Desinfec’t 2020

Was das Anti-Viren-System alles kann

Bild: Andreas Martini

Die aktualisierte Version des seit über 15 Jahren bewährten Sicherheitstools der c't-Redaktion ist da. Neben den vier Virenscannern ist neuerdings ein offener Threat-Scanner mit an Bord, der Emotet und andere Bedrohungen sehr effektiv aufspürt. Hier lesen Sie, wie Desinfec't Ihnen beim Reinigen vermutlich infizierter Windows-Systeme hilft.

Von Dennis Schirrmacher

Desinfec't 2020 richtet sich an Windows-Nutzer und kann von Trojanern verseuchten Systemen auf die Beine helfen. Damit spüren Sie Viren auf und erledigen diese. Dafür bringt das Sicherheitstool vier Virenscanner von Eset, F-Secure, Kaspersky und Sophos mit. Damit die Scanner auch aktuelle Schädlinge nicht übersehen, sind ein Jahr lang kostenlose Signatur-Updates inklusive.

Das Sicherheitstool ist nicht nur was für Profis, sondern holt auch Einsteiger ab. Computer-Neulinge unterstützt Desinfec't mit dem Easyscan-Modus. Über die integrierte Fernwartungsanwendung TeamViewer hilft ein computerversierter Bekannter oder ein Familienmitglied direkt über das Internet. Profis leben sich mit verschiedenen Tools aus und retten damit unter Umständen versehentlich gelöschte Daten. Außerdem fungiert Desinfec't als Notfallsystem, wenn Windows nicht mehr startet. Auf diesem Weg bringen Sie wichtige Daten wie Abschlussarbeiten auf einem USB-Stick in Sicherheit.

Wer Desinfec't bereits kennt, kann diesen Einleitungsartikel überspringen und direkt mit dem folgenden Artikel in die Praxis eintauchen.

Trojaner im Winterschlaf

Der Clou von Desinfec't ist, dass es ein eigenes Betriebssystem auf Linux-Basis mitbringt. Dieses startet anstelle von Windows direkt von USB-Stick oder DVD. Das hat den Vorteil, dass Schädlinge in einem zur Fehlerdiagnose gestarteten, verseuchten Windows nicht noch mehr Unheil anrichten. Beim Verdacht eines Trojanerbefalls fahren Sie Windows zügig herunter und starten im Anschluss das Notfallsystem. Damit schauen Sie aus sicherer Entfernung auf die inaktive Windows-Installation und spüren in Ruhe Trojaner auf. Damit nichts schiefgeht, kann Desinfec't standardmäßig nicht auf Windows-Festplatten schreiben und somit nichts verändern.

Für den Start wählen Sie das Medium mit Desinfec't in den Bootoptionen des Computers aus. Wie das im Detail funktioniert, beschreibt ein bebilderter Kasten im Praxisartikel auf Seite 21. Dort gibt es auch Tipps, wie Sie Startprobleme lösen. In der Redaktion haben wir das System auf älterer und aktueller Hardware ausgiebig getestet. Damit Desinfec't optimal läuft, sollte der Computer mindestens 8 GByte RAM mitbringen. Das System läuft auch auf 32-Bit-Hardware. Aufgrund von unzähligen Hardware-Konfigurationen können wir aber nicht garantieren, dass es auf jedem Computer läuft.

Aus Performancegründen empfehlen wir, Desinfec't von einem USB-Stick zu starten. Die Installation auf einem Stick mit mindestens 16 GByte gelingt direkt aus Windows oder einem laufenden Desinfec't. Von einem Stick läuft das System deutlich flinker als von DVD. Außerdem kann es nur so Daten wie Signatur- und System-Updates dauerhaft speichern. Von DVD gestartet, merkt sich das System nichts davon und Sie müssen die Virenscanner nach jedem Start erneut aktualisieren.

Desinfec't 2020 bringt neben den vier Scannern von Eset, F-Secure, Kaspersky und Sophos noch den Open-Threat-Scanner mit. Dieser entdeckt Schädlinge wie Emotet besonderes effektiv.

Da Desinfec't auf der Linux-Distribution Ubuntu basiert, brauchen Sie keine Angst zu haben, dass Windows-Trojaner beim Scannen auf das System überspringen. Da die Schädlinge auf Windows ausgelegt sind, funktionieren sie unter Linux schlicht nicht. Darüber hinaus setzt sich das System nach jedem Neustart in den Werkszustand zurück. So sollte selbst Linux-Malware keine Chance haben.

Jeder kann scannen

Da der Desktop von Desinfec't dem von Windows ähnelt und die Icons aussagekräftig beschriftet sind, sollten auch Nutzer ohne Linux-Erfahrung damit klar kommen. Wir haben das zugrunde liegende Ubuntu-System bewusst reduziert, damit nichts vom Einsatzzweck von Desinfec't ablenkt. Wer dennoch überfordert ist, kann beispielsweise einen Familien-Admin über die integrierte Fernwartungslösung TeamViewer zu Hilfe rufen. Der kann sich über das Internet auf den Problem-PC schalten und die Kontrolle über den Mauspfeil und Tastatureingaben übernehmen.

Alternativ wählen Computer-Einsteiger den Easyscan-Modus im Startmenü von Desinfec't aus. Hier präsentiert sich das System noch reduzierter und statt der Desktop-Umgebung gibt es nur ein Scan-Fenster. Auf Knopfdruck schaut sich der Scanner von Eset auf der Festplatte um.

Als Familien-Admin können Sie gerne mehrere Desinfec't-Sticks erzeugen und diese im Freundes- und Familienkreis verteilen. Bei der Stick-Erstellung kann man den Easyscan als Standardoption auswählen. Derartige Sticks starten so direkt in diesem Modus. Der Einsatz an Unis und Firmen ist ebenfalls erlaubt. Planen Sie Desinfec't im größeren Stil einzusetzen, sollten Sie der Fairness halber pro aktiv genutzter Desinfec't-Instanz eine Lizenz in Form eines Heftes erwerben. Allein die Nutzung von TeamViewer ist auf den privaten Bereich beschränkt.

Emotet-Jäger

Neu in Desinfec't 2020 ist der Open-Threat-Scanner, der die kommerziellen Virenscanner ergänzt. Den füttern wir mit tagesaktuellen Hashwerten aktueller High-End-Schädlinge. Damit ist die Chance höher, die hochentwickelte Malware zu entdecken.

Aber um eins gleich vorweg zu nehmen: Wenn sich ein Trojaner vom Schlage Emotet auf Ihrem Computer eingenistet hat, kann Desinfec't nur bedingt helfen. Vielmehr dient es dazu, die Infektion überhaupt zu entdecken und beispielsweise wichtige Daten in Sicherheit zu bringen. In einem derartigen Fall kommen Sie nicht um die Neuinstallation von Windows auf einer frisch formatierten Festplatte herum.

Viren aufspüren

Für den Auftakt der Virenjagd reicht es in der Regel für einen ersten Überblick aus, nur einen Scanner loszuschicken. Sie können aber auch alle vier Virenscanner und den Emotet-Scanner hintereinander von der Leine lassen und sich so die Meinung mehrerer Instanzen einholen. Dafür muss man aber viel Zeit mitbringen: Wenn alle Scanner eine Windows-Installation inklusive persönlicher Daten untersuchen, kann das durchaus die ganze Nacht dauern. Die Scanner schauen sich werkseitig die komplette Windows-Installation an. Bei Bedarf kann man aber auch einzelne Ordner auswählen, was den Vorgang deutlich beschleunigt.

Vor dem Scan holen sich die Virenscanner automatisch die aktuellen Virensignaturen. Damit das klappt, muss der Computer via WLAN oder per Kabel am Internet hängen. Nicht wundern: Wenn Sie Desinfec't das erste Mal oder nach einer längeren Zeit wieder nutzen, dauert das Signaturupdate schon mal eine halbe Stunde oder länger.

Eine einhundertprozentige Trefferquote gibt aber es nicht: Es kann vorkommen, dass für neue Trojaner noch gar keine Signaturen existieren. Einen derartigen Schädling erkennen die Scanner nicht. Eset, F-Secure, Kaspersky und Sophos stellen bis Juni 2021 Signaturupdates bereit.

Virenfund! Oder Fehlalarm?

Nach einem Scan bekommt man eine Ergebnisliste serviert, die sich automatisch in Firefox öffnet. Schlägt ein Scanner Alarm, muss man nicht gleich in Panik verfallen. Schließlich sind Fehlalarme nicht auszuschließen. Um das effektiv einzugrenzen, lädt man Funde direkt aus der Ergebnisliste per Mausklick zur Analyseplattform VirusTotal hoch. Dort untersuchen über 60 Virenscanner die Datei und geben eine Einschätzung ab. Zusätzlich sind in Firefox Links zu weiteren Analysediensten gespeichert.

Deuten alle Zeichen auf einen Virenbefall, kann Desinfec't Trojaner mit wenigen Klicks direkt aus der Ergebnisliste heraus unschädlich machen. Dazu benennt Desinfec't die Datei so um, dass sie nicht mehr ausführbar ist. Im Fall eines Versehens können Sie das jederzeit rückgängig machen. Wichtig ist, dass Desinfec't zwar die ausführbare Datei eines Trojaners unbrauchbar macht, von einem Schädling verbogene Systemeinstellungen kann das Sicherheitstool aber nicht automatisch reparieren. Um auf der sicheren Seite zu sein, kommt man nicht um die komplette Neuinstallation eines PCs herum.

In einem für jeden Computer automatisch erstellten individuellen Projektordner sammelt Desinfec't die Scan-Ergebnisse. Das ist praktisch, wenn man das System auf mehreren PCs einsetzt. Um den Überblick zu behalten, vergibt man Ordnernamen wie „Spiele-PC“ und „Arbeits-PC“. So liegen die Ergebnisse der Computer stets sortiert vor und man kann diese auch auf einem anderen PC einsehen.

Hilfe bekommen

Desinfec't spürt aber nicht nur Viren auf und erledigt diese, sondern kann auch Daten retten. Wenn Windows beispielsweise nicht mehr bootet, startet man das Notfallsystem von einem USB-Stick. Über diesen Weg greift man auf die Festplatten der kaputten Windows-Installation zu und bringt wichtige Dokumente auf dem Stick in Sicherheit.

Mit etwas Glück stellt man sogar versehentlich gelöschte Fotos von einer Speicherkarte wieder her. Das funktioniert mit PhotoRec, einem von mehreren Expertentools. Darunter befinden sich auch Werkzeuge, um Festplatten zu klonen.

Wenn Sie Probleme mit Desinfec't haben, lesen bitte zuerst den Folgeartikel sorgfältig durch. Dort finden Sie beispielsweise Hinweise zu Startproblemen. Oft lassen sich diese mit wenig Aufwand lösen. Eine Adresse zur Lösung von Problemen ist das offizielle Desinfec't-Forum (siehe ct.de/ypah). Dort hat die Community schon viele Probleme gelöst. Wenn gar nichts mehr geht, können Sie sich gerne via Mail an die Redaktion wenden. Um Fehler in Desinfec't auszubügeln, unterstützen wir das System nach Erscheinen ein Jahr lang mit Updates. Diese installieren sich automatisch, sobald Desinfec't bei Ihnen online ist. *(des@ct.de)* c't

Desinfec't-Forum: ct.de/ypah