende Nacht verschieben können.

Kalkulierbares Risiko

Anschließend sollten Sie Ihr Augenmerk zunächst auf eine weitere Gruppe von Schädlingen werfen, nämlich auf Ad- und Spyware-Programme.

Weitere Schädlinge suchen

Ad- und Spyware-Programme mit Ad-Aware 2007 aufspüren und beseitigen

Setzen Sie Spezialprogramme ein

Bislang ist es bei Tests von Antiviren-Programmen noch nie vorgekommen, dass das leistungsfähigste Antiviren-Programm zugleich den besten Schutz vor Trojanern und Spyware bot. Daher ist eine intensive Untersuchung mit Spezialprogrammen wie „Spybot – Search & Destroy“ oder „Ad-Aware 2007 Free“ Pflicht.

Ad-Aware bietet eine intuitive Bedienung

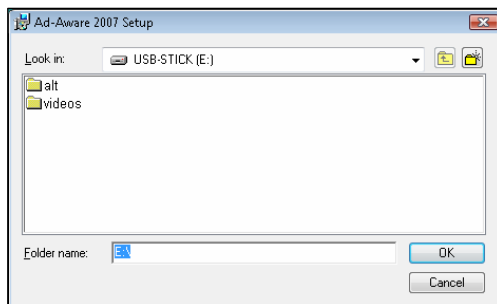
Die Suchleistung der beiden Programme ist vergleichbar, sodass es genügt, sich für eines zu entscheiden. Wir haben uns für diesen Beitrag für Ad-Aware 2007 Free entschieden, da die Benutzeroberfläche etwas übersichtlicher als bei Spybot – Search & Destroy gestaltet ist und sich daher leichter bedienen lässt.

Installation zwingend nötig

Anders als die bis dato eingeführten Programme kommt Ad-Aware – wie im Übrigen auch Spybot – Search & Destroy – nicht ohne Installation aus, was das Programm prinzipiell anfällig für Manipulationen durch Schädlinge macht.

USB-Stick als Installationsort angeben

Das Risiko lässt sich allerdings minimieren, indem Sie das Programm von vornherein auf Ihrem USB-Rettungsmedium installieren. Lediglich einige Registry-Schlüssel landen dann noch auf der Festplatte Ihres PCs.



Indem Sie die Installation von Ad-Aware direkt auf dem Stick durchführen, können Sie das spätere Manipulationsrisiko auf ein Minimum reduzieren.

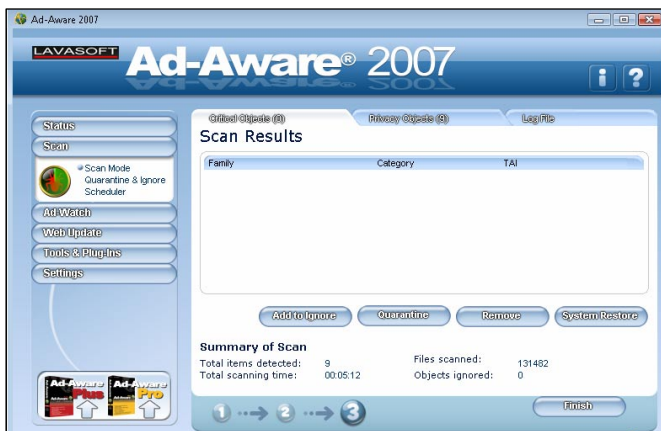
Im Krisenfall gehen Sie dann wie folgt vor:

1. Starten Sie Ad-Aware direkt vom Stick aus und klicken Sie im Hauptprogrammfenster unter „System Scan“ auf „Scan Now“.
2. Im nächsten Schritt wählen Sie dann die Scan-Methode aus. Wir empfehlen Ihnen, den voreingestellten „Smart Scan“-Modus beizubehalten. Er bietet einen sinnvollen Kompromiss zwischen Aufwand und Nutzen.
3. Klicken Sie anschließend auf die Schaltfläche „Scan“, um die Suche zu starten.

**Programm
starten**

**Scan-Methode
auswählen**

Scan starten



Einmal auf dem Stick installiert, verrichtet Ad-Aware auch bei aktiviertem Schreibschutz seinen Dienst und bescheinigt uns ein Ad- und Spyware-freies Testsystem.

Nacharbeiter: So überprüfen Sie Ihr System über Nacht intensiv auf Viren

Letzte Zweifel ausräumen

Im letzten Schritt gilt es, das verbleibende Restrisiko einer Vireninfektion zu minimieren. Das gelingt am besten, indem Sie Ihr System mithilfe von Knoppix über Nacht einem intensiven Virens캔 unterziehen.

Leistungsfähige Viren-scanner

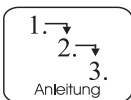
Dazu benötigen Sie zu allererst eine leistungsfähige Antiviren-Software für Linux wie beispielsweise „avast! Home“, „F-Prot Antivirus“ oder „BitDefender Free Edition“.

Lokaler Download möglich

In aller Regel können Sie die gepackten Antiviren-Programme bedenkenlos auf Ihren PC herunterladen – selbst wenn dieser möglicherweise infiziert ist: Bisher ist uns kein Windows-Virus bekannt, das in der Lage ist, Linux-Archivformate wie DEB oder RPM zu lesen, geschweige denn zu infizieren.

Direkter Download

Sofern Ihr PC über einen Router mit dem Internet verbunden ist, können Sie die Antivirenprogramme allerdings genauso gut direkt unter Knoppix herunterladen und installieren. Knoppix stellt die nötige Internetverbindung in diesem Fall automatisch her.



avast! Home for Linux unter Knoppix installieren

Um den avast!-Scanner direkt unter Knoppix herunterzuladen und zu installieren, gehen Sie wie folgt vor:

PC booten

1. Booten Sie Ihren PC von der Knoppix-DVD.

Web-Browser starten

2. Starten Sie den Web-Browser „Firefox“ alias „Iceweasel“, indem Sie in der Button-Leiste am unteren Bildschirmrand auf das zweite Symbol von rechts klicken.



Unter Knoppix firmiert der Firefox-Browser unter dem Namen „Iceweasel“.

3. Klicken Sie dann unter der Adresse <http://www.avast.de/index.php/avast-Home-for-Linux.html> auf den Link „avast! 4.7 Free Home Linux Edition – DEB Paket“ und laden Sie die dazugehörige Datei herunter.

Programmpaket herunterladen

Hinweis: Sie finden die mit Iceweasel heruntergeladenen Dateien auf dem Knoppix-Desktop. Physikalisch landen die Dateien allerdings nicht auf der Festplatte Ihres PCs, sondern sie werden lediglich temporär im Arbeitsspeicher (RAM-Disk) gespeichert.

Alle Daten landen im Arbeitsspeicher

4. Anschließend klicken Sie im Browser-Fenster auf den Link „avast! 4.7 Free Home Linux Edition – Lizenzschlüssel“ und registrieren sich. Per E-Mail erhalten Sie dann eine kostenlose Lizenz für ein Jahr.

Lizenzschlüssel beantragen

5. Als Nächstes öffnen Sie eine Konsole – das Pendant zur Windows-Eingabeaufforderung –, indem Sie in der Button-Leiste am unteren Bildschirmrand auf das Bildschirm-Symbol klicken.

Konsole öffnen

```
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe
knoppix@knoppix:~$ su
root@knoppix:/ramdisk/home/knoppix# dpkg -i /home/knoppix/Desktop/
p/avast4workstation_1.0.8-2_i386.deb
Wähle vormals abgewähltes Paket avast4workstation.
(Lese Datenbank ... 552355 Dateien und Verzeichnisse sind derzeit
installiert.)
Entpacke avast4workstation (aus .../avast4workstation_1.0.8-2_i3
86.deb) ...
Richte avast4workstation ein (1.0.8-2) ...
root@knoppix:/ramdisk/home/knoppix#
```

Den Virens Scanner gilt es per Konsole zu installieren.

Programm installieren



6. Im Konsolenfenster geben Sie dann nacheinander die beiden folgenden Befehle ein (jeweils mit der Enter-Taste, wo angezeigt, abschließen):

```
su [Enter]
dpkg -i
/home/knoppix/Desktop/avast4workstation_1.0.8-
2_i386.deb [Enter]
```

Dateipfad kontrollieren

Hinweis: Sofern Sie das Programm nicht auf dem Desktop zwischengespeichert haben oder eine neue Version erhältlich ist, müssen Sie den Dateipfad entsprechend anpassen.

Benutzeroberfläche starten

7. Um die grafische Benutzeroberfläche des Scanners zu starten, geben Sie den Befehl „avastgui“ ein. Es öffnet sich ein Registrierungsdialog, in dem Sie zuvor noch den per E-Mail erhaltenen Lizenzschlüssel eingeben müssen.

Den PC mit avast! Home for Linux auf Viren untersuchen

Die Benutzeroberfläche der Linux-Version des avast!-Scanners unterscheidet sich erheblich von der der Windows-Version, sodass wir die Bedienschritte hier kurz erklären:

Eigenes Linux-Design

Signaturen aktualisieren

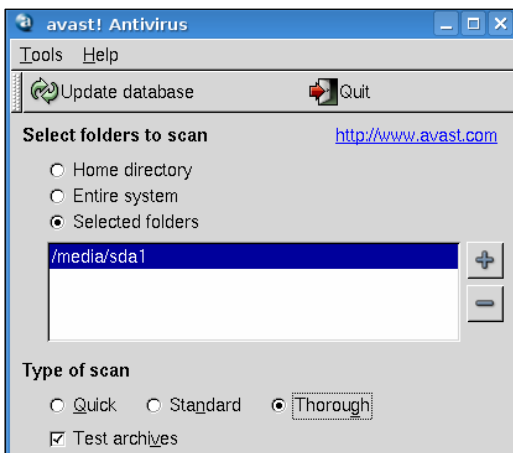
1. Führen Sie zunächst ein Update der Virensignaturen durch, indem Sie auf die Schaltfläche „Update database“ klicken.

Zu scannende Laufwerke auswählen

2. Anschließend klicken Sie unter „Select folder to scan“ auf die Option „Select folders“ und wählen dann die Festplatte(n) Ihres PCs aus.

Hinweis: Anders als Windows bindet Linux die lokalen Festplatten grundsätzlich als normale Dateiodner in den Verzeichnisbaum ein. Die Festplatten Ihres Rechners finden Sie im Linux-Verzeichnisbaum unter „/media/[Linux-Name des Laufwerks]“.

3. Unter „Type of scan“ wählen Sie die gründliche „Thorough“-Methode aus, setzen ein Häkchen vor „Test archives“ und klicken abschließend auf „Start Scan“.



Mit avast! steht Ihnen ein leistungsfähiger und zugleich kostenloser Virens Scanner zur Verfügung.

Je nach Anzahl der zu überprüfenden Dateien kann die Überprüfung des Systems durchaus einige Stunden dauern. Ein intensiver Scan bietet sich daher über Nacht an.

Laufwerke als gewöhnliche Dateiodner

Scan-Methode auswählen und Scan starten

Scan über Nacht durchführen



Entwarnung: In unserem Fall gibt der avast!-Scanner grünes Licht.

Verhalten im Ernstfall

Sollte avast! fündig werden, öffnet sich ein Dialogfenster, in dem Sie verschiedene Aktionen durchführen können. Sofern Sie sich unsicher sind, wählen Sie die vom Programm vorgeschlagene Aktion aus.



Ruhe bewahren: Wenn der Scanner Alarm schlägt, folgen Sie im Zweifelsfall der empfohlenen Anweisung.

B-Probe mit BitDefender Free Edition für Linux

Zwei Scanner entdecken mehr als einer

Wie schon bei der Rootkit-Suche sollten Sie sich auch beim Virensan durch den Einsatz eines zweiten Scanners absichern.

Wir empfehlen für diesen Zweck die Linux-Version des „BitDefender“-Scanners. Die Installation meistern Sie wie folgt:

1. Laden Sie zunächst unter der Adresse:
„http://download.bitdefender.com/SMB/Workstation_Security_and_Management/BitDefender_Antivirus_Scanner_for_Unices/Unix/Current/EN/Version_7.x/Linux/“ die Datei „BitDefender-scanner-7.5-4.linux-gcc3x.i586.deb.run“ herunter.
2. Öffnen Sie eine Konsole und geben Sie nacheinander die folgenden Befehle ein:

**Programm
herunterladen**

**Programm
installieren**

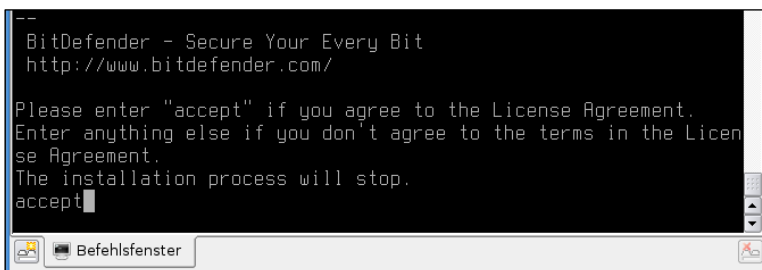
```
su [Enter]
sh /home/knoppix/Desktop/BitDefender-scanner-
7.5.4.linux-gcc3x.i586.deb.run [Enter]
```

Hinweis: Im Beispiel gehen wir davon aus, dass Sie das heruntergeladene Programmarchiv auf dem Knoppix-Desktop gespeichert haben. Andernfalls müssen Sie die Dateipfade entsprechend anpassen.

**Dateipfad
anpassen**

3. Mithilfe der Leertaste blättern Sie sich anschließend durch die Nutzungsbedingungen. Am Ende des Dokuments geben Sie den Befehl „accept“ ein und bestätigen mit der Enter-Taste.

**Nutzungsbe-
dingungen
abnicken**



Vor der ersten Verwendung müssen Sie die Nutzungsbedingungen per Kommandozeilenbefehl abnicken.

Scannen per Kommandozeile



**Diese Befehle
benötigen Sie
Signaturen
aktualisieren**

Wie viele Anwendungen unter Linux verzichtet auch die Linux-Variante des Bitdefender-Scanners auf eine grafische Benutzeroberfläche. Die Bedienung erfolgt stattdessen per Kommandozeile. Dennoch kommen Sie mit wenigen Kommandos zum Ziel:

1. Aktualisieren Sie zunächst die Virensignaturen, indem Sie in der Konsole die folgenden beiden Befehle eingeben:

```
su [Enter]
bdscan --update [Enter]
```

Scan starten

2. Mit dem folgenden Befehl starten Sie den Scan:

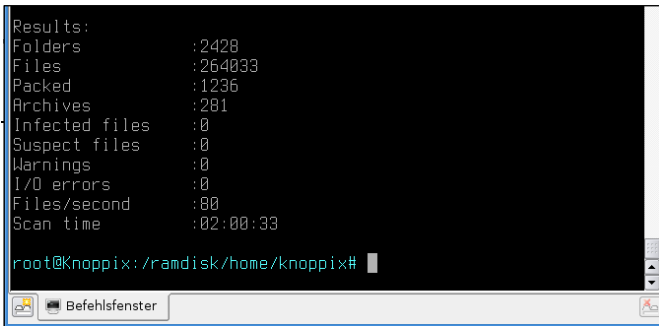
```
bdscan /media/sda1/ --action=quarantine
```

**Lokale Fest-
platten scan-
nen**

Zur Erklärung: Der Befehl weist den Scanner an, das Verzeichnis „/media/sda1/“, also die primäre Systempartition, auf Viren zu untersuchen. Wird der Scanner fündig, werden die betroffenen Dateien standardmäßig in das Verzeichnis „/opt/BitDefender-scanner/“ verschoben.

**Quarantäne-
verzeichnis
anpassen**

Da dieses Verzeichnis nur virtuell im Arbeitsspeicher existiert, gehen die Dateien verloren, sobald Sie Knoppix beenden. Dem können Sie vorbeugen, indem Sie mittels des Befehls „--quarantine=*[Pfad]*“ den Speicherpfad entsprechend umleiten – beispielsweise in ein Verzeichnis auf der lokalen Festplatte.



```
Results:
Folders      :2428
Files        :264033
Packed       :1236
Archives     :281
Infected files :0
Suspect files :0
Warnings     :0
I/O errors   :0
Files/second :80
Scan time    :02:00:33

root@Knoppix:/ramdisk/home/knoppix#
```

Systemüberprüfung erfolgreich abgeschlossen: Der BitDefender-Scanner hat nichts gefunden.