Desinfec’t 2019

Was das Notfallsystem Desinfec’t alles kann

Wer befürchtet, sich einen Virus eingefangen zu haben, sollte das Sicherheitstool Desinfec't starten. Das Live-System läuft eigenständig und von Windows abgeschottet. So können Sie Trojaner aus sicherer Entfernung aufspüren und ausschalten. Das Tool kann aber noch mehr und beispielsweise Daten retten.

Von Dennis Schirrmacher

Desinfec't ist das seit mehr als 15 Jahren etablierte Notfallsystem der c't-Redaktion, dass direkt von DVD oder einem USB-Stick startet. Mit den integrierten Scannern von Eset, F-Secure, Kaspersky und Sophos spürt man nicht nur Viren auf, sondern macht sie auch unschädlich. Außerdem kann man über das Notfallsystem Daten von einem nicht mehr startenden Windows auf USB-Datenträger kopieren und somit wichtige Dokumente wie eine Abschlussarbeit retten. Unter Umständen ist es sogar möglich, versehentlich gelöschte und somit verloren geglaubte Dateien wiederherzustellen. Für all das braucht man keinen Titel in Raketenwissenschaften. Die Bedienung ähnelt der von Windows und auf dem Desktop sollte sich die meisten sofort zurechtfinden. So kann jeder ohne viel Vorwissen direkt eine Virenjagd starten und eine ganze Reihe typischer PC-Probleme lösen.

Sie dürfen das Notfallsystem gerne Familienmitgliedern und Bekannten in die Hände drücken. Auch der Einsatz von Desinfec't beispielsweise an Unis und in Firmen ist erlaubt. Fairerweise sollten sie für jede aktiv genutzte Desinfec't-Instanz eine Lizenz in Form eines Heftes erwerben. Nur die Software TeamViewer zum Fernsteuern von Computern ist auf den privaten Gebrauch beschränkt.

Neu in Desinfec't 2019 ist der Projektordner. Dieser bildet den zentralen Punkt bei der Arbeit mit dem zu untersuchenden System. Sie können diesen Ordner mit einem individuellen Namen wie „Papas Spielekiste“ versehen. Dort landen neben Ergebnislisten von Scans auch andere Daten. Beispielsweise wichtige von einem möglicherweise infizierten Windows-Computer gerettete Dokumente und Fotos. Die Dateien in diesem Ordner bleiben beim Start von einem USB-Stick auch nach einen Neustart von Desinfec't erhalten und man kann sie zudem an einem anderen Computer öffnen. Desinfec't erkennt diesen PC übrigens beim nächsten Start wieder und verknüpft ihn erneut mit dem selben Projektordner. So bewahrt man beispielsweise die Scan-Ergebnisse vom Arbeits- und Heim-PC übersichtlicher auf. Wer das Sicherheitstool schon kennt, kann übrigens gleich zum nächsten Artikel springen und direkt in die Praxis einsteigen.

Das ist Desinfec't

Desinfec't ist ein Live-System auf Basis der Linux-Distribution Ubuntu. Für den Betrieb muss Windows komplett heruntergefahren sein. So kann man aus einem sicheren Abstand auf das inaktive Betriebssystem gucken und ein Trojaner kann nicht noch mehr Schaden anrichten. Da Desinfec't auf Linux basiert, braucht man keine Angst haben, dass für Windows geschriebene Viren auf das System überspringen. Außerdem versetzt sich Desinfec't nach jedem Neustart in den Werkszustand zurück und es ist nach jedem Reboot wie neu. Als Vorsichtsmaßnahme kann Desinfec't standardmäßig von Windows-Festplatten nur lesen und nicht darauf schreiben und Daten verändern. Erst wenn Sie etwas verändern wollen, um etwa den aufgespürten Trojaner unschädlich zu machen, schalten Sie den Schreibmodus explizit ein. So brauchen Sie auch keine Angst zu haben, etwas kaputt zu machen.

»Desinfec't kann neben Windows auch verloren geglaubte Dateien retten.«

Das System startet direkt von der Heft-DVD – merkt sich Daten aber nur flüchtig im RAM. So kann man nichts dauerhaft speichern und muss Signaturen und Updates nach jedem Reboot neu aus dem Internet herunterladen. Besser ist es, Desinfec't auf einen USB-Stick zu kopieren. Das kann man direkt unter Windows machen oder man startet Desinfec't und erzeugt aus dem laufenden System einen Stick mit dem Notfallsystem. In beiden Fällen benötigt man zwingend einen USB-Stick mit mindestens 16 GByte Speicherplatz. Von einem Stick läuft das System nicht nur deutlich verlässlicher, sondern es kann sich auch Sachen wie aktualisierte Virensignaturen oder Desinfec't-Updates merken. Diese Daten landen auf einer beschreibbaren Partition.

Virenjäger am Start

Da Desinfec't keine Windows-Anwendung ist, muss man das Betriebssystem herunterfahren und in den Bootoptionen des Computers das Medium mit Desinfec't auswählen. Wie das im Detail funktioniert, erklärt der direkt im Anschluss folgende Praxisartikel verständlich in einer Bilderstrecke. Dort stehen auch Tipps, wie man das Notfallsystem unter Umständen auf Computern zum Laufen kriegt, auf denen es mit der Standard-Startmethode den Dienst verweigert. In der Redaktion haben wir das System auf verschiedenen Desktop-Computern und Laptops mit brandneuer, aber auch älterer Hardware erfolgreich getestet.

Der Desktop des Systems und die Startleiste sind bewusst reduziert gehalten, damit nichts vom eigentlichen Zweck des Sicherheitstools ablenkt. Aussagekräftige Icons erleichtern die Bedienung – hier sollten sich neben Windows-Nutzern auch Computer-Neulinge zurechtfinden. Um einen Virenscan zu starten, muss man lediglich das entsprechende Icon doppelt anklicken. Die Scanner schauen sich standardmäßig die komplette Windows-Installation an. Es ist aber auch möglich, nur einzelne Ordner auf Festplatten oder USB-Sticks untersuchen zu lassen.

Standardmäßig ist nur Eset als Scanner ausgewählt, bei Bedarf kann man weitere hinzuwählen. Oft reicht es, um einen ersten Eindruck von einer möglicherweise

verseuchten Windows-Installation zu bekommen, erst mal nur einen Scanner von der Leine zu lassen. Wer möchte, kann aber auch alle vier Scanner hintereinander laufen lassen. Nicht wundern: Machen sich alle vier Scanner auf die Jagd, kann das schon mal die ganze Nacht dauern. Mit den Einstellungen in den Expertenfunktionen kann man die Scanner noch tiefer graben lassen.

Vor einem Scan aktualisiert Desinfec't automatisch die Virensignaturen, damit die Scanner auch die neuesten Schädlinge erkennen. So ist man in der Regel gut gerüstet. Man muss sich aber darüber im Klaren sein, dass es für brandneue Trojaner mitunter noch keine Signatur gibt und ein Virus nicht erkannt wird. Nimmt man Desinfec't zum ersten Mal in Betrieb, kann es bis zu einer halben Stunden oder sogar länger dauern, bis die Signaturen aktualisiert sind. Eset, F-Secure, Kaspersky und Sophos stellen dafür bis Juni 2020 kostenlose Signaturupdates bereit.

Fehlalarme deuten

Wer sich mit Computern nicht so gut auskennt, sollte im Startmenü des Notfallsystems den Easy-Scan-Modus auswählen. Hier landet man ohne Umwege direkt in einem Scan-Assistenten und der Scanner von Eset schaut automatisch auf Windows-Festplatten. Das ist übersichtlich und unkompliziert. Wer einen Desinfec't-Stick etwa für den Onkel ohne große Computer-Kenntnisse erstellt, kann den Easy-Scan auch als Standard voreinstellen.

Egal wie man scannt, am Ende bekommt man im Webbrowser eine Ergebnisliste serviert. In dieser Liste finden sich weiterführende Infos zu Funden, damit man eventuelle Fehlalarme besser einschätzen kann. So lädt man verdächtige Dateien zum Beispiel mit einem Klick zur kostenlosen Untersuchung zur Analyse-Plattform VirusTotal hoch. Dort schauen nochmal rund 60 Scanner auf die Datei und geben eine Einschätzung ab. Außerdem bietet Firefox Links zu verschiedenen Viren-Datenbanken und weiteren Analyse-Websites.

Deutet alles auf einen Trojaner hin, kann man diesen mit Desinfec't natürlich auch unschädlich machen. Das geht ganz einfach mit einem Mausklick. Allerdings muss man sich der Tatsache bewusst sein, dass man auf diesem Weg nicht alle Veränderungen am System erkennen und beseitigen kann. Hat der Trojaner etwa automatische Sicherheits-Updates und Firewall abgeschaltet oder einen neuen Benutzer und Dateifreigaben angelegt, wird das Desinfec't nicht erkennen oder gar reparieren können. Deshalb sollte man einen verseuchten Windows-PC in der Regel komplett neu aufsetzen. Dafür löscht man das Betriebssystem und alle Daten auf der Festplatte komplett und installiert Windows neu.

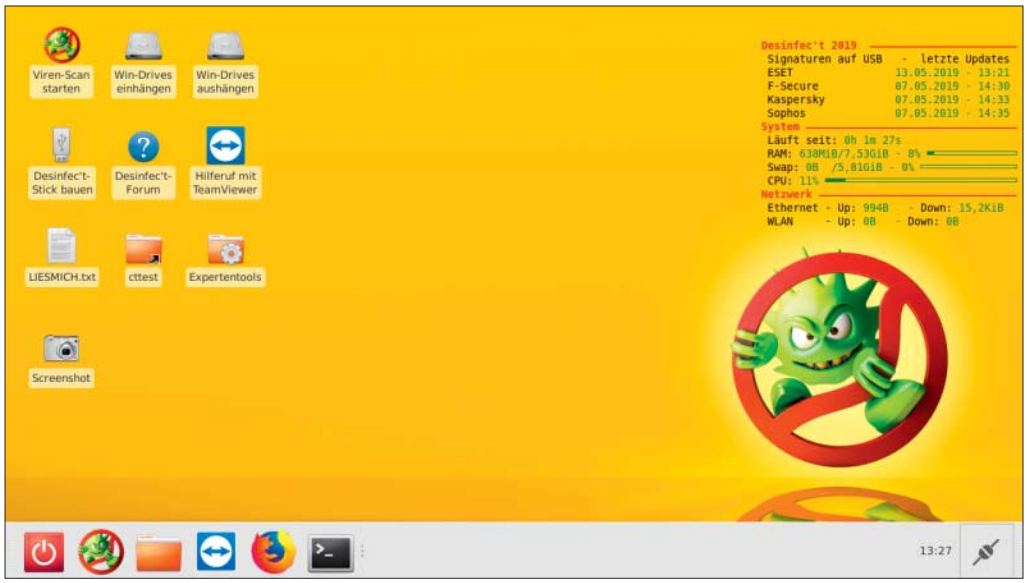
Wer im normalen Desinfec't-Betrieb Hilfe benötigt, kann sich beispielsweise den Familien-Admin direkt auf den Computer holen. Das funktioniert mit der vorinstallierten Fernwartungssoftware TeamViewer. Dafür müssen beide Seiten nur über eine Internetverbindung verfügen und die Anwendung starten. Ist das gegeben, kann der Familien-Admin die Kontrolle übernehmen und mit seiner Maus und Tastatur den Problem-PC fernsteuern, um nach dem Rechten zu sehen.

Für Profis

Auf dem Desktop ist ein Ordner mit Expertentools. Mit den darin befindlichen Werkzeugen können Nutzer mit guten Computer-Kenntnissen beispielsweise versehentlich gelöschte Fotos von einer Speicherkarte wiederherstellen und ganze Festplattenpartitionen klonen oder Datenträger sicher löschen. Doch aufgepasst: Wie der Name schon sagt, sind diese Werkzeuge nur für Nutzer, die genau wissen, was sie tun. Hier findet man auch ein Skript, das mit Desinfec't behandelte Dateien wieder in den Originalzustand zurückversetzen kann. Das ist zum Beispiel hilfreich, falls ein Virenscanner eine wichtige Systemdatei fälschlicherweise als Virus erkannt hat und diese dann unschädlich gemacht hat.

Natürlich haben wir ein offenes Ohr für Probleme mit Desinfec't. Doch bevor Sie sich via Mail oder über das offizielle Forum (siehe ct.de/yxs4) an uns wenden, lesen Sie den folgenden Praxisartikel bitte ganz genau. In den vergangenen Jahren haben sich vor allem Start-Probleme oft von selbst gelöst, wenn Nutzer den Artikel nochmal ganz genau gelesen haben. Taucht ein echter Bug auf, versuchen wir, den Fehler so schnell wie möglich zu lösen und ein Desinfec't-Update bereitzustellen. Dieses installiert sich in der Regel vollkommen automatisch, wenn Sie Desinfec't bei einer bestehenden Internetverbindung starten. *(des@ct.de)* c't

Desinfec't-Forum: ct.de/yxs4



Das Live-Sytem Desinfec't 2019 bringt vier Viren-Scanner von Eset, F-Secure, Kaspersky und Avira mit, um Windows-Installationen zu untersuchen.