

# c't Desinfec't

*Das Rettungssystem bei Virenbefall*

NEUE  
VERSION  
2023/24



## *DAS c't-Sicherheitstool als Download für USB-Sticks*

- ▶ Entfernt Trojaner und Viren unter Windows
- ▶ Mit 3 Scannern: ClamAV, Eset, WithSecure
- ▶ Signatur-Updates gratis bis Oktober 2024

## **Das kann das c't-Sicherheitstool**

Windows-Trojaner & andere Schädlinge finden und löschen  
Fernhilfe für Familien-PCs leisten

## **Daten retten**

Verloren geglaubte Fotos und Dateien finden und wiederherstellen  
Daten aus defektem NAS bergen

## **Zusatz-Werkzeuge für Profis nutzen**

Malware-Analyse mit Experten-Tools  
3 Extra-Scanner selbst konfigurieren  
Desinfec't erweitern

€ 14,90  
CH CHF 27.90  
AT € 16,40  
LUX € 17,10



14. bis 16. November in Köln

# Das Update für Frontend Devs

**Die Konferenz für Frontend-Entwicklung**

Die Konferenz bietet eine gute Gelegenheit für die Frontend-Gemeinschaft, sich zu treffen und auszutauschen. Hier kannst du nicht nur drei bereichernde Tage erleben, sondern auch wertvolle Kontakte knüpfen.

Lass dich von inspirierenden Talks begeistern, teile dein Wissen und entdecke die neuesten Trends und Techniken der Webentwicklung.



Über  
40 Talks  
und Work-  
shops



Sichere dir jetzt dein  
Ticket unter [ctwebdev.de](http://ctwebdev.de)



Goldsponsor:



Silbersponsor:



# Editorial

---

**Liebe Leserin, lieber Leser,**

---

wenn Sie beim Surfen oder Lesen von E-Mails nicht aufpassen und auf mittlerweile häufig wirklich gut gemachte Finten von Cybergangstern hereinfallen, macht sich nach unüberlegtem Öffnen von Dateianhängen oft innerhalb von Sekunden ein Trojaner auf Ihrem Computer breit. Dann verschlüsselt Ransomware Ihre Daten und fordert Lösegeld oder Betrüger kopieren die Log-ins Ihrer Online-Banking-Accounts.

Ist das Unglück bereits eingetreten, hilft das Sicherheitstool der c't-Redaktion Desinfec't. In der aktuellen Version 2023/24 gehen Sie mit mehreren Virensuchern von unter anderem Eset und WithSecure auf Virenjagd und schalten PC-Schädlinge aus. Dafür müssen Sie Desinfec't lediglich herunterladen und auf einem USB-Stick installieren. Davon startet das Sicherheitstool dank eines Live-Systems statt Windows und Sie untersuchen das Betriebssystem aus sicherer Entfernung.

Desinfec't kann aber noch mehr: Wenn Windows gar nicht mehr bootet, bringen Sie damit Ihre wichtigen Dateien auf einem externen Laufwerk in Sicherheit. Außerdem können Sie mit dem Tool in vielen Fällen versehentlich gelöschte Daten wiederherstellen.

Dank der einfachen Bedienung kommen auch Computereinsteiger mit Desinfec't zurecht. Wenn gar nichts mehr geht, rufen Sie mittels der integrierten Fernwartung den Familien-Admin über das Internet zu Hilfe. Doch auch für Malware-Profis ist etwas dabei: Sie analysieren mit mehreren Expertentools Systeme auf Schadcodebefall.

Bleiben Sie im Internet stets wachsam! Und wo das nicht geklappt hat:  
Viel Erfolg bei der PC-Rettung mit Desinfec't 2023/24!



Dennis Schirrmacher

# Inhalt

**6** **Desinfec't 2023/24** Das Notfallsystem Desinfec't kann die letzte Rettung für ein verseuchtes Windows sein. Um Trojanern auf die Spur zu kommen und Windows zu säubern, schickt es mehrere Viren-Scanner von unter anderem Eset und WithSecure los.

**10** **Im Einsatz** Die Virenjagd startet man ganz einfach – dafür sind nur wenige Mausklicks nötig. Wer das Maximum aus dem Sicherheits-Tool herausholen möchte, muss nur ein paar Tipps beachten.

**16** **FAQ Desinfec't** Antworten auf die häufigsten Fragen.

**Direkt  
loslegen!**

## Viren jagen mit Desinfec't

Mit dem c't-Sicherheits-Tool Desinfec't 2023/24 untersuchen Sie Windows aus sicherer Entfernung auf Trojaner. Das Live-System startet von DVD oder USB-Stick und schaut mit mehreren Viren-Scannern von unter anderem Eset und WithSecure auf das inaktive Windows. Damit Desinfec't auch aktuelle Schädlinge erkennt, sind ein Jahr lang kostenlose Signatur-Updates inklusive. Schlägt einer der Scanner an, können Sie die Gefahr eingrenzen und gegebenenfalls be seitigen. Dank diverser Tools bringen Sie mit Desinfec't

**20** **Microsoft Defender installieren** Mit vergleichsweise wenig Aufwand kann man Desinfec't nachträglich mit dem Anti-Viren-Scanner Microsoft Defender ausstatten. Der Scanner überzeugt mit einer hohen Erkennungsrate.

**24** **Individueller AV-Scanner** Der Open Threat Scanner bildet die Basis für Ihren eigenen Antiviren-Scanner mit maßgeschneiderten Regeln. Damit gehen Sie tagesaktuell gegen Emotet & Co. vor.



zudem beispielsweise wichtige Daten in Sicherheit. Um das Sicherheitstool zu nutzen, laden Sie zuerst das Zip-Archiv von Desinfec't 2023/24 herunter. Anschließend erstellen Sie einen USB-Stick und starten es von dort. Weitere Informationen dazu finden Sie im Artikel „Desinfec't bestmöglich nutzen“ ab Seite 10.

**30** **Erweiterung via Btrfs** Wer sich ein bisschen mit Linux auskennt, kann Desinfec't mithilfe des Btrfs-Dateisystems zu einem vollständigen Notfallarbeitsplatz inklusive Office-Anwendungen und aktuellen Treibern ausbauen.

**36** **Windows aufhelfen** Nicht nur Schädlinge setzen Windows-Installationen zu, sondern auch Fehlbedienung oder Hardware-Probleme. Desinfec't hilft, Probleme von außen zu analysieren und zu beseitigen.

**40** **Datenrettung** Mit Desinfec't kann man zerschossene Partitionen restaurieren, gelöschte Dateien wiederherstellen und verunfallte Fotodateien auffinden und retten.

**46** **Hardware-Diagnose** Desinfec't sieht genau auf Hardware, spuckt detaillierte Infos aus und liefert eine zweite Meinung, um durchdrehende Software von matschiger Hardware zu unterscheiden.

**54** **Offline-NAS-Reparatur** In den meisten NAS-Boxen steckt ein Linux, sodass Desinfec't die Daten auf den Platten eines nicht mehr betriebsbereiten Gerätes oft zugänglich machen kann.

**62** **Netzwerk-Troubleshooting** Keine Panik, wenn das Internet mal streikt: Das Live-Linux-System von Desinfec't bringt einige Tools mit, um Probleme im Netzwerk aufzuspüren und zu lösen.



**70** **Booten aus dem Netz** Das Notfallsystem startet nicht nur von einem USB-Stick, sondern auch aus dem Netzwerk. Das funktioniert sogar mit einem Raspberry Pi als Server. Wir zeigen die nötigen Handgriffe.

## Zum Heft

- 3 Editorial**
- 69 Impressum**



# Das kann das c't-Sicherheitstool

Mit Desinfec't 2023/24 jagen und erledigen Sie Trojaner und andere Schädlinge. Außerdem können Sie damit verloren geglaubte Daten retten. Das ist alles gar nicht schwer, meist genügen wenige Klicks auf der übersichtlichen Oberfläche. Wer trotzdem nicht weiterkommt, ruft den Familien-Admin über die integrierte Fernwartung zu Hilfe.

Von **Dennis Schirrmacher**

**E**in unüberlegter Klick auf den Link in einer Phishing-Mail genügt und schon macht sich ein Virus in Windows breit. Solche Mails sind oft so gut gemacht, dass man es ihren Opfern gar nicht vorwerfen kann, darauf hereinzufallen. Doch jetzt ist das Kind in den Brunnen gefallen und verschärfend kommt hinzu, dass auf dem Computer wichtige Daten lagern, auf die Sie dringend zugreifen müssen.

Genau für solche Situationen ist das c't-Sicherheitstool Desinfec't 2023/24 für Windows-PCs gemacht. Es bringt sein eigenes Linux-Live-System mit, hat mehrere Virenscanner von unter anderem Eset und WithSecure (ehemals F-Secure) an Bord und startet direkt von einem USB-Stick. Demzufolge müssen Sie ein möglicherweise infiziertes Windows zur Analyse nicht starten. Das ist eine sehr sichere Vor-

gehensweise, schließlich kann ein Trojaner in einem ruhenden System kein weiteres Unheil anrichten.

Mit dem Sicherheitstool analysieren Sie die interaktive Windows-Installation also sozusagen aus sicherer Entfernung und verschaffen sich einen Überblick. Der Linux-Ansatz bringt aber noch einen weiteren Sicherheitsgewinn: Dank des grundlegend unterschiedlichen Betriebssystems sind Windows-Trojaner nicht kompatibel und können dementsprechend nicht auf den Stick überspringen.

## Umgehend starten

Für die Installation benötigen Sie lediglich einen USB-Stick mit mindestens 16 GByte Speicherplatz. Dann müssen Sie das Zip-Archiv von Desinfec't

## Das ist neu in Desinfec't 2023/24

- Gratis Signatur-Updates bis Oktober 2024
- Monitoring-Tool Checkmk implementiert
- Checkmk-Funktionen: Check Status der Virensignaturen, Monitoring von Desinfec't-Gesundheit
- Malware-Analysetool FLOSS implementiert

2023/24 herunterladen (siehe Kasten „Wo Sie Desinfec't zum Download finden“) und mit unserem Installationstool Desinfect2USB\_64\_Bit.exe auf dem Stick installieren. Das dauert nur wenige Minuten. Ist das erledigt, müssen Sie den Computer so einstellen, dass er statt von der Festplatte das Live-System vom Stick bootet. Wie das geht, steht im Artikel „Desinfec't bestmöglich nutzen“ auf Seite 10. Läuft das System, können Sie direkt mit der Trojaner-Hatz loslegen. Für einen reibungslosen Betrieb sollte der Computer mindestens 4 GByte RAM haben. Das System läuft nämlich direkt aus dem Arbeitsspeicher und die Scanner machen sich dort bei Benutzung ebenfalls breit.

Alternativ startet Desinfec't auch von einer DVD. Das ist aber aus mehreren Gründen nicht zu empfehlen: Von einem USB-Stick läuft das System nicht nur deutlich flinker, es merkt sich auch aktualisierte Virensignaturen. Mit einer DVD klappt das nicht und Sie müssen die Scanner nach jedem Neustart erneut auf den aktuellen Stand bringen, was schon mal mehr als ein Viertelstündchen dauern kann.

## Jeder kann Viren jagen

Lassen Sie sich von Begriffen wie Linux-Live-System nicht abschrecken: Der folgende Artikel nimmt Sie an die Hand und erläutert Schritt für Schritt, wie Sie Desinfec't auf einem USB-Stick installieren, das System im Anschluss starten, wie die Virenjagd vonstattengeht und wie Sie sogar versehentlich gelöschte Daten wiederherstellen.

Damit die Bedienung für Windows-Nutzer so einfach wie möglich von der Hand geht, orientiert sich die Desktopdarstellung an Microsofts Betriebssystem. Zusätzlich haben wir für die Kernfunktion von Desinfec't unnötige Linux-Dienste entfernt, sodass so wenig wie möglich vom eigentlichen Einsatzzweck ablenkt. Prägnant beschriftete Icons erleichtern die Bedienung.

Für Computereinsteiger eignet sich der Easy-Scan-Modus. Wenn Sie diese Option im Desinfec't-Start-

**Desinfec't-Neulingen den Start so einfach wie möglich zu machen, orientiert sich die Desktopansicht an Windows.**





Während der Viren-scans vertreibt man sich die Zeit mit diversen Mini-Spielen.

menü auswählen, aktualisiert sich der Scanner von Eset automatisch und schaut sich auf der gesamten Windows-Festplatte um. Beim Easy Scan sieht man während des Vorgangs nur das Scan-Fenster. Der Desktop ist bewusst ausgeblendet, damit nichts vom Scannen ablenkt.

Wer gar nicht mit Desinfec't zurechtkommt oder Hilfe bei der Einschätzung von vermeintlichen PC-Schädlingen benötigt, ruft mit dem integrierten TeamViewer-Client den Familien-Admin oder einen Freund übers Internet zu Hilfe. Der Helfer installiert TeamViewer kostenlos auf seinem PC. Steht die Verbindung, kann er sich auf dem Computer des Rat-suchenden umsehen und mit Tipps zur Hand gehen.

## Kernfunktion

Damit den Scannern bei der Untersuchung keine aktuellen Computerschädlinge durchrutschen, sind ein Jahr lang kostenlose Signaturupdates inklusive. Wenn der Computer eine aktive Internetverbindung hat und Sie den Scan starten, aktualisieren sich die Scanner automatisch. Das Scannen selbst klappt dann auch offline.

Standardmäßig untersuchen die Scanner die komplette Windows-Installation. Auf Wunsch können Sie aber auch nur bestimmte Ordner oder Par-

tionen scannen. So ist es etwa möglich, einen gefundenen USB-Stick sicher auf Virenbefall zu untersuchen oder ausschließlich den Download-Ordner zu inspizieren.

Dank der integrierten Bitlocker- und VeraCrypt-Unterstützung können sich die Scanner auch auf verschlüsselten Datenträgern umschauen. Das funktioniert selbst dann, wenn Windows vollständig verschlüsselt ist.

Nach der Untersuchung öffnet sich die Ergebnisliste automatisch im integrierten Webbrowser Firefox und Sie können die Funde begutachten. Die Scan-Ergebnisse werden in einem Projektordner gespeichert. Damit Sie nicht den Überblick verlieren, erstellt Desinfec't pro Computer einen individuellen Ordner. So können Sie den Stick an einen anderen Computer stecken und dort die Analyse weiterführen.

Nach einem Scan mit Funden sollten Sie nicht gleich in Panik verfallen: Die Scanner können sich durchaus irren und einen Fehlalarm auslösen. Um das einzufangen, laden Sie Funde direkt zur Analyseplattform VirusTotal hoch. Bei dem Dienst schauen sich über 60 Online-Scanner die Datei an und geben eine Einschätzung ab. Mit diesen Informationen ausgestattet kann man Fehlalarme in der Regel gut erkennen.

Wenn alles auf einen echten Trojaner hindeutet, können Sie diesen mit wenig Aufwand unschädlich machen. Desinfec't löscht den vermeintlichen Schädling jedoch nicht, sondern benennt die identifizierte Datei um. Wenn sich im Nachhinein herausstellt, dass es doch eine legitime Datei war, stellen Sie diese umgehend wieder her. Um ganz auf Nummer sicher zu gehen, bringt Desinfec't noch eine weitere Vorsichtsmaßnahme mit: Nach dem Start kann das Sicherheitstool ausschließlich lesend auf Windows-Festplatten zugreifen und so nichts kaputt machen. Wollen Sie einen Trojaner ausmerzen, fragt das System explizit nach Schreibrechten, die Sie erlauben müssen.

Aber Vorsicht: Desinfec't ist kein Allheilmittel. Es ist vielmehr ein Analysetool, um von Malware verursachten Systemproblemen auf die Spur zu kommen. Es kann keine von Trojanern verbogenen Systemeinstellungen geraderücken. Wenn sich wirklich Schadcode auf Ihrem System breit gemacht hat, hilft für eine absolute Sicherheit nur das komplette Löschen der Windows-Festplatte und eine Neu-Installation des Betriebssystems.

Wenn ein Windows-PC gar nicht mehr startet, schlägt die Stunde von Desinfec't abermals: Über das Live-System greifen Sie auf die Windows-Parti-

tionen zu und bringen so wichtige Daten in Sicherheit, indem Sie etwa Dokumente auf den Stick kopieren. Handelt es sich um größere Datenmengen, können Sie auch eine USB-Festplatte zusätzlich anschließen und die Daten dort ablegen.

## Da geht noch mehr

Mit den Scannern von Eset und WithSecure gehen Computer-Einsteiger auf Trojaner-Jagd. Oft reicht es für eine erste Einschätzung, lediglich den voreingestellten Scanner von Eset von der Leine zu lassen. Profis können aber noch tiefer graben. Dafür eignen sich der individuell konfigurierbare Open Threat Scanner (OTS) und der Thor-Lite-Scanner, die auf Wissen und Erfahrung erfahrener Incident-Response-Profis zurückgreifen und so selbst Bedrohungen aufspüren, die sich erfolgreich vor Antiviren-Software verstecken. Mit dem in Desinfec't neu enthaltenen Tool FLOSS können Malware-Analysten Schadcode, der sich versteckt, aufspüren.

Außerdem gibt es noch verschiedene Experten-tools, mit denen Sie etwa versehentlich gelöschte Daten wiederherstellen. Auch das Klonen von ganzen Partitionen ist möglich. Doch wie der Name schon sagt, richten sich diese Tools an Computer-Profis, die wissen, was sie tun. Also Vorsicht: Im schlimmsten Fall kann man mit den Tools eine Windows-Installation unrettbar zerstören.

## Nicht verzweifeln

Wenn es trotz Fernhilfe immer noch hakt, finden Sie in unserem Forum Hilfe (siehe [ct.de/wa27](http://ct.de/wa27)). Dort wurden bereits viele Probleme mithilfe der Community gelöst. Das gilt auch für Hardwareprobleme, die sich manchmal etwa durch alternative Startoptionen oder nachinstallierte Treiber in den Griff bekommen lassen. Im Forum gibt es auch Informationen zu Desinfec't-Updates, die wir wenn nötig veröffentlichen, um Fehler zu beseitigen. Solche Aktualisierungen installieren sich in der Regel automatisch. Ist danach ein Neustart nötig, weist Desinfec't darauf hin. Ob das Update geklappt hat, erkennen Sie im Statusfenster oben rechts auf dem Desktop. Steht dort etwa Desinfec't 2023/24 p1, ist das System auf dem aktuellen Stand. Nach der Veröffentlichung von Desinfec't sind für einige Wochen auch der Entwickler und die Redaktion im Forum aktiv. Doch in vielen Fällen hilft auch schon der folgende Artikel, der viele Fragen zur Installation und zum Start des Sicherheitstools klärt.

Desinfec't-Forum

[ct.de/wa27](http://ct.de/wa27)

## Wo Sie Desinfec't zum Download finden

Käufer der digitalen Einzelausgabe bekommen mit ihrer Auftragsbestätigung via E-Mail einen Downloadlink für die Zip-Datei mit Desinfec't 2023/24.

Auch Kioskkäufer können Desinfec't herunterladen. Dafür müssen Sie lediglich die Website [ct.de/desinfect2023-sh](http://ct.de/desinfect2023-sh) öffnen. Nach der Angabe Ihrer E-Mail-Adresse erhalten Sie einen Downloadlink, der dreimal gültig ist. Bei Problemen wenden Sie sich bitte an [leserservice@heise.de](mailto:leserservice@heise.de).

Anhand der SHA256-Prüfsumme können Sie prüfen, ob das ISO-Image unverändert auf Ihrem Computer gelandet ist. Stimmt der SHA256-Wert nicht überein, ist es beim Download zu Fehlern gekommen. Laden Sie die Datei erneut herunter. Prüfsummen erzeugt man mit kostenlosen Tools wie HashCheck. Die Prüfsumme der ISO-Datei finden Sie über [ct.de/wa27](http://ct.de/wa27)

# Desinfec't bestmöglich nutzen

Wenn Trojaner Windows auseinandernehmen, hilft Desinfec't bei der Analyse und Wiederherstellung. Das Einrichten und der Start des Sicherheitstools gelingen mit wenigen Handgriffen. Mit den integrierten Tools kann es sogar noch viel mehr.

Von **Dennis Schirrmacher**

**V**erhält Ihr Computer sich seltsam und Sie vermuten, dass ein Trojaner sein Unwesen treibt? Dann lautet die Devise: Ruhe bewahren, PC runterfahren und Desinfec't 2023/24 starten. Im Anschluss scannen Sie die inaktive Windows-Installation auf Viren und bringen wichtige Daten auf dem Desinfec't-Stick in Sicherheit. Wie das alles geht, erklärt dieser Artikel.

Viele Familien-Admins haben bereits einen Desinfec't-Stick in der Schublade liegen und können direkt loslegen. Ist das bei Ihnen der Fall, springen Sie gleich zum Abschnitt „Desinfec't starten“. Anderer müssen das Sicherheitstool zuerst auf einem USB-Stick installieren. Es startet zwar auch von einer DVD, das geht aber aufgrund der vergleichsweise langsamen Zugriffe zur Geduldsprobe und macht keinen Spaß. Außerdem kann es sich auf einer DVD keine Daten merken und Sie müssen Virensignatur- und Systemupdates nach jedem Neustart wieder installieren. Das kostet Zeit und Nerven.

Also organisieren Sie sich für die im Folgenden beschriebene Installation besser einen USB-Stick mit mindestens 16 GByte Speicherplatz. Hier zahlt es sich aus, wenn Sie zu einem Stick eines Markenherstellers mit USB 3.2 Gen 1 – früher: USB 3.0 – oder besser greifen; minderwertige Sticks sorgen oft für Probleme im Betrieb. Wenn Desinfec't auf dem Stick installiert ist, booten Sie Ihren PC direkt davon statt von der Windows-Festplatte. Nach dem Start schauen

Sie sich mit dem Sicherheitstool in der inaktiven Windows-Installation um, spüren Trojaner auf und machen sie unschädlich.

Sie können Desinfec't gerne an Familienmitglieder oder Freunde weitergeben. Auch die Nutzung in Firmen und Organisationen ist gestattet. Für die Nutzung mehrerer Sticks in einem kommerziellen Umfeld kontaktieren Sie bitte den heise Shop (support@shop.heise.de). Beachten Sie aber, dass der Einsatz des Fernwartungstools TeamViewer auf den privaten Kreis beschränkt ist.

Da es immer wieder zu Missverständnissen kommt, müssen wir vor dem Start noch eine Sache klären: Desinfec't ist keine Windows-Anwendung, die Sie im laufenden System via Doppelklick starten. Sie müssen das Linux-Live-System direkt vom USB-Stick anstatt Windows starten.

## Die Installation

Um Desinfec't 2023/24 zu nutzen, müssen Sie zuerst das Zip-Archiv mit dem Installer herunterladen. Wie das geht, steht im Kasten „Wo Sie Desinfec't zum Download finden“ auf Seite 9. Wer auf Nummer sicher gehen möchte, dass der Download nicht manipuliert wurde, kann das anhand der Prüfsumme sicherstellen (siehe ct.de/wr4w). Liegt die Datei auf Ihrer Festplatte, müssen Sie sie entpacken, um das Sicherheitstool auf einem USB-Stick zu installieren.



Achtung: Das bloße Kopieren der im Zip-Archiv enthaltenen ISO-Datei auf einen Stick oder der Einsatz von Tools wie Rufus zum Erstellen von bootfähigen USB-Sticks funktionieren nicht. Sie müssen das System zwingend mit unserem Tool „Desinfect2USB“ installieren. Andernfalls startet es im schlimmsten Fall nicht oder es kommt zu Problemen beim Betrieb. Unter Linux darf der Stick nicht eingebunden sein. Ist das gegeben, tippen Sie als Root im Ordner mit dem ISO folgende Befehle ein: dd if=desinfect-202324-amd64.iso of=/dev/sdx status=progress. Wie üblich müssen Sie dabei „sdx“ durch den Gerätename des USB-Sticks ersetzen und dabei extrem aufpassen, dass Sie nicht versehentlich ein anderes Gerät wie die Festplatte erwischen.

Nur unser Tool bereitet die notwendige Unterteilung in Partitionen korrekt vor, Desinfect' bestehen nämlich aus mehreren. Etwa der Abschnitt, in dem

das System liegt, setzt sich nach jedem Neustart aus Sicherheitsgründen zurück, sodass sich dort nichts einstellen kann. Damit aber aktualisierte Virensignaturen oder gesicherte Dateien gespeichert werden können, braucht Desinfect' dauerhaft beschreibbare Partitionen. Ein Upgrade von älteren Desinfect'-Versionen ist nicht möglich. Desinfect2USB finden Sie im entpackten Zip-Archiv. Stecken Sie nun den USB-Stick an den Windows-Computer und starten die Installation mit einem Doppelklick auf Desinfect2USB.

Im Anschluss öffnet sich das Tool Win32 Disk Imager, in dem die Image-Datei von Desinfect' 2023/24 vorausgewählt ist. Unter „Device“ wählen Sie nun den Laufwerksbuchstaben des USB-Sticks aus. Welcher Buchstabe das ist, sehen Sie im Explorer von Windows. Die Auswahl des korrekten Laufwerksbuchstabens ist an dieser Stelle extrem

## Desinfect' starten

Vermuten Sie, dass ein Schädling sein Unwesen auf Ihrem Windows-PC treibt, kommt Desinfect' zum Einsatz. Fahren Sie dazu den PC herunter. Schließen Sie dann den Desinfect'-Stick an. Schalten Sie den PC wieder ein und drücken sofort entweder F8, F10, F11 oder F12, damit das BIOS-Bootmenü erscheint. Bei manchen Computern rufen Sie dieses Menü mit der Esc- oder Enter-Taste auf. Wenn all das nicht klappt, suchen Sie auf Ihrem Smartphone nach Ihrem Computermodell sowie „BIOS Bootmenü“, um die richtige Taste zu finden.

Erscheint das Menü, wählen Sie im Anschluss das Medium mit Desinfect' aus und starten Sie davon. Funktioniert das nicht, müssen Sie den Umweg über das vollständige BIOS-Menü gehen. Dieses rufen Sie meist durch das Drücken der

Taste Entf oder F2 auf, aber je nach PC sind auch andere Tasten denkbar.

Im BIOS stellen Sie die Boot-Reihenfolge so ein, dass das Medium mit Desinfect' zuerst startet. Wollen Sie nur einen Routinecheck machen, können Sie Desinfect' auch direkt aus einem Windows 10 oder 11 starten. Das funktioniert aber nur, wenn das System im UEFI-Modus läuft. Dafür halten Sie die Umschalttaste (Shift) gedrückt (1) und klicken im Startmenü auf Neustart. Im anschließend auftauchenden Bildschirm bestätigen Sie den Punkt „Ein Gerät verwenden“ (2). Als Nächstes wählen Sie das Medium mit Desinfect' aus (3). Nun fährt Windows herunter und bootet automatisch das Notfallsystem. Klappt der Start partout nicht, wählen Sie bitte im Desinfect'-Bootmenü die Option „Safe Mode“ aus.



wichtig, denn mit den nächsten Schritten löschen Sie den Stick unwiederbringlich. Wenn Sie das geprüft haben und sich sicher sind, starten Sie die Installation mit einem Klick auf „Write“. Bei einem flinken USB-Stick sollte der Vorgang nur wenige Minuten dauern. Wundern Sie sich nicht, wenn Windows den Stick nach der Installation nicht als Laufwerk anzeigt. Das ist in diesem Stadium normal und wird mit dem nächsten Schritt behoben.

## Stick konvertieren

Nach dem Abschluss der Installation bietet der Assistent direkt an, den Computer herunterzufahren und Desinfec't zu starten. Dieses Angebot sollten Sie aber nur annehmen, wenn Sie bereits wissen, wie der Start eines Live-Systems von einem Stick vonstatten geht (siehe Kasten „Desinfec't starten“ auf S. 11). Ansonsten landen Sie aufgrund der Standard-Booteinstellung des PCs doch wieder in Windows.

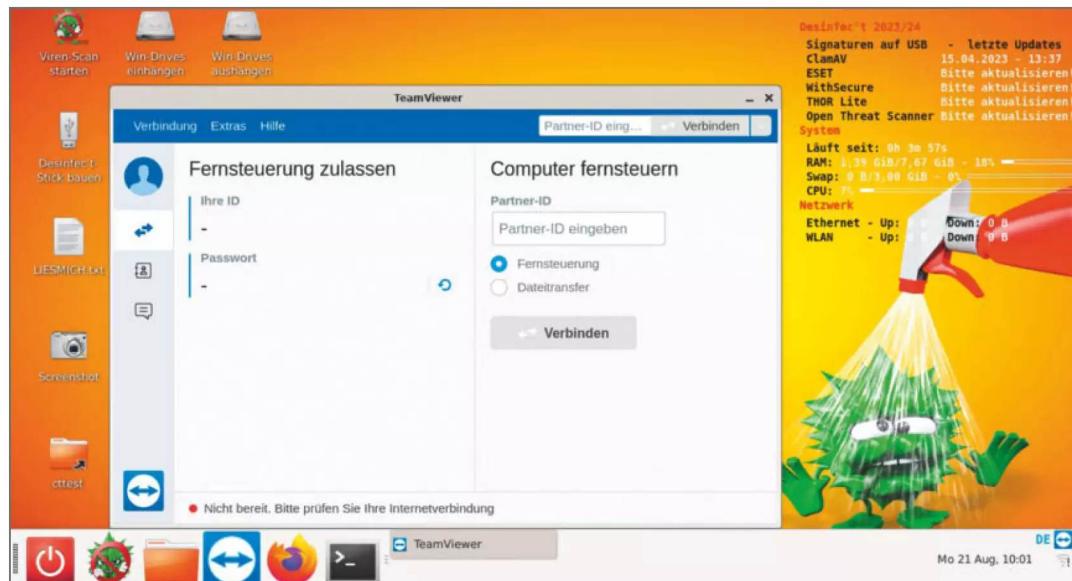
Beim ersten Start müssen Sie den Desinfec't-Stick einmalig umwandeln, damit er korrekt funktioniert. Geschieht dies nicht, verhält sich das System wie eine DVD und speichert keine Daten. Erst nach dem Umbau bleiben aktualisierte Virensignaturen nach einem Neustart erhalten. Dafür müssen Sie lediglich den obersten Punkt im Desinfec't-Startmenü „in nativen Desinfec't-Stick umwandeln“ auswählen. Im

Zuge dessen werden unter anderem die für den Betrieb notwendigen weiteren Partitionen angelegt. Dabei wird auch geprüft, ob der Stick für einen reibungslosen Betrieb schnell genug Daten lesen und schreiben kann. Ist das nicht der Fall, erscheint eine entsprechende Warnung und es wird ein Löschen des Sticks angeboten.

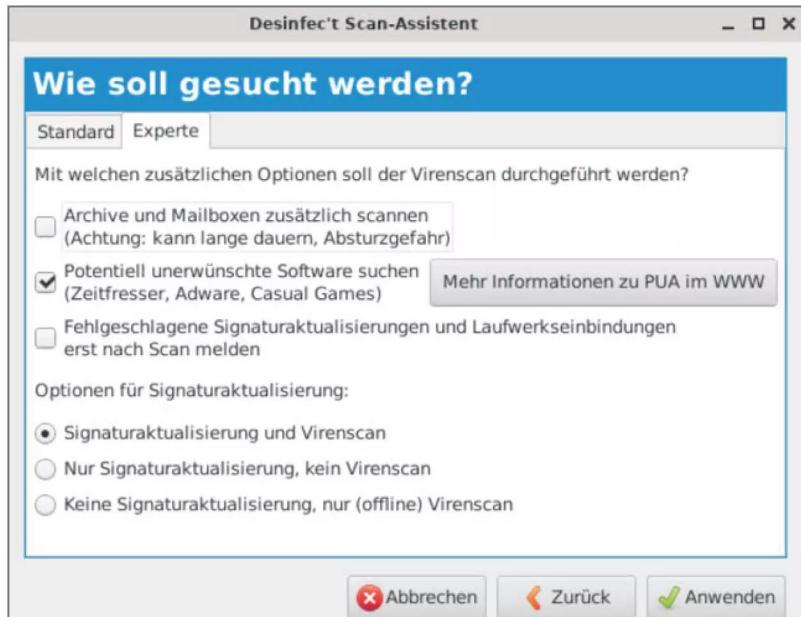
## Alternativer Installationsweg

Wenn Windows infiziert ist, sollten Sie das System selbstverständlich nicht zum Erstellen eines Desinfec't-Sticks verwenden. Doch auch hier gibt es Möglichkeiten: Führen Sie die beschriebene Installationsprozedur auf dem Computer eines Bekannten durch. Alternativ können Sie auch einen Stick aus einem laufenden Desinfec't heraus erzeugen. Das bringt sogar mehrere Vorteile mit, unter anderem müssen Sie einen so erstellten Stick nicht konvertieren und bekommen direkt einen Desinfec't-Stick mit vollem Funktionsumfang.

Wenn das Sicherheitstool läuft, klicken Sie zum Start der Installation auf das Desktop-Icon „Desinfec't-Stick bauen“. Nun wählen Sie unter „Ziellaufwerk“ den an den PC angeschlossenen USB-Stick aus. Achtung: Er wird im Zuge der Installation vollständig gelöscht. Die Voreinstellungen belassen Sie. Über einen Klick auf „Anwenden“ starten Sie die Installation, die nur wenige Minuten dauern sollte.



**Wenn es bei der Bedienung klemmt, rufen Sie über den integrierten TeamViewer-Client den Familien-Admin zu Hilfe.**



**Bei Bedarf kann man im Scan-Assistenten auch nur die Virensignaturen aktualisieren, ohne einen Scan zu starten. So bringen Sie die Scanner etwa für einen Offline-PC im Vorfeld auf den aktuellen Stand.**

Wer einen Desinfec't-Stick an Familienmitglieder oder Freunde mit wenig Computerkenntnissen weitergeben will, kann den Stick entsprechend vorbereiten. Dafür wählen Sie unter dem Punkt „Easy Scan“ die Option „Automatik-Modus als Standard verwenden“ aus. So ein Stick startet automatisch im Easy-Scan-Modus und untersucht die komplette Windows-Installation. Damit kommen auch Computerneulinge zurecht.

Die BTRFS-Option richtet sich hingegen an Linux-Profis. Ein damit erstellter Stick kann dank des BTRFS-Dateisystems eine Snapshot-Funktion nutzen. Darüber können Sie Desinfec't dauerhaft mit zusätzlicher Software wie Office-Anwendungen ausstatten oder sogar Treiber für etwa standardmäßig nicht unterstützte WLAN-Sticks nachinstallieren [1]. Doch dafür sind weiterführende Linux-Kenntnisse unabdingbar. Außerdem befindet sich die Option noch im Test-Stadium.

## Desinfec't starten

Um die Kompatibilität von Desinfec't 2023/24 zu testen, probieren wir das Sicherheitstool auf ver-

schiedenen aktuellen, aber auch älteren PCs aus. Im Zuge dessen prüfen wir unter anderem, ob das System startet, Netzwerkverbindungen funktionieren und NVMe-SSDs erkannt werden. Ist das der Fall, aktualisieren wir die Virensignaturen und lassen Virensans laufen. Zusätzlich prüfen wir, ob das Einbinden von mit Bitlocker oder VeraCrypt verschlüsselten Daten klappt. Angesichts der Vielzahl von PC-Konfigurationen und Hardware-Komponenten können wir nicht garantieren, dass Desinfec't zu jedem System kompatibel ist.

Damit Desinfec't statt Windows bootet, müssen Sie Ihren PC so einstellen, dass er vom Stick und nicht von der Festplatte startet. Wie das funktioniert, steht im Kasten „Desinfec't starten“ auf Seite 13.

Wenn Desinfec't den Start mit den Standardeinstellungen verweigert, gibt es noch ein paar alternative Startoptionen. Falls Ihr Computer über brandneue Hardware verfügt, können Sie versuchen, das System mit dem alternativen Kernel 6.2 zu starten. Dieser Kernel bringt viele Treiber für funkelnde neue PC-Komponenten mit. Klappt das auch nicht, können Sie es noch über die Safe-Start-Option probieren. Bleibt der Bildschirm trotzdem schwarz oder erscheinen Fehlermeldungen, ist Ihr PC wahrscheinlich nicht kompatibel.

## Scanner aktualisieren

Läuft Desinfec't erst einmal, haben Sie die größte Hürde genommen. Nach dem ersten Start müssen Sie noch den Projektordner einrichten. Dank eines automatisch auftauchenden Fensters ist das schnell erledigt. Dort brauchen Sie lediglich den Namen des Ordners einzugeben. Da Desinfec't verschiedene PCs anhand von Hardware-IDs identifiziert, bieten sich hier Bezeichnungen wie „Arbeitskiste“ und „Spiele-PC“ an. So nutzen Sie das Sicherheitstool auf verschiedenen Computern, ohne den Überblick zu verlieren. Im Projektordner speichert das System seine Scan-Ergebnisse. Dort können Sie aber auch eigene Daten wie Screenshots ablegen. Da die Daten auf einer speziellen Partition liegen, bleiben sie über einen Neustart hinweg erhalten.

Damit die Scanner ihre Virensignaturen aktualisieren können, muss der PC mit dem Internet verbunden sein. Das gelingt über ein LAN-Kabel oder ohne Strippe via WLAN. Um eine kabellose Verbindung herzustellen, wobei sich Desinfec't das Passwort für eine automatische Verbindung nach dem Start merken soll, doppelklicken Sie auf das Icon „Viren-Scan starten“. Der Assistent öffnet automa-

tisch ein Fenster, um die Verbindung herzustellen. Dort müssen Sie Ihr WLAN auswählen, das Kennwort eingeben und die Option zum Speichern des Passworts auswählen. Achtung: Das Kennwort liegt unverschlüsselt auf dem Stick. Verlieren Sie diesen, kennt der Finder Ihren WLAN-Zugang. Wollen Sie das Kennwort nicht speichern, stellen Sie die Verbindung nach jedem Neustart manuell über das WLAN-Symbol unten rechts in der Taskleiste her.

Vor jedem Scan aktualisieren sich die Virensignaturen automatisch. Da diese beim ersten Start von Desinfec't bereits mehrere Wochen alt sind, dauert der Vorgang mit rund 15 Minuten vergleichsweise lang. Nutzen Sie das System regelmäßig, gehen die Updates schneller vonstatten. Desinfec't merkt sich diese Signaturen, sodass Sie nach einer Aktualisierung auch Offline-PCs scannen können. Um Virensignaturen vorab zu aktualisieren, starten Sie den Viren-Scan-Assistenten und wählen im Reiter „Experte“ die Option „Nur Signaturaktualisierung, kein Virenscan“ aus.

## Viren jagen

Im Scan-Assistenten selektieren Sie die System-Partitionen, die der Scanner untersuchen sollen. Weiter unten im Fenster können Sie auch einen bestimmten Ordner oder einen angeschlossenen USB-Datenträger auswählen. Im nächsten Schritt entscheiden Sie, welcher Scanner auf Virenjagd gehen soll. Für

einen ersten Überblick reicht es meist aus, den vor eingestellten Scanner von Eset von der Leine zu lassen. Wird dieser fündig, können Sie im Nachgang noch weitere Scanner auf Windows hetzen. Schlagen auch diese Alarm, sollten Sie sich die in Firefox automatisch öffnende Ergebnisliste genauer anschauen. Im Reiter „Experte“ können Sie noch das Durchsuchen von Archiven und Mailboxen aktivieren. Doch Vorsicht: Da Desinfec't solche Dateien im Arbeitsspeicher entpacken muss, kann das bei sehr großen Archiven zu Abstürzen führen.

Wenn Scanner eine Datei für schädlich halten: Bewahren Sie Ruhe. Es kann sich durchaus um einen Fehlalarm handeln. Vor allem ClamAV neigt dazu, Dateien vorschnell zu verurteilen. Um Funde besser einschätzen zu können, laden Sie die Dateien direkt aus der Ergebnisliste zum Online-Analysedienst VirusTotal hoch. Dort schauen rund 60 Scanner auf den potenziellen Schädling und geben ihre Einschätzung ab. Oft helfen auch von anderen Nutzern verfasste Kommentare beim Einordnen.

Handelt es sich allem Anschein nach tatsächlich um einen Schädling, machen Sie diesen in der Ergebnisliste über die Schaltfläche „Umbenennen“ unschädlich. Dabei löscht Desinfec't die Datei nicht, sondern hängt an den Dateinamen die Endung .VIRUS an. Das führt dazu, dass Windows etwa die Datei „Trojaner.exe.VIRUS“ nicht mehr ausführen kann. Dieser Ansatz hat den Vorteil, dass Sie den Vorgang durch einfaches Entfernen von .VIRUS rück-

ESET NOD32	WithSecure	ClamAV	Aktion
/media/desinfect/desinfDATA/Test-Viren/ALL/Viren7/Virus.Win16.AEP.1129	Malware.Win32.WINVIK.D	Win.Trojan.V.11	<a href="#">VirusTotal umbenennen</a>
/media/desinfect/desinfDATA/Test-Viren/ALL/Viren7/Virus.Win16.AEP.b	Malware.W16/Aep.A	Win.Trojan.W.20	<a href="#">VirusTotal umbenennen</a>
/media/desinfect/desinfDATA/Test-Viren/ALL/Viren7/Virus.Win16.AEP.b	Malware.W16/Aep.1563	Win.Trojan.W.19	<a href="#">VirusTotal umbenennen</a>
/media/desinfect/desinfDATA/Test-Viren/ALL/Viren7/Virus.Win16.Apparition.b			

**In der Ergebnisliste sehen Sie, welcher Scanner auf welche Datei angeschlagen hat. Zum Eingrenzen von Fehlalarmen laden Sie potenzielle Schädlinge direkt zum Online-Analysedienst Virus Total hoch.**

# Verschlüsselte Festplatten scannen

Wer seine Festplatte mit Microsofts Bitlocker verschlüsselt hat, kann das Laufwerk direkt aus dem Scan-Assistenten heraus einbinden. Dafür müssen Sie es lediglich auswählen und nach den Scanner-Updates das Bitlocker-Passwort eingeben. Das klappt auch, wenn Sie den PC via TPM entsperren und den 48-stelligen Wiederherstellungsschlüssel eingeben.

Im Test hat das in der Redaktion problemlos mit einer unter Windows 10 21H2 sowie mit einer unter Windows 11 22H2 verschlüsselten Systempartition und mit einem USB-Stick geklappt. Mit kommenden Windows-Updates könnte es aber nicht mehr funktionieren. Das Problem ist, dass Microsoft in Windows-Updates manchmal an der Bitlocker-Schraube dreht und die Entwickler der Mount-Tools unter Linux erst mal nachziehen müssen. Wenn das erfolgt ist, bringen wir Desinfec't auf den aktuellen Stand.

Wer mit VeraCrypt verschlüsselte Daten scannen möchte, muss die Container beziehungsweise Laufwerke über den VeraCrypt-Client im Expertentools-Ordner einbinden. Um Festplatten einzubinden, müssen Sie VeraCrypt starten. Nun wählen Sie den verschlüsselten Datenträger aus und mounten diesen im VeraCrypt-Client. Die Festplatte taucht dann im

Scan-Assistent zur Auswahl auf. Haben Sie Ihre Systemplatte komplett verschlüsselt, müssen Sie noch die Option „Partition mithilfe der Systemverschlüsselung einhängen (Pre-Boot Authentifizierung)“ auswählen. Im Scan-Assistenten taucht die Festplatte aber nicht als Windows-Partition auf, sondern Sie müssen sie über „einen Ordner scannen“ auswählen.



gängig machen können. Das ist hilfreich, wenn eine legitime Datei irrtümlich als Virus abgestempelt wurde und beispielsweise ein Dienst nicht mehr funktioniert. Ist das bei vielen Dateien passiert, hilft das auf die Dateiendung .VIRUS zugeschnittene Skript „Umbenennung rückgängig machen“ im Ordner „Expertentools“ weiter.

## Für Profis

Achtung: Die zwei im Expertentools-Ordner aufrufbaren Virenjäger Open Threat Scanner (OTS) und Thor Lite richten sich an Nutzer, die sich mit Malware-analyse und Incident Response auskennen. Damit kann man hoch entwickelter Malware wie Emotet auf die Spur kommen. Damit das gelingt, braucht es aber Erfahrung, die Ergebnisse richtig zu deuten. Auf Windows-PCs von Onkeln und Tanten ist diese Vorgehensweise überdimensioniert.

OTS baut auf Yara-Regeln, mit denen man sehr allgemein nach bestimmten Dingen in Dateien su-

chen kann und so gezielt bestimmte Schädlinge aufspürt. Diese Erkennungsregeln bezieht der Scanner bei der Aktualisierung aus dem GitHub-Repository von Reversing Labs. Die Regeln kommen von erfahrenen Sicherheitsforschern und sie gelten als äußerst präzise, sodass Fehlalarme selten sind. Sie können OTS aber auch mit eigenen Yara-Regeln ausstatten [2]. Der Thor Lite Scanner von Nextron setzt auf eine Mischung aus regelmäßig aktualisierten Yara-Regeln und anderen Indicators of Compromise (IOC).

Im Expertentools-Ordner finden Sie noch weitere Werkzeuge für Profis. Mit FRED greifen Sie etwa auf die Registry der inaktiven Windows-Installation zu. Vorsicht: Wer hier nicht weiß, was er tut, kann ein Windows so beschädigen, dass das System nicht mal mehr startet. Mit PhotoRec stellen Sie mit etwas Glück versehentlich gelöschte Dateien wieder her. Mit dem Monitoring-Tool Checkmk können Admins neuerdings unter anderem den Status der Viren-signaturen prüfen. Mit FLOSS kommen Profis versteckter Malware auf die Spur.

(des)

# Desinfec't 2023/24

Das c't-Sicherheitstool bietet Hilfe für virenverseuchte Windows-PCs. Hier finden Sie Tipps zu den häufigsten Problemen bei der Vorbereitung und beim Einsatz von Desinfec't.

Von **Dennis Schirrmacher**



## Installation nicht möglich

**?** Ich halte mich penibel an die Anleitung im Heft, aber beim Einrichten des Sticks taucht bereits am Anfang unter Windows eine Fehlermeldung mit „Error 5: Zugriff verweigert“ auf und es geht nicht weiter. Was mache ich falsch?

**!** Sie machen gar nichts falsch. Da funkts ein Virenschanner oder Software von Acronis dazwischen und stuft den Zugriff auf den USB-Stick fälschlicherweise als gefährlich ein. Das ist ein Fehlalarm. Deaktivieren Sie dementsprechend für die Dauer der Installation den Echtzeitschutz, damit es klappt. Vergessen Sie aber nicht, den Scanner wieder einzuschalten, wenn der Desinfec't-Stick fertig ist.

## Desinfec't startet nicht

**?** Ich habe die aktuelle Version heruntergeladen, aber bekomme die Scanner unter Windows nicht zum Laufen. Was mache ich falsch?

**!** Desinfec't ist keine Windows-Anwendung, die Sie mit einem Doppelklick starten. Es bringt ein Live-System mit, welches direkt von einem USB-Stick startet. Sie müssen Ihren PC also von einem Desinfec't-Stick statt von der Windows-Festplatte starten.

Dafür wählen Sie im BIOS-Bootmenü den am Computer angeschlossenen Stick aus.

## Firefox fehlt

**?** Ich habe Desinfec't mit Rufus auf einem USB-Stick installiert. Es hat auch alles geklappt. Das System startet, aber Firefox fehlt. Was ist da schiefgelaufen?

**!** Sie haben den Desinfec't-Stick mit einem nicht kompatiblen Tool erstellt. Die Installation unter Windows funktioniert ausschließlich mit unserem Installationstool „Desinfect2USB\_64\_Bit.exe“. Das finden Sie im heruntergeladenen Zip-Archiv. Nur die Installation damit stellt sicher, dass alle für den reibungslosen Betrieb notwendigen Partitionen erstellt werden. Der Aufbau von Desinfec't ist nämlich vergleichsweise komplex. Das System befindet sich etwa auf einer Partition, die keine Daten dauerhaft speichert. Das bedeutet, dass sich das System nach einem Neustart wieder in den Werkszustand zurückgesetzt. Die aktualisierten Virensignaturen oder in Sicherheit gebrachte Daten von einem Problem-PC liegen wiederum auf anderen Partitionen, in denen Daten dauerhaft erhalten bleiben. Damit diese Partitionen korrekt angelegt werden, müssen Sie den Stick einmal umwandeln. Das geschieht beim ersten

Start über den obersten Menüpunkt im Desinfec't-Bootmenü.

## Desinfec't-Stick löschen

**?** Ich würde meinen alten Desinfec't-Stick gerne löschen und ihn wieder ausschließlich zum Speichern von Fotos und Videos nutzen. Leider steht nach der Formatierung unter Windows nicht mehr der komplette Speicherplatz zur Verfügung.

**!** Ein Desinfec't-Stick besteht aus mehreren Partitionen, von denen einige aufgrund ihres Linux-Dateisystems unter Windows nicht sichtbar sind. Sie formatieren nur die unter Windows sichtbare Partition, die aber nicht den gesamten Speicherplatz beinhaltet. Um den vollen Speicherplatz wiederherzustellen, gehen Sie wie folgt vor: Geben Sie unter Windows 10/11 im Suchfeld den Befehl cmd, um die Eingabeaufforderung zu öffnen und starten Sie diskpart. Nun müssen Sie den zu löschenen Desinfec't-

Stick auswählen. Geben Sie dafür zuerst list disk ein, damit die am PC angeschlossenen Datenträger angezeigt werden. Vorsicht: In der Auflistung tauchen auch interne Festplatten auf. Stellen Sie im nächsten Schritt also sicher, dass Sie wirklich den Stick ausgewählt haben, da dieser im weiteren Verlauf unwiederbringlich gelöscht wird. Zu Auswahl des Sticks geben Sie select disk ? ein. Das Fragezeichen ersetzen Sie mit der Nummer des korrekten Laufwerks. Im Anschluss tippen Sie zum Löschen des Datenträgers clean ein. Nach der Eingabe von create partition primary können Sie den Stick wie gewohnt unter Windows mit der vollen Speichergröße formatieren.

## Desinfec't-Upgrade

**?** Ich habe hier noch einen Desinfec't-Stick aus dem Jahr 2023. Kann ich den auf Desinfec't 2023/24 upgraden?

**!** Ein Upgrade von älteren Desinfec't-Versionen ist nicht vorgesehen. Installieren Sie ein neues Desinfec't über eine ältere Version, kann es im Betrieb zu Problemen kommen und Desinfec't meldet veraltete Signaturen der Vorversion. Um solche Probleme zu vermeiden, sollten Sie das Sicherheitstool stets auf einem korrekt gelöschten Stick installieren. Wie das funktioniert, steht unter dem Punkt „Desinfec't-Stick löschen“.

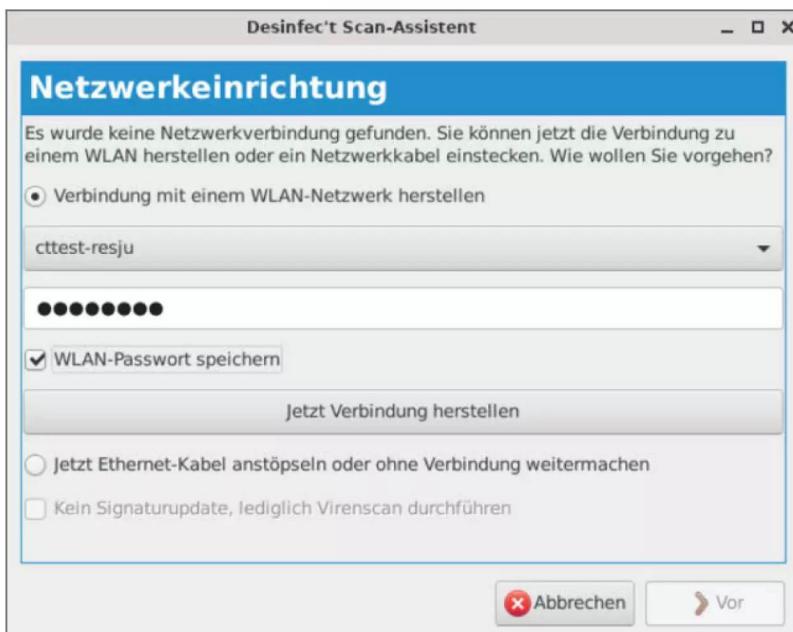
## Updates

**?** Ich habe gelesen, dass es bereits eine Aktualisierung für Desinfec't 2023/24 gibt. Im Artikel stand ja auch, dass sich Updates bei aktiver Internetverbindung automatisch installieren. Bei mir klappt das aber nicht.

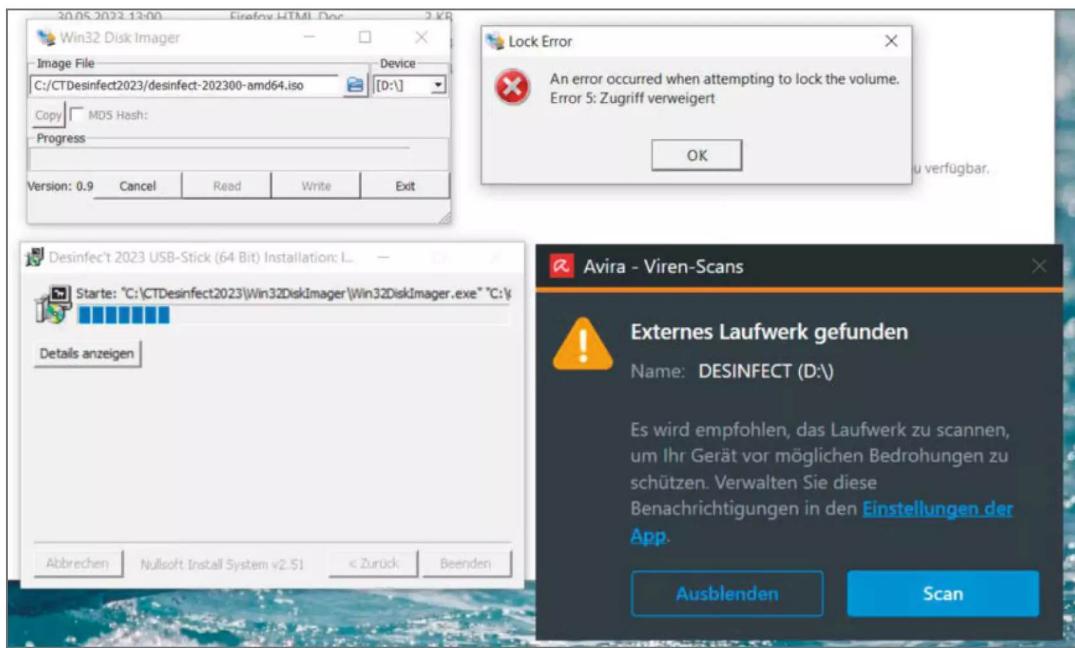
**!** Ja, eigentlich sollten sich Updates automatisch installieren. Leider klappt das in einigen Fällen aus uns bislang unbekannten Gründen nicht. Ist das der Fall, können Sie das Update mit folgenden Befehlen direkt aus unserem Repository installieren. Öffnen Sie dafür das Terminal aus der Taskleiste und bestätigen Sie jeden Befehl mit der Eingabetaste.

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

Den aktuellen Patch-Versionsstand können Sie oben rechts im Statusfenster auf dem Desktop ablesen.



Nur, wenn Sie den Scan-Assistenten auf einem PC ohne Internetverbindung via Ethernetkabel starten, können Sie auf Wunsch das WLAN-Passwort speichern.



**Wenn die Desinfec't-Stick-Installation unter Windows nicht gelingt und der Zugriff verweigert wird, funktioniert in der Regel der Echtzeitschutz von Virensuchern dazwischen. Deaktivieren Sie den Scanner einfach für die Dauer der Installation.**

## NVME SSD nicht erkannt

**?** Leider erkennt Desinfec't meine Festplatte nicht und ich kann die Windows-Installation nicht scannen. Ich habe eine NVME-SSD. Kann ich da irgendwas machen?

**!** Ja, starten Sie Desinfec't mal mit dem alternativen Kernel 6.2. Der bringt noch weitere Treiber unter anderem für NVME SSD mit. Den Kernel wählen Sie im Bootmenü von Desinfec't aus.

## WLAN-Passwort nicht gespeichert

**?** Ich möchte Desinfec't via WLAN nutzen. Ich habe aber keine Lust, das WLAN-Passwort nach jedem Reboot erneut einzugeben. Kann man das Kennwort speichern?

**!** Desinfec't merkt sich das WLAN-Passwort nur, wenn das System noch keine Internetverbindung über Ethernet hat und Sie den Scan-Assistenten starten. Nun taucht das Fenster „Netzwerkeinstellung“ auf. Dort wählen Sie Ihr WLAN aus, geben das Passwort ein und setzen einen Haken bei „WLAN-

Passwort sichern“. Erst dann merkt sich das System das Kennwort. Aber Achtung: Das WLAN-Passwort liegt im Klartext auf dem Desinfec't-Stick vor. Verlieren Sie ihn, kennt der Finder Ihren WLAN-Zugang.

## Alle Scanner notwendig?

**?** Ich möchte den PC meiner Tante auf Trojaner überprüfen und habe, um auf Nummer sicher zu gehen, neben ClamAV, Eset und WithSecure auch den Open Threat Scanner und Thor Lite Scanner gestartet. Vor allem die letzten beiden Scanner brauchen Stunden. Was passiert da?

**!** Sie schießen mit Kanonen auf Spatzen. In der Regel reicht es im privaten Umfeld aus, eine Untersuchung mit dem voreingestellten Scanner von Eset zu starten. Im Anschluss bekommt man in der Regel einen guten Eindruck, ob sich Schadcode auf einem PC befindet. Vor allem Open Threat Scanner und Thor Lite Scanner sind für Profis gedacht, die etwa in Firmen Computer und Netzwerke auf Schadcode analysieren. Diese können mit den „kryptischen Ergebnissen“ umgehen und damit auch sehr ausgereifte Attacken aufspüren. (des)

Desinfec't-Forum  
[ct.de/w55n](http://ct.de/w55n)

# Technik oder Kultur? Automatisierung ist mehr als ein paar Klicks

In der heutigen schnelllebigen Geschäftswelt ist Effizienz der Schlüssel zum Erfolg. Unternehmen stehen vor der Herausforderung, sich ständig weiterzuentwickeln und Prozesse zu optimieren, um wettbewerbsfähig zu bleiben. Eine wichtige Strategie, um diese Ziele zu erreichen, ist der Aufbau einer Kultur der Automatisierung in den IT-Betriebsabläufen. Automatisierung ermöglicht nicht nur eine höhere Effizienz, sondern reduziert auch menschliche Fehler und rationalisiert Prozesse.

## Die fünf Säulen der Automatisierungskultur

Wie gelingt es Unternehmen, eine Kultur der Automatisierung aufzubauen und zu etablieren?

### Ohne Strategie geht's nicht

Wer im großen Stil auf Automatisierung setzen will, braucht einen nachvollziehbaren Plan, klar definierte Ziele und eine transparente Strategie.

### Erfolg entsteht gemeinsam

Gamification oder Incentives sind gute Anreize, um das Team für ein groß angelegtes Automatisierungsprojekt zu gewinnen. Wenn alle an einem Strang ziehen, rückt das Ziel schneller in greifbare Nähe.

### Steter Tropfen höhlt den Stein

Regelmäßige Meetings mit dem Fokus Automatisierung sorgen dafür, dass das Thema im Fokus bleibt. Hier können die Teams offene Tickets besprechen und Vorschläge der Mitarbeitenden gemeinsam diskutieren.

### Testen, testen, testen

Neue Automatisierungen von bisher manuellen Prozessen können auch mal fehlerhaft sein – egal, wie gut sie vorher analysiert und geplant wurden. Daher lohnt es sich, Geräte zu Testzwecken anzuschaffen und diese als Spielwiese für neue Ideen zu nutzen, ohne dabei die Produktivumgebung zu gefährden.

### Die Ergebnisse zählen

Je besser die Automatisierungsvorhaben von Anfang an überwacht werden, umso leichter fällt es später, Ergebnisse zu präsentieren und anhand von transparenten Reports zu verdeutlichen, dass sich die Anstrengungen gelohnt haben.

### Wozu brauchen Unternehmen Automatisierung?

Von den Vorteilen automatisierter Prozesse können IT-Teams an den unterschiedlichsten Stellen in ihrem täglichen Wirken profitieren.

Hier nur einige Beispiele:

#### GERÄTE-ONBOARDING

Die Automatisierung kann bei der Einbindung neuer Geräte helfen. Die manuelle Einbindung von Geräten ist fehleranfällig, selbst wenn das Team eine Checkliste verwendet. Durch automatisierte Workflows können diese Fehler reduziert werden und die Integration neuer Geräte in das Netzwerk erfolgt reibungslos.

## BENACHRICHTIGUNGEN

Die Plattform von NinjaOne kann automatisch auf Benachrichtigungen reagieren. Zum Beispiel kann die Überwachung von fehlgeschlagenen Anmeldungen automatisch Antworten auslösen, wenn es mehrere fehlgeschlagene Versuche innerhalb kurzer Zeit gibt. Ein solches Event deutet in der Praxis häufig auf mögliche Brute-Force-Angriffe hin, auf die die Lösung automatisch reagiert.

## TICKETING

Die Ticketing-Plattform von NinjaOne kann automatisch auf häufig auftretende Probleme reagieren und die Belastung des Helpdesks reduzieren. Dies umfasst die Bereitstellung von Ressourcen oder Richtlinien für gängige Probleme wie Passwortrücksetzungen, wodurch die Effizienz des Supportteams gesteigert wird.

## INDIVIDUELLE SKRIPTE UND VORLAGEN

NinjaOne bietet eine Bibliothek mit vorgefertigten Skripten und Vorlagen. User können darüber hinaus ihre eigenen Skripte für spezifische Anforderungen erstellen und anpassen. Dies ermöglicht eine hohe Flexibilität bei der Automatisierung von Aufgaben, die genau auf die Bedürfnisse des Unternehmens zugeschnitten sind.

## REMOTE-ZUGRIFFSANWENDUNGEN

Nicht alle Remote-Zugriffsanwendungen werden als herkömmliche Anwendungen installiert. Einige funktionieren als Dienste oder Prozesse. Diese Unterscheidung ist wichtig, wenn es um Automatisierung geht: Unternehmen müssen sicherstellen, dass die gewählte Automatisierungslösung die Vielfalt der Anwendungsfälle und Zugriffsmethoden unterstützt, die in ihrer IT-Umgebung vorhanden sind.

## Sind Sie bereit?

Mit NinjaOne haben Sie die Möglichkeit, die Effizienz Ihrer IT-Betriebsabläufe zu steigern, Fehler zu reduzieren und Prozesse zu rationalisieren. Erfahren Sie mehr auf [www.ninjaone.de](http://www.ninjaone.de)

**ninjaOne**



# Microsoft Defender nachinstallieren

Seit geraumer Zeit bietet Microsoft seinen Virensensor Defender auch für Linux an. In Desinfec't 2023/24 können Sie ihn nun in einer Preview-Version mit wenig Aufwand installieren und zur Virenjagd einsetzen.

Von **Mattias Schlenker**

Desinfec't 2023/24 hat standardmäßig bereits mehrere Scanner von etwa Eset und WithSecure im Gepäck, mit denen Sie eine Windows-Installation auf Schädlinge untersuchen. Im Falle des Verdachts auf eine relativ frische Malware ist es aber immer besser, noch mehr Virensensor zur Hand zu haben. So holen Sie sich verschiedene Meinungen ein, um die Bedrohung besser einschätzen zu können.

Microsofts Defender hat sich in den letzten Jahren vom halbwegen brauchbaren Basisschutz zu einem vollwertigen Antiviren-Programm hochgearbeitet, das in Tests regelmäßig mit als eines der besten

abschneidet. Darum ließ uns der mit dem Linux-System von Desinfec't kompatible „Microsoft Defender Advanced Threat Protection“-Scanner freudig aufhorchen. Er punktet mit einer hohen Erkennungsrate und gibt sich hinsichtlich Arbeitsspeicher- und Festplattenbedarf genügsam. Das sind beste Voraussetzungen für den Betrieb des Live-Systems von einem USB-Stick. Leider gestattete uns Microsoft nicht, den Defender direkt in Desinfec't einzubauen, was technisch kein Problem gewesen wäre.

Es ist jedoch legitim, dass Sie sich selbst eine entsprechende Lizenz besorgen und die Software in Ihre persönliche Desinfec't-Installation einbauen.

Also haben wir die dafür benötigte Infrastruktur vorbereitet und liefern hier die Anleitung, wie Sie das am besten anstellen. Dabei sind aber einige Feinheiten zu beachten und der Vorgang richtet sich explizit an Linux-Bastler. Nach der Installation können Sie direkt mit Desinfec't und dem Defender auf Virenjagd gehen.

## Erste Voraussetzung

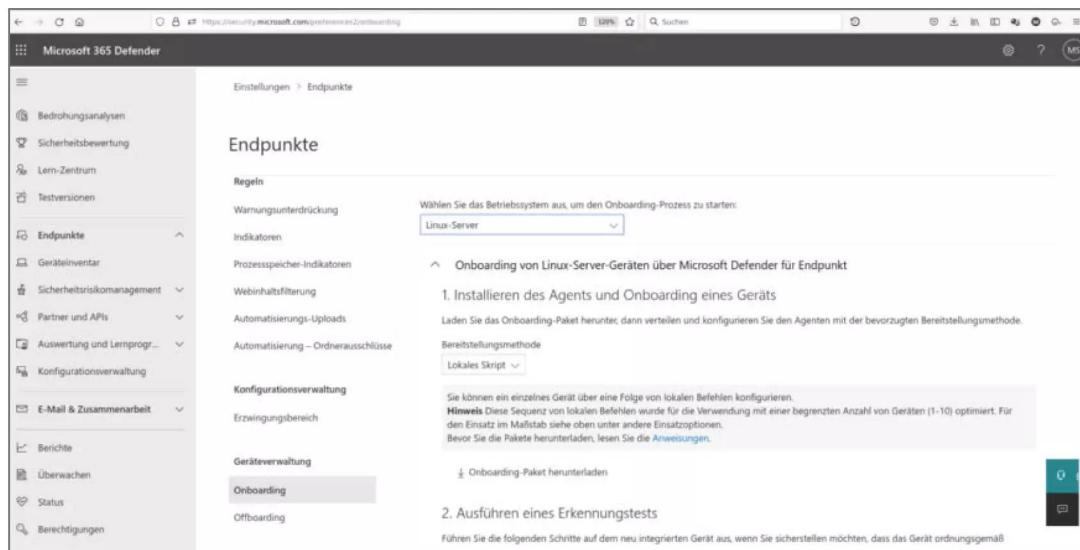
Damit Sie den Defender-Scanner nutzen können, benötigen Sie eine Lizenzdatei. Diese stellen sich Firmenkunden im Dashboard von Microsoft 365 Defender dauerhaft aus. Alle anderen fordern über einen kostenlosen Testaccount eine sieben Monate lang gültige Lizenz an. Da der Testaccount keinerlei Nachweise erfordert und schnell angelegt ist, ist diese Hürde marginal. Nach den sieben Monaten können Sie einfach einen neuen Account erstellen, erneut eine Lizenz erzeugen und mit den folgenden Schritten installieren.

Melden Sie sich mit einem Microsoft-Account unter [security.microsoft.com](https://security.microsoft.com) an. Falls das verwendete Konto kein Firmenkonto ist, wird Ihnen angeboten, eins zu erstellen. Bekommen Sie dieses Angebot nicht oder tauchen auf der Website Einträge wie „End-

punkte“ nicht auf, müssen Sie die Account-Erstellung selbst in die Hand nehmen (siehe [ct.de/wkjk](#)).

Hat alles geklappt, loggen Sie sich ins Dashboard von Microsoft 365 Defender ein. Klicken Sie darin auf „Endpunkte/Geräteinventar“. Ziemlich weit unten im Fenster befindet sich der Punkt „Onboarding von Geräten“, den Sie anklicken. Wählen Sie im Drop-down-Menü für Betriebssysteme „Linux-Server“ aus. Beim Punkt „Bereitstellungsmethode“ muss „Lokales Skript“ stehen. Mit dem Link „Onboarding-Paket herunterladen“ erhalten Sie eine Zip-Datei, welche ein Python-Skript enthält. Das Skript prüft die Rechte und schreibt eine JSON-Konfigurationsdatei. Kopieren Sie diese Zip-Datei auf die unter Windows sichtbare Partition des Desinfec't-Sticks. Um die Einbettung der Lizenz ins System kümmert sich später ein Desinfec't-Skript.

Für die Defender-Installation muss Desinfec't zwingend von einem USB-Stick laufen. Microsofts Paketschlüssel und die für die Nachinstallation des Defender notwendigen Abhängigkeiten sind bereits in Desinfec't 2023/24 enthalten. Für die Installation müssen Sie lediglich das Microsoft-Netzfilter-Modul (mnde-netfilter, wenige KByte) und den Defender (mmdatp, 60 MByte) herunterladen, was ein Skript für Sie erledigt.



**Um mit „Defender Advanced Threat Prevention“ Viren aufzuspüren, benötigen Sie eine gültige Lizenz. Diese erstellen Sie über einen kostenlosen Microsoft-365-Defender-Account.**

**Der Defender überträgt Funde in Microsofts Sicherheitsportal. Die Einträge sind nur für Sie sichtbar. Dennoch sollten Sie beachten, dass bereits Dateinamen sensible Informationen enthalten können.**

## Die Installation

Um das Skript nutzen zu können, müssen Sie nichts weiter tun, Desinfec't 2023/24 bringt bereits alles Nötige mit. Starten Sie einfach das Skript im Terminal via `sudo /opt/desinfect/update_msdefender.sh`.

Nach der Ausführung lädt es die benötigten Pakete herunter, installiert sie, bittet die Lizenz ein und aktualisiert die Virensignaturen. Wenn alles geklappt hat, erscheint nach wenigen Minuten der Eintrag „Microsoft Defender“ mit einem aktuellen Signatur-Datum im Statusfenster oben rechts auf dem Desktop. Die Defender-Daten landen auf der persistenten Partition des Sticks, damit der Scanner auch nach einem Neustart noch verfügbar ist. Zum Abschluss modifiziert das Skript einige Einstellungen. Zum Beispiel haben wir den im Fall des Desinfec't-Systems sinnlosen Echtzeitschutz deaktiviert und unterbinden die Übermittlung verdächtiger Dateien an Microsoft. Unter `ct.de/wkjk` finden Bastelwillige weitere Parameter, um den Defender noch individueller anzupassen.

Falls Sie neugierig sind und einen Blick in die Verzeichnisstrukturen `/var/opt/microsoft/mdatp` und `/opt/microsoft/mdatp` werfen, mag Ihnen der Name vieler Shared Objects und der Signaturdateien von älteren Versionen von Desinfec't bekannt vorkommen. Tatsächlich nutzt der Microsoft Defender in den

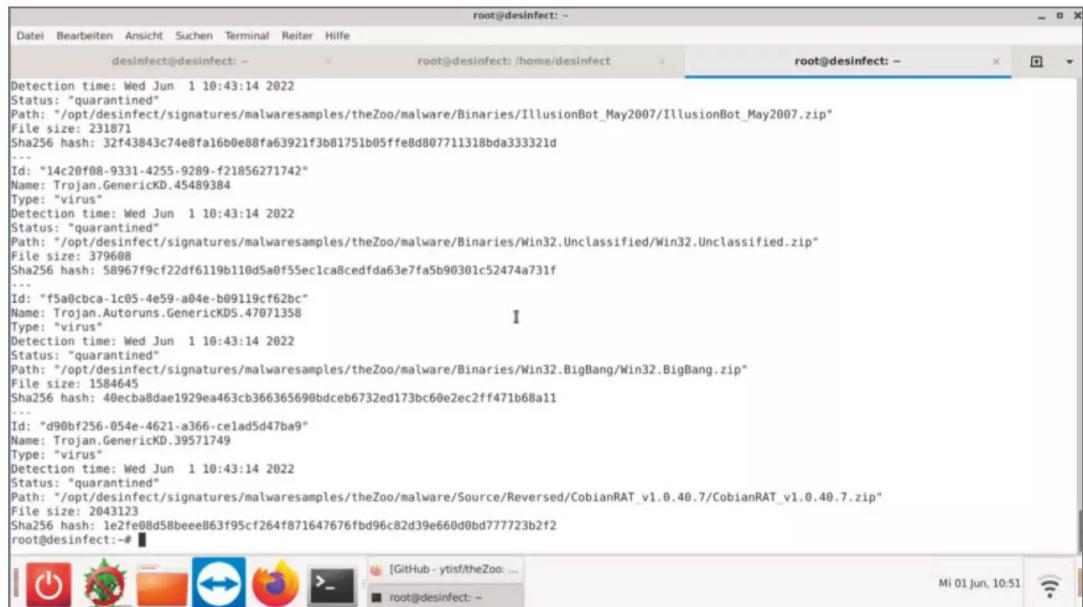
Varianten für Linux und macOS die Scan-Engine von Bitdefender. Dieser Scanner war eine Zeit lang in Desinfec't integriert, bis wir ihn aus Lizenzgründen entfernen mussten. Marketing-Aussagen von Bitdefender legen darüber hinaus nahe, dass auch ein Teil der Signaturen von Bitdefender stammt. Dagegen bilden die Management-Schnittstellen und das Standardverhalten die Windows-Variante des Defenders nach.

## Bedienung

Nach der Installation und dem Update der Signaturen gibt das Skript die Informationen zu Lizenzierung, Konfiguration und Update-Zustand aus. Das können Sie auch jederzeit im Terminal mit dem Befehl `mdatp health` anfordern. Einen Virenscan starten Sie mit `mdatp scan custom --path /media/sdx1`. Wobei `/media/sdx1` durch einen beliebigen Mountpoint oder einen anderen Ordner zu ersetzen ist. Der Befehl `df -h` zeigt die Bezeichnungen für Mountpoints an. Während des Scans werden mehrzeilige Blöcke ausgegeben, welche den Namen der Schadsoftware enthalten, nicht jedoch den Dateipfad.

Standardmäßig kann Desinfec't nur lesend auf Festplatten zugreifen und keine Dateien verändern. Mounten Sie Laufwerke über den Explorer mit einem Rechtsklick und der Auswahl von „Einhängen“, kann

**Mit dem Befehl  
mdatp threat list  
erhalten Sie nach  
dem Scan die Liste  
der gefundenen  
Schadsoftware.**



```

root@desinfect: ~
Datei Bearbeiten Ansicht Suchen Terminal Reiter Hilfe
desInfect@desinfect: ~ root@desinfect: /home/desinfect root@desinfect: ~
Detection time: Wed Jun 1 10:43:14 2022
Status: "quarantined"
Path: "/opt/desinfect/signatures/malwaresamples/theZoo/malware/Binaries/IllusionBot_May2007/IllusionBot_May2007.zip"
File size: 231871
Sha256 hash: 32f43843c74e8fa16b0e88fa63921f3b81751b05ffe8d087711318bda333321d
...
Id: "14c20f08-9331-4255-9289-f21856271742"
Name: Trojan.GenericKD.45489384
Type: "virus"
Detection time: Wed Jun 1 10:43:14 2022
Status: "quarantined"
Path: "/opt/desinfect/signatures/malwaresamples/theZoo/malware/Win32.Unclassified/Win32.Unclassified.zip"
File size: 379688
Sha256 hash: 58967f9cf22df6119b110d5a0f55ec1ca8cedfd863e7fa5b90301c5247a731f
...
Id: "f5a0cba-1c05-4e59-a04e-b09119cf62bc"
Name: Trojan.Autoruns.GenericKD.47071358
Type: "virus"
Detection time: Wed Jun 1 10:43:14 2022
Status: "quarantined"
Path: "/opt/desinfect/signatures/malwaresamples/theZoo/malware/Binaries/Win32.BigBang/Win32.BigBang.zip"
File size: 1584645
Sha256 hash: 40ecba8dae1929ea463cb366365690bdceb6732ed173bc60e2ec2ff471b68a11
...
Id: "d90bf256-054e-4621-a366-ce1ad5d47ba9"
Name: Trojan.GenericKD.39571749
Type: "virus"
Detection time: Wed Jun 1 10:43:14 2022
Status: "quarantined"
Path: "/opt/desinfect/signatures/malwaresamples/theZoo/malware/Source/Reversed/CobianRAT_v1.0.40.7/CobianRAT_v1.0.40.7.zip"
File size: 2043123
Sha256 hash: 1e2fe08d58beee863f95cf264f871647676fb96c82d39e660d0bd777723b2f2
root@desinfect: ~

```

Desinfec't auch schreibend darauf zugreifen. Vorsicht: Ist das der Fall, verschiebt Defender jeden Schädlingsfund sofort in Quarantäne. Das verstößt eigentlich gegen die Desinfec't-Philosophie, dass der Scan keine Veränderungen am System vornehmen darf und selbst bei einer vom Anwender angestoßenen „Reinigung“ Dateien lediglich an Ort und Stelle umbenenn und damit unschädlich macht. Den Lesen-(ro) und Schreiben-Status (rw) einzelner Laufwerke prüfen Sie mit `cat /proc/mounts`.

Bei unseren Tests ist es uns bislang nicht gelungen, das automatische Verschieben von potenziellen Trojanern in einen Quarantäne-Ordner abzuschalten. Sollten Sie einen Schalter dafür entdecken, geben Sie uns gerne Bescheid.

Welche Gefahren Defender entdeckt und verschoben hat, verrät der Befehl `mdatp threat list`. Sollte eine Datei verschoben worden sein, die Sie noch benötigen oder die Sie beim Online-Analysedienst VirusTotal hochladen wollen, holen Sie sie mit folgenden Befehlen zurück:

```

mdatp threat quarantine restore ↵
--id [threat-id] ↵
--path [zielordner]

```

Den Quarantäne-Ordner finden Sie unter `/var/opt/microsoft/mdatp` oder `/opt/microsoft/mdatp`. Die

Ordner befinden sich auf einer persistenten Stick-Partition und sie sind auch nach einem Neustart noch verfügbar.

## Ausblick

Der Microsoft Defender ist zum jetzigen Zeitpunkt als Preview-Version mit Basisfunktionen für Experimentierfreudige integriert. Desinfec't 2023/24 bringt das Installations- und Update-Skript `update_msdefender.sh` für Microsoft Defender mit und Sie können den Scanner über das Terminal nutzen. Zudem zeigt der Systemmonitor in der rechten oberen Ecke des Desktops den Zeitpunkt der Signaturaktualisierung an, sobald der Defender installiert ist.

Gerne würden wir an einer weiteren Integration des Defenders arbeiten. Allerdings erhebt Microsofts Scanner einen Alleinvertretungsanspruch und er mag keine anderen Scanner im Parallelbetrieb - das kann zu Problemen bei der Nutzung führen. Da die Bitdefender-Engine aber ordentliche Erkennungsraten liefert und für Nutzer von Microsofts Sicherheitsportal einen Mehrwert bietet, belassen wir es bis auf Weiteres bei der Implementation auf experimenteller Basis.

Im offiziellen Desinfec't-Forum (siehe [ct.de/wkjk](http://ct.de/wkjk)) freuen wir uns über Ihre Erfahrungen und Verbesserungsvorschläge.

**Weitere Infos zum  
Defender, Desinfec't-Forum  
[ct.de/wkjk](http://ct.de/wkjk)**

# Open Threat Scanner erweitern

In der Regel sind Malware-Entwickler von Emotet & Co. Anbietern von Antivirensoftware einen Schritt voraus. Bauen Sie doch Ihren eigenen AV-Scanner! Das funktioniert mit Desinfec't 2023/24 und ist gar nicht schwer.

Von **Mattias Schlenker**

**A**m 2. Advent 2019 wurde die Justus-Liebig-Universität Gießen von einer Emotet-Welle überrollt. Das Rechenzentrum beschloss daraufhin, alle vernetzten Windows-Systeme herunterzufahren und erst nach einer Prüfung auf Infektionen wieder ins Netzwerk zu lassen.

Doch wie erkennt man eine Malware, die für Virensucher noch unbekannt ist? Bei diesem Katz-und-Maus-Spiel hinken Hersteller von AV-Software stets hinterher: Sie müssen die passenden Signaturen erst erstellen und an die AV-Clients ausliefern – das kostet wertvolle Zeit. In Gießen identifizierte AV-Software die Schädlingsdateien erst fünf Tage nach der Entdeckung des Angriffs.

Hier kommt der universelle Yara-Scanner ins Spiel, den man mit eigenen Malware-Erkennungsregeln füttern kann. Das sind beispielsweise Muster wie Textstrings oder Prüfsummen. Darüber hinaus kann man die Untersuchung auf bestimmte Dateitypen oder auf Teile einer Datei beschränken. Das ist effizient und spart Zeit.

Das Rechenzentrum der Uni Gießen stellte dem Helmholtz Center for Information Security (CISPA) ein Festplatten-Image eines infizierten Systems zur Verfügung. Deren Schadsoftware-Experten identifizierten darin Ryuk- und Emotet-Komponenten und gestalteten daraus einen Satz Yara-Regeln.

Um damit Rechner zu scannen, beauftragte die Uni die Entwicklung einer Desinfec't-Version mit einem Yara-Scanner. Durch den speziell angepassten Scanner konnten die Uni-Admins äußerst effizient vorgehen und eindeutig infizierte PCs binnen einer halben Stunde identifizieren. Der Yara-Scanner hat es in Form des Open Threat Scanners (OTS) in Desinfec't 2023/24 geschafft. Out-of-the-box versorgen wir ihn mit tagesaktuellen Signaturen vom GitHub-Repository von ReversingLabs. Diese Regeln weisen generell eine hohe Erkennungsquote auf. Demzufolge sollte es zu weniger Fehlalarmen kommen. Sie können den Scanner aber auch mit selbst erstellten Regeln erweitern.

## Funktionsweise

Als Basis für die Suche nach Malware setzt der OTS auf Skripte und Konfigurationsdateien mit Yara-Regeln. Nach dem Booten von Desinfec't können Sie den OTS direkt starten: Der Scanner aktualisiert sich automatisch und durchsucht Festplatten mit unserem Standard-Yara-Regelsatz.

Ausgangspunkt ist das Skript „/opt/desinfect/yara-ots-wrappersh“. Starten Sie den OTS über das Icon auf dem Desktop, hängt das Skript zunächst alle Windows-Laufwerke ein. Anschließend startet



das automatische Update über das Skript „/opt/desinfect/update\_yara.sh“.

Dieses lädt die Pattern basierten Signaturen aus dem Github-Repository von ReversingLabs herunter, entpackt sie und trägt die Regeln zur Erkennung von Schädlingen in die Datei „/opt/desinfect/signatures/desinfect/yara/emetot.yar“ ein. Da sich Trojaner stetig verändern, kann OTS auch mal einen Virus übersehen. Im Zweifel müssen Sie wie später in diesem Artikel beschrieben, eigene Regeln erstellen.

Diese Methode ist aber effektiver, als die zu Beginn vom OTS eingesetzte MD5-Methode, bei der wir die Yara-Integration mit den Hashes per Honeypot „eingefangenen“ Schadsoftware-Samples füttern. Sollten neue Wellen von Krypto-Tojanern durch das Internet rollen, können wir per Online-Update zusätzlich zu den ReversingLabs-Regeln die Regeln anderer Anbieter wie Nextron oder Eigenkreationen hinzufügen.

## Erste eigene Regel

Starten Sie unter Desinfec't mit dem Erstellen einer Yara-Regel nebst einer Köder-Datei. Auf diese Datei lassen Sie den OTS los, um zu prüfen, ob Ihre Regel anschlägt. Verwenden Sie den integrierten Editor.

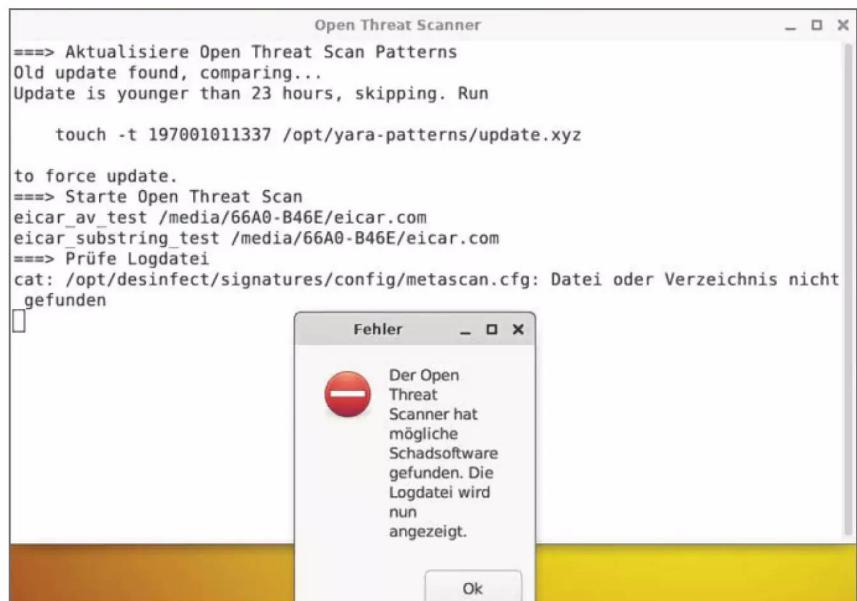
Zum Öffnen tippen Sie scite im Terminal ein. Im Editor erstellen Sie als Köder eine Textdatei, die ein paar markante Strings wie E-Mail- (erpresser@domain.xyz) oder Bitcoin-Adressen (1DeaDBEefXulub-MiRF4311tN1xE1n) enthält.

Damit simulieren Sie eine typische Erpresser-Notiz. Speichern Sie diese Datei auf dem Desktop mit dem Namen „erpressung.txt“. Als Nächstes erstellen Sie eine Datei mit der Bezeichnung „ransom.yar“, die Sie im Ordner „/tmp“ speichern. Diese enthält Yara-Regeln:

```
rule ransom_html
{
    strings:
        $s1 = "erpresser@domain.xyz"
        $s2 = "1DeaDBEefXulub-MiRF4311tN1xE1n"
    condition:
        filesize < 16KB and all of them
}
```

Der Aufbau ist simpel: Die Datei enthält eine einzige Regel, die aus zwei Such-Strings und einer Bedingung besteht. Einzelne Yara-Dateien können aber auch mehrere Regeln enthalten. Arbeitet der OTS die gezeigte Datei ab, schaut sich der Scanner ausschließlich Dateien an, die kleiner als 16 Kilobyte

**Das OTS-Skript  
mountet Lauf-  
werke und zeigt  
nach Abschluss  
des Scans, ob  
Schadsoftware  
gefunden wurde.**



sind. Alarm schlägt der OTS, wenn eine Datei beide Strings (\$s1 und \$s2) enthält.

Starten Sie den OTS aus dem Terminal von Desinfec't und lassen den Scanner auf das Home-Verzeichnis los. Dabei schaut der Scanner auch auf den Desktop und die Köder-Datei:

```
yara -r /tmp/ransom.yar /home/desinfect
```

Da das Home-Verzeichnis eine überschaubare Zahl kleiner Dateien enthält, ist die Suche schnell abgeschlossen. In der Ergebnisdatei zeigt der OTS einen Fund pro Zeile an: In der ersten Zeile findet sich die Regel ransom\_html, die angeschlagen hat. Hinter einem Leerzeichen steht der Name der verdächtigen Datei, hier ist es „/home/desinfect/Desktop/erpressung.txt“.

Hat das funktioniert, kopieren Sie Ihre ransom.yar-Datei in den Ordner „/opt/desinfect/signatures/desinfect-signatures/yara“. Das ist der Sammelort für Yara-Regeln. Öffnen Sie die dort befindliche Datei „everything.yar“ im Editor (sudo scite). Um eigene Regeln zu aktivieren, fügen Sie den Namen der Datei ein, die sie enthält:

```
include "eicar.yar"  
include "emotet.yar"  
include "ransom.yar"
```

Hier können Sie durch Auskommentieren (*/\*...\*/*) die langsame MD5-Regel emotet.yar deaktivieren. Wenn Sie den OTS anschließend über das Icon auf dem Desktop starten, sucht der Scanner mit Ihren Regeln. Glückwunsch, Sie haben Ihren ersten eigenen Virenscanner gebaut. In [1] finden Sie Tipps für weitere Matching-Methoden, um manuell Yara-Patterns zu erstellen.

## Automatisch Regeln erzeugen

In manchen Fällen gelingt es, einem Trojaner auf einem infizierten Rechner bei seinem zerstörerischen Tun zuzusehen. Dann kann man den Prozess und schließlich den Namen der Binärdatei, welche gerade munter Dateien verschlüsselt, identifizieren und isolieren. Doch was soll man mit dieser Datei tun?

Ein Profi-Forensiker sucht im Assembler-Code nach Routinen für die Verschlüsselung und ermittelt Sequenzen von Maschinenbefehlen, die mutmaßlich in verwandter Malware zu finden sind. Zusätzlich hält er in den Programmdateien nach Textsequenzen Ausschau, beispielsweise dem Aufruf externer Pro-

gramme, Ausgaben oder eindeutige Funktionsnamen. Da dieser Vorgang viel Zeit und noch mehr Expertise erfordert, liegt eine Automatisierung nahe.

Hier hilft das Tool „yarGen“ von Florian Roth. Dabei handelt es sich um eine Sammlung von Python-Skripten. Diese analysieren Malware-Samples automatisch und generieren daraus Yara-Regeln, die der OTS direkt nutzen kann.

Matching-Kriterien sind entweder Strings und Textsequenzen oder zusätzlich Sequenzen von Maschinenbefehlen. Um Fehlalarme zu vermeiden, nutzt yarGen eine Datenbank von „Goodware“-Code-sequenzen, die in den erzeugten Regelsätzen als Erkennungsmerkmale vermieden werden. Für eine bessere Performance beschränkt das Tool die zu durchsuchende Dateigröße.

Da yarGen ein Python-Skript ist, können Sie es universell unter Desinfec't, Linux, Windows oder macOS nutzen. Achtung: yarGen kopiert seine initiale Datenbank von 900 Megabyte beim Aufruf des Skriptes komplett ins RAM. Damit alles geschmeidig läuft, sollten Sie an einem Computer mit mindestens 8 GByte RAM und einer SSD arbeiten. Mit einem langsamem Desinfec't-USB-Stick vergehen mitunter volle drei Minuten zum Laden der Datenbank. Deshalb: Experimentieren Sie für die Regelerstellung mit yarGen auf einem Desktop-PC oder Notebook und kopieren Sie die fertigen Regelsätze dann auf einen Desinfec't-Stick. Dafür nutzen Sie temporär die unter Windows sichtbare Datenpartition. Anschließend verschieben Sie die yar-Datei im laufenden Desinfec't an den Sammelort für yar-Dateien.

## YarGen installieren

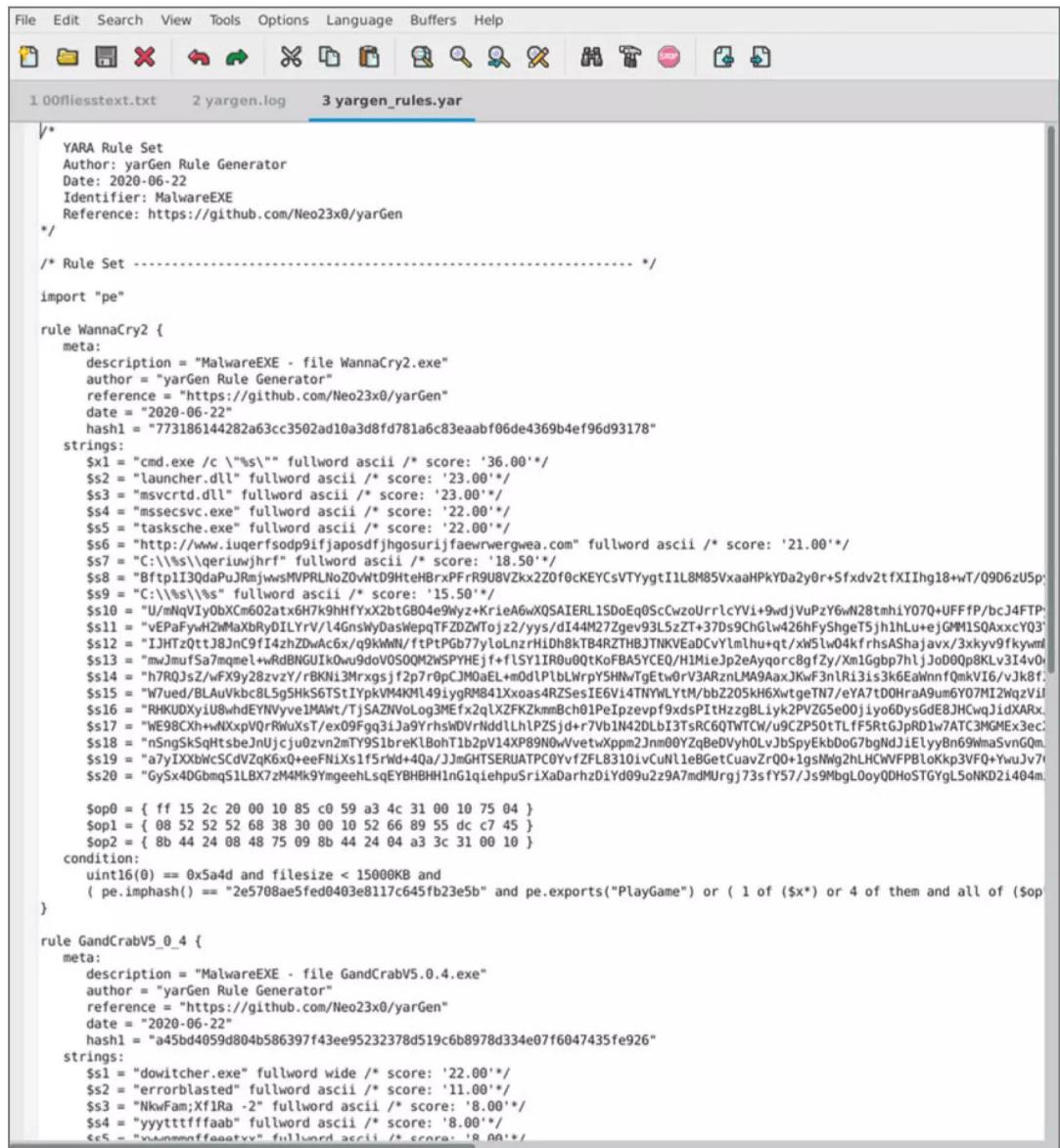
Seit Version 0.23 nutzt YarGen Python3, das in jeder modernen Linux-Distribution Standard sein darf. Unter Windows ist ohnehin zunächst ein Python-Interpreter einzurichten. Anschließend steht in jedem Fall die Installation einiger Python-Module an, die yarGen nutzt. Wir verwenden hierfür Pythons eigenen Paketmanager „pip“. Unter Unix-Systemen funktioniert die Installation so:

```
sudo pip install pefile scandir lxml  
naiveBayesClassifier
```

Unter Windows tippen Sie folgenden Befehl in die PowerShell oder die Eingabeaufforderung:

```
python.exe -m pip install pefile  
scandir lxml naiveBayesClassifier
```

**Das kostenlose Tool  
yarGen analysiert  
mögliche Trojaner-  
Dateien und erzeugt  
daraus automatisch  
mit OTS kompatible  
Yara-Regeln.**



```

File Edit Search View Tools Options Language Buffers Help
1 00filesstext.txt 2 yargen.log 3 yargen_rules.yar

/*
YARA Rule Set
Author: yarGen Rule Generator
Date: 2020-06-22
Identifier: MalwareEXE
Reference: https://github.com/Neo23x0/yarGen
*/

/* Rule Set -----
import "pe"

rule WannaCry2 {
meta:
  description = "MalwareEXE - file WannaCry2.exe"
  author = "yarGen Rule Generator"
  reference = "https://github.com/Neo23x0/yarGen"
  date = "2020-06-22"
  hash1 = "773186144282a63cc3502ad10a3d8fd781a6c83eaabf06de4369b4ef96d93178"
strings:
  $x1 = "cmd.exe /c \"%s\" fullword ascii /* score: '36.00'*/
  $s2 = "launcher.dll" fullword ascii /* score: '23.00'*/
  $s3 = "msvcrtd.dll" fullword ascii /* score: '23.00'*/
  $s4 = "mssecsvc.exe" fullword ascii /* score: '22.00'*/
  $s5 = "task sche.exe" fullword ascii /* score: '22.00'*/
  $s6 = "http://www.iugerfsod9ifaposdf9hgsosurfaewrvergwea.com" fullword ascii /* score: '21.00'*/
  $s7 = "C:\\%s\\queriuwhrf" fullword ascii /* score: '18.50'*/
  $s8 = "Bftp1130daPuJRmjwsMVPRLN0Z0vHtD9HtehBrxPfr9U8V2kx220f0cKEYCsVTYygtI1L8M85VxaahPKyDa2y0r+Sfxdv2tfXIIhg18+wT/Q9D6zU5p
  $s9 = "C:\\%s\\%" fullword ascii /* score: '15.50'*/
  $s10 = "U/mNqV1y0bxKm602atxGHTk9HHTYx2btGB04e9Wyz+KrlEa6wvQSAIER1S0doEg05CcWzoUrr1cYV1+9wdjVuPzY6wN28tmh1Y070+UFFfP/bcJ4FTP
  $s11 = "vEPaFywH2wMaXbRy01LYrV/14GnshyDasIeqqTFDZwT0jz2/yys/d144M27Zgev93L5zZT+370s9Ch6lw426HfyShqeT5jh1hLu+ejGM15QaXXXcYQ3
  $s12 = "IJHTzQttJ8JnC9f14zhZdwAc6x/q9kWm/ftPtPGb77yloLnrH1Dh8TB4RZTHBjTNKVEaDcvYlmhhu+qf/xh5lw04kfrhsAShajavx/3xky9fkywnt
  $s13 = "mwJmuTsa7mqmel+wRdBNGuIK0kwu9doV0S0Qm2WSPYHEJ+f+lSY11R0u00tkoF85YCE0/H1M1e2p3eAyqorC8gFzY/Xm1Ggbp7h1jJo00Qp8KL3V40v
  $s14 = "h7R0J5z/wFx9y28zvzY/rBKN13Mrxgsjz2p7r0pM0aEL+m0d1p1blWrp5HN7WgtEw0rV3ArznlM9AaxJxkF3n1R131s3k6Eawnnfomkv16/vJk8f
  $s15 = "W7ued/BLAUkvbC8L5g5Hk56TS1tYpkVM4KML491ygRM841Xoas4RZSeIE6V14TNVYLTM/bb2Z05Kh6XwgtetN7/eY7tD0Hra9u9mGy07M12wq2V1
  $s16 = "RHKUDXy1U8whdEYNyve1M4Wt/TjSAZnVbLoq3MExfzqLXFKZkmmBch01PeIpzevpf9xdsP1thHzg8Liyk2PVZG5e00jiy60ysGdE8JHcwnJidXArx
  $s17 = "WE98Xh+Dxvp0rRwXp1T/ex0Fgq19YrhswDrrNdlhPZ5jd+r7vb1n420Lb13tsRC607WtC/u9CZP501TLFF5RtGjP01w7ATC3MGME3ec
  $s18 = "nSngkS5qhtsbeJnUjcu0zvn2mY951brekLBohT1bzpV14XP89N0wVvetwXppm2Jnm0Y0ZqB0eVyh0LvbSpypkDg7bgDj1eLy8n69wmaSvnG0n
  $s19 = "a7yIXXbWcSCdVZqK6x0+eeFN1x15fwrD+40a/JmGHTSERUATPC0Y1fZFLB3101vcuH1le8GetCuavZr0+1gsNg2hLHCWVFPBlokKp3VFO+YwUjv7
  $s20 = "GySx4DgbmqS1LBX7z4M4Mk9YmgcehLsqYbH8H1nLqiehpsRxiuDarhZD1yD09u229A7mdMurgj73sfY57/Js9MbgLoyQDHoSTGYgL5oNKO21404m

$op0 = { ff 15 2c 20 00 85 c0 59 a3 4c 31 00 10 75 04 }
$op1 = { 08 52 52 52 68 38 30 00 10 52 66 89 55 d c7 45 }
$op2 = { 8b 44 24 08 48 75 09 8b 44 24 04 a3 3c 31 00 10 }

condition:
  uint16(0) == 0x5a4d and filesize < 15000KB and
  ( pe.imphash() == "2e5708ae5fed0403e8117c645fb23e5b" and pe.exports("PlayGame") or ( 1 of ($x*) or 4 of them and all of ($op
}

rule GandCrabV5_0_4 {
meta:
  description = "MalwareEXE - file GandCrabV5.0.4.exe"
  author = "yarGen Rule Generator"
  reference = "https://github.com/Neo23x0/yarGen"
  date = "2020-06-22"
  hash1 = "a45bd4059d804b586397f43ee95232378d519c6b8978d334e07f6047435fe926"
strings:
  $s1 = "dowitcher.exe" fullword wide /* score: '22.00'*/
  $s2 = "errorblasted" fullword ascii /* score: '11.00'*/
  $s3 = "NkwFam;Xf1Ra -2" fullword ascii /* score: '8.00'*/
  $s4 = "yyttttfffaab" fullword ascii /* score: '8.00'*/
  $s5 = "vununnnnnfffaaaatvv" fullword ascii /* score: '8.00'*/
}

```

Anschließend laden Sie yarGen von GitHub (Download via ct.de/wces) über „Download ZIP“ herunter. Nach dem Entpacken öffnen Sie je nach System das Terminal, die PowerShell oder die Eingabeaufforderung im Ordner mit den yarGen-Daten. Dort wechseln Sie in den neuen Ordner „yarGen“. Hier müssen Sie zunächst die Datenbank mit den „Goodstrings“ herunterladen und aufbauen. In den folgenden Bei-

spielen kann der Python-Interpreter python, python3 oder python.exe sein:

python3 yarGen.py --update

Der Vorgang dauert circa zehn Minuten. Leider kann es im Zusammenspiel von Python und Windows Zertifikatsprobleme geben. In so einem Fall sollten



```

d616c8e9c84012
2018-07-19 08:24:33 Hashes: 160ce2e72ab5682d2e82ea129db72022, 9771700a6063d40e45
0aa5acc11ab8d1
2018-07-02 04:51:41 Hashes: 9230cacbc92a9229aaaf0c7bcbe709d4b, 9fd6185f389a55ebfc
1616849aa89e35
2018-05-30 07:01:33 Hashes: 82d2d07bdcce9b0ae19f61c2d9d1f9d1, c0alcc305307d6064b
75cba876ec938e
2018-05-25 19:55:41 Hashes: ecaf811373c49185f9d0c4beb4d0c09, ea7615aa7c237dd497
ed6074a465804b
2018-05-17 18:38:25 Hashes: 35832c2b7c2287d532ee0e0abclae5f1, 35eedf96ce4560bc01
fa7108763ffffe9
2018-05-16 12:45:02 Hashes: 96985dff8be2912fe2d02752b5d4a073, 8e957840019b780a52
f87c4176aafc43
2018-05-15 06:39:03 Hashes: f7fcad3b21710555994776ef2d5cfb2d, 15b89d1ebcc8ea0146
8c9ad8ebd61ff4
2018-05-02 06:27:42 Hashes: 038445ddb96e1bbe89072adecac1123e, 7e300630af2923f0ca
5c79811993e982
2018-04-27 05:13:26 Hashes: 8aabeb90eb19326d6332ba6a44b909ea, 88c726bfff5eb834000
ef0cc313d00f09
2018-04-16 13:27:22 Hashes: 90eee0624377283c4051f75e3752494, 5f3969937055daddfb
338dbcda32c518
'/opt/yara-patterns/emotet.tmp' -> '/opt/yara-patterns/emotet.yar'
==> Starte Open Threat Scan

```

**Die von uns verwendeten Regeln von ReversingLabs suchen in erster Linie eindeutige Bytesequenzen, die über mehrere Samples eines Malware-Typs ermittelt wurden.**

Sie ein Ubuntu im Windows-Subsystem für Linux (WSL) laufen lassen und Yargen damit nutzen.

## Malware analysieren

Erstellen Sie einen Ordner namens „Malware“, in den Sie die beispielsweise auf einem infizierten Windows-PC entdeckten Samples kopieren. Falls Sie keinen akut von Emotet betroffenen Computer zur Hand haben und zunächst den Umgang mit yarGen üben wollen, durchsuchen Sie Ihren Spam-Ordner nach vermeintlichen Bewerbungen. In solchen Mails finden Sie häufig Word-Dokumente mit Makros, die Trojaner herunterladen. Weitere Malware-Samples zum Üben finden Sie auf einer GitHub-Website (siehe ct.de/wces).

Aber Vorsicht! Es handelt sich um echte Trojaner! Öffnen Sie die Dateien keinesfalls! Wenn Sie mit solchen Dateien unter Windows hantieren, müssen Sie Ihren VirensScanner temporär deaktivieren. Ansonsten funkts der Scanner bei der Analyse durch yarGen immer dazwischen.

Kopieren sie die Schadsoftware-Beispiele in Ihren Malware-Ordner. Rufen Sie das yarGen-Skript für diesen Ordner auf:

```
python3 yarGen.py -m Malware
```

Nun analysiert yarGen die Dateien im Ordner. Das Tool geht per se davon aus, dass die ihm vorgesetzte Datei böse ist. Während der Analyse leitet yarGen Strings aus der Datei ab, die die Schadfunktionen abbilden. Diese Kriterien sind die Basis für die Untersuchung verdächtiger Dateien. Nach der Analyse spuckt das Tool im aktuellen Arbeitsverzeichnis die Datei „yarGen\_rules.yar“ aus. Standardmäßig bildet yarGen einen Schädling in 20 Strings ab und fügt als Matching-Kriterium hinzu, dass eine bestimmte Zahl der Strings gefunden werden muss. Darauf beruft sich der OTS beim Scan als Erkennungskriterium.

An der Zahl der Matches können Sie drehen, um das Verhältnis zwischen Fehlalarmen und echten Funden zu beeinflussen. Für die Beurteilung der Qualität einzelner Strings verwendet yarGen ein Scoring-System: Niedriges Scoring bedeutet, dass Treffer nicht eindeutig sind. Mit einem zusätzlichen Parameter schreibt yarGen diese Scores mit in die erzeugte Regeldatei. Diese Scores geben dem OTS keine Anweisungen, sondern dienen Ihnen nur als Information beim Bearbeiten der Regel:

```
python3 yarGen.py --score -m Malware
```

Da Scores unterhalb von sechs oder fünf Fehlalarmen begünstigen, ist es sinnvoll, einen Mindestwert festzulegen:

```
python3 yarGen.py --score -z 6 -m Malware
```

Handelt es sich bei den Samples nicht um Office- oder PDF-Dateien, sondern um Programmdateien, kann es sinnvoll sein, Folgen von Maschinenbefehlen ins Matching aufzunehmen. Das bietet sich beispielsweise an, wenn nicht genügend Strings mit hohen Scores gefunden werden. Legen Sie hierfür einen zweiten Ordner „MalwareEXE“ an, um für verschiedene Typen von Malware verschiedene yarGen-Einstellungen wählen zu können. Das gelingt mit der Eingabe folgender Befehle:

```
python3 yarGen.py --opcodes -z 6 -m MalwareEXE
```

## Literatur

[1] Olivia von Westernhagen, **Gut aufgestellt gegen Schadcode**, Malware-Signaturen mit Yara einfach selbst erstellen, c't 20/2018, S. 15

Download yarGen,  
Befehle yarGen,  
Malware-Samples  
[ct.de/wces](http://ct.de/wces)

Auf der GitHub-Seite des yarGen-Projektes (siehe [ct.de/wces](https://ct.de/wces)) finden sich noch weitere Befehle nebst Erklärungen, die Sie zum Erstellen von Yara-Regeln nutzen können.

Geben Sie der mit yarGen erzeugten Datei „yarGen\_rules.yar“ jeweils einen aussagekräftigen Namen und integrieren Sie diese über include-Zeilen in der everything.yar-Datei auf Ihrem Desinfec't-Stick. Starten Sie danach den OTS, nutzt der Scanner die von Ihnen erstellten Regeln.

## Fazit

Yara ist ein mächtiges Tool, das sich jeder anschauen sollte, der auf mit Schadsoftware befallene Rechner reagieren muss. YarGen macht Yara auch für Nutzer praktikabel, die keinen Binärkode lesen können und auch keine Zeit für Analysen haben. Mit der Integration ist Desinfec't die ideale Plattform für schnelle Reaktionen mit eigens erstellten Yara-Regeln.

(des) 



## Unified Security

eine einheitliche IT-Sicherheitsplattform  
für eine neu vernetzte Welt:



Firewall / VPN



Sicheres  
WLAN



Endpoint  
Security



Multifaktor  
Authentifizierung

Wir beraten Sie gerne!

[www.boc.de](http://www.boc.de)

(0800) 9440440

Besuchen Sie  
uns auf der  
**it-sa 2023**  
HALLE 7  
STAND 7-327

WatchGuard Cloud  
Visibility & Management

 CERTIFIED TRAINING PARTNER

 PLATINUM PARTNER



# Desinfec't via Btrfs erweitern

Bisher konnte man Desinfec't nur bis zu einem gewissen Grad modifizieren, etwa um kleine Tools nachzuinstallieren. Dank dem hinzugekommenen Btrfs-Dateisystem können Sie Desinfec't nun beispielsweise zu einem vollständigen Notfallarbeitsplatz inklusive Office-Anwendungen und aktuellen Treibern ausbauen.

Von **Mattias Schlenker**

Wer das Live-System Desinfec't auf einem USB-Stick mit Tools aus den Ubuntu-Paketquellen erweitern will, musste bis jetzt immer einen Umweg gehen. Der Grund dafür ist, dass Desinfec't selbst auf einem USB-Stick nicht veränderbar ist und nach jedem Neustart wieder den Originalzustand herstellt. Damit man Tools dennoch dauerhaft installieren kann, müssen die einzelnen Debian-Pakete auf der beschreibbaren Signatur-Partition liegen. Die Desinfec't-Startskripte installieren diese dann bei jedem Systemstart neu. Dieser Ansatz klappt in der Regel mit kompakten Tools problemlos – darauf setzen wir auch bei der Installation von Desinfec't-Updates. Doch will man komplexere Anwendungen oder Treiber nachinstallieren, klappt das auf diesem Weg nicht.

Seit Desinfec't 2017 haben wir diese Probleme gelöst und führen ein gänzlich anderes Konzept ein: Mit ein paar Vorbereitungen installieren Sie Anwendungen, Tools und Treiber ab sofort dauerhaft direkt im System.

Dazu setzt Desinfec't auf das Dateisystem Btrfs, mit dem man Veränderungen in sogenannten Snapshots abspeichern kann. Diese liegen dann in Form von Subvolumes schichtweise über dem nach wie vor unveränderten Original (siehe Grafik unten „So funktioniert ein Btrfs-Stick“). Schlägt eine Modifikation fehl, wechseln Sie einfach zu einem funktionierenden Subvolume zurück.

## Btrfs-Stick erstellen

Standardmäßig setzt ein Desinfec't-Stick allerdings noch nicht auf Btrfs: Sie müssen ihn erst mit einer

speziellen Option erstellen. Damit Desinfec't mit Btrfs vernünftig läuft, ist ein flinker USB-Stick mit mindestens 32 GByte erforderlich. Dieser Platz ist nötig, da Desinfec't durch das Anlegen neuer Subvolumes mittels der Snapshot-Funktion wächst.

Am einfachsten erstellen Sie einen Btrfs-Stick aus einem laufenden Desinfec't: Dort klicken Sie auf dem Desktop das Icon „Desinfec't-Stick bauen“ an. Im Anschluss setzen Sie lediglich ein Häkchen bei „Btrfs als Standard nutzen“.

In den folgenden Beispielen erweitern Sie Desinfec't, erzeugen Snapshots und starten das angepasste System aus einem neuen Subvolume.

## Los gehts!

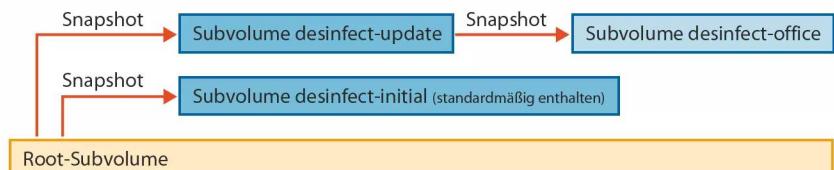
Als erstes Praxisbeispiel aktualisieren Sie Desinfec't und machen das Update persistent. Dafür installieren Sie es zuerst nach der alten Methode, sodass es aus dem RAM läuft. Dann verweben Sie das Update mit einem neu angelegten Subvolume, damit es dauerhaft in Desinfec't integriert ist.

Prüfen Sie zuerst, ob das Desinfec't-Update bereits installiert ist – das sollte in der Regel automatisch geschehen. Steht im Statusfenster oben rechts auf dem Desktop zum Beispiel „Desinfec't 2023/24 p1“, hat es geklappt. Steht dort nur „Desinfec't 2023/24“, müssen Sie den Update-Vorgang manuell anstoßen. Dafür öffnen Sie zunächst das Terminal, holen das Update aus unserem Repository und machen ein Upgrade von Desinfec't:

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

### So funktioniert ein Btrfs-Stick

Im Root-Subvolume befindet sich das Original-Desinfec't. Via Snapshot erstellt man ein neues Subvolume, das zunächst ein Klon des vorhergehenden ist. Neue Daten werden erst kopiert, wenn sich etwas ändert – etwa wenn Tools dazukommen. Nach einer Erweiterung startet man Desinfec't aus dem neuen Subvolume. Da das darunterliegende Subvolume unangetastet bleibt, kann man bei Problemen zurückwechseln.



Als Nächstes müssen Sie Schreibrechte für den Speicherort der Subvolumes unter /cdrom vergeben und die LZO-Komprimierung für neu geschriebene Dateien aktivieren – das spart Speicherplatz auf dem Stick. Dieser Schritt ist essenziell und für jede Subvolume-Operation in /cdrom nötig. Wenn im Folgenden mal etwas nicht klappt, prüfen Sie, ob Sie den Befehl eingegeben haben. Darüber hinaus sind für nahezu jede Aktion Root-Rechte (sudo) unabdingbar – wenn es hängt, überprüfen Sie auch das:

```
sudo mount -o remount,rw,compress=lzo /cdrom
```

Nun erstellen Sie via Snapshot ein neues Subvolume namens „desinfect-update“:

```
sudo btrfs subvolume snapshot ↵
↳ /cdrom /cdrom/desinfect-update
```

Unter cdrom/desinfect-update/casper/filesystem.dir findet sich darauffolgend eine deckungsgleiche Kopie vom Original-Desinfect'. Damit Sie die Updates dort installieren können, hängen Sie den Ordner mit den deb-Archiven in das neu angelegte Subvolume:

```
sudo mount -o bind/var/cache/apt/archives
↳ /cdrom/desinfect-update/casper/
↳ filesystem.dir/var/cache/apt/archives
```

Nun wechseln Sie mit chroot (change root) in das neu angelegte Subvolume desinfect-update und installieren vorhandene Desinfect'-Update-Pakete dort:

```
sudo chroot /cdrom/desinfect-update/
↳ .casper/filesystem.dir
dpkg -i /var/cache/apt/archives/
↳ .desinfect-meta*.deb
```

Mit exit verlassen Sie die chroot-Umgebung.

Nun sind Sie fast fertig und müssen nur noch das neue Subvolume mit aktualisiertem Desinfect' als Standard-Subvolume setzen, damit das Sicherheits-Tool künftig daraus startet. Dafür brauchen Sie zunächst die ID des neuen Subvolumes, die sich via

```
sudo btrfs subvolume list /cdrom
```

ablesen lässt. Dort steht ganz oben immer das Subvolume desinfect-initial mit der ID 261. Neu angelegte Subvolumes zählt Btrfs jeweils immer um eins hoch. In diesem Beispiel trägt das Subvolume mit dem Desinfect'-Update die ID 262. Um dieses als



**Um einen Desinfect'-Stick mit Btrfs zu erstellen, müssen Sie die Option „Btrfs als Standard nutzen“ explizit anwählen.**

neues Standard-Subvolume festzulegen, geben Sie Folgendes ein:

```
sudo btrfs subvolume set-default 262 /cdrom
```

Nun müssen Sie noch das Update-Paket „desinfect-meta“ aus /opt/desinfect/signatures/deb löschen, damit sich Btrfs und die alte Installationsmethode nicht in die Quere kommen. Das können Sie über den Filemanager machen (sudo thunar). Nach dem Löschen booten Sie Desinfect' neu und fortan sollte das Sicherheits-Tool immer in der aktualisierten Version starten. Aus welchem Subvolume Desinfect' bootet, sehen Sie nach der Eingabe von

```
cat /proc/mounts | grep /cdrom
```

unter „subvolid=ID“.

## Ubuntu-Pakete installieren

Um zusätzliche Anwendungen, Aktualisierungen und Treiber aus den Ubuntu-Paketquellen nachzuinstallieren, ist etwas mehr Vorbereitung als beim Desinfect'-Update nötig. Das liegt daran, dass Sie hier Anwendungen direkt in ein Subvolume downloaden

und installieren und dafür eine vollständige chroot-Umgebung benötigen. In den folgenden Beispielen rüsten Sie Desinfec't in einem Rutsch mit LibreOffice aus und installieren einen Treiber für einen WLAN-Stick. Die folgende Herangehensweise ist exemplarisch für die Nachinstallation und Aktualisierung von Anwendungen und Treibern und muss bei jeder neuen Subvolume-Session von Anfang an durchgeführt werden. Damit sich die folgende Vorbereitung lohnt, empfiehlt es sich, wie in diesem Beispiel gleich mehrere Sachen hinzuzufügen.

Ausgangspunkt ist der Start aus dem Subvolume `desinfect-update`. Daraus erzeugen Sie mit der Snapshot-Funktion ein neues Subvolume namens „`desinfect-office`“ – dieses ist ein direkter Abkömmling von `desinfect-update`. Damit Ubuntu-Pakete mittels `apt-get` im neuen Subvolume landen, sind weitere Mounts nötig:

```
sudo su
mount -o remount,rw,compress=lzo /cdrom
btrfs subvolume snapshot /cdrom ↵
↳/cdrom/desinfect-office
$CHROOT=/cdrom/desinfect-office ↵
↳casper/filesystem.dir
mount --bind /dev $CHROOT/dev
mount --bind /proc $CHROOT/proc
```

```
mount --bind /sys $CHROOT/sys
mount -t devpts devpts $CHROOT/dev/pts
mount -t tmpfs tmpfs $CHROOT/tmp
```

Nun machen Sie Nameserver in der chroot-Umgebung bekannt. Die DNS-Einstellung gelingt via

```
mount --bind /run/resolvconf ↵
↳resolv.conf $CHROOT/run/ ↵
↳resolvconf/resolv.conf
```

Jetzt erzeugen Sie noch ein Dummy-Shell-Skript, damit bei der Nachinstallation keine Dienste dazwischenfunkeln. Das gelingt mit einem Editor wie Scite:

```
scite $CHROOT/usr/sbin/policy-rc.d
```

Das Skript umfasst nur zwei Zeilen:

```
#!/bin/sh
exit 101
```

Nun speichern Sie die Änderungen, schließen die Datei und machen sie ausführbar:

```
chmod 0755 $CHROOT/usr/sbin/policy-rc.d
```

Ein kleines Skript kümmert sich um die Mounts, die DNS-Einstellung und das Dummy-Shell-Skript. Sie installieren und starten es wie folgt:

```
sudo su
apt-get update
apt-get install desinfect-btrfs-tools
$CHROOT=/cdrom/desinfect-office/ ↵
↳casper/filesystem.dir
chrootbindmounts mount $CHROOT
```

Damit Desinfec't auf die Ubuntu-Paketquellen zugreifen kann, müssen Sie diese via

```
scite $CHROOT/etc/apt/sources.list
```

aktivieren. Dafür entfernen Sie in der Liste die Doppelkreuze vor den Einträgen „Main“, „Updates“ und „Security“ und sperren den Zugriff auf das Desinfec't-Repository mittels eines Doppelkreuzes, sonst könnte es im Folgenden zu Konflikten kommen. Speichern und schließen Sie die Datei. Anschließend wechseln Sie per chroot in das Verzeichnis des Subvolumes und aktualisieren die Paketlisten:

## Desinfec't, Btrfs und Windows 10

Bei Desinfec't 2023/24 haben wir uns dazu entschieden, Btrfs nicht als Standard zu nehmen – Sie müssen diese Option explizit auswählen. Im aktuellen Desinfec't hat das Dateisystem noch experimentellen Status. Der Grund dafür ist, dass wir die Integration von Btrfs zurückstellen mussten, weil Windows 10 seit Version 1703 zusätzliche Partitionen auf USB-Sticks erkennt. Steckt man einen Btrfs-Stick in den Rechner, bietet das Betriebssystem jetzt eine Formattierung aller für Windows unlesbaren Partitionen an. Das ist nicht nur lästig, sondern auch gefährlich: Dadurch kann man sich einen Btrfs-Stick zerschießen. Da wir bislang keinen Weg gefunden haben, Windows das abzugewöhnen, mussten wir zu einem Hack greifen: Das reguläre Desinfec't 2023/24 arbeitet mit versteckten Partitionen. Bisher konnten wir dieses Schema allerdings nicht für einen Btrfs-Stick anwenden – aber wir arbeiten daran.

```
chroot $CHROOT
apt-get update
```

Nun können Sie mittels

```
apt-get install libreoffice libreoffice-l10n-de
```

das LibreOffice-Paket installieren. An dieser Stelle müssen Sie nichts aus /opt/desinfect/signatures/deb löschen, da Anwendungen aus den Ubuntu-Paketquellen im Gegensatz zu Desinfect's-Updates nicht standardmäßig auf der Signatur-Partition landen.

Zusätzlich fügen Sie mit dieser Installationsmethode neue Firmware und Treiber hinzu. Das folgende Beispiel stattet den in Desinfect's enthaltenen Treiber für WLAN-Sticks auf Broadcom-Basis für eine erweiterte Kompatibilität mit einer proprietären Firmware aus. Alternativ können Sie das Ganze natürlich auch mit passenden Treibern für WLAN-Sticks mit Chips von anderen Herstellern durchspielen:

```
apt-get install b43-fwcutter ↵
firmware-b43-installer
```

Erkennt Desinfect nach dem Neustart Ihren Broadcom-Stick immer noch nicht, können Sie mit den folgenden Befehlen einen proprietären Broadcom-Treiber installieren. Erstellen Sie dafür zuerst eine Datei via

```
scite /etc/modprobe.d/blacklist-b43.conf
```

und fügen Sie folgende Zeilen ein:

```
b43
b43legacy
```

Anschließend installieren Sie wie folgt den proprietären Broadcom-Treiber:

```
sudo apt-get install broadcom-sta-source ↵
broadcom-sta-common broadcom-sta-dkms
```

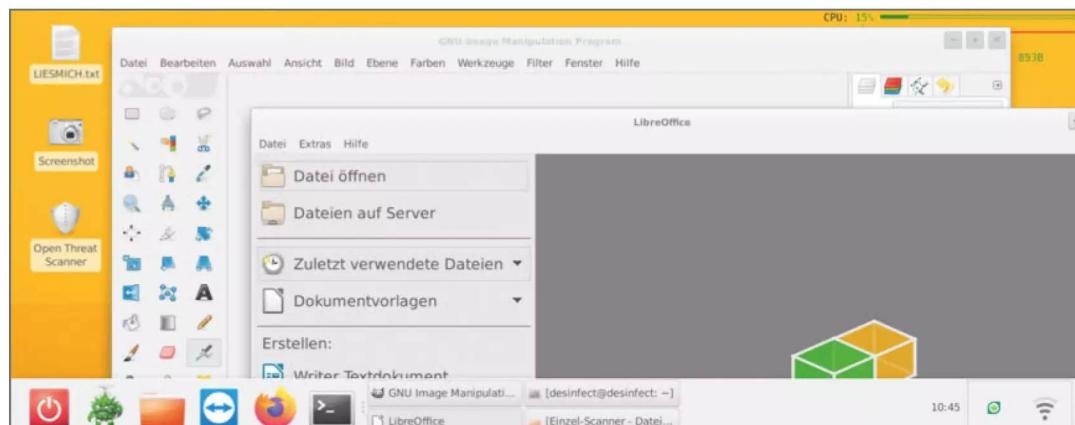
Wenn Sie eine Subvolume-Session aus den Ubuntu-Repositorys beenden und nichts mehr installieren möchten, leiten Sie dies mit dem Befehl apt-get clean ein. Nun verlassen Sie mit exit die chroot-Umgebung. Dann löschen Sie die eingangs angelegte Datei mit

```
sudo rm $CHROOT/usr/sbin/policy-rc.d
```

Alternativ erledigen Sie dies und das Lösen der Mounts nach der Eingabe von apt-get clean mit dem Skript aus unseren Btrfs-Tools.

```
chrootbindmounts umount $CHROOT
```

Als Nächstes kommentieren Sie noch die Ubuntu-Repositories via



**Dank Btrfs können Sie Desinfect um größere Anwendungen erweitern und sich so ein Notfallsystem mit kompletter Office-Umgebung bauen.**

## Mountpoint /cdrom fehlt?

Mit neueren Kerneln kann es vorkommen, dass der Mountpoint /cdrom nicht mehr sichtbar ist, nachdem Ubuntus Bootscripte das Rootverzeichnis gewechselt haben. Für diesen Fall haben wir im Bootmenü den Eintrag „Desinfec't im DVD Modus booten“ hinzugefügt. Er startet nicht vom /cdrom/casper/filesystem.dir, sondern einem auf der Btrfs-Partition abgelegten ISO-Image. Die weitere Vorgehensweise ist dann identisch zur bisherigen.

```
scite $CHROOT/etc/apt/sources.list
```

aus und reaktivieren die Desinfec't-Paketquelle. Abschließend legen Sie `desinfect-office` als Standard fest:

```
sudo btrfs subvolume set-default 263 /cdrom
```

Jetzt starten Sie Desinfec't neu – erst dann stehen die eben installierten Anwendungen und Treiber zur Verfügung.

## Andere Kernel nutzen

Ist die verwendete Hardware zu neu oder zu alt, helfen oft ältere oder neuere Kernel. Bei betagten PCs kann es sinnvoll sein, einen der alten Long-Term-Support-Kernel zu nutzen. Ist die Hardware brandneu, müssen aktuelle Mainline-Kernel her – bei Redaktionsschluss war dies 6.4 Ubuntu stellt diese Kernel ohne Patches und ohne Tests bereit. Seit Ubuntu 18.04 kann man die Mainline-Kernel auch mit Live-Systemen verwenden. Der einfachste Weg ist, zunächst auf [www.kernel.org](http://www.kernel.org) nachzusehen, welche Mainline-Kernel aktuell sind. Dann kann man direkt im Mainline-Archiv (siehe [ct.de/wpjv](http://ct.de/wpjv)) den gewünschten Kernel herunterladen – brandneue Kernel sind in der Regel bereits einige Stunden nach der Veröffentlichung erhältlich.

Installieren Sie `linux-modules*generic*.deb` und `linux-image*generic*.deb` des gewünschten Kernels simpel mit den Befehlen `dpkg -i dateiname`. Nach der Installation kopieren Sie den Kernel „`vmlinuz**`“ und das Initramfs „`initrd**`“ des neuen Kernels auf

die Boot-Partition (Label „`desinfSYS`“) in den Ordner „`casper`“. Entweder überschreiben Sie den vorhandenen Kernel oder Sie benennen ihn entsprechend um, beispielsweise „`initrd.6x` und `vmlinuz.6x`“. Beachten Sie, dass Syslinux Dateinamen in der 8.3-Konvention erfordert. Editieren Sie dann die beiden Bootdateien „`boot/grub/grub.cfg`“ und „`isolinux/os.cfg`“, wo Sie einfach den ersten vorhandenen Eintrag kopieren und mit angepassten Dateinamen versehen, damit Desinfec't den neu installierten Kernel nutzt.

## Zurücksetzen

Wenn beim Anpassen etwas schiefgelaufen ist, können Sie mit wenigen Schritten zum Root-Subvolume wechseln, um Desinfec't in den Originalzustand zurückzuversetzen:

```
sudo mount -o remount,rw,compress=lzo /cdrom
sudo btrfs subvolume set-default 5 /cdrom
```

Falls Desinfec't nach einer Modifikation nicht mehr startet, müssen Sie den Umweg über die DVD, einen Desinfec't-Stick oder eine andere Linux-Distribution gehen. Läuft das System, greifen Sie daraus auf den am Computer angeschlossenen defekten Btrfs-Stick zu, in unserem Fall ist das `sdd5`, und führen folgende Befehle aus:

```
mkdir /tmp/btrfs
sudo umount /dev/sdd5
```

Nun aktivieren Sie auf dem Stick das Root-Subvolume:

```
sudo mount -o rw /dev/sdd5 /tmp/btrfs
sudo btrfs subvolume set-default 5 /tmp/btrfs
sudo umount /tmp/btrfs
```

Anschließend sollte Desinfec't wieder laufen und im Originalzustand starten.

## Basteln auf eigene Gefahr

Dank Btrfs und unseren Anleitungen können Sie Desinfec't quasi grenzenlos erweitern. Geht dabei etwas kaputt, wechseln Sie problemlos zu einem funktionierenden Subvolume zurück. Im offiziellen Desinfec't-Forum (siehe [ct.de/wpjv](http://ct.de/wpjv)) tauschen sich außerdem Tüftler aus. Also keine Angst und viel Spaß beim Basteln!

(des) 



# Hilfe bei Windows-Problemen

Wenn Windows brachliegt, kann unser Linux-basiertes Notfallsystem helfen – egal, ob nun gerade kein anderes Werkzeug zur Hand ist oder Sie sich auf der Unix-Kommandozeile wohler fühlen. Dieser Artikel lotet die Möglichkeiten aus.

Von **Peter Siering**

**B**ei Schädlingsverdacht ist es immer eine gute Idee, ein neutrales Werkzeug von einem Wechseldatenträger zu starten und das vermeintlich verseuchte System zu untersuchen. Nur das liefert unabhängige Ergebnisse. Unser Desinfec't ist genau dafür gemacht: Sie können es aber ebenso gut dafür verwenden, eine aus anderen Ursachen vergurkte Windows-Installation zu reparieren oder ihr nur auf den Zahn zu fühlen, etwa sonst nicht zugängliche Dateien zu inspizieren.

Im Grundlagen-Artikel „Desinfec't bestmöglich nutzen“ ab Seite 10 steht, wie Sie Desinfec't auf einen USB-Stick bannen und benutzen. Das Folgende baut darauf auf und geht davon aus, dass Sie einen solchen Stick erfolgreich an einem Windows-PC starten konnten. Um überhaupt auf ein auf dem PC installiertes Windows und seine Laufwerke zunächst lesend zugreifen zu können, sollten Sie auf dem Desinfec't-Desktop „Win-Drives einhängen“ doppelt anklicken. Anschließend können Sie sich

im Dateimanager (Desinfec'ts Explorer) gefahrlos umsehen, den Sie über das Ordnersymbol in der Taskleiste erreichen. Die Windows-Laufwerke finden Sie in der Seitenleiste des Dateimangers unter „Andere Orte“. Sie tauchen dort namentlich auf, oft aber mit kryptischer Bezeichnung. Achtung: Wenn Sie direkt eine solche Bezeichnung anklicken, hängt Desinfec't das Laufwerk beschreibbar ein.

Wenn Sie sich im Dateibaum eines Windows-Systemlaufwerks umsehen, fällt auf, dass die Ordner englische Namen in Desinfec't tragen; der Windows-Explorer zeigt normalerweise deutsche Bezeichnungen. Anders als unter Windows ist auch: Sie können sich frei in allen Verzeichnissen bewegen. Desinfec't schert sich nicht um die in Windows gesetzten Zugriffsrechte, beachtet also die ACLs nicht. Sollten Sie bisher geglaubt haben, dass Zugriffsrechte für Dateien neugierigen Zeitgenossen den Zugriff verwehren, werden Sie hier eines Beseren belehrt.

## Windows-Daten finden

Somit ist es mit Desinfec't einfach möglich, Dateien von einem Windows-PC herunterzukratzen, eben auch dann, wenn Sie sich nicht einmal mit einem Konto daran anmelden können. Die Dateien der Nutzer finden Sie üblicherweise unterhalb des Ordners „Users“. Dort speichert Windows wirklich alles, was ein Konto betrifft, auch den benutzerspezifischen Teil der Registry, später mehr dazu.

Der Dateimanager kennt die üblichen Operationen wie Kopieren und Einfügen. Sie können Tastenkürzel (Strg+C und Strg+V) nutzen oder das Menü dazu bemühen. Beachten Sie: So wenig, wie sich Desinfec't überhaupt um die ACLs kümmert, kopiert es sie auch. Die einzige Möglichkeit, unter Linux Dateien auf einem NTFS-Laufwerk inklusive der ACLs auf ein anderes zu kopieren, besteht im Anfertigen einer 1:1-Kopie (etwa mit ntfsclone oder dem nachinstallierbaren Clonezilla).

Sollten Sie Ihre Windows-Partition nicht finden, etwa weil mehrere kleinteilig partitionierte Festplatten im System stecken, hilft die Laufwerksübersicht „Gnome Disks“ im Expertentools-Ordner auf dem Desinfec't-Desktop. Dort können Sie gezielt

einzelne Partitionen einhängen, also erreichbar machen. Doch Vorsicht: Wenn Sie diesen Weg gehen, dann bindet Desinfec't diese nicht nur les-, sondern beschreibbar ein. Unsere Empfehlung ist, das nur in begründeten Ausnahmefällen zu tun.

Die Linux-Funktionen für Zugriffe auf NTFS benutzen eine eigene Implementierung des Dateisystems - die birgt immer die Gefahr, dass beim Schreiben Daten in Mitleidenschaft gezogen werden. Deswegen geht Desinfec't auch konservativ vor und benennt als schädlich erkannte Dateien nur um, anstatt sie zu verschieben oder zu löschen. Wann immer möglich sollten Sie ebenso vorgehen. Wenn Sie schreiben lassen, tun Sie das idealerweise nur mit einem Backup oder Image in der Hinterhand.

Es gibt Dateien, an die Desinfec't nicht herankommt: Einzelne verschlüsselte NTFS-Dateien (EFS) erreicht es nicht ohne vorherigen Export von Schlüsseln, da die an Windows-Benutzerkonten geknüpft sind. Kein Problem stellen hingegen Laufwerke dar, die mit Bitlocker geschützt sind, also mit der Laufwerksverschlüsselung von Windows. Ein solches Laufwerk lässt sich auf der Kommandozeile mit wenigen Befehlen aufsperrern. Wie das geht, steht im Artikel „Desinfec't bestmöglich nutzen“ ab Seite 10.

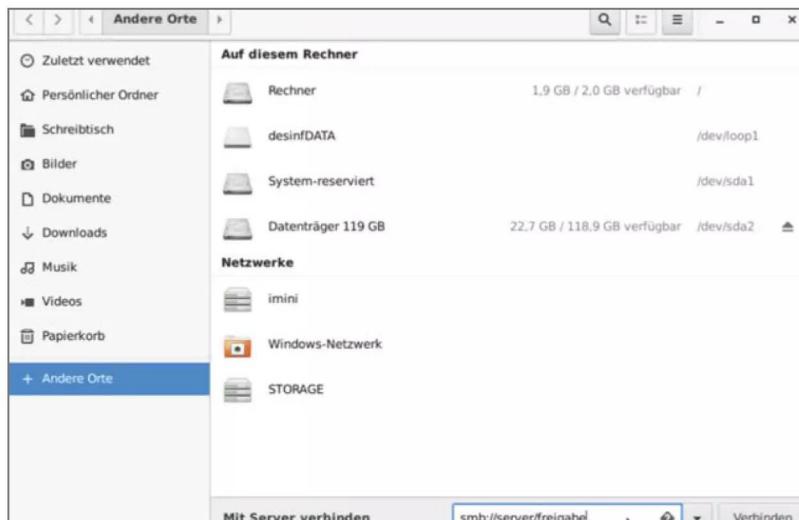
Eine Anmerkung noch zu Windows-Installationen oder Datenplatten, die auf einem Software- beziehungsweise BIOS-RAID gründen: Das hinter dem Symbol auf dem Desinfec't-Desktop „Win-Drives einhängen“ hinterlegte Skript schafft es nicht, die Windows-Partition zu finden und einzuhängen. Benutzen Sie in einem solchen Fall besser die Laufwerksübersicht.

Halten Sie dort Ausschau nach RAID-Laufwerken, meiden Sie andere, die Teil eines RAID-Verbundes sind. Die Warnung ist präventiv: Bei uns weigerte sich Desinfec't, RAID-Mitglieder anzurühren, aber wir sind nicht sicher, ob das in jedem Fall so ist. Da die Laufwerksübersicht stets beschreibbar einhängt, können Sie im Nachgang Desinfec't die Schreiboption entziehen - den Namen des Einhängpunktes müssen Sie anpassen:

```
sudo mount -o ro,remount ↳
↳ /media/desinfect/thinkssd
```

## Passwort vergessen

Ein typisches Problem auf Windows-PCs ist, dass sie von einem auf den anderen Tag den Benutzer nicht mehr hineinlassen. Das kann diverse Ursachen haben: Der Benutzer hat sein Kennwort vergessen



**Im Desinfec't-Dateimanager führt „+Andere Orte“ zu den Windows-Partitionen und auch ins Netzwerk. Vorsicht beim Klicken auf Windows-Laufwerke: Sie werden gleich beschreibbar eingehängt. Besser bemühen Sie „Win-Drives einhängen“ auf dem Desktop. So besteht keine Gefahr, dass Sie versehentlich Daten auf die Laufwerke schreiben.**

oder das Benutzerprofil ist so stark beschädigt, dass Windows die Anmeldung verweigert oder ein Ersatzprofil verwendet. Ein Seiteneffekt kann sein, dass keine Anmeldung mehr mit administrativen Rechten möglich ist.

Das vergessene Kennwort kann man mit verschiedenen Mitteln angehen: Desinfect' enthält das Programm `chntpw`, das direkt die Benutzerdatenbank in der Registry einer Windows-Installation (SAM genannt) bearbeiten kann. Dabei verhält es sich wie mit den Schreibzugriffen auf NTFS: Man sollte das nur in Notfallsituationen und nicht ohne Backup seiner Daten tun. Und ganz wichtig: Finger weg von Passwortänderungen, wenn Dateien EFS-verschlüsselt sind, die kriegt man danach nie wieder im Klartext zu sehen.

Damit der Zugriff auf die Passwortdatenbank gelingt, müssen Sie die Windows-Partition so einhängen, dass sie beschreibbar ist. Das muss in jedem Fall sein, selbst wenn Sie zunächst nur schauen, aber nichts ändern wollen. Klicken Sie auf dem Desktop „Win-Drives aushängen“ (wenn Sie die zuvor einge-hängt haben). Öffnen Sie dann in den Expertentools die Laufwerksübersicht „Gnome Disks“, wählen Sie die Windows-Partition aus und klicken Sie den „Play“-Knopf (das nach rechts gerichtete Dreieck) an. Desinfect' hängt die Partition dann beschreibbar ein.

Achtung: Die anderen Bedienelemente in der Laufwerksübersicht bergen hohes Gefahrenpotenzial. Sie können hier mit wenigen Klicks auch Ihre Windows-Partition löschen – die Programme fragen nach, aber wir wollten das hier nicht unangesprochen lassen. Generell sollten Sie sich stets bewusst sein, dass Sie Ihre Windows-Partition als beschreibbares Medium eingehängt haben – minimieren Sie den Zeitraum. Lassen Sie die Laufwerksübersicht offen und betätigen Sie den Stop-Knopf zum Aushängen so bald wie möglich.

Zunächst aber entnehmen Sie dem Programm den Eihängpunkt für Ihre Windows-Installation. Öffnen Sie ein Terminalfenster und wechseln Sie mit

```
cd /media/desinfect/WinPladde/➥
➥Windows/System32/config
```

in das Verzeichnis, in dem die Registry Ihrer Windows-Installation liegt. `WinPladde` müssen Sie durch den Volume-Namen Ihrer Systempartition ersetzen.

Jetzt können Sie mit `chntpw -l SAM` eine Liste der bekannten Konten ausgeben lassen. Mit `chntpw -u <user> SAM` rufen Sie ein Konto zur Bearbeitung auf. Das Programm zeigt dann ein detailliertes Menü mit

diversen Details zum jeweiligen Benutzerkonto. So können Sie zum Beispiel das standardmäßig nicht benutzbare Administrator-Konto aktivieren oder das Kennwort eines Benutzers löschen, sodass er sich ohne anmelden kann (Vorsicht: EFS-Dateien des Benutzers sind danach nicht mehr lesbar).

Wir empfehlen vor solchen Eingriffen, die betroffene Datei „SAM“ als Versicherung zunächst auf den USB-Stick zu kopieren (mit `sudo/opt/desinfect/signatures`). Geht der Eingriff schief, können Sie die gegebenenfalls wiederherstellen – sollte Ihnen das Schreiben von NTFS mit Linux missfallen, können Sie dafür einen anderen Windows-PC einspannen, an den Sie die Festplatte stöpseln, auf der Ihre Windows-Installation residiert. Das Rücksetzen des Passwortes klappt leider nur für lokale Konten, nicht aber für ein Microsoft-Konto.

## Profil futsch

Mit `chntpw` können Sie auf der Kommandozeile auch die Registry durchstöbern und ändern. Das Prinzip ist das gleiche wie beim Ändern von Kennwörtern. Als Parameter übergeben Sie den Namen der Registry-Datei (die Sie idealerweise vorher kopieren): `chntpw -e SYSTEM` würde beispielsweise den Systemteil der Registrierung Ihrer Windows-Installation zugänglich machen. Wenn Sie lieber mit der Maus unterwegs sind: Starten Sie im Terminalfenster `fred`.

Die Datei, die die benutzerspezifischen Teile der Registry enthält, finden Sie als versteckte Datei `NTUSER.DAT` in den Profilverzeichnissen der Konten unter „Users“ (in einem solchen Verzeichnis mit `chntpw -e NTUSER.DAT` zu öffnen). Solch eine Datei nimmt durchaus mal Schaden.

Dass das der Fall ist, merkt der Nutzer beim Anmelden: Windows sagt plötzlich, es bereite etwas vor (wie bei der allerersten Anmeldung). Manchmal weist es direkt darauf hin, dass eine Anmeldung beim Konto nicht möglich sei. Oft erscheint der Hinweis „Sie wurden mit einem temporären Profil angemeldet“ gekoppelt mit der Drohung, dass angelegte Dateien verloren gehen. Ältere Windows-Versionen legen von sich aus neue Profilverzeichnisse in `Users` an, Windows 10 gerät gern in eine Anmeldeschleife.

Desinfect' kann vornehmlich bei der Diagnose helfen: Eine Null Byte große `NTUSER.DAT` ist eindeutig. Eine `NTUSER.DAT`, die nicht mal der Registry-Editor von `chntpw` zu öffnen vermag, kann man wohl auch abschreiben. Wenn das betroffene Konto das einzige auf dem PC war, das über Administrationsrechte verfügt hat, können Sie mit dem zuvor ge-

Weitere Hinweise  
[ct.de/w6nc](http://ct.de/w6nc)

nannten Kniff, das bei der Installation angelegte, aber deaktivierte Konto namens „Administrator“ anknipsen und sich auf diese Weise Zutritt zum PC verschaffen.

Das weitere Vorgehen hängt von Ihrem Experimentierwillen ab: Man könnte die NTUSER.DAT eines frisch angelegten neuen Nutzers in das Verzeichnis des beschädigten Profils kopieren und eine Anmeldung versuchen. Besser ist es in der Regel, gezielt die alten Daten in ein neues Profil zu kopieren, also sich einzeln die Verzeichnisse vorzunehmen wie Desktop, Documents, Links und woran sonst das Glück des betroffenen Nutzers hängt.

Wenn Windows partout auf das falsche Profil-Verzeichnis zugreift (manchmal legt es die auch einfach unter einem abgewandelten Namen neu an), hilft womöglich ein Eingriff in der Registry. Unter HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList (Datei SOFTWARE im o.g. Verzeichnis) existiert für jeden dem System bekannten Benutzer ein Schlüssel, der als Namen den SID des Nutzers hat (eine Windows-interne ID für Benutzer).

Klicken Sie sich einfach durch, bis Sie den richtigen Nutzer identifiziert haben und passen Sie gegebenenfalls den Wert in ProfileImagePath an.

**Mit WoeUSB kommt man auch ohne lauffähiges Windows nur mit Desinfec't im Gepäck zu einem USB-Installationsstick für eine frische Windows-Installation – ISO, Installationsmedium oder Internet-Zugang vorausgesetzt.**



## Desinfec't erweitern

Die soweit erwähnten Werkzeuge stecken bereits in Desinfec't. Eine Stick-Installation können Sie in Eigenregie erweitern, indem Sie Pakete über die Debian-/Ubuntu-Paketverwaltung installieren. Das geht mit wenigen Handgriffen – öffnen Sie ein Terminalfenster und bearbeiten Sie in einem Editor die Paketquellen

```
sudo nano /etc/apt/sources.list
```

Entfernen Sie das Kommentarzeichen (#) vor den ersten drei Zeilen und speichern Sie mit Strg+O. Mit STRG+X beenden Sie den Editor Nano.

Mit sudo apt-get update müssen Sie zuerst die Paketverzeichnisse einlesen lassen und können dann mit sudo apt-get install <Paketname> jedes erreichbare Paket installieren. Das Ganze hat Grenzen: Nicht alles aus der Ubuntu-Welt lässt sich installieren (das aktuelle Desinfec't baut auf Jammy Jellyfish auf). Das Live-System zwackt Teile des Hauptspeichers ab und der ist nun mal begrenzt. Dasselbe gilt für den Stick: Auch hier ist der Platz endlich.

Die Änderung der Paketquellen und die anschließend hinzugefügten Pakete gehen verloren, wenn Sie Desinfec't herunterfahren. Die Paketeinrichtung können Sie erhalten, indem Sie nach der Installation die Pakete in einem Terminalfenster auf den Stick kopieren:

```
sudo cp /var/cache/apt/archives/* ↴  
↳/opt/desinfect/signatures/deb
```

Ein nützliches Programm ist WoeUSB. Es bringt Desinfec't bei, bootfähige Installationssticks für Windows anzufertigen. Wenn Sie die Pakete nicht wie zuvor beschrieben dauerhaft auf Ihren Stick packen, ist der Spuk aber nach einem Reboot vorbei, denn Desinfec't verwirft hinzugefügte Paketquellen bei jedem Neustart. Zunächst aber fügen Sie das Hilfsprogramm hinzu:

```
sudo apt-get update  
sudo apt-get install woeusb
```

Anschließend können Sie mit woeusbgui die Bedienoberfläche des Helfers starten. Er erwartet eine ISO-Datei oder DVD als Quelle (Source) und einen USB-Stick als Kopierziel (Target). Achten Sie darauf, dass Sie nicht versehentlich den Desinfec't-Stick erwischen – davor schützt das Programm nicht. (ps) ↗



# Fotos und Dateien retten

Hat man versehentlich den falschen USB-Stick formatiert oder die USB-Festplatte vom Schreibtisch gefegt, wird einem oft erst bewusst, welch wichtige Daten darauf gespeichert waren. Mit Desinfec't haben Sie ein gutes Werkzeug, um zumindest einen Teil Ihrer Daten zu retten.

Von **Mirko Dölle**

Ein kurzer Moment der Unachtsamkeit genügt, um Hochzeitsfotos, Buchführungsunterlagen oder die E-Mails der letzten Jahre ins Nirvana zu befördern, weil man den falschen USB-Stick oder die falsche SD-Karte formatiert oder überschreibt. Auch wenn heutige USB-Sticks und SSDs robuster als frühere externe Festplatten sind, Hardware-Defekte treten weiterhin auf: Bei billigen Sticks versagen die Flash-Speicher, beim Runterfallen reißen Lötpads ab oder die Controller werden Opfer statischer Elektrizität - das Spektrum ist breit.

Zeigen sich die ersten Anzeichen von Datenverlust, fehlen Dateien oder ganze Verzeichnisse oder Sie

können auf einzelne Dateien oder ganze Laufwerke nicht mehr zugreifen, sollten Sie zunächst den Stand Ihres letzten Backups prüfen: Von wann ist es und wie viel Arbeit müssten Sie investieren, um die Daten aus dem Backup auf den aktuellen Stand zu bringen?

Der Hintergrund ist, dass Datenrettung viel Zeit erfordert und der Ausgang ungewiss ist. Im Zweifel sind Sie besser beraten, mit dem Backup vom Vortag weiterzuarbeiten und die heutige Arbeitszeit verloren zu geben, als sich stundenlang mit der Datenrettung zu versuchen und am Ende nichts zu gewinnen.

Auch die Möglichkeit, einen professionellen Datenretter zu beauftragen, sollte man nicht vergessen.

Die Erstdiagnose, die einen verbindlichen Kostenvoranschlag für die spätere Datenrettung umfasst, kostet je nach Anbieter und Dringlichkeit zwischen 50 und 300 Euro.

Je nach Schaden (physisch oder logisch), Speicher-typ und -größe kostet die Datenrettung im Schnitt zwischen 60 und 1500 Euro. Das ist für die Rettung einer Schulhausaufgabe sicher zu viel, für die gerade aufgenommenen Hochzeitsfotos, um eine Steuer-erschätzung des Finanzamts zu verhindern oder um eine Abschlussarbeit termingerecht fertigzubekom-men aber wahrscheinlich gerechtfertigt. In diesen Fällen sollten Sie jedoch alle Selbstversuche unter-lassen, denn dadurch können die Daten schlimmsten-falls unwiederbringlich zerstört werden.

## Physisch, logisch?

Wie gut Ihre Aussichten sind, die Daten in Eigen-regie wiederherstellen zu können, hängt von der Art der Beschädigung ab. Hardware-Fehler lassen sich mit Hausmitteln fast nie reparieren. Hinzu kommt, dass sich mechanische Defekte auf Fest-platten und nicht mehr zugreifbare Zellen in Flash-Speichern schnell vermehren, wenn das Medium weiter in Betrieb bleibt.

Deshalb gilt es bei Hardware-Defekten, das Me-dium in einem Durchgang ein letztes Mal auszule-sen, bevor Sie es außer Betrieb nehmen. Das dabei erstellte Abbild dient Ihnen anschließend als Grund-lage für die Datenrettung.

Für diesen Zweck eignet sich Desinfec't beson-ders gut, da es die wichtigsten Tools zur Datenrettung bereits an Bord hat und die Dateisysteme von Win-dows, macOS und Linux unter-stützt. Alles, was Sie benötigen, ist die Desinfec't-DVD oder einen USB-Stick mit Desinfec't. Außerdem eine ausreichend große Datenhalde, die Ihre geretteten Daten auf-nimmt – ein großer USB-Stick oder eine externe Fest-platte sind hierfür gut geeignet. Wie Sie Desinfec't auf einem USB-Stick installieren und booten, haben wir im Artikel „Desinfec't bestmöglich nutzen“ ab Seite 10 bereits ausführlich beschrieben.

Ein erstes Indiz für einen mechanischen Defekt sind veränderte Laufgeräusche und Zugriffsgeräu-sche der Festplatte. SSDs und andere Flash-Speicher machen natürlich keine Geräusche, sodass Sie hier per Software nach Fehlern fahnden müssen (siehe Artikel „PCs mit Diagnose-Tools untersuchen“ ab Seite 46). Für die Diagnose der Hardware eignet sich vor allem die Self-Monitoring, Analysis and Report-ing Technology, kurz S.M.A.R.T oder auch Smart genannt.

Dabei überprüft sich das Laufwerk in regelmäßigen Abständen selbst und zeichnet außerdem beson-dere Vorkommnisse wie Lese- und Schreibfehler, aber auch zu hohe Laufwerkstemperaturen auf.

Um die Daten mit den Smartmon-Tools unter Linux abzurufen, müssen Sie zunächst den Lauf-werksnamen ermitteln. Dazu rufen Sie, bevor Sie das defekte Laufwerk anschließen, im Terminal den Befehl `lsblk` auf. Er listet alle aktuell verfügbaren physischen und virtuellen Laufwerke auf. Dann schließen Sie das defekte Laufwerk an und rufen erneut `lsblk` auf. Durch den Vergleich der beiden Aufrufe finden Sie zuverlässig den Namen Ihres Laufwerks heraus.

Etwas schwieriger ist es, wenn die defekte Fest-platte oder SSD noch im Rechner eingebaut ist. Dann müssen Sie die Einträge durchforsten und anhand der Größenangaben der Laufwerke herausfinden, welchen Namen Ihre interne Festplatte hat, etwa `/dev/sda` oder `/dev/sdb`. Doch Vorsicht, auch ein Des-infec't-USB-Stick bekommt einen Laufwerknamen zugeordnet, manchmal sogar `/dev/sda`.

Sofern die Partitionstabelle des defekten Lauf-werks noch lesbar war, zeigt `lsblk` neben dem Lauf-werksnamen, zum Beispiel `/dev/sdb`, auch noch die Namen der einzelnen Partitionen an, etwa `/dev/sdb1` oder `/dev/sdb2`. Auch hier können Sie anhand der Größenangabe abschätzen, welche Daten wohl darauf gespeichert sind. Um die Beispiele verständ-lich zu halten, verwenden wir nachfolgend `/dev/sdb` als Laufwerknamen. Sollte Ihr Laufwerk einen anderen Namen erhalten haben, müssen Sie das in den Beispielen entsprechend anpassen. Mit dem Befehl

```
sudo smartctl -a /dev/sdb
```

bekommen Sie die Selbsttestdaten des Laufwerks `/dev/sdb` angezeigt. Die zugegeben wenig übersicht-liche Liste hat numerische IDs am Anfang der Daten-zeilen, über die Sie die einzelnen Angaben leicht wiederfinden können.

Bei defekten Laufwerken finden Sie üblicher-weise eine hohe Raw Read Error Rate (ID 1), die (korrigierbare) Lese Fehler anzeigt. Da Festplatten und SSDs automatisch schlechte Sektoren gegen gute aus einem reservierten Bereich tauschen, sollten Sie außerdem ein Auge auf die IDs 5, 196 und 197 haben: Hier finden Sie heraus, wie viele schlechte Sektoren bereits ausgetauscht wurden (ID 5), wie oft das vorkam (ID 196) und wie viele schlechte Sek-toren noch nicht ausgetauscht werden konnten, weil

sie noch mit Daten belegt sind (ID 197) – der Austausch erfolgt immer dann, wenn ein schlechter Sektor überschrieben wird.

Während Sie bei rein logischen Laufwerksfehlern risikolos mit dem Befehl

```
sudo dd if=/dev/sdb of=disk.img
```

ein vollständiges Image des beschädigten Laufwerks im aktuellen Verzeichnis erstellen können, müssen Sie bei Hardware-Defekten abwägen, mit welcher Methode Sie das Image Ihrer Daten erstellen: Jeder Leseversuch eines beschädigten Bereichs kann dazu führen, dass noch mehr Daten unlesbar werden. Außerdem bricht dd beim ersten Lesefehler ab.

Ist das beschädigte Laufwerk größtenteils belegt, verwenden Sie am Besten ddrescue, um das Image zu erstellen:

```
ddrescue -A /dev/sdb disk.img
```

Während dd das Medium sequenziell, Sektor für Sektor, ausliest, springt ddrescue beim ersten Lesefehler großzügig über den beschädigten Sektor hinweg und versucht, sich vom hinteren Ende dem defekten Bereich zu nähern. Das verlangsamt durch die längeren Zugriffszeiten zwar den Kopiervorgang, vermeidet aber, dass sich das Programm an einem größeren defekten Bereich „festfrisst“ und stattdessen einen Bereich anspringt, wo es möglicherweise noch gute Daten gibt.

Müssen Sie die Daten einer weitgehend leeren Windows-Partition retten, können Sie zu ntfsclone greifen:

```
ntfsclone --rescue -o ntfs.img ↵
/dev/sdb1
```

## Auf Eis gelegt

Lesefehler bei Festplatten und Flash-Speichern treten häufig temperaturabhängig auf oder verschlimmern sich mit zunehmender Laufwerkstemperatur. So werden defekte MicroSD-Karten mitunter derart heiß, dass sie manchmal sogar das Gehäuse des Kartenlesers anschmelzen.

Kühlt man die Medien, lassen sich manchmal mehr Daten wiederherstellen als bei höheren

Temperaturen. Ein Tipp ist deshalb, widerspenstige Medien sprichwörtlich auf Eis zu legen und sie im Tiefkühler per USB-Adapter auszulesen, indem man das USB-Kabel durch die Dichtung nach außen zum Rechner führt. Zur besseren Wärmeableitung sollte man außerdem das Plastikgehäuse von USB-Sticks und -Kartenlesern entfernen.

Bei Festplatten ist es wichtig, Feuchtigkeitsschäden durch Tauwasser zu vermeiden. Deshalb müssen Festplatten zunächst auf Zimmertemperatur abgekühlt werden, bevor man sie für einige Stunden in den Kühlschrank legt und sie unter den Taupunkt herunterkühlt. Erst dann kommen sie in den Tiefkühler.



**Lesefehler nehmen oft mit steigender Temperatur des Mediums zu. Im Tiefkühler auf Eis gelegt lassen sich mitunter mehr Daten wiederherstellen, als wenn das Medium heiß läuft.**

Denken Sie daran, dass Sie bei `ntfsclone` als letzten Parameter die auszulesende Partition und nicht wie bei `dd` und `ddrescue` den Laufwerknamen angeben müssen.

Damit greift das Programm lediglich auf Bereiche der Festplatte zu, die tatsächlich noch mit Nutzdaten belegt sind. Damit werden Sektoren gar nicht erst angesteuert, die zu gelöschten Dateien oder zu sonstigen freien Bereichen der NTFS-Partition gehören – Sie erhalten also die reinen Nutzdaten Ihrer Windows-Partition. Damit ist ein mit `ntfsclone` erzeugtes Image allerdings auch ungeeignet, um verloren gegangene oder versehentlich gelöschte Dateien wiederherzustellen.

## Eingeht

Ein weiterer Vorteil der Dateisystem-Images von `ntfsclone`: Sie können sie ohne Umwege direkt einhängen. Dazu klicken Sie das Image im Dateimanager mit der rechten Maustaste an und wählen im Kontextmenü unter „Öffnen mit“ die Option „Einhängen von Laufwerksabbildern“. Im Terminal verwenden Sie folgenden Befehl:

```
sudo mount -o loop ntfs.img /mnt
```

Dann können Sie sich auf dem Image umsehen und etwa mit dem grafischen Dateimanager von Desinfect Ihre Dateien auf ein anderes Laufwerk kopieren, etwa einen zusätzlich angeschlossenen USB-Stick oder eine externe Festplatte.

Bei Laufwerks-Images, die Sie mit `dd` oder `ddrescue` erstellt haben, führt der Weg über die Kommandozeile. Der Grund dafür ist, dass diese Images nicht mit dem Dateisystem der ersten Partition beginnen, sondern mit dem Bootsektor und der Partitionstabelle des ursprünglichen Mediums. Die Dateisystemanfänge der einzelnen Partitionen sind also nach hinten verschoben. Das Kommandozeilenprogramm `kpartx` liest die Partitionstabelle eines solchen Images ein und erstellt virtuelle Laufwerke, die auf die Anfänge der jeweiligen Dateisysteme zeigen:

```
sudo kpartx -av disk.img
```

Wenn alles gut geht, verrichtet `kpartx` seine Arbeit wortlos. Die virtuellen Laufwerke finden Sie anschließend im Verzeichnis `/dev/mapper`, `loop0p1` ist die erste Partition, `loop0p2` die zweite und so weiter. Das Einbinden müssen Sie anschließend ebenfalls von Hand erledigen:

```
sudo mount /dev/mapper/loop0p1 /mnt
```

Anschließend können Sie das Verzeichnis `/mnt` nach zu rettenden Dateien durchstöbern. Wenn Sie fertig sind, dürfen Sie nicht vergessen, das virtuelle Laufwerk mittels

```
sudo umount /mnt
```

wieder auszuhängen und die virtuellen Laufwerke mit dem Befehl

```
sudo kpartx -d disk.img
```

zu entfernen, bevor Sie Desinfect herunterfahren oder den Datenträger mit dem Laufwerks-Image herausziehen.

## Aufgestöbert

Bei größeren Defekten oder logischen Fehlern, wo etwa ein Absturz des Treibers oder Rechners das Dateisystem beschädigt hat, lassen sich die Dateisysteme nicht mehr einbinden oder es fehlen ganze Verzeichnisse, weil die Verzeichnisstruktur fehlerhaft ist. Selbst wenn Sie das Medium versehentlich (schnell-)formatiert und somit sämtliche Dateiinformationen zerstört haben, gibt es noch Chancen, Daten retten zu können.

Die erste Wahl ist das interaktive Konsolenprogramm `photorec`. Es durchsucht das Image oder Laufwerk nach typischen Dateianfängen verschiedenster Dateiformate. Ursprünglich war es zum Wiederherstellen versehentlich formatierter Speicherkarten von Kameras gedacht, daher der Name. Inzwischen beherrscht Photorec jedoch Dutzende Dateiformate, von Bildern über Office-Dokumente bis hin zu Dateiarchiven.

Soll Photorec den Datenträger direkt auslesen, etwa weil nur ein logischer Fehler vorliegt, aber die Hardware in Ordnung ist, so müssen Sie Photorec beim Aufruf Root-Rechte verschaffen:

```
sudo photorec /dev/sdb1
```

Arbeiten Sie hingegen mit einem Image, genügen die Standardrechte des Desinfect-Benutzers. Dann sollten Sie den Dateinamen der Image-Datei aber auch gleich beim Start von Photorec als Parameter angeben, um sich nicht erst umständlich durch den gesamten Verzeichnisbaum von Desinfect hängeln zu müssen:

**Terminal**

Datei Bearbeiten Ansicht Suchen Terminal Hilfe

PhotoRec 7.2-WIP, Data Recovery Utility, March 2023  
 Christophe GRENIER <grenier@cgsecurity.org>  
<https://www.cgsecurity.org>

PhotoRec is free software, and  
 comes with ABSOLUTELY NO WARRANTY.

Select a media and choose 'Proceed' using arrow keys:

Disk /dev/sda - 250 GB / 232 GiB (R0) - Crucial\_CT250MX200SSD1  
 Disk /dev/sdb - 30 GB / 28 GiB (R0) - ASolid USB  
 Disk /dev/loop0 - 3134 MB / 2989 MiB (R0)  
**>Disk /dev/loop1 - 16 GB / 15 GiB (R0)**  
 Disk /dev/loop2 - 9661 MB / 9214 MiB (R0)  
 Disk /dev/loop3 - 16 GB / 15 GiB (R0)  
 Disk /dev/loop4 - 9661 MB / 9214 MiB (R0)  
 Disk /dev/loop5 - 3221 MB / 3072 MiB (R0)

**>[Proceed ] [ Quit ]**

Note:  
 Disk capacity must be correctly detected for a successful recovery.  
 If a disk listed above has an incorrect size, check HD jumper settings and BIOS  
 detection, and install the latest OS patches and disk drivers.

Ursprünglich entwickelt, um Fotos von versehentlich formatierten Kamera-Speicherkarten zu retten, beherrscht Photorec inzwischen unzählige Dateiformate.

photorec disk.img

Leider wurde die Photorec-Version mit grafischer Oberfläche noch nicht für das Framework Qt 6 portiert. Demzufolge finden Sie im Expertentools-Ordner von Desinfect nur die Version, die auf der Kommandozeile läuft. Doch die Bedienung ist gar nicht schwer.

Nach der Auswahl eines Laufwerks mit wiederherstellenden Daten können Sie im Grunde direkt über die Auswahl von „Search“ loslegen. Damit der Wiederherstellungsvorgang startet, müssen Sie nach der Auswahl von Search noch das Dateisystem des zu durchsuchenden Datenträgers festlegen. Unter „Options“ können Sie etwa den Betrieb auf Systemen mit wenig Arbeitsspeicher optimieren.

Unter „File Opt“ wählen Sie die zu suchenden Dateitypen aus.

Für die Dateiwiederherstellung benötigt Photorec viel Platz, weshalb Sie unbedingt einen zusätzlichen USB-Stick oder eine Festplatte als Datenhalde anschließen müssen. Wichtig ist, dass Sie den Zieldatenträger zunächst im Dateimanager einhängen, bevor Sie ihn in Photorec über die Verzeichnisstruktur als Ziel auswählen.

## Musterknabe

Das ursprünglich von der NSA entwickelte Konsolen-Tool foremost ist weniger komfortabel zu bedienen als Photorec. Dafür ist es aber flexibler, wenn es darum geht, eigene Datenfilter zu definieren. So

kann man effektiver Suchen. Ein gutes Beispiel sind dafür Visitenkarten im VCARD-Format, wie sie auch von verschiedenen Smartphone-Apps als Backup-Format verwendet werden.

Foremost unterstützt bereits out of the box nahezu alle Standard-Dateiformate, die auch Photorec beherrscht. Das VCARD-Format jedoch nicht, weshalb Sie zum Wiederherstellen Ihrer Kontaktdaten erst die Filterdatei vcf.conf anlegen und dort das Dateiformat beschreiben müssen. Hier ein Beispiel einer solchen Visitenkarte, die wiederhergestellt werden soll:

```
BEGIN:VCARD
VERSION:2.1
N:;Koch;;
TEL;CELL:01711111
END:VCARD
```

Am Anfang steht die Analyse, welche Elemente konstant und welche variabel sind. Visitenkarten beginnen stets mit der Zeile BEGIN:VCARD und enden mit END:VCARD, die eigentlichen Kontaktdaten liegen dazwischen. Damit Foremost nach diesen Zeichenketten sucht und sie als Datei mit der Endung .vcf speichert, tragen Sie folgende Zeile in der Filterdatei vcf.conf ein:

```
vcf y 10000 BEGIN:VCARD END:VCARD
```

Am Anfang steht die Dateiendung, das „y“ dahinter bedeutet, dass Foremost Groß-/Kleinschreibung beachten soll. Dahinter steht die maximale Größe einer Datei, hier 10000 Bytes – das sollte selbst umfangreiche Kontaktdaten abdecken.

Am Ende der Zeile stehen die Zeichenketten für den Anfang und – optional – für das Ende der Datei. Sofern es sich um Klartext handelt, können Sie diesen direkt eingeben, für Bytefolgen verwenden Sie am besten die hexadezimale Schreibweise, etwa \x20. Außerdem kennt Foremost den Platzhalter ?, der für ein beliebiges einzelnes Zeichen steht, und die Escape-Sequenz \s für das Leerzeichen. Die Escape-Sequenz ist notwendig, weil für Foremost alle sogenannten White Spaces Trennzeichen zwischen den einzelnen Parametern sind. Soll eine Zeichenkette also ein Leerzeichen enthalten, so müssen Sie es durch die Escape-Sequenz \s ersetzen.

Wählen Sie die maximale Größe mit Bedacht, denn Foremost wird, nachdem es die Anfangs-Zeichenkette gefunden hat, so lange Daten herauskopieren, bis es entweder die End-Zeichenkette gefunden oder

das Größenlimit erreicht hat. Bei einem zu hohen Limit entstehen schnell viele große Dateien mit Datenmüll, weil Foremost über den Anfang einer vor langer Zeit gelöschten Datei gestolpert ist. Damit Foremost ausschließlich nach dem gerade beschriebenen Dateiformat sucht, rufen Sie das Programm folgendermaßen auf:

```
foremost -v -c vcf.conf -i disk.img
```

Foremost ist standardmäßig äußerst schweigsam, mit dem Parameter -v erfahren Sie mehr darüber, was das Programm gerade tut. Hinter -c steht der Name der Filterdatei und hinter -i der Name des Laufwerkabbilds.

Bei manchen Dateiformaten gibt es keine Zeichenfolge, die das Ende definiert. Ein Beispiel dafür sind E-Mails, deren Anfang man zwar gut anhand des Mail-Headers erkennen kann, wo es aber kein Ende-Zeichen gibt. In diesen Fällen lassen Sie die End-Zeichenkette weg:

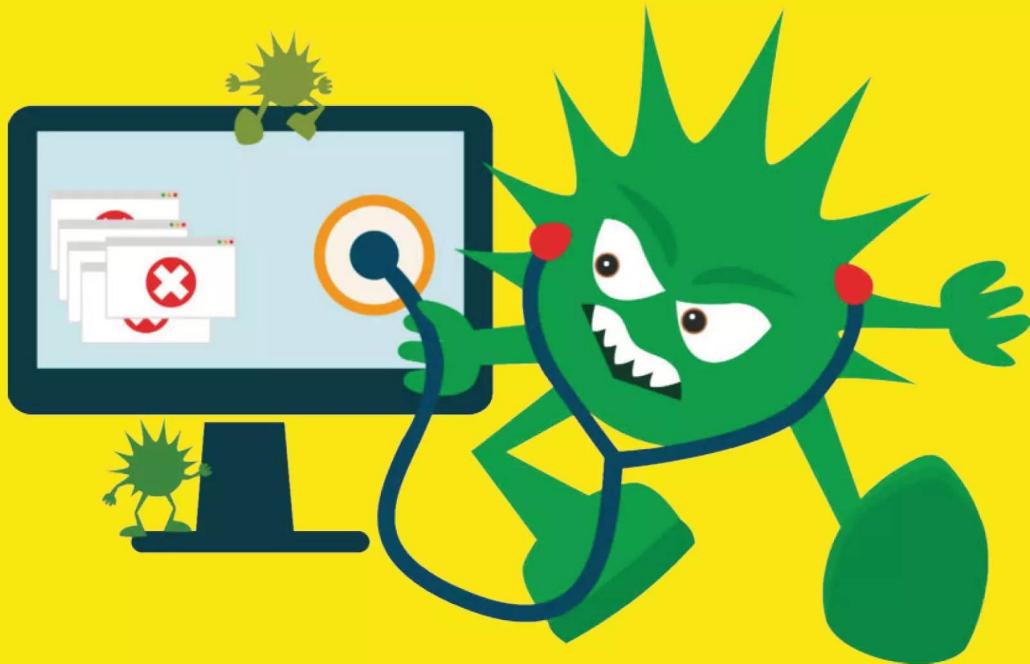
```
eml n 20000000 \x0aMessage-ID:\s
```

Das führt allerdings dazu, dass Foremost für jede gefundene E-Mail 20 MByte Daten sichert. Zwar gibt es keine Zeichenkette, die das Ende einer Nachricht kennzeichnet – doch wenn Foremost über den Beginn der nächsten Nachricht stolpert, darf es aufhören zu kopieren. Dafür definieren Sie die Beginn-Zeichenkette gleichzeitig als End-Zeichenkette und fügen den Parameter NEXT an:

```
eml n 20000000 \x0aMessage-ID:\s \x0aMessage-ID:\s NEXT
```

Damit weiß das Konsolen-Tool Foremost, dass die End-Zeichenkette bereits der Beginn der nächsten Datei ist und kopiert sie nicht mit, sondern verarbeitet sie – und das ist entscheidend – ein zweites Mal: Ohne den Parameter NEXT würde Foremost die weiteren Daten erst hinter der End-Zeichenkette untersuchen – und somit die unmittelbar folgende E-Mail nicht erkennen, da ja die Beginn-Zeichenkette bereits als End-Zeichenkette der vorherigen E-Mail verarbeitet wurde.

Auf diese Weise können Sie selbst ungewöhnliche oder proprietäre Dateiformate wiederherstellen. Besser als jede Datenrettung ist jedoch die Datensicherung: Mit täglichen Backups, so unkomfortabel sie sind, benötigen Sie die hier beschriebenen Klimmzüge erst gar nicht. (mid) **ct**



# PCs mit Diagnose-Tools untersuchen

Von DVD oder Stick ein Live-Linux wie Desinfec't starten und eines von vielen Diagnosetools aufrufen: Schon sprudeln Informationen aus eigenen oder fremden Systemen nur so heraus. So können Sie Hardware eindeutig identifizieren und dafür passende Treiber beschaffen. Auch Reparaturwerkzeuge sind dabei.

Von **Thorsten Leemhuis**

Möchtet Ihr Betriebssystem? Oder wollen Sie einen fremden, unbekannten Rechner untersuchen, der womöglich keines hat? Dann sind von USB-Stick oder DVD startende Linux-Distributionen wie Desinfec't ideal, denn sie haben Hunderte Diagnose-Tools bereits an Bord. Die Testumge-

bung ist sofort einsatzbereit, nachdem Sie Desinfec't von DVD oder einem damit bespielten USB-Stick booten. Wie das geht, haben wir bereits ausführlich beschrieben (siehe Artikel „Desinfec't bestmöglich nutzen“ auf Seite 10). Die erwähnten Diagnose-Tools sind übrigens auch Bestandteil anderer Linux-Distri-

butionen, daher funktionieren nahezu alle der im Folgenden genannten Kommandos auch mit den Live-Versionen von Ubuntu, Fedora & Co.

Alle der erwähnten Testwerkzeuge müssen Sie in einem Kommandozeilen-Terminal ausführen. Bei Desinfec't starten Sie ein solches über das überwiegend schwarze Icon mit der Eingabeaufforderung, das in der Bedienleiste am unteren Bildschirmrand rechts vom Firefox-Symbol liegt. Falls Ihnen die Schrift im daraufhin erscheinenden Terminal-Fenster zu klein sein sollte, können Sie deren Größe über Bearbeiten/Einstellungen beim Reiter „Aussehen“ erhöhen.

## Hardware auflisten

Einen groben Überblick über die im System verbaute Hardware samt Einteilung der erkannten Datenträger liefert das Kommandozeilenprogramm lshw:

```
sudo lshw -short
```

Durch das vorangestellte sudo läuft das Programm mit Systemverwalterrechten, die es braucht, um gewisse Informationen abzurufen.

Ignorieren Sie ruhig die numerischen Angaben, die lshw in der ersten Spalte zeigt: Sie spezifizieren lediglich eine Position in einer Baumstruktur, die die Hardware-Komponenten abbildet. Die wichtigsten Informationen finden Sie in der dritten und vierten Spalte, denn dort nennt das Programm den Typ einer Komponente samt einer Beschreibung. Ganz oben in der Aufstellung steht der Name des Systems, sofern der Hersteller ihn beim BIOS hinterlegt hat. Es folgen meist die Bezeichnung des Mainboards sowie einige Informationen zu Prozessor und Speichermodulen; anschließend listet das Programm die per PCIe, USB & Co. erreichbaren Chips auf, bevor die erkannten Datenträger samt der Partitionen, die es Volume nennt, an die Reihe kommen. Bei einigen der Komponenten zeigt lshw in der zweiten Spalte die Gerätebezeichnung, über die sich die Hardware unter Linux ansprechen lässt.

Deutlich mehr Infos erhalten Sie, wenn Sie die Option -short weglassen. Die Detailfülle erschlägt dann aber leicht; der Umbruch langer Zeilen erschwert den Überblick weiter. Übersichtlicher wird es auf diese Weise:

```
sudo lshw | gedit -
```

Die Ausgaben von lshw landen dabei in einem neuen Fenster des Texteditors Gedit, der einen besseren

Überblick verschafft. Auf Wunsch können Sie die Ausgaben dort auch gleich in eine Datei speichern oder einzelne Angaben über die Zwischenablage abgreifen, um etwa danach mit Firefox im Web zu suchen. Der Trick mit dem angehängten | gedit - funktioniert übrigens auch mit allen anderen Kommandozeilenbefehlen, die der Text im Folgenden nennt. Erfahrene Linuxer können die Ausgaben auch via | less an einen Textbetrachter übergeben, den man mit der Taste Q beendet.

lshw bietet aber noch eine weitere Ansicht, die mehr Überblick bietet: die HTML-Ausgabe. Diese können Sie in eine Datei umleiten und gleich mit Firefox anzeigen lassen:

```
sudo lshw -html >hwliste.htm  
firefox hwliste.htm
```

Auf einigen Testsystemen konnte Firefox die Datei allerdings nicht darstellen, weil lshw aufgrund von Warnmeldungen unsauberer HTML produzierte. Das Programm hat noch andere Schwächen. Für einen kurzen Überblick ist es gut genug, für einen genaueren Blick sollten Sie aber zu spezialisierten Werkzeugen greifen, die besser gepflegt und enger mit der Linux-Entwicklung verzahnt sind.

## BIOS und Speichermodule

Eines davon ist dmidecode, das vom BIOS generierte DMI-Tabellen mit der Selbstbeschreibung des Systems anzeigt. Der Befehl

```
sudo dmidecode
```

gibt im oberen Bereich beispielsweise Mainboard-Name und BIOS-Version aus. Das Programm zeigt dort auch Modellnamen und Seriennummer des Systems an, sofern der Hersteller diese Infos hinterlegt hat; gerade kleinere Unternehmen vergessen das oft. Ignorieren Sie die Angaben daher, wenn diese offensichtlich fehlerhaft sind. Die Details zu den verbauten Speichermodulen sind indes akkurat, denn die bezieht das BIOS direkt aus den DIMMs. Eine Suche nach dem Text „DIMM“ führt Sie schnell zu den Bereichen mit diesen Daten. Alternativ können Sie die Ausgabe via

```
sudo dmidecode -t memory
```

auf Informationen rund um den Arbeitsspeicher beschränken, darunter etwa die Speicherkapazität der

```
desinfect@desinfect: ~
```

desinfect@desinfect:~\$ sudo lshw -short

	Gerät	Klasse	Beschreibung
/0		system	K523r
/0/0		bus	K523r
/0/4		memory	64KiB BIOS
/0/4/5		processor	Intel(R) Core(TM) i3 CPU M 350 @ 2.27GHz
/0/4/6		memory	32KiB L1 Cache
/0/4/7		memory	256KiB L2 Cache
/0/4/1		memory	3MiB L3 Cache
/0/4/1/0		memory	4GiB Systemspeicher
/0/4/1/1		memory	4GiB SODIMM DDR3 Synchron 1067 MHz (0,9 ns)
/0/4/1/2		memory	DIMMProject-Id-Version: lshwReport-Msgid-Bugs-To: FULL NAME <EMAIL@ADDRESS>P0-Revision-Date: 201
/0/4/1/3		memory	DIMMProject-Id-Version: lshwReport-Msgid-Bugs-To: FULL NAME <EMAIL@ADDRESS>P0-Revision-Date: 201
/0/100		bridge	DIMMProject-Id-Version: lshwReport-Msgid-Bugs-To: FULL NAME <EMAIL@ADDRESS>P0-Revision-Date: 201
/0/100/1		bridge	Core Processor PCI Express x16 Root Port
/0/100/1/0		display	Card [Mobility Radeon HD 5430/5450/5470]
/0/100/1/0.1		multimedia	Cedar HDMI Audio [Radeon HD 5400/6300/7300 Series]
/0/100/16		communication	5 Series/3400 Series Chipset HECI Controller
/0/100/1a		bus	5 Series/3400 Series Chipset USB2 Enhanced Host Controller
/0/100/1a/1	usb1	bus	EHCI Host Controller
/0/100/1a/1/1		bus	Integrated Rate Matching Hub
/0/100/1a/1/2		multimedia	CNF7129
/0/100/1b		multimedia	5 Series/3400 Series Chipset High Definition Audio
/0/100/1c		bridge	5 Series/3400 Series Chipset PCI Express Root Port 1
/0/100/1c.1		bridge	5 Series/3400 Series Chipset PCI Express Root Port 2
/0/100/1c.1/0	wl51	network	AR9285 Wireless Network Adapter (PCI-Express)
/0/100/1c.2		bridge	5 Series/3400 Series Chipset PCI Express Root Port 3
/0/100/1c.5		bridge	5 Series/3400 Series Chipset PCI Express Root Port 6
/0/100/1c.5/0		generic	SD/MMC Host Controller
/0/100/1c.5/0.2		generic	Standard SD Host Controller
/0/100/1c.5/0.3		generic	MS Host Controller
/0/100/1c.5/0.4		generic	xD Host Controller
/0/100/1c.5/0.5	ens5f	network	JMC250 PCI Express Gigabit Ethernet Controller

```
desinfect@desinfect: ~
```

[Einzel-Scanner - Datei...]

```
desinfect@desinfect: ~
```

Desinfec't bringt viele Kommandozeilenwerkzeuge mit, die Details zur Hardware-Ausstattung liefern; einen guten Kurzüberblick bietet der Befehl Ishw.

verbauten Speichermodule und freie DIMM-Slots. Vor einer Speicheraufrüstung sollten Sie diese Angabe aber durch einen Blick in das Gehäuse verifizieren, denn es kommt vor, dass Hersteller bei günstigeren Board-Varianten weniger DIMM-Socket auflöten.

## Prozessor

dmidecode liefert auch Infos zum Prozessor. Die bessere Anlaufstelle dafür ist aber das Kommando `lscpu`. Das nennt 64-Bit-Tauglichkeit, Cache-Größen, Turbo-Takt und vieles andere. Detaillierte Angaben wie den Codenamen oder die maximale Leistungsaufnahme fehlen allerdings auch dort. Diese liefert das Web – für Intel-CPUs beispielsweise, wenn Sie auf [ark.intel.com](http://ark.intel.com) nach dem von `lscpu` angezeigten Modellnamen wie „i5-3350P“ suchen.

`lscpu` gibt auch aus, ob der Prozessor Virtualisierungsfunktionen wie AMD-V oder Intels VT-x beherrscht. Das heißt aber nicht, dass diese auch nutzbar sind, denn bei vielen PCs müssen die im BIOS-Setup freigeschaltet sein. Das ist der Fall, wenn ein `ls /dev/kvm` keine Fehlermeldung erzeugt.

Der Linux-Kernel liefert auch einige Hinweise, ob der Prozessor für Sicherheitslücken anfällig ist:

```
head /sys/devices/system/cpu/vulnerabilities/*
```

Bei Desinfec't zeigt das den Inhalt von Dateien zu vielen Sicherheitslücken, die seit Anfang 2018 bekannt wurden. Findet sich in den Dateien ein mit „Vulnerable“ oder „Mitigation“ beginnender Text, dann ist Ihr Prozessor für die im Dateinamen genannte Sicherheitslücke anfällig.

Die erwähnten Dateien unterhalb von `/sys/` erzeugt der Kernel von Desinfec't dynamisch selbst. Dort finden sich daher nur Angaben zu Schwachstellen, die er kennt. Daher fehlen Infos zu Prozessorenlücken, die erst nach Fertigstellung von Desinfec't bekannt wurden.

## PCI- und USB-Geräte

Für die meisten Funktionen eines Systems sind PCI- und PCIe-Chips zuständig, die auf dem Mainboard oder Erweiterungskarten sitzen. Diese fragen Sie mittels `lspci` ab. In der meist ein oder zweidutzend Einträge langen Liste finden sich oft die Grafik- und Netzwerkprozessoren, die Klassenbezeichnungen wie „VGA compatible controller“ oder „Ethernet controller“ kennzeichnen. Die dahinterstehenden Bezeichnungen erhält das Diagnosewerkzeug nicht von der Hardware, sondern aus einer lokalen Datei, die einige falsche oder irreführende Informationen enthält. Das liegt an Hardware-Herstellern, die dieselben oder eng verwandte Chips

**Das Werkzeug lscpu  
nennt die Zahl der  
CPU-Kerne sowie  
Minimal- und Turbo-  
Taktfrequenz.**

```

root@desinfect: /home/desinfect
Datei Bearbeiten Ansicht Suchen Terminal Reiter Hilfe
root@desinfect@desinfect: ~
root@desinfect: /home/desinfect
root@desinfect: /home/desinfect# lscpu
Architektur: x86_64
CPU Operationsmodus: 32-bit, 64-bit
Byte-Reihenfolge: Little Endian
Adressgrößen: 36 bits physical, 48 bits virtual
CPU(s): 4
Liste der Online-CPU(s): 0-3
Thread(s) pro Kern: 2
Kern(e) pro Socket: 2
Sockel: 1
NUMA-Knoten: 1
Anbieterkennung: GenuineIntel
Prozessorfamilie: 6
Modell: 42
Modellname: Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz
Stepping: 7
CPU MHz: 818.581
Maximale Taktfrequenz der CPU: 3200.0000
Minimale Taktfrequenz der CPU: 800.0000
BogoMIPS: 4983.76
Virtualisierung: VT-x
L1d Cache: 64 KiB
L1i Cache: 64 KiB
L2 Cache: 512 KiB
L3 Cache: 3 MiB
NUMA-Knoten0 CPU(s): 0-3
Vulnerability Itlb multihit: KVM: Mitigation: VMX disabled
Vulnerability L1tf: Mitigation; PTE Inversion; VMX conditional cache flushes, SMT vulnerable
Vulnerability Mds: Mitigation; Clear CPU buffers; SMT vulnerable
Vulnerability Meltdown: Mitigation; PTI

```

manchmal unter ganz unterschiedlichen Bezeichnungen vertreiben – der Grafikkern eines Intel-Core-i-Prozessors wird daher vielleicht als GPU eines Xeon dargestellt. Da auch das eingangs erwähnte lshw auf solche Daten zurückgreift, sollten

Sie dessen Ausgaben ebenfalls mit Vorsicht begreifen. Oft lassen sich Unklarheiten ausräumen, indem Sie im Internet nach den Hersteller- und Gerätebezeichnern des Bausteins suchen. Diese Device- und Vendor-IDs wirft lspci bei Angabe von

```

root@desinfect: /home/desinfect
Datei Bearbeiten Ansicht Suchen Terminal Reiter Hilfe
root@desinfect@desinfect: ~
root@desinfect: /home/desinfect
root@desinfect: /home/desinfect# head /sys/devices/system/cpu/vulnerabilities/*
==> /sys/devices/system/cpu/vulnerabilities/itlb_multihit ==
KVM: Mitigation: VMX disabled

==> /sys/devices/system/cpu/vulnerabilities/l1tf ==
Mitigation: PTE Inversion; VMX: conditional cache flushes, SMT vulnerable

==> /sys/devices/system/cpu/vulnerabilities/mds ==
Mitigation: Clear CPU buffers; SMT vulnerable

==> /sys/devices/system/cpu/vulnerabilities/meltdown ==
Mitigation: PTI

==> /sys/devices/system/cpu/vulnerabilities/spec_store_bypass ==
Mitigation: Speculative Store Bypass disabled via prctl and seccomp

==> /sys/devices/system/cpu/vulnerabilities/spectre_v1 ==
Mitigation: usercopy/swaps barriers and _user pointer sanitization

==> /sys/devices/system/cpu/vulnerabilities/spectre_v2 ==
Mitigation: Full generic retpoline, IBPB: conditional, IBRS_FW, STIBP: conditional, RSB filling

==> /sys/devices/system/cpu/vulnerabilities/srbd ==
Not affected

==> /sys/devices/system/cpu/vulnerabilities/tsx_async_abort ==
Not affected
root@desinfect:/home/desinfect# 

```

**Desinfect klärt,  
ob Ihr Prozessor für  
die Sicherheitslücken  
Meltdown und  
Spectre anfällig ist.**

```
desinfect@desinfect:~
```

Datei Bearbeiten Ansicht Suchen Terminal Hilfe

```
desinfect@desinfect:~$ lspci
00:00.0 Host bridge: Intel Corporation Core Processor DRAM Controller (rev 12)
00:01.0 PCI bridge: Intel Corporation Core Processor PCI Express x16 Root Port (rev 12)
00:16.0 Communication controller: Intel Corporation 5 Series/3400 Series Chipset HECI Controller (rev 06)
00:1a.0 USB controller: Intel Corporation 5 Series/3400 Series Chipset USB2 Enhanced Host Controller (rev 06)
00:1b.0 Audio device: Intel Corporation 5 Series/3400 Series Chipset High Definition Audio (rev 06)
00:1c.0 PCI bridge: Intel Corporation 5 Series/3400 Series Chipset PCI Express Root Port 1 (rev 06)
00:1c.1 PCI bridge: Intel Corporation 5 Series/3400 Series Chipset PCI Express Root Port 2 (rev 06)
00:1c.2 PCI bridge: Intel Corporation 5 Series/3400 Series Chipset PCI Express Root Port 3 (rev 06)
00:1c.5 PCI bridge: Intel Corporation 5 Series/3400 Series Chipset PCI Express Root Port 6 (rev 06)
00:1d.0 USB controller: Intel Corporation 5 Series/3400 Series Chipset USB2 Enhanced Host Controller (rev 06)
00:1e.0 PCI bridge: Intel Corporation 82801 Mobile PCI Bridge (rev a6)
00:1f.0 ISA bridge: Intel Corporation HM55 Chipset LPC Interface Controller (rev 06)
00:1f.2 SATA controller: Intel Corporation 5 Series/3400 Series Chipset 4 port SATA AHCI Controller (rev 06)
00:1f.3 SMBus: Intel Corporation 5 Series/3400 Series Chipset SMBus Controller (rev 06)
01:00.0 VGA compatible controller: Advanced Micro Devices, Inc. [AMD/ATI] Park [Mobility Radeon HD 5430/5450/5470]
01:00.1 Audio device: Advanced Micro Devices, Inc. [AMD/ATI] Cedar HDMI Audio [Radeon HD 5400/6300/7300 Series]
03:00.0 Network controller: Qualcomm Atheros AR9285 Wireless Network Adapter (PCI-Express) (rev 01)
05:00.0 System peripheral: JMicron Technology Corp. SD/MMC Host Controller (rev B8)
05:00.2 SD Host controller: JMicron Technology Corp. Standard SD Host
05:00.3 System peripheral: JMicron Technology Corp. MS Host Control
05:00.4 System peripheral: JMicron Technology Corp. xD Host Control
05:00.5 Ethernet controller: JMicron Technology Corp. JMC250 PCI Express
ff:00.0 Host bridge: Intel Corporation Core Processor QuickPath Architecture
ff:00.1 Host bridge: Intel Corporation Core Processor QuickPath Architecture
ff:02.0 Host bridge: Intel Corporation Core Processor QPI Link 0 (PCIe)
ff:02.1 Host bridge: Intel Corporation 1st Generation Core i3/5/7 Family
ff:02.2 Host bridge: Intel Corporation 1st Generation Core i3/5/7 Family
ff:02.3 Host bridge: Intel Corporation 1st Generation Core i3/5/7 Family
desinfect@desinfect:~$
```

desinfect@desinfect:~

Datei Bearbeiten Ansicht Suchen Terminal Hilfe

```
desinfect@desinfect:~$ lsusb
Bus 002 Device 003: ID 8564:1000 Transcend Information
Bus 002 Device 004: ID 050d:705a Belkin Components F5U050
Bus 000 Device 001: ID Ralink RT2571W
Bus 002 Device 002: ID 8087:0020 Intel Corp. Integrated
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0
Bus 001 Device 003: ID 04f2:b071 Chicony Electronics
Bus 001 Device 002: ID CNF7129
```

Desinfec't listet per PCI/PCIe oder USB erreichbare Geräte auf, selbst dann, wenn es sie nicht unterstützt.

```
desinfect@desinfect:~
```

Desinfect@Desinfect: ~

Desinfect@Desinfect:~

```
desinfect@desinfect:~$ lsusb
```

Bus 002 Device 003: ID 8564:1000 Transcend Information, Inc. JetFlash

Bus 002 Device 004: ID 050d:705a Belkin Components F5D7050 Wireless G Adapter v3

  [0000:Ralink RT2571W]

Bus 002 Device 002: ID 8087:0020 Intel Corp. Integrated Rate Matching Hub

Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub

Bus 001 Device 003: ID 04f2:b071 Chicony Electronics Co., Ltd 2.0M UVC Webcam /

  CNF7129

Bus 001 Device 002: ID 8087:0020 Intel Corp. Integrated Rate Matching Hub

Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub

```
desinfect@desinfect:~$
```

-mm aus; bei einer Radeon HD 6450 lautete die Kombination etwa „1002:6779“.

Eine Liste der USB-Geräte erhalten Sie mittels lsusb. Hier liegen die angezeigten Gerätbezeichnungen aus den erwähnten Gründen manchmal auch daneben, sodass Sie die numerischen Bezeichner im Zweifel auch hier zu Hilfe nehmen sollten.

Die Liste der PCI/PCIe- und USB-Geräte beziehen `lscpi` und `lsusb` direkt vom Mainboard und den jeweiligen Hardware-Komponenten. In den Aufstellungen tauchen daher auch Komponenten auf, die der von Desinfect' verwendete Linux-Kernel nicht unterstützt. Ausgeschaltete Hardware kann in den Listen allerdings fehlen. Das kann etwa bei Notebooks passieren, bei denen Bluetooth- und WLAN-Chips per USB angebunden sind: Die tauchen womöglich erst auf, wenn Sie den Flugmodus per Schalter oder Funktionstaste deaktivieren. Letztere arbeiten unter Desinfect' aber in Einzelfällen nicht – das ist einer von mehreren Gründen, warum Desinfect' hin und wieder mal eine Hardware-Komponente nicht sieht.

## Datenträger

Das Werkzeug `lsblk` zeigt die von Linux erkannten Datenträger an; dabei liefert es auch den Mount-Punkt mit, sofern das System die darauf befindlichen Partitionen eingehängt hat. Durch Angeben

der Option `--fs` erhalten Sie auch Informationen zum Dateisystem, deren Bezeichnung (Label) und dem normalerweise eindeutigen Bezeichner (UUID / Universally Unique Identifier).

Sie wollen lediglich Datenträger samt Ihren Modellbezeichnung auflisten? Dann verwenden Sie `lsblk --nodeps -o +MODEL`, damit das Werkzeug alle Volumes ignoriert. Dabei zeigt es in der ersten Spalte die von Linux vergebene Gerätbezeichnung. Der zuerst entdeckte Datenträger bekommt beispielsweise „`sda`“, der zweite „`sdb`“. Bei ATA-Datenträgern kann man diese Device-Angaben nutzen, um weitere Informationen abzurufen:

```
sudo hdparm -I /dev/sda
```

Das nennt etwa die Seriennummer, die unterstützten Übertragungsstandards und vieles andere. Die Gerätbezeichnung brauchen Sie auch, um mit der Self-Monitoring, Analysis and Reporting Technology (SMART) von SSDs und Festplatten zu interagieren. Diese liefert unter anderem Informationen zu Nutzungsdauer und Gesundheitszustand des Datenträgers:

```
sudo smartctl -A /dev/sda
```

Die zweite Spalte erwähnt dabei die kryptisch anmutenden Namen der unterstützten SMART-Attribute.

**Die SMART-Daten dieser Festplatte zeigen, dass bislang keine defekten Sektoren gefunden wurden, für die Reservesektoren einspringen mussten.**

```
desinfect@desinfect: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
desinfect@desinfect:~$ sudo smartctl -A /dev/sda
smartctl 6.6 2016-05-31 r4324 [x86_64-linux-5.3.0-51-generic] (local build)
Copyright (C) 2002-16, Bruce Allen, Christian Franke, www.smartmontools.org

== START OF READ SMART DATA SECTION ==
SMART Attributes Data Structure revision number: 16
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME FLAG VALUE WORST THRESH TYPE UPDATED WHEN_FAILED RAW_VALUE
 1 Raw_Read_Error_Rate 0x002f 200 200 051 Pre-fail Always - 0
 3 Spin_Up_Time 0x0027 186 151 021 Pre-fail Always - 1658
 4 Start_Stop_Count 0x0032 075 075 000 Old_age Always - 25804
 5 Reallocated_Sector_Ct 0x0033 200 200 140 Pre-fail Always - 0
 7 Seek_Error_Rate 0x002e 100 253 000 Old_age Always - 0
 9 Power_On_Hours 0x0032 088 088 000 Old_age Always - 8890
10 Spin_Retry_Count 0x0032 100 100 051 Old_age Always - 0
11 Calibration_Retry_Count 0x0032 100 100 000 Old_age Always - 0
12 Power_Cycle_Count 0x0032 097 097 000 Old_age Always - 3092
191 G-Sense_Error_Rate 0x0032 001 001 000 Old_age Always - 392
192 Power-Off_Retract_Count 0x0032 199 199 000 Old_age Always - 1011
193 Load_Cycle_Count 0x0032 099 099 000 Old_age Always - 303005
194 Temperature_Celsius 0x0022 100 086 000 Old_age Always - 47
196 Reallocated_Event_Count 0x0032 200 200 000 Old_age Always - 0
197 Current_Pending_Sector 0x0032 200 200 000 Old_age Always - 0
198 Offline_Uncorrectable 0x0030 200 200 000 Old_age Offline - 0
199 UDMA_CRC_Error_Count 0x0032 200 200 000 Old_age Always - 0
200 Multi_Zone_Error_Rate 0x0008 200 200 051 Old_age Offline - 0

desinfect@desinfect:~$
```

die letzte deren aktuellen Wert. Hier finden Sie etwa Angaben zu Fehlern, die Anzahl der Betriebsstunden, die Temperatur oder die Menge der geschriebenen und gelesenen Daten. Der Wert in der Zeile mit der ID 5 (meist „Reallocated Sector Count“) ist einer der wichtigsten: Er zeigt, wie viele schlechte Sektoren bereits gegen Reservesektoren ausgetauscht wurden. Falls das schon vorgekommen ist, sollten Sie den Wert fortan im Auge behalten; steigt er stetig oder gar sprunghaft, sollten Sie zügig ein

Vollbackup anlegen und einen Ersatzdatenträger beschaffen.

Einige der Attribute finden sich bei allen Datenträgern, manche sind aber optional oder herstellerspezifisch; darunter leider auch jene, die Informationen zur Abnutzung der SSD liefern.

ersetzen Sie das **-A** durch ein **--all**, um noch mehr SMART-Informationen abzurufen. Via

```
sudo smartctl -t short /dev/sda
```

### SMART-Attribute bei Festplatten und SSDs (Auswahl)

Attribut	Bedeutung
Raw Read Error Rate	Häufigkeit von Lesefehlern
Reallocated Sector Count	Anzahl der bereits genutzten Reservesektoren
Seek Error Rate	Anzahl von Positionierungsfehlern der Festplattenköpfe (nur HDD)
Program Fail Count	Flash-Programmierfehler (nur SSD)
Erase Fail Count	Flash-Lösche Fehler (nur SSD)
Spin Up Time	Zeit für das Hochfahren der Festplatte
CRC Error Count	aufgetretene SATA-Schnittstellenfehler
Media Wearout Indicator/SSD Life Left	Indikator für Flash-Abnutzung (nur SSD)
Power On Hours	Gesamtbetriebszeit des Laufwerks
Power Cycle Count	Anzahl der Einschaltvorgänge
Host Writes/Total LBAs Written	geschriebene Gesamtdatenmenge in Sektoren
Host Reads/Total LBAs Read	gelesene Gesamtdatenmenge in Sektoren
Temperature	Betriebstemperatur

können Sie den Datenträger auffordern, einen kurzen Selbsttest auszuführen, der meist nur einige Minuten dauert und keine Daten gefährdet; der längere Test, für den Sie short in long ändern müssen, prüft den ganzen Speicherbereich; bei großen Festplatten kann das daher leicht eine Stunde oder länger dauern. Beide Aufrufe starten den Selbsttest im Hintergrund und beenden sich gleich wieder. Dabei nennen sie die geschätzte Testzeit. Währenddessen arbeitet der PC nahezu normal weiter, denn bei Zugriffen unterbricht der Datenträger seinen Selbsttest automatisch für einen kurzen Moment. Das Testergebnis erfahren Sie über folgenden Befehl:

```
sudo smartctl -l selftest /dev/sda
```

Der jeweils neueste Test hat die niedrigste Nummer; falls er noch im Gange ist, zeigt die Spalte „Remaining“ den prozentualen Fortschritt. Bei einem Lesefehler bricht das Laufwerk den Test ab und nennt den beschädigten Sektor im Testergebnis. Dieser wird gegen einen Reservesektor ausgetauscht, sobald der angeschlagene Sektor das nächste Mal überschrieben wird. Details zur Lösung solcher Probleme und weitere SMART-Tricks erläutern [1] und der Artikel „Fotos und Dateien retten“ auf Seite 40.

## UEFI-Bootdiagnose

Falls Ihr System die installierten Betriebssysteme per UEFI startet, können Sie folgenden Befehl nutzen, um sich die beim BIOS hinterlegte UEFI-Boot-Einträge anzuzeigen:

```
sudo efibootmgr
```

Das klappt aber nur, wenn Sie auch Desinfec't über UEFI-Mechanismen booten; Sie dürfen es daher nicht mit den Methoden eines klassischen BIOS starten („Legacy Boot“), wie es viele moderne BIOSe per CSM (Compatibility Support Module) ermöglichen.

Sie können efibootmgr mit dem Schalter `-v` aufrufen, um neben den Bezeichnungen auch etwas kryptisch wirkende Details zu den Boot-Einträgen auszugeben. Über die darin stehenden Datenträger- und Pfadangaben findet das BIOS beim Systemstart den Boot-Loader, die Betriebssysteme bei der UEFI-Installation auf der ESP (EFI System Partition) ablegen. Diese meist 100 bis 500 MByte große FAT-Partition können Sie mit Linux auch einhängen und durchstöbern. Wenn Sie hier einen EFI-Boot-Loader

finden, für den kein UEFI-Boot-Eintrag mehr existiert, können Sie den mit efibootmgr anlegen:

```
sudo efibootmgr --create ↵
  --disk /dev/sda --part 1 ↵
  --loader '\EFI\ubuntu\shimx64.efi' ↵
  --label 'Mein Ubuntu'
```

Dieser Befehl funktioniert bei einem System, bei dem die ESP über die Gerätebezeichnung /dev/sda1 erreichbar ist; falls die ESP bei Ihrem System woanders liegt, müssen Sie die Angaben hinter `--disk` und `--part` anpassen. Das gilt auch für den Pfad zum Bootloader, den Sie durch einfache Anführungszeichen schützen müssen, denn sonst gehen die Backslashes verloren.

Ob UEFI Secure Boot aktiv ist, zeigt das folgende Kommando:

```
sudo dmesg | grep -i 'Secure boot'
```

Der Befehl durchsucht das Log des Kernels nach einer Statusausgabe.

Die Kernel-Meldungen enthalten noch eine ganze Menge anderer Details zur Hardware und deren Verwendung durch Linux. Durch `sudo dmesg --human` wird die Ausgabe etwas übersichtlicher, denn dann verwendet das Programm verschiedene Farben und relative Zeitangaben.

## Netzwerkgeräte

Ein `ip link show` liefert Ihnen eine Liste der Netzwerkschnittstellen, die neben Netzwerkchips auch virtuelle Geräte wie das Loopback-Device enthält. Naturgemäß klappt das nur bei Netzwerkhardware, für die Desinfec't einen Treiber mitbringt. Bei Ethernet-Hardware ist das meist der Fall; bei WLAN-Chips passiert es aber hin und wieder, dass ein Treiber fehlt oder er die Hardware nur rudimentär unterstützt. Über das Werkzeug `ethtool` können Sie die Übertragungsgeschwindigkeit und andere Details zur Netzwerkverbindung abrufen. Die wesentlichen Attribute können Sie aber auch den Verbindungsinformationen entnehmen, die das grafische Netzwerkkonfigurationstool von Desinfec't anzeigt.

## Thermometer

Der Befehl `gnome-power-statistics` liefert Details zu Notebooks-Akkus. Das Kommando `sensors` zeigt die Temperaturdaten an, die vom Kernel automatisch

erkannte Sensoren liefern. Meist enthalten die einen Abschnitt, der „coretemp“ (Intel) oder „k10temp“ (AMD) im Namen enthält: Dort findet sich die Temperatur des Prozessors und oft auch die der einzelnen Kerne. Falls es einen Abschnitt „acpitz“ gibt, stehen hier via ACPI abgefragte Werte der Thermal Zones des Mainboards; meist sitzt einer der darüber abfragbaren Sensoren in der Nähe des Prozessorsockels. PCs mit Radeon-Grafik geben manchmal auch ein mit „radeon“ oder „amdgpu“ betitelten Abschnitt mit der Temperatur des Grafikchips aus. Es gibt aber auch PCs, wo das Programm keinerlei Informationen liefert: Manchmal unterstützt Desinfec't die Monitoring-Chips gar nicht, manchmal erst nach der eher mühsamen Konfiguration über `sudo sensors-detect`. Die ist bei vielen PCs leider nötig, um Lüfterdrehzahlen abzufragen oder die Spannungsversorgung zu überprüfen.

## Befeuer

Nutzen Sie den Speedtest von OpenSSL, um Lüfterdrehzahlen und Prozessortemperatur versuchsweise nach oben zu treiben, indem sie allen CPU-Kernen etwas zu tun geben:

```
openssl speed -multi $(nproc --all)
```

Desinfec't bringt kein Programm mit, um die Grafikkarte zu beladen. Für diese Aufgabe können Sie den Furmark von GpuTest nutzen. Laden Sie dessen Linux-Version via [ct.de/wjjr](http://ct.de/wjjr) herunter, um es dann wie folgt zu starten:

```
cd Downloads
unzip GpuTest_Linux_x64_0.7.0.zip
cd GpuTest_Linux_x64_0.7.0/
./GpuTest /test=fur
```

Achtung: Sie sollten die beiden zuletzt genannten Lasttests nicht als einhundert Prozent stichhaltigen Stabilitätstest betrachten, denn Desinfec't konfiguriert und nutzt Ihre Hardware womöglich anders als Ihr regulär genutztes Betriebssystem. Stürzen sowohl letzteres als auch Desinfec't sporadisch ab, heißt das daher keineswegs, dass die Schuld bei der Hardware liegt. Die kann trotzdem beim Betriebssystem oder seinen Treibern liegen. Das gilt insbesondere bei Systemen mit GeForce-Grafikchips, denn Nvidias proprietärer Linux-Grafiktreiber liegt Desinfec't aus Lizenzgründen nicht bei. Stattdessen kommt ein Treiber zum Einsatz, der ohne nennens-

werte Unterstützung von Nvidia entwickelt wird. Er kann daher oft nur einen Bruchteil des Leistungspotenzials von GeForce-GPUs ausschöpfen. Naturgemäß brauchen diese daher bei einem Lasttest weniger Strom, wodurch beispielsweise Probleme bei der Spannungsversorgung nicht zutage treten, aber im dümmsten Fall hält zu anderen Fehlern führen. Das Gleiche gilt auch für Grafikchips, für die Desinfec't keine 3D-Treiber mitbringt.

Auch Interrupts (IRQs), Stromsparmechanismen und viele andere Hardware-Parameter konfiguriert Desinfec't womöglich nicht so wie Ihr reguläres Betriebssystem. Das ist ganz normal; Ähnliches kann auch passieren, wenn Sie das altbackene Windows 7 auf einem modernen und mit Windows 10 ausgelieferten System einrichten. Wenn es für Reklamationen um die Klärung von Instabilitäten geht, sind Sie daher mit dem Betriebssystem am besten bedient, für das der Hersteller die Hardware ausgelegt hat. Falls Sie das nutzen, aber die Ursache bei der verwendeten Installation vermuten, sollten Sie das Betriebssystem ein zweites Mal parallel installieren und damit testen.

## Detaillierter

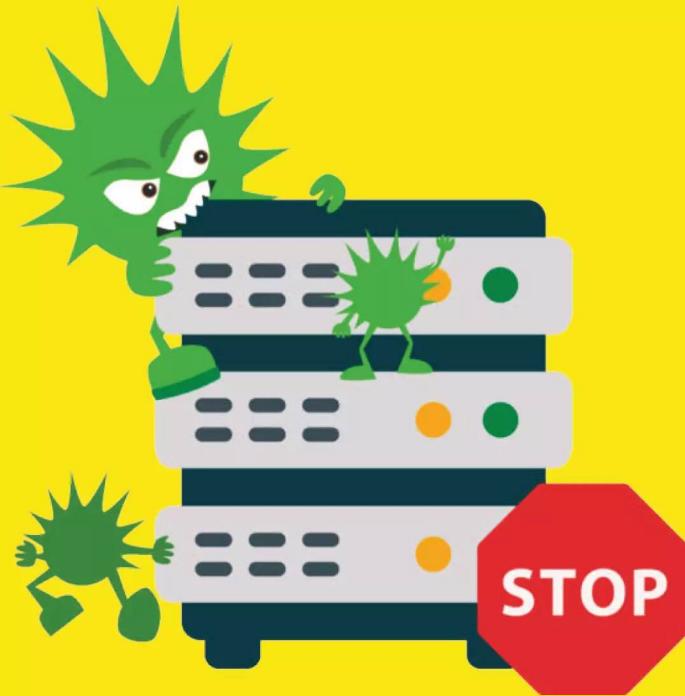
Viele der erwähnten Programme bieten Optionen, mit denen sie mehr Ausgaben liefern oder weitere Aufgaben erledigen. `lspci` gibt bei Angabe des Parameters `-k` etwa umfangreichere Informationen aus, die auch den vom Kernel verwendeten Treiber nennen. Noch viel mehr Details zu PCI/PCIe-Geräten und ihrer Konfiguration spuckt das Programm aus, wenn Sie es via `sudo lspci -v` aufrufen; mit `-vv` oder `-vvv` sind es sogar noch mehr. Auch `lssub` gibt durch ein `-v` mehr Informationen aus. Der Schalter `-t` bewegt beide Programme dazu, die Hardware in einer Baumstruktur darzustellen. Bei PCs mit USB-2- und USB-3-Controllern können Sie dort sehen, an welchem der beiden ein USB-Gerät hängt.

Das sind einige Möglichkeiten, die die erwähnten Programme bieten. Diese liefern oft selbst eine Übersicht, wenn man sie mit `--help` aufruft. Noch ausführlicher sind die Handbuchseiten, die man mit Befehlen wie `man lspci` aufruft und durch Drücken von `Q` wieder verlässt. Achtung: Detaillierte Diagnoseaufgaben erfordern manchmal Systemverwalterrechte, worauf die Ausgaben meist hinweisen; starten Sie die Programme dann mit einem vorangestellten `sudo`. Desinfec't bietet noch einen anderen Vorteil: Es ermöglicht eine Problemrecherche im Internet, wenn das installierte Betriebssystem zickt. (des) 

## Literatur

[1] Boi Feddern, **Gucken kost' nix**, SSD-Diagnose mit SMART, c't 15/2013, S. 152

GpuTest herunterladen  
[ct.de/wjjr](http://ct.de/wjjr)



# Daten von NAS-Platten kratzen

In den meisten Netzwerkspeichern steckt ein mehr oder minder umfrisiertes Linux. Streikt die Hardware, sind die Daten deshalb nicht verloren. Ein Live-System wie unser Desinfec't, das wir dafür ein wenig aufgebretzt haben, genügt meist, um sie mit überschaubarem Aufwand zu bergen.

Von **Peter Siering**

**E**in NAS stellt im Netzwerk Speicherplatz bereit. Selbst 08/15-NAS-Geräte vom Lebensmitteldiscounter mit Platz für zwei Festplatten bemühen in der Regel die Standardtechniken des Linux-Kernels, um sie zu einer großen zusammenzufassen (RAID0) oder die Daten redundant darauf abzulegen (RAID1). Als Dateisystem kommt oft das gängige ext4 zum Einsatz. Größere Geräte variieren: Sie nutzen andere RAID-Techniken, etwa RAID5 mit mehr als zwei Platten, oder greifen auf Dateisysteme zurück, die selbst auch die Plattenverwaltung übernehmen. So findet sich

zunehmend Btrfs auf NAS-Platten. Auf Selbstbau-NAS-Systemen mit FreeNAS ist außerdem ZFS anzutreffen.

Linux, wenn es denn mit passenden Treibern wie unser Desinfec't ausgestattet ist, stellt das Lesen solcher Festplatten vor keine schwierige Aufgabe – schwieriger ist es, überhaupt herauszufinden, was ein NAS nutzt, und dann schließlich die Daten so auszulesen, dass die Platten möglichst unverändert blieben, worauf dieser Artikel besonderen Wert legt. Die folgenden Hinweise taugen begrenzt auch dann, wenn es zu einer Datenhavarie gekommen



**Sicher ist sicher: Das Blacklisten der RAID-Module im Bootmanager verhindert, dass Desinfec't solche Platten voreilig schon konfiguriert. Auf das Hinzufügen der eingekreisten Optionen kommt es an. Die vorgegebenen Parameter variieren je nach Boot-Medium und Methode.**

ist, die NAS-Hardware also noch lebt, es aber nicht schafft, die gespeicherten Daten bereitzustellen. Falls Sie Daten von Platten kratzen müssen, die an einem (Hardware-)RAID-Controller hingen: Das ist ein anderes Kapitel, auf das wir hier nicht weiter eingehen.

## Entdeckungsreisen

Unverzichtbar, um Dateninhalte eines nicht mehr funktionstüchtigen NAS in Sicherheit zu bringen, ist ein PC, den Sie als Rettungssystem verwenden. An den schließen Sie eine hinreichend große leere Festplatte an, um drauf die wiederhergestellten Daten zu sichern. Hilfreich ist es, wenn diese Rettungssplatte deutlich mehr Platz bereithält, dann passt gegebenenfalls auch ein Image für Experimente darauf, sodass Sie die Originalplatten nicht verändern, falls doch ein professioneller Datenretter helfen soll.

Idealerweise handelt es sich um einen vollwertigen PC mit vielen freien SATA-Anschlüssen. So können Sie alle Platten des NAS gleichzeitig an den PC anschließen. Nutzen Sie dafür SATA- oder eSATA-Ports. Eine USB-Dockingstation oder ein USB-Adapter führt eine zusätzliche Ebene ein, die gern mal Ärger macht: Bei unseren Experimenten für diesen Artikel kappten ältere USB-Dockingstationen die Kapazität großer Festplatten. Oft handelt man sich mit USB auch unnötige Performance-Nachteile ein, wenn es um große Datenmengen geht.

Wenn Sie alle Komponenten zusammengestöpselt haben und den PC einschalten, sollten Sie unbedingt Desinfec't daran hindern, automatisch Festplatten aus RAID-Verbunden einzubinden.

Das geht, indem Sie im Bootmanager spezielle Startparameter eingeben. Die vom Kernel dafür vorgesehenen Parameter `raid=nodetect` oder `md_mod.start_ro=1` bewähren sich aus unserer Sicht bei Desinfec't nicht: Der erste greift dort offenbar nicht und der zweite hat den Nachteil, dass nur anfängliche Schreibzugriffe auf einen RAID-Verbund verhindert werden. Nachhaltig funktioniert das zeitweise Deaktivieren sämtlicher RAID-Module.

Die nötigen Handgriffe variieren, je nachdem, wie der PC startet. Auf dem grafischen Bootscreen drücken Sie die Tab-Taste und tippen die Ergänzung direkt am Ende der Startparameter ein. Auf UEFI-Systemen bearbeiten Sie die vorselektierte Boot-Auswahl durch Drücken der Taste E, springen mit dem Cursor in die zweite Zeile und mit End ans Ende der Zeile. Fügen Sie in beiden Fällen mit einem Leerzeichen an: `modprobe.blacklist=raid0, raid1, raid456, raid10`. Starten Sie die Auswahl jetzt mit Return im grafischen Bootscreen oder mit F10 im UEFI-Grub.

Wenn der Desinfec't-Desktop zu sehen ist, öffnen Sie ein Terminal-Fenster und geben als Befehl erst einmal `sudo su` ein. Das hat den Vorteil, dass Sie im Folgenden nicht jedem Befehl ein `sudo` voranstellen müssen. Anders als sonst in c't üblich zeigen in diesem Artikel die grauen Kästen die Ausgaben der empfohlenen Befehle. Mit `lsblk` können Sie sich einen kompakten Überblick über die vorhandenen Datenträger verschaffen:

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
Loop1	7:1	0	5,5G	0	loop	
sdb	8:16	0	232,9G	0	disk	
+sdb2	8:18	0	231G	0	part	
\-sdb1	8:17	0	2G	0	part	
Loop2	7:2	0	7G	0	loop	/opt/.../signatures
Loop0	7:0	0	1,7G	1	loop	/rofs
sdc	8:32	1	14,7G	0	disk	/cdrom
\-sdc1	8:33	1	5,5G	0	part	
sda	8:0	0	894,3G	0	disk	
\-sda1	8:1	0	894,3G	0	part	
Loop3	7:3	0	2G	0	loop	[SWAP]

Benutzen Sie die SIZE-Spalte, um sich zu orientieren. Das Gerät „sdc“ ist der Desinfec't-Stick. Die Geräte mit „loop“ im Namen sind Hilfsgeräte, die Desinfec't benötigt. Bei „sda“ handelt es sich um eine zusätzlich angeschlossene Rettungsfestplatte. Aus einem einfachen 2-Bay-NAS von Allnet stammt das Gerät „sdb“. Die Festplatte bildete darin zusammen mit einer weiteren redundanten Verbund (RAID1).

Obwohl Sie die RAID-Module durch die Boot-Option abgeklemmt haben, läuft die automatische Erkennung derselben. Die Ergebnisse können Sie mit `cat /proc/mdstat` anzeigen lassen.

```
Personalities : [linear] [multipath]
md126 : inactive sdb2[1]($)
    242149440 blocks
md127 : inactive sdb1[1]($)
    2047936 blocks
unused devices: <none>
```

Die Platte enthält augenscheinlich zwei RAID-Verbunde, „md126“ und „md127“. Um etwas über deren Beschaffenheit herauszufinden, befragen Sie mit dem Linux-eigenen Kommando für den Umgang mit Software-RAID idealerweise die in einem Verbund sichtbaren Partitionen oder Geräte, hier etwa „sdb2“: `mdadm -Evv /dev/sdb2`:

```
/dev/sdb2:
    Magic : a92b4efc
    Version : 0.90.00
    UUID : a945e406:6ce45545:0284e52d:87b2d038
Creation Time : Thu Jan 1 01:13:39 1970
    Raid Level : raid1
    Used Dev Size : 242149440
                    (230.93 GiB 247.96 GB)
    Array Size : 242149440
                    (230.93 GiB 247.96 GB)
    Raid Devices : 2
    Total Devices : 2
Preferred Minor : 0
    Update Time : Wed Jul 4 14:54:20 2018
    State : clean
    Active Devices : 2
    Working Devices : 2
    Failed Devices : 0
    Spare Devices : 0
    Checksum : b338ed83 - correct
    Events : 23
Number Major Minor RaidDevice State
this 1      8      18      1      active sync/dev/sdb2
0      0      8      2      0      active sync
1      1      8      18      1      active sync/dev/sdb2
```

Die Ausgabe zeigt die Daten einer speziellen Datenstruktur namens Superblock, die RAID-Geräte beschreibt, und bedarf nicht vieler Kommentare: Sie sehen, dass es sich um ein RAID1 handelt,

wie viele Platten zum Verbund gehören (2), und, dass `/dev/sdb2` als eine von zwei Platten im Verbund vorhanden ist.

Ein ähnlicher Befehl auf das RAID-Gerät selbst angewendet, nämlich `mdadm --detail /dev/md126`, liefert übrigens mitunter irre-führende Erkenntnisse – lassen Sie sich davon nicht verwirren. Er weist manchmal solche als „inactive“ geführten Geräte als Mitglied eines RAID0-Verbunds aus. Lassen Sie sich davon nicht täuschen. Erst wenn ein RAID-Gerät als „active“ geführt wird, passt dann die Angabe zu den realen Verhältnissen.

## Zwiebeliges QNAP

Unsere Erwartung bei der Vorbereitung des Artikels war, dass es recht einfach sein sollte, die Daten von den Festplatten Linux-basierter NAS-System herunterzu-kratzen. Die Produkte der Firma QNAP haben die nicht erfüllt: Die 2018 aktuellen Geräte packen die Platten in ein RAID-Array, legen auf dieses RAID-Array ein DRBD-Volume (Distributed Replicated Block Device, eine Art RAID1 fürs Netz), fügen dieses Volume als physisches Volume dem Logical Volume Management zu, um es dann mithilfe des Device Mappers mit einem optionalen SSD-Cache zu versehen, gegebenenfalls mit LUKS zu verschlüsseln und schließlich als Laufwerk zugänglich zu machen. Das ist alles durchaus plausibel, wenn auch nur schwer zu durchdringen. Manches ist sogar ge-schickt, etwa der Einsatz von DRBD, um NAS-Inhalte übers Netz direkt auf ein anderes NAS zu replizieren.

Leider hat QNAP aber das Logical Volume Management von Linux modifiziert, sodass man die Volumes nicht mit einer herkömmlichen Linux-Distribution erreicht – ob das der Fall ist, hängt auch davon ab, wie das NAS ein-gerichtet wurde beziehungsweise sein Speicherplatz provisioniert worden ist (thick oder thin). Obendrein gibt es wohl noch eine Legacy-Konfiguration, die kompati-ibel zu regulären Linux-Techniken bleibt. Ob Ihre QNAP-Platten von einer regulären Linux-Distribution lesbar sind oder nicht, finden Sie beim Suchen nach physi-schen Volumes heraus (`pvscan`). Kann der Befehl einem Volume keine Volume Group zuordnen und gibt er als Fehlermeldung Hinweise zur Provisionierung aus, haben Sie am eigenen Leib erfahren, was ein Vendor-Lock ist. QNAP bestätigte diese Sonderlocken und wollte sie vorerst beibehalten. Andere Hersteller hingegen werben sogar damit, dass man die Platten ihrer Geräte mit regu-lären Linux-Distributionen auslesen kann.

## Sicherheitsumstand

Ein RAID muss, bevor man es als Dateisystem in den Dateibaum einhängen kann, zunächst aktiviert werden. Das ist nach dem zwangswise Auslassen der RAID-Module beim Systemstart etwas umständlich. Zunächst laden Sie die Module mit:

```
echo raid0 raid1 raid456 raid10 | xargs modprobe
```

Anschließend werfen Sie die im Device-Mapper beim Start ermittelten Erkenntnisse zu dem jeweiligen Gerät weg, indem Sie das RAID-Gerät stoppen: `mdadm -S /dev/md126`. Anschließend „starten“ Sie es erneut:

```
mdadm --assemble --readonly --run /dev/md126 /dev/sdb2
```

Vorsicht, hier müssen Sie achtsam vorgehen, damit Sie nicht Geräte ins falsche Array stecken. Dadurch würden Sie im unglücklichen Fall Daten verlieren. Oft fängt `mdadm` solche Eseleien aber ab. Bei einem inkonsistenten Verbund kann es nötig sein, den Aufruf zusätzlich mit der Option `-f` zu versehen, um die Inbetriebnahme zu erzwingen. Damit steigern Sie allerdings auch das Risiko, Daten zu verlieren.

Ob der Verbund läuft, können Sie überprüfen, indem Sie erneut den Status mit `cat /proc/mdstat` abfragen:

```
md126 : active (read-only) raid1 sdb2[1]
        242149440 blocks [2/1] [_U]
```

Das Starten hat geklappt („active (read-only)“). Sie können die enthaltenen Daten jetzt eventuell schon als nur lesbares Dateisystem einhängen, etwa mit `mount /dev/md126 /mnt -o ro`. Die Wahrscheinlichkeit ist aber groß, dass der `mount`-Befehl meckert, weil die wenigsten NAS-Geräte direkt auf dem Verbund Daten speichern.

Klüger ist es deshalb zu untersuchen, was auf dem RAID-Gerät eigentlich liegt. `wipefs /dev/md126` liefert für unsere Testplatte:

offset	type
0x218	LVM2_member [raid] UUID: V6vY1Q-...-21L4-7QFs-hVRgX3

Keine Bange: `wipefs` löscht erst auf explizite Anforderung per Parameter. Ohne zeigt es nur an, was es löschen könnte. Mit

`file -s /dev/md126` können Sie eine zweite Meinung einholen, die im konkreten Beispiel der ersten entspricht:

```
/dev/md126: LVM2 PV (Linux Logical Volume Manager),
UUID: V6vY1Q-...-21L4-7QFs-hVRgX3, size: 247961026560
```

Die Erkenntnis ist, dass der NAS-Hersteller den RAID-Verbund mit dem Logical Volume Management weiter aufteilt. Der RAID-Verbund ist ein physisches Volume, das Sie `Desinfec't` erkennen lassen müssen, `pvscan` erledigt das, sollte es nicht bereits automatisch passiert sein:

```
PV /dev/md126 VG vg0 lvm2 [230,93 GiB / 11,93 GiB free]
Total: 1 [... GiB]/in use: 1 [... GiB] / in no VG: 0 [0 ]
```

Mit `vgs` können Sie sich vergewissern, dass die Automatik beziehungsweise der vorangehende Befehl gleich eine passende Volume Group eingerichtet hat:

```
VG #PV #LV #SN Attr  VSize  VFree
vg0  1   1   0  w--n- 230,93g 11,93g
```

Das ist in der Regel der Fall. Wenn nicht, kann man analog zu `pvscan` mit `vgscan` eine Suche starten. Unter Umständen (siehe Kasten „Zwiebeliges QNAP“) geben die Befehle Fehlermeldungen aus, denen man dann hinterherrecherchieren kann – eventuell ist das aber auch der Moment, wo man aufgeben und andere Wege suchen sollte, weil man ansonsten anfangen muss, Kernel-Patches zu lesen und anzupassen.

Mit einer aktiven Volume Group müssen Sie im nächsten Schritt ermitteln, welche logischen Volumes das NAS angelegt hat, `lvs` hilft dabei:

```
LV  VG  Attr      LSize  Pool Origin Data%  Meta% ...
lv0  vg0  -wi-a--- 219,00g
```

Bei einfachen Geräten sind Sie jetzt fast am Ziel, `wipefs/dev/vg0/lv0` verrät, was auf dem logischen Volume gespeichert ist; `file` meckert über den Gerätenamen, der nur ein symbolischer Link ist, und verweist Sie an die „echte“ Gerätedatei, etwa `/dev/dm-4`, rufen Sie `wipefs` mit diesem Namen erneut auf:

offset	type
0x0	xfs [filesystem] UUID: 978f3d2a-...-5e0c4248fabd

Mit `mount /dev/vg0/lv0 -t xfs -o ro /mnt/` können Sie das offenbar enthaltene XFS-Dateisystem nun unter `/mnt` einhängen und auch mit dem Desinfec't-Dateimanager ansehen. Je nach NAS werden Sie nicht nur Ihre Dateien dort vorfinden, sondern auch Systemdateien, die das Gerät benötigt. Sie sollten dort also nicht anfangen aufzuräumen, wenn die Chance besteht, die Platten etwa in einem Ersatzgerät wieder in Betrieb zu nehmen.

## Image nutzen

Um Images von NAS-Platten anzufertigen und nicht das Original zu verhunzen, brauchen Sie einen hinreichend großen Rettungsdatenträger. Bezogen auf die bisherigen Beispiele, also der NAS-Platte als „`sdb`“ und dann als `/target` eingehängtem Rettungsdatenträger, erstellen Sie 1:1-Kopien auf folgende Weise:

```
dd if=/dev/sdb of=/target/mein.img bs=1M status=progress
```

Wenn die NAS-Platte nicht mehr vollständig lesbar ist, verwenden Sie stattdessen `ddrescue` – je nach Beschädigungsgrad läuft das deutlich länger, weil es beim Lesen defekte Sektoren umschifft. Die Parameter unterscheiden sich vom einfachen `dd`. Details zu `ddrescue` und das Retten von Dateien führen wir im Artikel „Fotos und Dateien retten“ auf Seite 40 aus.

Anschließend fahren Sie Desinfec't herunter, trennen die echte RAID-Platte von Ihrem PC und starten es erneut. Das Ausschließen der RAID-Module im Bootmanager per `modprobe.blacklist` ist bei diesem Start nicht mehr nötig. Die zuvor als Rettungsdatenträger formatierte Platte müssen Sie erneut einhängen (Desinfec't merkt sich so etwas nicht). Prüfen Sie zuvor mit `lsblk`, ob die Gerätenamen durch das Entfernen der einen Platte eventuell versprungen sind, etwa von `sda` auf `sdb`.

Nach dem Einhängen der Rettungsplatte (etwa mit `mount /dev/sda1 /target`) müssen Sie jetzt dafür sorgen, dass Desinfec't die Image-Datei mit den Partitionen des RAID-Mitglieds auch als solche behandelt. Dabei hilft ein weiterer Befehl, `kpartx -av /target/mein.img`:

```
add map loop4p1 (253:0): 0 4096000 linear 7:4 2048
add map loop4p2 (253:1): 0 484299087 linear 7:4 4098048
```

Alle Partitionen, die in der Image-Datei enthalten sind, bindet `kpartx` in einem Rutsch über ein Loop-Device und den Device-Mapper als Partitionen ein. Sie sind dann im Gerätebaum unter `/dev/mapper` als Geräte zu sehen. (Sollten Sie das eingebundene Image in der laufenden Sitzung wieder loswerden wollen, wiederholen Sie den `kpartx`-Aufruf und ersetzen Sie dabei die Option `-a` durch `-d`.)

Die eingangs zur Orientierung empfohlenen Befehle wie `lsblk`, `wipefs` und `file` liefern nun auch Informationen für das eingebundene Image unter dem Namen des loop-Device `/dev/loop4` beziehungsweise seiner Partitionen `/dev/mapper/loop4p1`. Die automatische RAID-Erkennung erfolgt im aktualisierten Desinfec't, sodass die in einem Image enthaltenen RAID-Geräte in `/proc/mdstat` sichtbar sind. Stoppen Sie diese zunächst mit `mdadm -S /dev/<md>`.

Detailinformationen zu den einzelnen RAID-Mitgliedern erhalten Sie aber über die bereits bekannten Befehle wie `mdadm -Evv /`

## Rettungsplatte vorbereiten

In der ersten Ausgabe von `lsblk` ganz zu Anfang des Artikels taucht eine Festplatte mit der Bezeichnung „`sda`“ auf. Das ist die Rettungsplatte unseres PC. Der Gerätenamen können bei Ihnen variieren. Eine fabrikfrische Platte, die Desinfec't als „`sda`“ erkennt, bereiten Sie mit folgenden Schritten für den Einsatz unter Linux vor: Starten Sie im Terminal nach einem `sudo su` mit `fdisk /dev/sda` die Partitionierung. Legen Sie eine GPT-Partition neu an und lassen Sie die Änderung auf die Festplatte schreiben. Beenden Sie `fdisk`. Formatieren Sie die Partition mit dem ext4-Dateisystem: `mkfs.ext4 /dev/sda1`. Anschließend erstellen Sie ein Verzeichnis und hängen Sie das Dateisystem dort ein `mkdir /target; mount /dev/sda1 /target`. Desinfec't kann auch andere Dateisysteme einrichten, etwa FAT32. Das eignet sich aber nur dann, wenn Sie lediglich kleine Dateien auf die Rettungsplatte spielen wollen (kleiner als vier GByte). Für größere ist ext4 die bessere Wahl. Ein als Ersatz beschafftes neues NAS sollte eine ext4-formatierte Platte eigentlich immer lesen können.

`dev/mapper/loop4p2` und `wipefs /dev/mapper/loop4p2`. Mit `mdadm --assemble --readonly --run md9 /dev/mapper/loop4p2` können Sie den Verbund starten. Als Verbundnamen nimmt man einen bisher freien – im Zweifel schauen Sie in `/proc/mdstat`, was dort bisher nicht auftaucht. Anschließend können Sie fortfahren, wie der Artikel es am Beispiel physischer Geräte zuvor gezeigt hat.

## Schutzzschirm

In besonders verzwickten Fällen, in denen man Schreibzugriffe auf die Daten braucht, etwa um ein Dateisystem zu reparieren, könnte `xmount` helfen. Das Programm kann Geräte oder Image-Dateien so einhängen, dass Linux alle daran ausgeführten Änderungen in eine Cache-Datei umleitet. Das heißt, das Original bleibt unverändert, es sind aber trotzdem Änderungen möglich. `xmount` müssen Sie in Desinfec't nachinstallieren: Entfernen Sie dazu alle Kommentarzeichen (#) am Beginn der Zeile in `/etc/apt/sources.list`. Lassen Sie anschließend neue Paketlisten holen und `xmount` installieren:

```
apt-get update; apt-get install xmount
```

Soll das Programm dauerhaft auf Ihren Desinfec't-Stick, kopieren Sie es in das dafür reservierte Verzeichnis:

```
cp /var/cache/apt/archives/*.deb ↗  
↳/opt/desinfect/signatures/deb
```

Ein vollständiger Aufruf von `xmount` sieht so aus:

```
xmount --in raw /dev/sdb --cache ↗  
↳/target/sdbcache --out raw/fakedev/
```

Er bindet das physische Gerät `/dev/sdb` als neues Gerät unter dem Pfad `/fakedev/sdb.dd` ein. Daten aus schreibenden Zugriffen, die auf dieses virtuelle Gerät erfolgen, landen in der Datei `/target/sdbcache` und nicht auf `/dev/sdb`. Gesetzt den Fall, `/dev/sdb` enthält wie in den bisherigen Beispielen zwei Partitionen, die je in einem RAID1-Verbund stecken (erkannt als `md126` und `md127`) und logische Volumes enthalten, würde man den `md126`-Teil des Ensembles mit folgender Befehlsfolge beschreibbar mounten:

```
mdadm -S /dev/md126  
mdadm -S /dev/md127  
mkdir /fakedev  
xmount --in raw /dev/sdb --cache ↗  
↳/target/sdbcache --out raw/fakedev/  
kpartx -av /fakedev/sdb.dd  
mdadm --assemble --run /dev/md126 /dev/mapper/loop4p2  
pvscan  
mount /dev/vg0/lv0 -t xfs /mnt
```

Dabei sind `md126` und `127` die automatisch erkannten RAID-Verbunde auf `/dev/sdb`. Das Verzeichnis `fakedev` nimmt das von `xmount` erstellte Gerät auf. Der Aufruf von `kpartx` hat `/dev/mapper/loop4p2` als beschreibbare Partition aus dem von `xmount` erstellten Gerät zugänglich gemacht. Scheitert der letzte Aufruf, kann man mit `fsck /dev/vg0/lv0` das Dateisystem reparieren lassen, ohne dass dabei auf der Originalplatte Daten verändert werden. So wäre es

**SICHER EINKAUFEN**  
Online-Shopping ohne Probleme

Schützen Sie sich vor Betrug  
Bankkarten und Kreditkarten schützen  
Sicheres Bezahlen auf Kleinhandelsgeschäften

Digital bezahlen  
PayPal, Banca, Konto, Websafe bezahlen?  
Probleme im Ausland verhindern

Kaufprobleme lösen  
Erfolgreich reklamieren  
Kaufschutz richtig einsetzen

Heft + PDF mit 29 % Rabatt

Datenrettung/Rechtliche Kundenschutztipps

## Online-Shopping ohne Probleme: ct hilft.

- Die wichtigsten Regeln für den Onlinekauf
- Schützen Sie sich vor Betrug
- Kaufprobleme lösen
- Käuferschutz richtig einsetzen
- Digital bezahlen
- Auch als Heft + digitale Ausgabe mit 29 % Rabatt

Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 €



[shop.heise.de/ct-sicher-einkaufen23](http://shop.heise.de/ct-sicher-einkaufen23)

bei einer misslungenen Rettungsaktion immer noch möglich, das Original einem Datenretter zu überantworten.

## Dateisystem-RAID

Auf verschiedenen NAS-Geräten findet man einen bunten Mix von Dateisystemen wieder: Neben XFS und ext3/4 sind wir auf Synology-Geräten auf Btrfs gestoßen. Obwohl das Dateisystem viele Möglichkeiten bietet, auch die Festplatten selbst zu verwalten und Redundanz herzustellen, setzt der Hersteller dafür bisher weiterhin auf das bewährte Linux-Software-RAID. Btrfs ist dann nur das Sahnehäubchen auf dem Storage-Stack. Entsprechend wenig gibt es deshalb zum Einbinden solcher RAID-Verbunde über die so weit erklärten Handgriffe hinaus zu sagen.

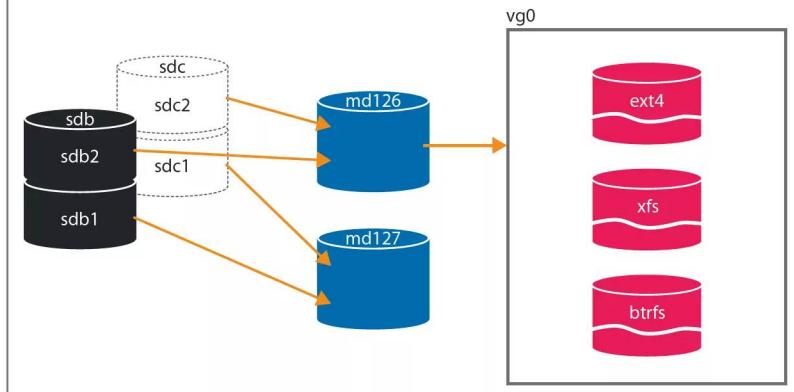
Einfacher ist das Auslesen von NAS-Daten, wenn die Platten direkt mit einem Dateisystem bespielt sind. Das ist etwa bei Platten aus einem Selbstbau-NAS mit FreeNAS als Software der Fall. Die kann Desinfec't von sich aus lesen (dank integriertem ZFS on Linux). ZFS kennt zwar unterschiedliche Feature-Sets, ist aber abwärtskompatibel; eine moderne Version soll immer ältere Versionen lesen können. Anders als einen Linux-eigenen RAID-Verbund erkennt Desinfec't einen ZFS-Pool nicht, aber mit `zpool import` kann man Pools sehen, auf deren Platten Desinfec't zugreifen kann:

```
pool: ptest
  id: 11197401931174254511
  state: UNAVAIL
  status: The pool was last accessed by another system.
  action: The pool cannot be imported due to damaged ...
  see: http://zfsonlinux.org/msg/ZFS-8000-EY
  config:
    ptest          UNAVAIL unsupported feature(s)
    mirror-0          ONLINE
      usb-Inateck_FE2005_00A1234595FF-0:0  ONLINE
      usb-Inateck_FE2005_00A123459600-0:0  ONLINE
```

Wenn der Pool aus dem blühenden Leben geschieden ist, dann kann man den Import forcieren: `zpool import -f ptest -o read only=on`. Wenn die Features nicht passen, dann empfiehlt ZFS einen schreibgeschützten Import (`readonly`) - was beim Wiederherstellen

## So strukturieren NAS-Geräte Festplatten

Beim Einrichten eines NAS entstehen aus physischen Platten (`/dev/sdb`, ...) oder Partitionen (`/dev/sdb1`, ...) RAID-Verbunde (`/dev/md126`, `/dev/md127` ...). Oft stecken sie einen RAID-Verbund als physisches Volume in eine Volume Group (`/dev/vg0`, ...). Aus dem Speicher einer Volume Group bilden sie logischen Volumes. Die kann man in ihrer Größe verändern. Die logischen Volumes versehen sie mit einem Datei-system (`ext4`, `xfs`, ...), auf denen die Dateien landen. Verschlüsselung oder Caching kann an verschiedenen Stellen zusätzliche Ebenen einführen. Wie viele Partitionen, Verbunde und Volume Groups ein NAS anlegt, hängt von der gewünschten Redundanz und den Herstellervorgaben ab. Dieses Bild gibt die Verhältnisse des im Artikel beispielhaft behandelten Allnet ALL NAS 200 wieder.



von NAS-Daten generell eine gute Idee ist. Mit der Option `-F` kann man ZFS auch dazu animieren, den Pool zu reparieren. Das sollte man idealerweise nur tun, wenn man ein Backup oder Image hat. Anders als Linux-Software-RAID arbeitet ZFS mit Namen für die Pools und benötigt zum Import, also zur Wiederinbetriebnahme, keine Gerätenamen.

## Komplikationen

Die Beispiele haben wir bewusst einfach gehalten. Wenn man die Platten aktueller Geräte untersucht, findet man in einem 2-Bay-NAS durchaus fünf oder mehr Partitionen, die nach einem Desinfec't-Start dann als `md123` bis `md127` sichtbar sind. Das ist normal, selbst wenn Sie auf dem NAS eine große, redundant ausgelegte Datenplatte eingerichtet haben. Die Hersteller nutzen die zusätzlichen RAID-Verbunde, um dort ihre Software und Konfigurationsdaten abzulegen. Bei einer Standardkonfiguration dürfen Sie Ihre Daten auf dem größten RAID-Verbund finden.

Die einzelnen RAID's sind dabei durchaus anders aufgebaut: So enthalten QNAP-Geräte zwei RAID-Verbunde, die bis zu 32 Platten aufnehmen können, obwohl als Redundanzstufe nur RAID1 gewählt ist. Womöglich macht es sich der Hersteller an dieser Stelle einfacher, die Betriebssoftware auch für Geräte anderer Ausstattungsklassen gleich mit abzuhandeln. Normalerweise sind solche Entdeckungen kein Grund zur Besorgnis.

Viele NAS-Geräte bieten an, die Festplatten zu verschlüsseln. Normalerweise greifen sie dabei ebenfalls auf bewährte Linux-Technik zurück, die auch unter dem Namen LUKS gehandelt wird. Sie erkennen eine Partition, einen RAID-Verbund oder ein logisches Volume daran, dass `file`, `wipefs` & Co. „LUKS“ nebst weiteren Attributen ausgeben. In einem solchen Fall brauchen Sie das Kennwort oder den Schlüssel, um das Gerät zu entsperren und auf Daten zugreifen zu können. Das kann, muss aber nicht das Kennwort sein, das Sie beim Einrichten vergeben haben.

QNAP beispielsweise salzt das in der Weboberfläche eingegebene Kennwort. Über [ct.de/wrgv](http://ct.de/wrgv) finden Sie eine Hilfe zum Berechnen solcher Kennwörter. Bei anderen NAS-Geräten bleibt nur Probieren und Forschen. Das Prinzip ist simpel: Mit

```
cryptsetup luksOpen /dev/sdb1 decrypted
```

weisen Sie Desinfec't an, die verschlüsselte Partition /dev/sdb1 entschlüsselt als /dev/mapper/decrypted bereitzustellen. Das Kennwort fragt cryptsetup ab. Alternativ kann man das Programm auch mit Schlüsseldateien füttern (–key-file).

Generell berücksichtigt dieser Artikel Erfahrungen der letzten Jahre mit Linux-Software-RAIDs [1] und Experimente mit ausgewählten Geräten. Wir können nicht ausschließen, dass in freier Wildbahn andere Techniken in NAS-Geräten zum Einsatz kommen oder dass Hersteller von gängigen Praktiken abweichen. Mit den so weit geschilderten Methoden sollte es möglich sein, solche Fälle bis zu der Grenze zu erkunden, an der es schließlich gefährlich wird. Mithilfe der mit `xmount` aufgezeigten Arbeitsweise kann

ein erfahrener Linux-Nutzer diese Grenze sogar hinter sich lassen, ohne Daten zu zerstren.

Der Vollständigkeit halber noch folgender Hinweis: Sollten Sie Platten aus einem sehr, sehr alten NAS geborgen haben, kann es sein, dass dessen Prozessor nicht mit der heute verbreiteten Byte-Folge „little-Endian“ arbeitet. `mdadm` kennt beim Zusammenbauen eines RAID-Verbunds die Option `--update=byteorder`, um solche Unterschiede auszugleichen. Ob das nötig ist und was passiert, wenn man es versäumt, konnten wir mangels geeigneter Hardware nicht probieren. Vielleicht ist der Hinweis aber für Ihren Fall eine nützliche Fährte.

Sollten die geschilderten Schritte bei Ihren NAS-Platten keine Daten fördern, die NAS-Hardware aber reif für die Elektroschrott- sammlung sein, hilft ein gebrauchtes Ersatzgerät. In der jeweiligen Gerätefamilie lassen sich die Platten oft einfach umbauen oder nach Inbetriebnahme mit einer fabrikfrischen Festplatte zumindest auslesen. Außerdem gibt es natürlich professionelle Datenretter. Manch einer hat sich sogar auf die NAS-Geräte ausgewählter Her- steller spezialisiert, weil die das mit der Offenheit von Linux nicht so ernst nehmen und eben mehr als nur die Frisur ändern. (ps) 

## Literatur

[1] Peter Siering, **Festplattenpuzzles**,  
Tipps und Tricks rund um Linux-  
Software-RAID, c't 6/2013, S. 184

## Ergänzende Hinweise

[ct.de/wray](http://ct.de/wray)

# Do **KI** Yourself!

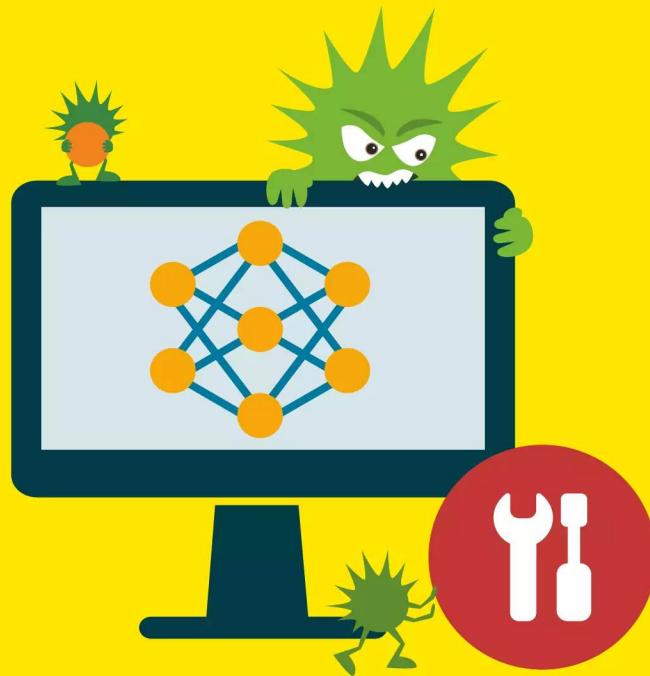
## Modelle anwenden und selbermachen

Heft für 14,90 € • PDE für 14,90 € • Bundle Heft + PDE 20,90 €

 [shop.heise.de/ix-ki](http://shop.heise.de/ix-ki)

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 € (innerhalb Deutschlands). Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

 heise Shop



# Netzwerkprobleme lösen

Unser Live-Notfallsystem auf Linux-Basis hilft nicht nur bei der Schädlingsjagd, sondern auch dann, wenn das Netzwerk in Unordnung geraten ist. Sei es, dass der Browser streikt, der DNS-Malwarefilter mehr bremst als schützt oder dass die NAS-Freigabe sich nicht zeigt – mit Desinfec't kommen Sie den Ursachen auf die Spur.

Von **Peter Siering**

Netzwerkprobleme gibt es reichlich. Die kann man am OSI-Schichtenmodell durchdeklinieren, muss man aber nicht. Mit dem folgenden Know-how und den Werkzeugen in Desinfec't setzen Sie gleich an den neuralgischen Stellen an, um Pro-

bleme im Netzwerk aufzuspüren und zu lösen. Wie in den vorhergehenden Praxisartikeln spielt sich dabei viel auf der Kommandozeile ab. Oft brauchen Sie root-Rechte, das dazu dem Befehl voranzustellende sudo führen wir hier nicht ständig auf.

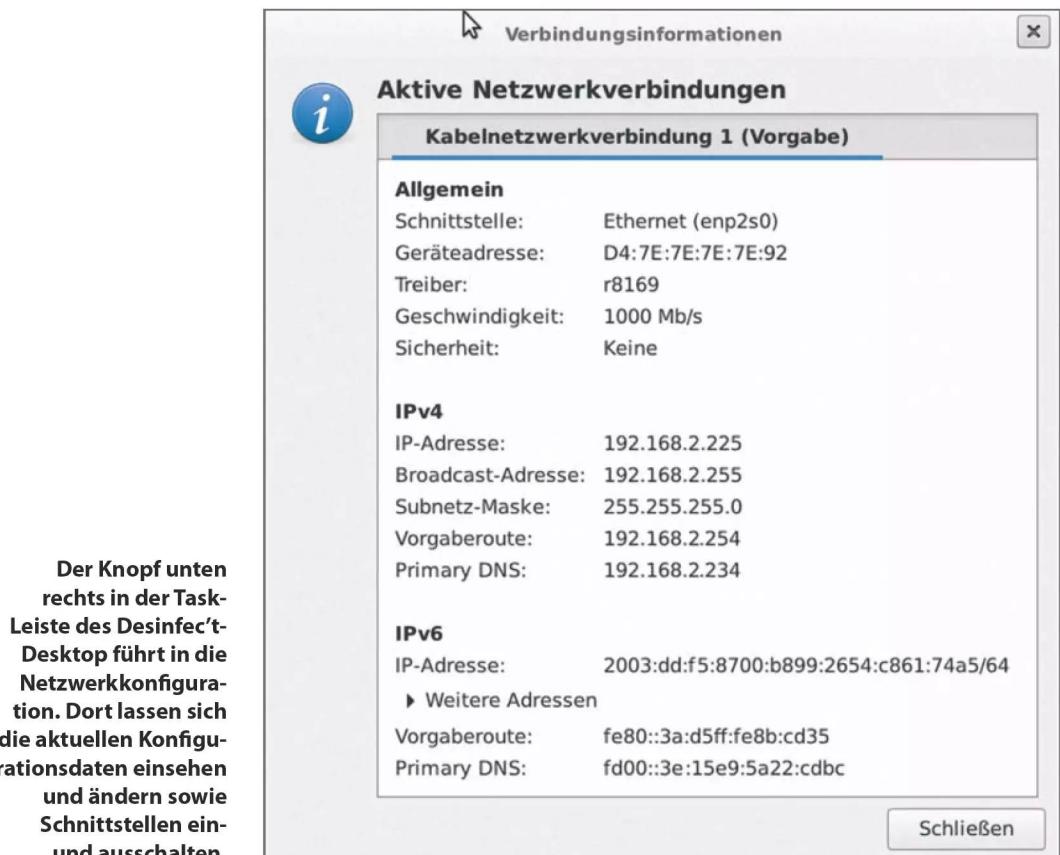
## Surf-Test

Auf den ersten Blick scheint es absurd, ein Live-System für die Diagnose im Netzwerk einzuspannen, doch das ist es nicht: Desinfec't ist dafür ausgerüstet, einen lokalen PC müssten Sie erst mit den Werkzeugen ausstatten. Einige davon gibt es für Windows gar nicht. Ein Live-System fällt keinem virtuellen Verschleiß anheim, der einer schon länger genutzten Betriebssysteminstallation nun mal zusetzt, etwa in Form von unerwünschten Browser-Plug-ins, Schädlingen ...

Insofern können Sie Desinfec't auch benutzen, um alltägliche Aufgaben zu erledigen und es in die Fußstapfen seiner nicht mehr weiterentwickelten Geschwister Surfix und Bankix zu setzen: Es eignet

sich, um mal eben eine Überweisung im Browser abzuschicken, mal eben zu surfen et cetera – von der DVD gebootet, muss man keine Änderung an Desinfec't selbst befürchten. Anders als seine ixigen Geschwister unternimmt Desinfec't jedoch keine Anstrengungen, Schreibzugriffe auf die Datenträger des PC zu unterbinden, auf dem Sie es starten!

In einem 1-PC-1-Router-Haushalt können Sie sich durch Starten von Desinfec't und dem testweisen Besuchen Ihrer Lieblingswebsites auch vergewissern, ob der Internet-Zugang und -Router einwandfrei arbeiten – dann hat offenbar Ihr PC ein Problem mit dem Netzzugang. Kommt auch Desinfec't nicht an die Websites heran, muss die Suche beim Router ansetzen. Schnell sind Sie dann bei den Klassikern der Netzwerkdagnostik.



## ntopng verrät, was im Netzwerk abgeht

Ist es der Sohn, der beim Update der Spiele-Konsole dem Rest der Familie die Bandbreite raubt, oder doch der Gastschüler, der mit Bild nach Hause telefoniert und nebenher Serien schaut? Der faule Familienadmin geht dieser Frage nicht per Pedes nach, sondern mit ntopng. Die Software frisst fortlaufend Netzwerkpakete, um sie zu analysieren und grafisch zusammenzufassen. So sieht man auf einen Blick, wer der größte Paketsauger im Netz ist, findet heraus, dass ein Gerät nicht nur mit den erwartbaren Servern spricht, und lernt dabei allerhand über das eigene Netz.

Desinfec't lässt sich nachträglich mit ntopng versorgen. Es empfiehlt sich, nicht die Version aus Ubuntu 22.04 zu nehmen, sondern gleich auf die Pakete zu setzen, die die ntopng-Macher bereitstellen (siehe auch [ct.de/wvvt](https://ct.de/wvvt)). Die sind aktuell allerdings nur für die 64-Bit-Ausgabe von Desinfec't zu haben. Dazu sind nur wenige Handgriffe nötig: Aktivieren Sie in `/etc/apt/sources.list` die auskommentierten Zeilen, damit Desinfec't fehlende Pakete gegebenenfalls aus den Ubuntu-Repositorien nachinstallieren kann, und rufen Sie dann folgende Befehle auf (stellen Sie ggf. `sudo` voran):

```
 wget http://apt-stable.ntop.org/22.04/all/apt-ntop-stable.deb  
 dpkg -i apt-ntop-stable.deb  
 apt-get update  
 apt-get install ntopng ntopng-data
```

Die fügen das ntopng-Paket-Repository hinzu, aktualisieren die Paketlisten und installieren die für den Einsatz auf Desinfec't hilfreichen Pakete (für stationäre, dauerhafte Installationen von ntopng würde man weitere einrichten). Standardmäßig lauscht ntopng sodann an allen lokalen Schnittstellen. Wenn Sie gezielt nur Ihr WLAN überwachen oder die Daten an Ihrer Fritzbox abzweigen wollen, beenden Sie das Programm mit `killall ntopng` und starten Sie es dann entweder unter Angabe der Netzwerkschnittstelle mit `ntopng -i wls1` oder mit dem im Kasten „Fritzbox als Horchposten für Wireshark & Co.“ auf der Seite 67 vorgeschlagenen Skript.

ntopng analysiert die Pakete im Hintergrund. Um die Auswertung zu sehen und Details betrachten zu können, verbinden Sie sich mit dem Web-Browser mit ntopng. Die URL lautet `localhost:3000`. Beim ersten Anmelden mit Benutzernamen und Passwort `admin` fordert Sie die Oberfläche auf, das Passwort zu ändern. Anschließend sehen Sie das Dashboard, in dem ntopng eine Zusammenfassung seiner Erkenntnisse zeigt. Nach jedem Start läuft ntopng zehn Minuten lang in der Enterprise-Ausgabe mit allen Funktionen.

Danach wechselt es in den abgespeckten Community-Modus – doch für die eingangs geschilderte Aufgabe eignet sich die ebenso gut: Ausgehend vom Traffic-Dashboard können Sie sich die „Top Hosts“ ansehen oder unter „Hosts“ den gleichnamigen Menüpunkt wählen. Der Host im Netz mit dem höchsten Traffic-Aufkommen steht standardmäßig oben. Wenn Sie auf die

Desinfec't prüft nach dem Booten, ob es das Internet erreichen kann. Wenn das nicht der Fall ist, erscheint eine entsprechende Warnung. Eventuell kann es nötig sein, dass Sie zunächst die Zugangsdaten für Ihr WLAN eintragen. Fruchtet das nicht, so sehen Sie sich im Detail um. Prüfen Sie, ob Desinfec't eine gültige IP-Adresse erhalten hat. APIPA-Adressen, die mit „169.“ beginnen, sucht sich ein System selbst. Sie sind ein Hinweis auf Probleme mit der automatischen Vergabe (DHCP). Wenn Desinfec't keine gültige Adresse erhalten hat, wechseln Sie wenn möglich das Medium, also von WLAN zu Kabel oder umgekehrt.

Hält das Problem an, starten Sie den Router neu. Hilft auch das nicht, prüfen Sie mit einem weiteren Gerät, ob vielleicht nur der PC ein Problem hat. Sur-

fen Sie aus dem WLAN die Lieblingswebsites mit einem Smartphone an. Besser wäre ein zweiter PC. Er sollte idealerweise nicht baugleich mit dem ersten sein – Desinfec't bringt zwar viele Treiber mit, aber sicher nicht für jedes Gerät.

## IPv4 und IPv6 richten

Hat Desinfec't eine gültige IP-Adresse erhalten und klappt es trotzdem nicht, per Browser Systeme im Internet zu erreichen, müssen Sie genauer nachsehen: Gelingt es, Namen in IP-Adressen zu verwandeln? Öffnen Sie ein Terminalfenster. Der Aufruf von `ping heise.de` dort sollte fortlaufend ausgeben, dass Antworten von unserem Server eingehen. `ping`

IP-Adresse klicken, gelangen Sie in eine Detailansicht für den Host, die ein weiteres Aufschlüsseln der Erkenntnisse etwa nach Traffic-Art erlaubt. Spannend ist die Ansicht Peers, sie verrät, mit wem sich der Host wie unterhält.

Die Möglichkeiten, die ntopng bietet, gehen wesentlich weiter. In einer regulären Installation kann man Nutzer einrich-

ten, lokale Netze definieren et cetera. Beim Betrieb aus Desinfect heraus ergibt das wenig Sinn, weil diese Daten nach einem Reboot weg sind. Für einfache Auswertungen genügt aber schon das Werkzeug, das ohne Detailkonfiguration zugänglich ist. Gegebenenfalls können Sie unter Einstellungen im Expertenmodus die Zeitspannen verlängern, für die ntopng Daten in einer Sitzung aufbewahrt.

**Mit wenigen Klicks in der ntopng-Weboberfläche erhält man Einsicht ins eigene Netzwerk, sei es zu Fehler suche oder zum Überprüfen von Geräten, die man der Datenschleuderei verdächtigt.**

Applikation	Protokoll	Client	Server	Dauer	Ausfall	aktuelle		
						Thpt	Total Bytes	Info
VNC	TCP	desinfect	10.76.23.5:5900	01:25	Server	0 bps	8.92 MB	—
G+ TLS	TCP	desinfect	172.217.18.106:https	00:53	Server	0 bps	4.67 MB	safebrowsing.googleapis...
TLS	TCP	desinfect	143.204.202.64:https	00:47	Server	0 bps	1.93 MB	tracking-protection.cdn...
TLS	TCP	desinfect	193.99.144.85:https	01:02	Server	0 bps	746.14 KB	www.heise.de
TLS	TCP	desinfect	193.99.144.85:https	00:54	Server	0 bps	678.34 KB	www.heise.de
TLS	TCP	desinfect	104.18.164.34:https	00:55	Server	0 bps	322.57 KB	www.mozilla.org

müssen Sie meist mit Betätigen der Tasten **Strg+C** abbrechen.

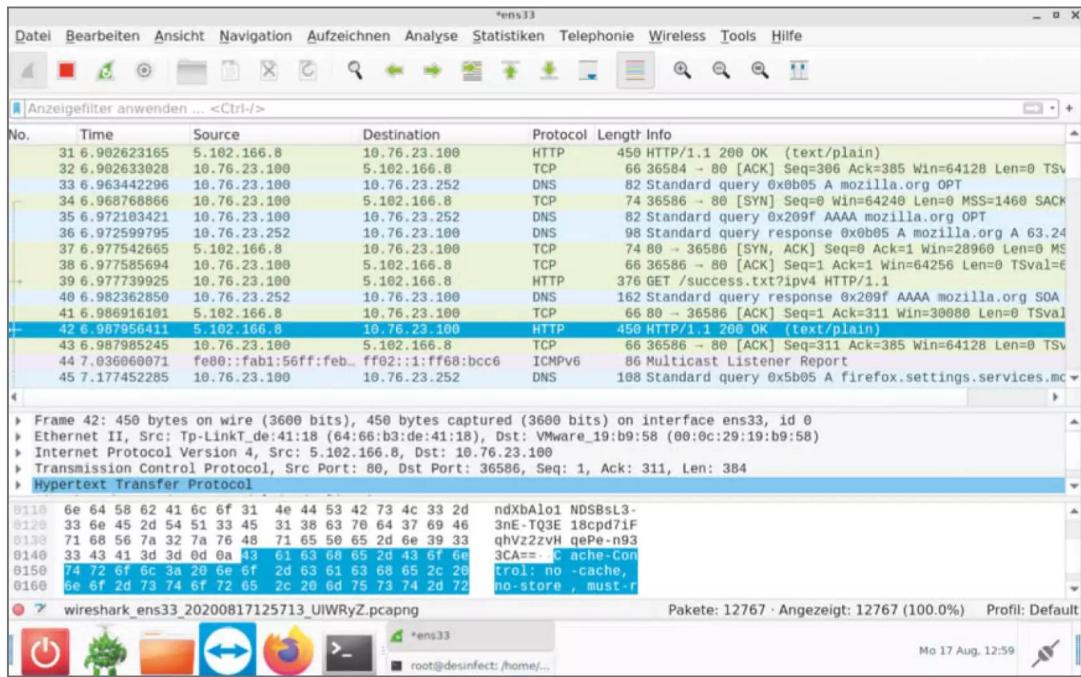
Kommt als Antwort „Unknown Host“, so klappt die Namensauflösung nicht. Prüfen Sie, welchen „Primary DNS“ Desinfect für die „Aktive Netzwerkverbindung“ anzeigt. Erhalten Sie eine Antwort, wenn Sie diese IP-Adresse mit **ping 192.168.2.234** ansprechen? (Ersetzen Sie die Adresse durch die Ihres DNS-Servers.) Wenn nach einiger Zeit „Destination Host Unreachable“ erscheint, sind Sie wahrscheinlich auf der richtigen Spur.

Antwortet der DNS-Server nicht, probieren Sie einen öffentlichen DNS-Server wie den von Google aus. Wenn Sie ihn mit **ping 8.8.8.8** ansprechen, sollte eine Antwort kommen. Tragen Sie diesen Server er-

satzweise in die Konfiguration von Desinfect ein. Jetzt sollte auch **ping heise.de** die erwarteten Antworten liefern und Surfen möglich sein.

Wenn Ihre Netzwerkanbindung selbst gestört ist, wird all das nicht fruchten. Versuchen Sie direkt die IP-Adresse unseres Servers oder die des Google-Namenservers anzusprechen: 193.99.144.80 oder 8.8.8.8. Kommt hier keine Antwort der Gegenseite, probieren Sie es mit der von Desinfect als „Vorgaberroute“ ausgegebenen Adresse. Das ist das Standard-Gateway Ihres Netzes, das alle Pakete weiterleiten soll – mithin der Router. Antwortet der nicht, müssen Sie sich seiner Konfiguration widmen.

Beachten Sie auch, dass viele Router und Provider von sich aus IPv6 aktivieren. Die so weit durchixer-



Ohne Monitoring-Port am Switch oder eine Fritzbox als Horchposten zeigt Wireshark nahezu ausschließlich den Desinfec't-eigenen Netzwerkverkehr. Um Konfigurationsprobleme im LAN oder WLAN zu erkennen, ist das oft schon genug.

zierten Beispiele stellen aber nur sicher, dass IPv4-Verkehr reibungslos läuft. Wenn in Ihrem Netz IPv6 aktiv ist, sollten Sie dieselben Schritte mit dem Pendant ping6 durchlaufen. Es kommt vor, dass Störungen im Netzwerk durch schlecht konfiguriertes IPv6 entstehen, etwa bei einem unzureichend eingerichteten Pi-Hole.

## Gehemmte Freigaben

Die Außenanbindung, die Sie mit den so weit gegebenen Hinweisen überprüfen können, sagt noch wenig über Verhältnisse im lokalen Netz aus. Klappt dort die Namensauflösung nicht, etwa beim Zugriff auf eine Freigabe, so hat das nichts zu tun mit dem DNS-Server des Providers, den Ihr Router befragt.

Die Server- und Freigabenamen von Windows-PCs werden in kleinen Netzen per Broadcast aufgelöst. Falsche Subnetzmasken garantieren Probleme. Was

helfen kann: akribisch die IP-Konfigurationen aller beteiligten Rechner daraufhin zu überprüfen, ob gemeinsame Informationen wie die Netzmasken identisch eingerichtet sind, und konsequent die Namen setzen, sodass auch der Router die beteiligten Geräte unter denselben Namen kennt.

Scheitern Zugriffe auf die Freigaben des NAS oder eines anderen Rechners, so kann Desinfec't eine zweite Meinung liefern. SMB-Zugriffe beherrscht es aus seinem Dateimanager heraus. Geben Sie in der Adresszeile den Namen des Servers und der Freigabe mit vorangestelltem SMB:// ein. Wenn das fehlschlägt, Probieren Sie es mit der IP-Adresse statt des Servernamens. Klappt der Zugriff mit Desinfec't, nicht jedoch mit Windows, müssen Sie dort nach den Ursachen fahnden. Eventuell hat sich in Windows ein falsches Passwort festgesetzt. Die zeigt cmdkey /list und cmdkey /delete tilgt sie gegebenenfalls.

# Fritzbox als Horchposten für Wireshark & Co.

AVM hat seinen Fritzboxen eine Funktion für den Paketmitschnitt spendiert. Die lässt sich leicht ansteuern, wenn man an den Namen oder die IP-Adresse der Box in der Adresszeile des Browser „support.lua“ anhängt, also dort fritz.box/support.lua eingibt. Nach dem Überprüfen des Passworts zeigt die Box eine lange Liste von Optionen an, die vor allem für den Hersteller im Supportfall nützlich sind. Unter „Paketmitschnitte“ gibt eine Fritzbox eine Tabelle von Schnittstellen aus, die sich belauschen lassen. Per Knopfdruck lässt sich ein solcher Mitschnitt starten und beenden. Er landet dann als Datei auf der Festplatte des PC. Die Daten haben das gängige PCAP-Format, das fast jeder Sniffer lesen kann, etwa Wireshark und tcpdump.

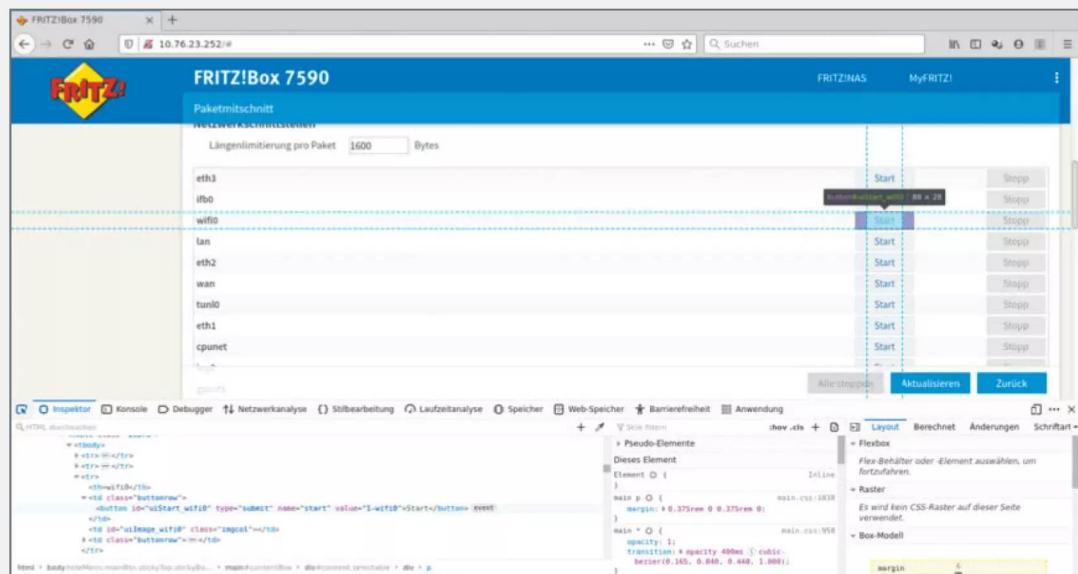
Das Shell-Skript fritzdump.sh automatisiert diese Handgriffe, indem es die Ausgaben direkt an ein Programm weiterleitet, das diese anzeigt – man muss also den Zwischenabschnitt über eine Datei nicht gehen. Das Skript stammt übrigens von den ntopng-Machern (siehe Kasten „ntopng verrät, was im Netzwerk abgeht“ auf der S. 64). Nach dem Herunterladen des Skripts und dem Setzen des Execute-Bits mit `chmod +x fritzdump.sh` müssen Sie im Skript die Adresse Ihrer Fritzbox und den Namen der Schnittstelle eintragen, an der

Sie lauschen wollen. Beim Aufruf erwartet das Skript als Parameter das Zugangspasswort Ihrer Fritzbox.

Am Ende des Skripts steht das Programm, das aufgerufen werden soll. Sie können das Programm (ntopng) zum Beispiel durch wireshark ersetzen. Löschen Sie dazu ntopng am Ende und schreiben Sie wireshark hin. Wenn Sie jetzt das Skript mit `./fritzdump.sh <Passwort>` starten (passendes Passwort vorausgesetzt), sollte sich Wireshark öffnen und bereits den von der Fritzbox gelieferten Paketmitschnitt live anzeigen. Wenn Sie währenddessen ein Browser-Fenster mit der Paketmitschnittseite der Fritzbox offen haben, sehen Sie dort, dass ein Mitschnitt läuft.

Diese Seite hilft auch dabei, den richtigen Namen der Netzwerkschnittstelle für Ihr Analysevorhaben zu finden. Aktivieren Sie einfach bei geöffneter Mitschnittseite die Entwicklerwerkzeuge im Browser, klicken Sie auf das Fadenkreuz und dann auf den Button der jeweiligen Netzwerkschnittstelle. Der Inspektor der Entwicklerkonsole zeigt dann in der hervorgehobenen Zeile den Namen der Schnittstelle als Wert in `value=""`. Experimentieren Sie gegebenenfalls, bis Sie die richtige Schnittstelle erwischt haben.

Fritzboxen bieten auf den Supportseiten ihrer Weboberfläche Funktionen, um Paketmitschnitte anzufertigen. Die lassen sich nicht nur speichern, sondern direkt weiterverarbeiten. Beim Herauspicken der Namen der richtigen Schnittstelle helfen die Entwicklerfunktionen des Browsers.



## Paketverlust

Unangenehme Fehler sind solche, die nur sporadisch auftreten. Ganz besonders lästig sind die beim Streamen, weil hier große Puffer im Spiel sind, die sogar eine Trennung der DSL-Verbindung überleben können, ohne dass Sie davon überhaupt Notiz nehmen. Schließen Sie in solchen Fällen zunächst technische Fehler aus.

Sehen Sie sich dazu in Desinfec't im Terminal mit `ifconfig` die Statistiken für die Netzwerkschnittstellen an. Die Zähler für Übertragungsfehler (Fehler, Verloren, Überläufe) sollten bei 0 stehen. Laufen die in kurzen Zeitabständen hoch, müssen Sie die Ursache dafür finden.

Das gleiche gilt dann, wenn die Schnittstelle häufig zwischen Betriebsmodi wechselt, etwa zwischen Halb- und Vollduplex- oder 10- und 100MBit/s-Betrieb umschaltet. Die letzten Zeilen solcher Kernel-Meldungen bekommen Sie mit `dmesg | tail` zu sehen.

Bei drahtgebundenen Netzwerken ist ein vom Hamster angefressenes oder vom Bürostuhl plattgewalztes Patch-Kabel dann oft die Ursache. Tauschen Sie es aus. Wechseln Sie Netzwerkdosen und Switchports nacheinander durch, bis Sie die matschige Komponente isoliert haben. Markieren Sie offenbar defekte Dosen oder Ports und führen Sie kaputte Kabel sofort dem Recycling zu.

Auch Funknetzwerke sind von Haustieren bedroht, jedenfalls wärmt im Winter die Katze eines Kollegen ihren Pelz auf dem Router und schaltete dabei das WLAN ab. Normalerweise aber sind andere WLANs der größere Feind: Wenn mehrere WLANs denselben Frequenzbereich nutzen, bleibt für jedes einzelne entsprechend weniger Bandbreite über. Die Automatiken der Router zum Finden eines wenig frequentierten oder besser noch freien Kanals funktionieren meist gut. In Problemfällen ergibt es Sinn, den Router fest auf einen Kanal zu konfigurieren. Packen Sie Ihr WLAN dorthin, wo der Nachbar funkt, der selten daheim ist.

Einen Überblick, welches Netz auf welchem Kanal mit welcher Stärke aktiv ist, verschaffen Sie sich unter Desinfec't zum Beispiel mit `LinSSID`. Das Programm müssen Sie nachinstallieren: Entfernen Sie die Kommentarzeichen (#) am Anfang der Zeilen in `/etc/apt/sources.list` und lassen Sie die Paketlisten aktualisieren: `apt-get update`. Jetzt können Sie mit `apt-get install linssid` das Paket für die WLAN-Anzeige-Software einrichten und mit `linssid` aufrufen.

## Profi-Werkzeuge

Desinfec't hat viele Werkzeuge an Bord, die auch passionierte Netzwerkbetreuer schätzen. Mit `curl` kann man Web-Dienste und -Seiten ansteuern, um die Erreichbarkeit zu prüfen, Status-Codes abzufragen oder auch nur um Dateien herunterzuladen. `curl` beherrscht alle wesentlichen Zugriffstechniken (POST, GET), kann mit Zertifikaten umgehen und liefert detaillierte Rückmeldungen. Ein paar Beispiele:

`curl -I heise.de` gibt normalerweise nicht sichtbare Informationen aus dem Header bei HTTP-Zugriffen aus. `curl -O example.com/test.zip` würde die Datei `test.zip` von `example.com` herunterladen (`example.com` ist nur ein Beispiel). `curl -X POST https://example.com/example.cgi?example=test` würde per Post-Request Daten an ein CGI-Skript auf dem Server senden.

Weniger spezialisiert, dafür aber universeller ist `netcat` (`nc`). Es kann sowohl als Client als auch als Server fungieren, verbindet nahezu beliebige Ports per TCP oder UDP und kann sogar Unix-Domain-Sockets verwenden. Will man etwa die Erreichbarkeit eines Mail-Servers prüfen, so kann man mit `nc <servername> 25` seinen TCP-Port 25 ansprechen.

Mit der zusätzlichen Option `-1` können Sie `netcat` anwenden, auf dem lokalen PC den TCP-Port 25 zu öffnen, sodass er Verbindungen von außen entgegennimmt. Wenn Sie dann mit `netcat` auf einem entfernten Host darauf zugreifen, wissen Sie, dass das untersuchte Netzwerk für Zugriffe über Port 25 in dieser Richtung durchlässig ist.

Der Netzwerkschnüffler `Wireshark` ist ebenfalls an Bord. Üblicherweise zeigt der nur den eigenen Verkehr und an alle Knoten im Netz adressierten Pakete an. Für die Fehlersuche auf dem eigenen System ist das ausreichend. Wer mehr sehen möchte, braucht in einem drahtgebundenen Netz einen Switch-Port, der allen Netzwerkverkehr oder den anderer Ports auf den Desinfec't-PC spiegelt. In einem – wie heute üblich verschlüsselten – Funknetz sind zusätzliche Verrenkungen nötig.

Wer eine Fritzbox als Router verwendet, kann hingegen bequem schnüffeln: Die Web-Oberfläche von AVMs Routern bietet Funktionen für Paketmitschnitte an. Die kann Desinfec't einsammeln und als Eingaben an `Wireshark` weitergeben. Das geht ebenso im Zusammenspiel mit anderen Netzwerkwerkzeugen, mehr dazu im Kasten auf Seite 64. Schnüffeln muss nicht unbedingt heißen, die Unterhaltung von Geräten zu debuggen, sondern kann auch helfen, statistische Daten zu sammeln und aufzubereiten, um unkooperative Mitbenutzer zu finden. (ps) 

Skripte, Software  
[ct.de/wvvt](http://ct.de/wvvt)

# IMPRESSUM

## Redaktion

Postfach 61 04 07, 30604 Hannover  
Karl-Wiechert-Allee 10, 30625 Hannover  
Telefon: 05 11/53 52-300  
Telefax: 05 11/53 52-417  
Internet: [www.heise.de](http://www.heise.de)

**Leserbriefe und Fragen zum Heft:**  
[sonderhefte@ct.de](mailto:sonderhefte@ct.de)

Die E-Mail-Adressen der Redakteure haben die Form xx@ct.de oder xxx@ct.de. Setzen Sie statt „xx“ oder „xxx“ bitte das Redakteurs-Kürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

**Chefredakteur:** Thorsten Beeck (tbe)  
(verantwortlich für den Textteil)

**Konzeption:** Dennis Schirrmacher (des)

**Koordination:** Jobst Kehrhahn (Leitung, keh),  
Pia Ehrhardt (piae), Angela Meyer (anm)

**Redaktion:** Mirko Dölle (mid), Dennis Schirrmacher (des),  
Peter Siering (ps)

**Mitarbeiter dieser Ausgabe:** Thorsten Leemhuis,  
Mattias Schlenker

**Assistenz:** Thorsten Leemhuis, Mattias Schlenker

**DTP-Produktion:** Dörte Bluhm, Lara Bögner,  
Beatrix Dedeck, Madlen Grunert, Lisa Hemmerling,  
Cathrin Kapell, Steffi Martens, Marei Stade,  
Matthias Timm, Christiane Tümmeler, Ninett Wagner

**Digitale Produktion:** Christine Kreye (Itg.),  
Kevin Harte, Thomas Kaltenschmidt, Martin Kreft,  
Pascal Wissner

**Illustration:** Steffi Martens, Ninett Wagner,  
[www.flaticon.com](http://www.flaticon.com), [www.freepik.com](http://www.freepik.com), [www.stock.adobe.com](http://www.stock.adobe.com)

**Titel:** Steffi Martens, [www.freepik.com](http://www.freepik.com)

## Verlag

Heise Medien GmbH & Co. KG  
Postfach 61 04 07, 30604 Hannover  
Karl-Wiechert-Allee 10, 30625 Hannover  
Telefon: 05 11/53 52-0  
Telefax: 05 11/53 52-129  
Internet: [www.heise.de](http://www.heise.de)

**Herausgeber:** Christian Heise, Ansgar Heise, Christian Persson

**Geschäftsführer:** Ansgar Heise, Beate Gerold

**Mitglieder der Geschäftsleitung:** Jörg Mühle, Falko Ossmann

**Anzeigenleitung:** Michael Hanke (-167)  
(verantwortlich für den Anzeigenteil),  
[www.heise.de/mediadaten/ct](http://www.heise.de/mediadaten/ct)

**Anzeigenverkauf:** Verlagsbüro ID GmbH & Co. KG,  
Tel.: 05 11/61 65 95-0, [www.verlagsbuero-id.de](http://www.verlagsbuero-id.de)

**Leiter Vertrieb und Marketing:** André Lux (-299)

**Service Sonderdrucke:** Julia Conrades (-156)

**Druck:** Firmengruppe APPL Druck GmbH & Co. KG,  
Senefelder Str. 3-11, 86650 Wemding

**Vertrieb Einzelverkauf:**  
DMV DER MEDIENVERTRIEB GmbH & Co. KG  
Meßberg 1  
20086 Hamburg  
Tel.: 040/3019 1800, Fax: 040/3019 145 1815  
E-Mail: [info@dermedienvertrieb.de](mailto:info@dermedienvertrieb.de)  
Internet: [dermedienvertrieb.de](http://dermedienvertrieb.de)

**Einzelpreis:** € 14,90; Schweiz CHF 27,90;  
Österreich € 16,40; Luxemburg € 17,10

**Erstverkaufstag:** 22.09.2023

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung des Verlages in irgendeiner Form reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Die Nutzung der Programme, Schaltpläne und gedruckten Schaltungen ist nur zum Zweck der Fortbildung und zum persönlichen Gebrauch des Lesers gestattet.

Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Honorierte Arbeiten gehen in das Verfügungsberecht des Verlages über. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes.

Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Hergestellt und produziert mit Xpublisher:  
[www.xpublisher.com](http://www.xpublisher.com)

Printed in Germany.

Alle Rechte vorbehalten.

© Copyright 2023 by  
Heise Medien GmbH & Co. KG



# Desinfec't 2023/24 vom Server booten

Nie mehr nach Desinfec't-USB-Sticks suchen, stattdessen den Virenjäger bequem aus dem Netzwerk starten? Ein Bootserver mit dem Sicherheitstool fürs Heim- oder Büronetz macht's möglich. Das funktioniert sogar mit einem Raspberry Pi.

Von **Mattias Schlenker**

Nicht nur für Admins in Unternehmen, auch im Privathaushalt ist ein eigener Bootserver mit Desinfec't praktisch: Damit überprüfen Sie etwa Notebooks von Schulkindern bequem auf Viren, ohne nach einem Desinfec't-Stick kramen zu müssen. Zu scannende Clients müssen lediglich über eine aktive Netzwerkverbindung verfügen und schon können sie das Sicherheitstool direkt über das Netzwerk starten.

Für das Einrichten benötigt man nur einen als Bootserver konfigurierten und dauerhaft eingeschalteten Computer, von dem Clients im Netzwerk, die man scannen will, die 64-Bit-Version von Desinfec't beziehen. Realisieren lässt sich das Ganze über Pre-boot Execution Environment (PXE).

Unter PXE versteht man ein Bündel von Verfahren, mit denen ein PC Startdateien statt von einer lokalen Festplatte aus dem Netzwerk lädt. So kann ein Server beispielsweise eine vollständige Betriebssystemumgebung bereitstellen, an der sich ein Client bedient. Heutzutage beherrschen im Grunde alle On-board-Ethernet-Karten PXE.

## Drei Netzwerkserver

Damit Desinfec't aus dem Netzwerk startet, benötigt man drei Serverdienste: einen DHCP-Server zur Konfiguration von unter anderem IP-Adressen, einen TFTP-Server zum Übertragen der Bootdateien und einen NFS-Server zum Bereitstellen der Systemdateien. Die Dateien für die Einrichtung finden Sie im Archiv, welches Sie über den Download-Link am Ende des Artikels herunterladen können. Doch Vorsicht: Das Einrichten eines DHCP-Servers in einem bestehenden Netzwerk ist nur etwas für Leute, die wissen, was sie tun. Alle drei Server können auf einem Linux-Computer im lokalen Netz laufen. Man kann sie aber auch auf mehrere Geräte verteilen.

In diesem Artikel konzentrieren wir uns auf das Setup mit Debian-basierten Systemen, wie Raspberry Pi OS und Ubuntu. Kommt als Bootserver ein Raspberry Pi zum Einsatz, müssen Sie ein paar Dinge beachten: Im Grunde reicht sogar ein Raspi 1 aus, um Desinfec't im Netzwerk an Clients zu verteilen. Mit dieser Version des Einplatinencomputers gestaltet sich das Starten des Bootservers jedoch als sehr langwierig und Desinfec't wird nur zäh an Clients ausgeliefert. Damit beides schneller vorstatten geht, sollte ein Raspi 3 in Kombination mit einer flinken SD-Karte zum Einsatz kommen. Falls Sie einen OpenWrt-Router zum Bootserver machen wollen, müssen Sie die DHCP- und TFTP-Konfigurationseinstellungen für den dort verwendeten Serverdienst dnsmasq konvertieren (siehe [ct.de/wmkg](http://ct.de/wmkg)).

Für ein besseres Verständnis empfehlen wir aber, zunächst unsere Musterkonfiguration auf Computern mit Ubuntu, Debian oder Raspberry Pi OS nachzustellen und erst dann die Server auf beispielsweise NAS und Router zu verteilen. Unter [ct.de/wmkg](http://ct.de/wmkg) finden Sie einen Link, wie man zum Beispiel auf einem mit OpenWrt laufenden DSL-Router und einem 4-GByte-Speicherstick eine PXE-Bootumgebung aufsetzt, die Desinfec't serviert.

Am Anfang steht die Einrichtung des DHCP-Servers. Die folgende Konfiguration ist für das in Debian enthaltene `isc-dhcp-server`-Paket geschrieben. Zunächst müssen Sie in der Datei `/etc/default/isc-dhcp-server` die Netzwerkinterfaces eintragen, an denen der Server lauschen soll. Das sieht beispielsweise wie folgt aus:

```
INTERFACES="enp2s0"
```

Danach bearbeiten Sie die Konfigurationsdatei `/etc/dhcp/dhcpd.conf`:

```
ddns-update-style none;
option domain-name "meinnetz.test";
option domain-name-servers 10.76.23.252;
option routers 10.76.23.252;
default-lease-time 600;
max-lease-time 7200;
authoritative;
subnet 10.76.23.0 {
  netmask 255.255.255.0 {
    range 10.76.23.80 10.76.23.220;
    use-host-decl-names on;
    option subnet-mask 255.255.255.0;
    option broadcast-address 10.76.23.255;
    next-server 10.76.23.250;
  }
  class "pxeclient" {
    match if substring (option vendor-class-identifier, 0, 9) = "PXEClient";
    if substring (option vendor-class-identifier, 15, 5) = "00000" {
      # BIOS client
      filename "pxelinux.0";
    } else {
      # default to EFI 64 bit
      filename "bootx64.efi";
    }
  }
}
```

Damit setzen Sie einen DHCP-Server auf, der das Netz 10.76.23.0/24 bedient; der Bootserver hat die Adresse 10.76.23.250. Gateway und Nameserver sind mit 10.76.23.252 ansprechbar. Der Parameter `0` sorgt dafür, dass dieser DHCP-Server maßgeblich für dieses Netzwerk ist.

Starten Sie jetzt den DHCP-Server neu:

```
service isc-dhcp-server restart
```

Nun kann man prüfen, ob der DHCP-Server via PXE-Boot sichtbar ist. Stellen Sie dafür beim PC, auf dem Desinfec't aus dem Netzwerk starten soll, die Bootreihenfolge auf „Network Boot“. Das gelingt temporär über das BIOS-Bootmenü oder dauerhaft im BIOS – oft heißt der Punkt mit dieser Option „Startup“. Läuft der DHCP-Server korrekt, sollten nun auf dem Client beim Booten die MAC-Adresse, die UUID des BIOS und die vom DHCP-Server erhaltenen Para-

meter zu sehen sein. Der Computer versucht nun per TFTP die Datei pxelinux.0 vom Server 10.76.23.250 zu laden. Da aber noch kein TFTP-Server läuft, bricht der Bootvorgang nach einigen Minuten ab.

## TFTP für den Bootloader

Für den TFTP-Server kommt der „Anvins TFTP-Server“ aus dem zu installierenden Paket tftpd-hpa zum Einsatz. Geben Sie dafür `apt install tftpd-hpa` ein. Die Konfiguration gelingt über die Datei `/etc/default/tftpd-hpa`. Passen Sie die IP-Adressen an die in Ihrem Netz verwendeten an und ändern Sie gegebenenfalls den Pfad des Ordners mit den Bootdateien:

```
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/opt/tftpboot"
TFTP_ADDRESS=":69"
TFTP_OPTIONS="--secure"
```

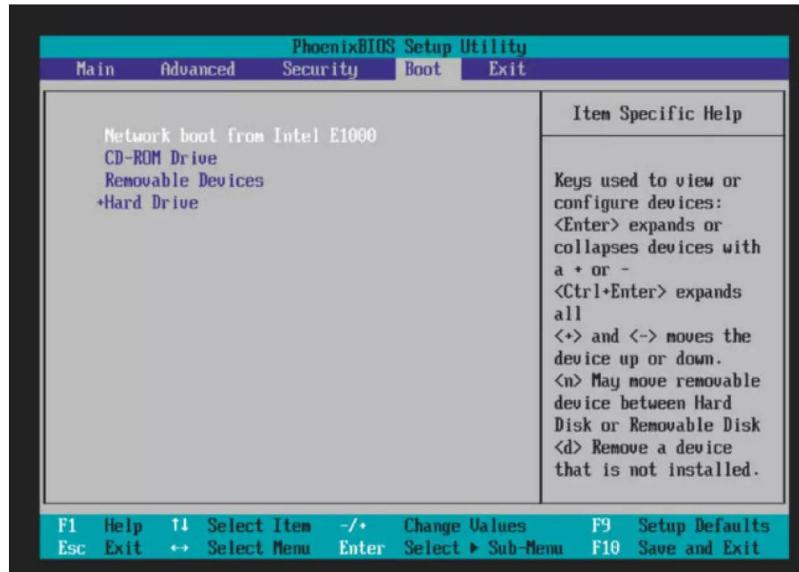
In diesem Schritt befüllen Sie das Bootverzeichnis `/opt/tftpboot`. Alle benötigten Dateien finden Sie im `tftpboot.tgz`-Archiv. Sie können diese einfach in Ihren Ordner `/opt/tftpboot` kopieren. Wenn Sie gerade kein Desinfec't 2023/24 zur Hand haben, können Sie die Bootdateien auch herunterladen (siehe ct.de/wmkg). Wenn Sie mit UEFI-Clients arbeiten, müssen Sie das

Paket zwingend herunterladen, da die benötigten Dateien im ISO-Image fehlen.

Zur Erläuterung: Ein BIOS-Client wird am Vendor-String „00000“ erkannt und erhält die Bootdatei „pxelinux.cfg“, bei allen anderen Clients wird angenommen, dass es sich um einen UEFI64-Client handelt, diese bekommen das EFI-Modul „bootx64.efi“. Falls Sie in Ihrem Netzwerk exotische Architekturen wie SPARC, Itanium oder alte UEFI32-Nettops über Netz booten, ist die Differenzierung der Klasse „pxe-client“ detaillierter vorzunehmen. Der Client holt sich im Falle des BIOS-Clients die COM32-Module und die Konfigurationsdatei `pxelinux.cfg/default` via TFTP vom Server. Sie können nun erste Tests mit einer minimalen Version fahren:

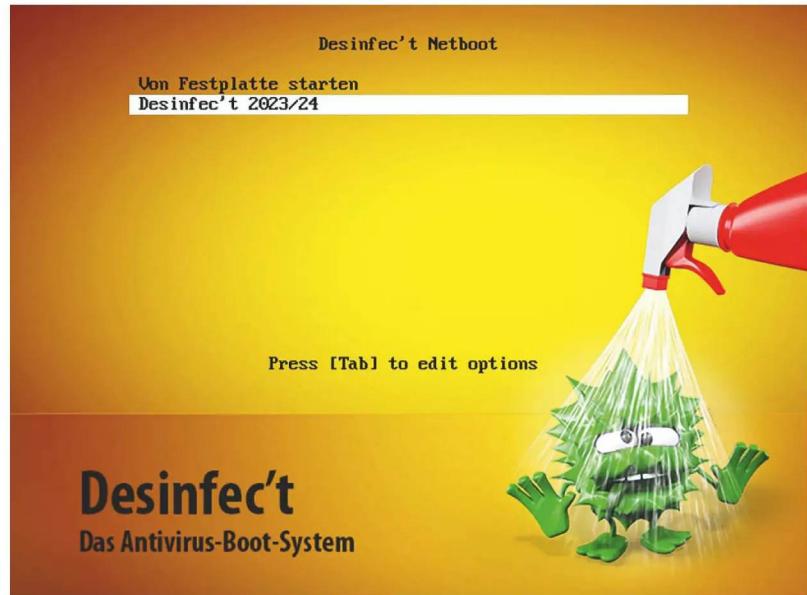
```
DEFAULT /menu.c32
TIMEOUT 300
MENU TITLE Desinfec't Netboot
LABEL local
MENU LABEL Von Festplatte starten
MENU DEFAULT
LOCALBOOT 01
```

Im Falle von UEFI-GRUB gilt die Konfigurationsdatei `grub/grub.cfg` mit der folgenden minimalen Konfiguration:



**Im BIOS-Setup können Sie PXE als bevorzugte Bootmethode dauerhaft aktivieren. Ist mal kein Server im Netz aktiv, startet nach einigen Sekunden das auf der Festplatte installierte System.**

Neben verschiedenen Desinfec't-Versionen kann man über ein modifiziertes Netboot-Menü auch andere Linux-Distributionen via PXE starten.



```
set default=0
set timeout=10
menuentry "Start von Festplatte" {
    exit
}
```

In beiden Fällen wird der Computer lediglich angewiesen, die PXE-Boot-Umgebung nach 10 Sekunden zu verlassen und mit dem nächsten Bootmedium in der festgelegten Reihenfolge fortzufahren. Sind die Konfigurationsdateien abgelegt, können Sie Ihre Clients bereits testen: Sobald der PXE-fähige Client Antwort vom DHCP-Server erhalten hat, lädt er das Menü.

### Desinfec't-Bootdateien ablegen

Kopieren Sie nun noch Kernel (vmlinuz) und Ramdisk (initrd.lz) aus dem Ordner /casper im Desinfec't-ISO-Image in den TFTP-Boot-Ordner und passen Sie die IP-Adressen in den Konfigurationsdateien im Archiv tftpboot.tgz an. Mit dieser Änderung können Sie in die initiale Ramdisk booten.

Falls Sie planen, TFTP-Boot langfristig auch fürs Deployment von Images oder zur Installation von Linux-Servern einzusetzen, haben Sie die Möglichkeit, in der DHCP-Konfiguration pro MAC-Adresse zu bestimmen, ob und wenn ja welche Bootdatei verwendet werden soll. Mit der Option, die Bootdatei per MAC-Adresse zu überschreiben, booten Sie auch exotische Hardware wie ARM SBC mit uBoot, alte SPARC-Maschinen oder PowerPC-Macs ohne Konflikte übers Netz.

Der Bootloader PXELINUX erlaubt Konfigurationsdateien für MAC- oder IP-Adressen, die vor „default“ gesucht werden, Details zeigt das Syslinux-Wiki (siehe ct.de/wmkg). Im Falle von GRUB empfehlen viele Tutorials, während des Bootvorgangs auf HTTP zu wechseln, dann kann ein Skript auf dem Webserver anhand der IP-Adresse bestimmen, welche Konfiguration ausgeliefert wird.

### Der NFS-Server

Nun installieren Sie das Paket nfs-kernel-server und setzen damit den NFS-Server auf. Die Konfiguration

# Visit <https://freefordownload.net/> for more!

geschieht in der Datei `/etc/exports`. An dieser Stelle müssen Sie folgende Zeile hinzufügen:

```
/opt/nfsboot/desinfect202324  ↵
↳10.76.23.0/24(ro,insecure, ↵
↳no_subtree_check,async, ↵
↳no_root_squash)
```

Damit stellt der Server den Ordner nur lesbar für das Netz 10.76.23.0/24 zur Verfügung. Die restlichen Optionen dienen der Performance und sind im Read-only-Modus gefahrlos nutzbar. Jetzt müssen Sie noch mit den folgenden Befehlen den Ordner mit dem Inhalt des inneren Desinfec't-ISOs befüllen:

```
mkdir -p /opt/nfsboot/desinfect202324
mkdir /tmp/desinfect202324
mount -o loop /tmp/desinfect202324- ↵
↳amd64.iso /tmp/desinfect202324
rsync -avHP /tmp/desinfect202324/ ↵
↳/opt/nfsboot/desinfect202324/
umount /tmp/desinfect202324
```

Starten Sie jetzt den NFS-Server neu:

```
service nfs-kernel-server restart
```

Anschließend können Sie Ihren PXE-Client resetten und Desinfec't starten.

## Signaturen speichern

Praktischerweise bringt Desinfec't 2023/24 die Möglichkeit mit, aktualisierte Signaturen der Virenscanner auf einem NFS-Share-Server zu speichern. Hierfür legen Sie einen leeren Export-Ordner an, der schreibbar freigegeben ist und eine leere Datei namens „`desinfect202324`“ enthält:

```
mkdir -p /mnt/archiv/202324
↳desinfect-signatures touch /mnt/archiv/desinfect- ↵
↳signatures/.desinfect202324
```

Dieser Ordner enthält den folgenden Eintrag in der Konfigurationsdatei `/etc/exports`:

```
/mnt/archiv/desinfect-signatures  ↵
↳10.76.23.0/24(rw,no_subtree_ ↵
↳check,no_root_squash)
```

Anschließend ergänzen Sie die PXELINUX-Konfiguration um den Parameter `nfssigs`:

```
nfssigs=10.76.23.250:/mnt/archiv/ ↵
↳desinfect-signatures
```

Bei der ersten Signaturaktualisierung wird dieser Ordner dann eingebunden und befüllt. Der Systemmonitor von Desinfec't zeigt dies mit „Signaturen auf NFS“ an. Bitte achten Sie darauf, dass zu keiner Zeit zwei aus dem Netz gebootete Clients gleichzeitig Signaturen aktualisieren dürfen. Wollen Sie mehrere Clients scannen, starten Sie zunächst einen, auf dem Sie das komplette Signaturupdate durchführen. Ist das geschehen, fahren Sie die anderen Clients hoch und starten Sie dort nach und nach den Virenscan mit ein paar Minuten Abstand.

Wenn Sie Desinfec't 2023/24 auf einem Btrfs-Stick mit Änderungen versehen haben, können Sie das modifizierte Rootverzeichnis der Btrfs-Partition in den Ordner `casper/filesystem.dir/` des exportierten Desinfec't kopieren (`rsync -avHP --delete-after quelle/ ziel/`) und anschließend das komprimierte Dateisystem `casper/filesystem.squashfs` einfach löschen. Beim Netzwerkboot wird nun dieser Ordner als Root-Dateisystem genommen, spätere Anpassungen wie der Austausch von Grafiken oder Anpassungen der Starter auf dem Desktop (`/etc/skel/Desktop`) sind dann mit geringem Aufwand auf dem Server möglich.

## Debugging

Falls mal etwas nicht funktioniert, schauen Sie noch einmal ganz genau hin: Mit dieser Schritt-für-Schritt-Anleitung sollten Konfigurationsprobleme schnell auffallen. Zusätzlich können sich erfahrene Linuxer beispielsweise mit einem TFTP-Client auf die Suche nach falsch gesetzten Berechtigungen für Dateien machen, die man per TFTP übertragen will. Problemen beim NFS-Mount kann man in der BusyBox-Shell eines unvollständig gestarteten Desinfec't auf den Grund gehen, beispielsweise indem man das Share manuell einbindet und dabei auf Fehlerausgaben achtet:

```
mount -t nfs server://share /cdrom
```

Klappt der Mount ohne Fehler, prüfen Sie, ob das richtige Verzeichnis exportiert wurde. Der Inhalt von `/cdrom` muss exakt wie bei einem von DVD gebooteten Desinfec't aussehen. Läuft alles, kann man die Optik noch etwas schicker machen: Im Syslinux-Wiki finden Sie viele Hinweise, um das PXE-Bootmenü aufzuhübschen (siehe [ct.de/wmkg](http://ct.de/wmkg)). (des) 

**Bootloader, PXE-Bootmenü aufhübschen, PXE-Bootumgebung auf DSL-Router**  
[ct.de/wmkg](http://ct.de/wmkg)

# JAVA 21

Die Heise-Konferenz zur neuen LTS-Version

**4. Oktober 2023 – Online**

- Bessere Nebenläufigkeit mit Virtual Threads, Structured Concurrency und Scoped Values
- Pattern Matching for Switch ist finalisiert
- Foreign Functions & Memory API
- Wie finden neue Features ihren Weg ins OpenJDK?
- Was bedeutet das LTS-Release für Projekte?

**[java.bettercode.eu](http://java.bettercode.eu)**

Workshop zu Spring Security am 29. September 2023

Veranstalter



# ICH WARTE NICHT AUF UPDATES. ICH PROGRAMMIERE SIE.

**40%**  
Rabatt!



## c't MINIABO PLUS AUF EINEN BLICK:

- 6 Ausgaben als Heft, digital in der App, im Browser und als PDF
- Inklusive Geschenk nach Wahl
- Zugriff auf das Artikel-Archiv
- Im Abo weniger zahlen und mehr lesen

Jetzt bestellen:  
[ct.de/angebotplus](http://ct.de/angebotplus)

