Desinfec’t 2017

Malware zuverlässig aufspüren und entfernen

Einmal kurz nicht aufgepasst und einen Klick später ist Windows verseucht. Ist ein Schädling wie WannaCry eingedrungen, hilft nur schnelles Ausschalten. Dann bietet sich Desinfec't als zuverlässiger Helfer in der Not an: Das Tool schickt vier Virenscanner von Avira, Eset, F-Secure und Sophos auf die Jagd, die das inaktive Windows-System von außen säubern.

Von Dennis Schirrmacher

Desinfec't ist ein von c't entwickeltes System zum Scannen und Reinigen von Windows-Rechnern. Wer es bereits kennt, kann ohne Umschweife zum nächsten Artikel springen, in dem es direkt ans Eingemachte geht. Außer der Beschreibung neuer Funktionen in Desinfec't 2017 lesen Sie dort Praxis-Tipps für den reibungslosen Start des Tools und wie Sie Windows-Computer am effektivsten von Trojanern säubern.

Helfer im Ernstfall

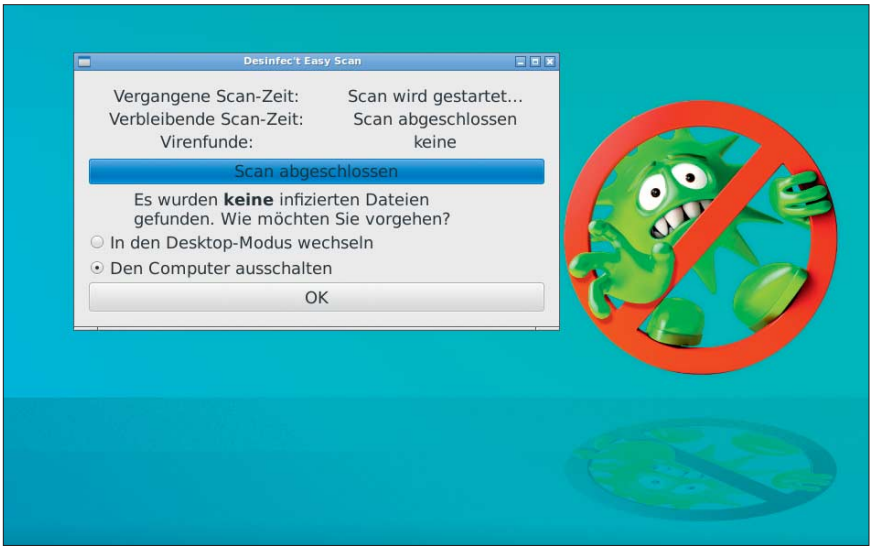
Desinfec't 2017 richtet sich an Windows-Nutzer und untersucht das komplette System auf Adware, Trojaner & Co. Das Sicherheitstool ersetzt dabei nicht den in Windows verankerten Virenscanner. Vielmehr ist es ein zusätzliches Werkzeug, das nach einer Infektion die letzte Rettung sein kann. Es wird nicht installiert, sondern bringt ein eigenes Live-System auf Linux-Basis mit, welches direkt von DVD oder USB-Stick startet. Damit untersucht man aus sicherer Entfernung ein möglicherweise infiziertes Windows.

Versucht man den Schädling im laufenden System aufzuspüren, kann er währenddessen weiteres Unheil anrichten. So könnte ein Erpressungstrojaner weitere Dateien verschlüsseln, um anschließend Lösegeld zu fordern. Sogenannte Rootkits manipulieren außerdem Systemfunktionen, um einer Entdeckung zu entgehen und sich auch vor Antiviren-Software zu verstecken. Wenn Windows jedoch gar nicht läuft, kann ein dort eingenisteter Schädling auch kein Unheil anrichten. Mit Desinfec't startet man ein garantiert sauberes System und hat somit eine optimale Basis für die nachfolgende Untersuchung. Dabei muss man keine Angst haben, dass ein Schädling das Live-System ansteckt: Schließlich können sich Windows-Trojaner nur innerhalb von Microsofts Betriebssystem breitmachen.

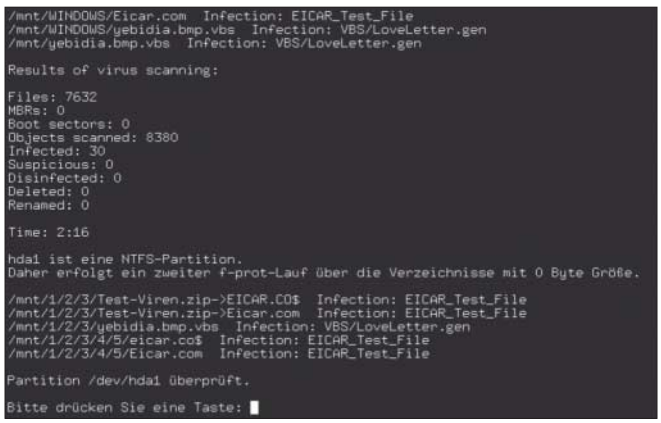
Desinfec't arbeitet gleich mit vier professionellen Viren-Jägern. Auf Wunsch kann man im Rahmen eines einzigen Komplettscans die Virenscanner von Avira, Eset, F-Secure und Sophos über das gesamte System schicken. Um auch neue Schädlinge zu erkennen, müssen die dazu auf aktuelle Virensignaturen zugreifen können. Das erforderliche Update erledigt Desinfec't automatisch. Alles was es dazu braucht, ist eine Internetverbindung. Die richtet es in einem herkömmlichen Netz mit Kabeln automatisch ein; mit dem WLAN kann man Desinfec't über wenige Mausklicks vernetzen. Die Updates sind bis Juni 2018 inklusive.

Nach dem Scan, der durchaus ein paar Stunden dauern kann, präsentiert Desinfec't eine übersichtliche Liste mit möglichen Virenfunden. Dabei liefert es eine Reihe verschiedener Infos, die dabei helfen, die Gefahr einzuschätzen oder einem durchaus möglichen Fehlalarm auf die Spur kommen.

Ist die Gefahr real, hilft Desinfec't auch beim Reinigen des Systems. Nach dem Start arbeitet es im Nur-Lese-Modus, um ungewolltes Löschen benötigter Dateien zu verhindern. Um einen Virus



Desinfec't 2017 untersucht ein verseuchtes Windows aus sicherem Abstand. Dank Easy Scan gelingt das auch Computer-Einsteigern.



In der ersten Version aus dem Jahr 2003 hieß Desinfec't noch Knoppicillin. Seitdem wurde die Bedienung viel einfacher und es kamen auch eine Menge neue Funktionen hinzu.

unschädlich zu machen, muss man Desinfec't explizit Schreibzugriff gewähren.

Standardmäßig löscht Desinfec't gefundene Viren nicht, sondern benennt sie um, indem es die Erweiterung .VIRUS an den Dateinamen anhängt. Das verhindert, dass der Schädling ausgeführt wird und hat einen wesentlichen Vorteil: Setzt man bei der Säuberung fälschlicherweise eine wichtige Datei schachmatt und startet etwa Windows im Anschluss nicht mehr, kann man das Umbenennen einfach rückgängig machen.

Eins darf man nicht vergessen: Trotz vier Scannern ist Desinfec't kein Allheilmittel. Viele Nebenwirkungen einer Infektion kann es prinzipbedingt nicht beseitigen. Verändert der Schädling etwa wichtige Systemeinstellungen von Windows, bleiben diese Änderungen auch nach dem Entfernen der bösartigen Datei erhalten und gefährden weiterhin Stabilität und Sicherheit des Systems. Hat ein Trojaner etwa die Windows Firewall durchlöchert, Freigaben aktiviert und zusätzliche Benutzer eingerichtet, hat man auch ohne Trojaner ein unsicheres System. Wer auf Nummer sicher gehen will, rettet seine wichtigen Daten etwa auf eine USB-Festplatte und installiert Windows neu.

Jeder kann loslegen

Die Oberfläche und die Bedienung von Desinfec't sind bewusst einfach gehalten. Einen Scan startet man mit wenigen Mausklicks und selbst für das Reinigen benötigt man keine Linux-Kenntnisse. Dank aussagekräftiger Symbole und Beschriftungen können sich auch Computer-Einsteiger auf die Pirsch nach Trojanern machen und Erfolge erzielen. Und wenn es dann doch einmal zu kompliziert wird, ruft man mit der integrierten Fernwartungssoftware TeamViewer den Familien-Admin zu Hilfe, damit sich dieser den zu verarztenden Computer aus der Ferne anschauen kann. Vorsorgliche c't-Leser statten deshalb Familie und Freunde mit Desinfec't-Sticks aus. Diese kann man ganz einfach über „Bootfähigen USB-Stick mit Desinfec't erzeugen" erstellen. Sie dürfen Desinfec't also nicht nur für den eigenen Bedarf nutzen, sondern auch an Verwandte und Freunde weitergeben.

Für den Onkel, der sich mit Technik überhaupt nicht auskennt, kann man den Desinfec't-Stick auch standardmäßig mit dem Easy Scan booten lassen. Er macht Desinfec't noch zugänglicher und startet das Tool in einem abgespeckten Modus, in dem nichts vom Scannen ablenkt.

Computer-Profis können sich mit Desinfec't auch austoben. Dazu bietet Desinfec't Experten-Tools zum Klonen von Partitionen, für die Suche nach gelöschten Dateien und zum sicheren Löschen. Aber Vorsicht: Wer nicht weiß, wie man diese Experten-Tools richtig bedient, kann im schlimmsten Fall eine Windows-Installation zerstören oder sogar alle Daten unwiederbringlich löschen. Bei Bedarf kann Desinfec't zudem auch verschlüsselte Dateien und Partitionen einbinden und diese untersuchen. Darüber hinaus können Profis mit etwas Aufwand weitere Programme aus der Linux-Welt nachinstallieren und Desinfec't den eigenen Bedürfnissen anpassen.

Digital-Abonnenten und Käufer der digitalen Ausgabe können ihre Kopie in Form einer ISO-Datei herunterladen (Anleitung siehe ct.de/ympe). Damit lässt sich unter Windows sogar ohne DVD-Laufwerk in wenigen Schritten ein USB-Stick bauen, von dem Desinfec't startet. Einen öffentlichen Download von Desinfec't dürfen wir aus lizenzrechtlichen Gründen nicht anbieten.

Auch in Behörden, Firmen und Schulen oder anderen Lehranstalten ist die Nutzung von Desinfec't ausdrücklich erlaubt. Lediglich der Einsatz des eingebauten TeamViewers ist auf den privaten Bereich beschränkt.

Offenes Ohr

Desinfec't hat mittlerweile eine große Fan-Gemeinde, die sich vor allem in unserem Forum austauscht (siehe ct.de/ympe). Dort ist auch der richtige Ort, um Fragen zu stellen oder Probleme zu schildern. Viele Nutzer helfen gerne mit ihrem Wissen weiter. Aber auch die Entwickler von Desinfec't lesen dort mit und stehen mit Tipps und Anregungen zur Seite. Zeichnen sich ernste Fehler ab, stellen wir möglichst zeitnah Updates zur Verfügung, die sich bei aktiver Internetverbindung automatisch installieren. Wir freuen uns über Kritik und Lob und ganz besonders über Ideen für neue Funktionen kommender Desinfec't-Editionen. *(des@ct.de)* c't

Download-Anleitung, Hilfe-Forum:
ct.de/ympe