



Desinfec't 2019

Mit unserem Sicherheitstool gehen Sie ohne viel Computer-Vorwissen auf Trojaner-Jagd. Dabei taucht jedoch mitunter die eine oder andere Frage auf. Viele Probleme kann man aber ohne viel Aufwand lösen, um Desinfec't so noch effizienter zu nutzen.

Von Dennis Schirmmacher

Kaspersky-Updates kaputt?

Ich nutze Desinfec't von einem USB-Stick. Nun wollte ich die Virensignaturen aktualisieren. Nach rund einer halben Stunde hat das auch bei allen bis auf Kaspersky geklappt. Nach einer weiteren halben Stunde erfolglosem Update habe ich den Computer heruntergefahren. Was ist da los?

Auf manchen Computern kommt es beim Update-Prozess von Kaspersky zu einer Endlosschleife. Mittlerweile konnten wir dieses Problem eingrenzen und haben einen Patch bereitgestellt. Damit die Aktualisierung runder läuft, müssen Sie lediglich Desinfec't updaten. Ist das System online, sollte sich der Patch automatisch aktualisieren. Steht oben rechts im Statusfenster „Desinfec't 2019 p1“, hat es geklappt. Ist das nicht der Fall, öffnen Sie das Terminal über das Icon in der Taskleiste, geben folgende Befehle ein und bestätigen diese mit der Eingabetaste:

```
sudo apt-get update
sudo apt-get -y dist-upgrade
```

Für alle Linuxer: Normalerweise führt man mit dem Befehl ein Ubuntu-Upgrade von beispielsweise 18.04 auf 19.04 durch. In diesem Fall installiert man damit aber nur Desinfec't-Updates. Auf einem USB-Stick behält Desinfec't den aktualisierten Versionsstand auch nach einem Neustart bei. Nutzen Sie das System von DVD, müssen Sie den Patch nach jedem Reboot erneut installieren.

Virensignaturen verschwinden nach Reboot

Ich nutze Desinfec't von einem USB-Stick, nur leider speichert dieser nicht wie im Artikel beschrieben die aktualisierten Virensignaturen. Nach jedem Neustart sind diese wieder im Auslieferungszustand und somit veraltet.

Das kann mehrere Ursachen haben. Stellen Sie sicher, dass Sie mindestens einen USB-Stick mit 16 GByte Speicherplatz benutzen. Außerdem dürfen Sie Desinfec't nur mit unseren Tools auf einen USB-Stick kopieren, damit eine Speicherung von aktualisierten Virensignaturen sichergestellt ist. Haben Sie den Stick mit dem Tool „Desinfec't2USB“ unter Windows erstellt, müssen Sie diesen beim ersten Neustart zwingend umwandeln – das geschieht automatisch nach der Auswahl der entsprechenden Start-Option. Geschieht das nicht, verhält sich das System wie von einer DVD und merkt sich Aktualisierungen nicht.

Desinfec't ohne DVD-Laufwerk nutzen

Ich habe mir die c't-Ausgabe 12/2019 mit der Heft-DVD im heise Shop nachbestellt. Ich habe aber in meinem Computer kein DVD-Laufwerk eingebaut. Kann ich das System jetzt gar nicht nutzen?

Doch. Käufer der Desinfec't-Ausgabe können auf verschiedenen Wegen das ISO-Image der DVD herunterladen, dieses beispielsweise unter Windows 10 mounten und so einen bootbaren Stick mit Desinfec't erstellen. Abonnenten und Käufer der digitalen Einzelausgabe starten den Downloadvorgang aus der c't-App. Unter Android wählen Sie die Ausgabe 12/2019 aus, klicken auf das Download-Symbol und dann auf den Punkt „DVD-Link anfordern“. Im nächsten Fenster geben Sie eine E-Mail-Adresse ein, an die der Downloadlink gesendet werden soll. Unter iOS klicken Sie in der ausgewählten Ausgabe auf das Symbol oben rechts neben dem Zahnrad und wählen dort „DVD-Download“ aus. Alternativ klicken Abonnenten im heise Shop in ihrem Konto auf den Reiter „Abo“ und

wählen dort die entsprechende Ausgabe aus. Nach einem Klick auf „DVD-Download“ landet das ISO-Image auf dem eigenen Computer. Auch Kiosk-Käufer des Heftes können Desinfec't herunterladen. Dafür müssen Sie lediglich den auf der DVD aufgedruckten Code im Betreff einer E-Mail an desinfec't2019@ct.de schicken. In der Antwortmail befindet sich ein individualisierter Link zum Download. Ein Downloadlink ist dreimal gültig. Bei Problemen wenden Sie sich bitte an leserservice@heise.de. Achtung: Wer die ISO-Datei auf eine DVD brennen möchte, benötigt zwingend einen Dual-Layer-Rohling.



Um Desinfec't herunterzuladen, muss man in der c't-App für Android lediglich die Ausgabe 12/2019 auswählen und dort auf „DVD-Link anfordern“ klicken.

Signaturen nicht mehr manuell aktualisierbar?

? Als ich Desinfec't 2019 zum ersten Mal gestartet habe, befand sich im Expertentools-Ordner auf dem Desktop eine Verknüpfung, über die ich die Virensignaturen aktualisieren konnte. Seit Neuestem ist das Icon verschwunden. Ich befürchte, dass ich es vielleicht selbst gelöscht habe. Können Sie mir das erklären?

! Keine Angst, System-Komponenten und Verknüpfungen von Desinfec't kann man im Grunde nicht löschen, da sich das System nach jedem Neustart wieder in den Ausgangszustand zurückversetzt. Das entfernte Icon ist Bestandteil des ersten Desinfec't-Updates „p1“. Wir haben es entfernt, da das System die Signaturen vor jedem Scan sowieso automatisch aktualisiert. Wer unbedingt eine manuelle Aktualisierung braucht, kann das nach folgendem Schema über die Kommandozeile anstoßen: `sudo bash /opt/desinfest/update_kaspersky.sh`

Stick-Installation schlägt fehl

? Ich habe nun schon mehrmals unter Windows versucht, Desinfec't mit dem Tool „Desinfect2USB_64_Bit“ auf einen USB-Stick zu kopieren. Ich habe die Anleitung in der c't-Ausgabe mit der Heft-DVD penibel befolgt, aber immer, wenn ich auf „Write“ klicke, erscheint die Fehlermeldung „Error 5: Zugriff verweigert“. Was mache ich falsch?

! Es kann vorkommen, dass Anti-Viren-Software den Blockzugriff auf USB-Sticks verweigert. Schauen Sie mal in den Optionen ihrer AV-Software nach einer derartigen Funktion (beispielsweise „Schutz vor Bootsekturviren“) und deaktivieren diese vorübergehend vor der Installation. Alternativ können Sie Desinfec't auch von DVD starten und den Stick aus dem laufenden System erzeugen.

Desinfec't löschen

? Ich würde gerne meinen Desinfec't-Stick wieder ganz normal nutzen und das System entfernen. Unter Windows wird mir aber nur ein Bruchteil des Speicherplatzes angezeigt. Wie kann ich den

Stick formatieren, sodass die volle Speichergröße wieder zur Verfügung steht?

! Desinfec't setzt auf verschiedene Partitionen, die zum Teil für Windows nicht ohne Weiteres sichtbar sind. Im Dateieexplorer sieht man nur die Partition zum Datenaustausch. Bei einem Stick mit 16 GByte umfasst diese rund 5 GByte. Um die volle Speichergröße wiederherzustellen, benutzen Sie am besten das Kommandozeilenprogramm `diskpart`. Um es unter Windows 10 zu starten, tippen Sie einfach `diskpart` in das Suchfeld in der Taskleiste ein und drücken die Eingabetaste. Mit den folgenden Befehlen identifizieren Sie den Stick, wählen ihn aus – das „?“ müssen Sie durch die korrekte Ziffer, die den Stick auszeichnet, ersetzen – und löschen diesen:

```
list disk
select disk ?
clean
create partition primary
```

Nun können Sie den Stick wie gewohnt in der Laufwerksauswahl mit der vollen Speichergröße formatieren.

Kompatibilität erhöhen

? Ich habe mir einen Laptop mit brandneuer Hardware gekauft. Leider startet Desinfec't auf diesem Computer nicht. Der Safe Mode im Desinfec't-Startmenü bringt leider keine Abhilfe. Kann ich das System jetzt gar nicht nutzen?

! Doch. Damit das klappt, haben wir alternativ einen 5.0er-Kernel für 64 Bit implementiert, der aktuellere Treiber an Bord hat. Als Voraussetzung müssen Sie Desinfec't zwingend von einem USB-Stick starten. Haben Sie den Stick unter Windows mit „Desinfect2USB“ erzeugt, müssen Sie diesen jedoch zuerst umwandeln. Ist das geschehen, drücken Sie im grafischen Desinfec't-Bootmenü (BIOS) die Tabulatortaste, um in den Editiermodus zu wechseln. Nun ändern Sie die Einträge „`vmlinuz`“ zu „`vmlinuz.50`“ und „`initrd.lz`“ zu „`initrd.lz.50`“. Starten Sie dann das System durch Drücken der Eingabetaste. Erscheint das Bootmenü nur in Schwarz-Weiß (UEFI), drücken Sie die Taste E, um die Einträge wie beschrieben anzupassen. Der Start des Systems gelingt in diesem Fall mit einem Druck auf F10. Kommt hingegen alte Hardware zum Ein-

satz, kann man Desinfec't im 32-Bit-Modus mit einem 4.4er-Kernel booten lassen. Ersetzen Sie dafür den Wert 50 durch 44.

Damit man das nicht bei jedem Neustart machen muss, können Sie die Dateien `/boot/grub.cfg` (UEFI) beziehungsweise `/isolinux.os.cfg` (BIOS) unter Windows mit einem Editor anpassen. Ändern Sie dafür einfach im Abschnitt „Desinfec't starten“ die Einträge zu `vmlinuz.50` und `initrd.lz.50` und speichern die Datei.

Starten mit Secure Boot?

? Kann ich Desinfec't eigentlich mit aktivierter Secure-Boot-Funktion nutzen? In älteren Versionen ging das ja nicht.

! Ja, aber das klappt nur, wenn Desinfec't im 64-Bit-Modus unter UEFI läuft. Dafür haben wir Ubuntu's signierten 64-Bit-SHIM/GRUB integriert. Für 32-Bit-UEFI haben wir keinen signierten Bootloader.

Desinfec't lässt sich nicht herunterfahren

? Bei mir war nun schon einige Male der Button zum Herunterfahren unten links in der Taskleiste ausgegraut und ich konnte den Computer so nicht sauber ausschalten. Was kann ich dagegen machen?

! Leider haben wir die Ursache für diesen Bug noch nicht ausfindig gemacht. Tritt der Fehler auf, können Sie das System aber trotzdem sauber herunterfahren. Unseren Test-Laptop konnten wir in so einem Fall erfolgreich herunterfahren, indem wir den Power-Knopf gedrückt haben.

Weitere Hilfe

! Das Desinfec't-Forum ist die erste Anlaufstelle, wenn Sie Schwierigkeiten oder sogar Lösungen für Probleme haben. Dort tauschen sich nicht nur Nutzer aus, auch die Redaktion und der Desinfec't-Entwickler sind dort aktiv.

(des@ct.de)

Hilfe-Forum: ct.de/ym8b