



Desinfec't

Das Rettungssystem bei Virenbefall

NEUE
VERSION
2021/22

Windows-PCs untersuchen und säubern

Jetzt mit verbesserter Hardware-Kompatibilität

Viren jagen, Daten retten, Fernhilfe leisten

Auf DVD & als Download für USB-Sticks



facebook.com/ctspecials

€ 14,90

CH CHF 27,90

AT € 16,40

LUX € 17,10



Verteidigen Sie Ihre Privatsphäre!



shop.heise.de/ct-datenschuetzen

Heft + PDF
mit 29% Rabatt



shop.heise.de/ct-datenschuetzen

In dieser neuen Auflage des c't-Sonderhefts „Daten schützen“ erfahren Sie detailliert, wie Sie Ihre Privatsphäre vor Übergriffen bewahren können. **Darum geht's im Heft:**

- ▶ E-Mails und Telefone absichern
- ▶ Welche Messenger verschlüsseln wirksam
- ▶ Welche Angriffe bedrohen Ihre Privatsphäre on- und offline
- ▶ Passwörter für alle Systeme sicher verwalten
- ▶ Für Abonnenten portofrei
- ▶ Auch im Set mit Reiner SCT Authenticator zum Sonderpreis

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

Editorial

Liebe Leserin, lieber Leser,

derzeit sorgen abermals Windows-Lücken wie PrintNightmare, PetitPotam etc. für Furore und verängstigen Nutzer. Die Angst ist nicht ganz ungerechtfertigt, schließlich könnten Angreifer Computer in einigen Fällen direkt über das Internet attackieren und Schadcode ausführen. Im Anschluss gelten PCs in der Regel als vollständig kompromittiert.

Vor diesem Hintergrund ist es umso wichtiger, dass Sie Ihren Computer effektiv absichern, indem Sie aktuelle Sicherheitsupdates installieren und Virens Scanner nutzen. Außerdem sollten Sie nur nach sorgfältiger Überlegung auf Links in Mails klicken oder gar Dateianhänge öffnen. Auch wenn Mails noch so glaubhaft aussehen, kann sich daran ein Trojaner klammern, der nur darauf wartet, auf Ihren Computer zu springen.

Wenn es trotz aller Vorsicht aber doch mal geknallt hat, kann Desinfec't 2021/22 der Retter in der Not sein. Dank des Live-Systems scannen Sie ein inaktives Windows-System mit vier Viren-Scannern von Avast, Eset, F-Secure und Sophos auf Trojaner und machen diese unschädlich. Außerdem können Sie mit dem Sicherheitstool auf ein nicht mehr startendes Windows zugreifen und so wichtige Dateien auf einem Desinfec't-USB-Stick in Sicherheit bringen.

Das System kann aber noch mehr. Ob Sie Dateien retten müssen, einen Notfallarbeitsplatz brauchen oder Ihr Netzwerk Sie im Stich lässt: Desinfec't hilft Ihnen auch in diesen Notlagen.

Lassen Sie sich nicht austricksen und bleiben Sie und Ihr PC gesund!

Dennis Schirmmacher

Dennis Schirmmacher



Inhalt

6 Desinfec't 2021/22 Das Notfallsystem Desinfec't kann die letzte Rettung für ein verseuchtes Windows sein. Um Trojanern auf die Spur zu kommen und Windows zu säubern, lässt es vier Viren-Scanner von Avast, Eset, F-Secure und Sophos von der Leine.

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.

18 FAQ Desinfec't Antworten auf die häufigsten Fragen.

22 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.

28 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.

34 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.

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

44 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.

52 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.

60 Netzwerk-Troubleshooting Wenn auf dem regulären PC das Internet kaputt ist, verbindet Desinfec't Sie nicht nur mit dem Online-Banking. Angehende Experten finden obendrein Werkzeuge für die Analyse auch diffiziler Netzwerkprobleme nebst Tipps.

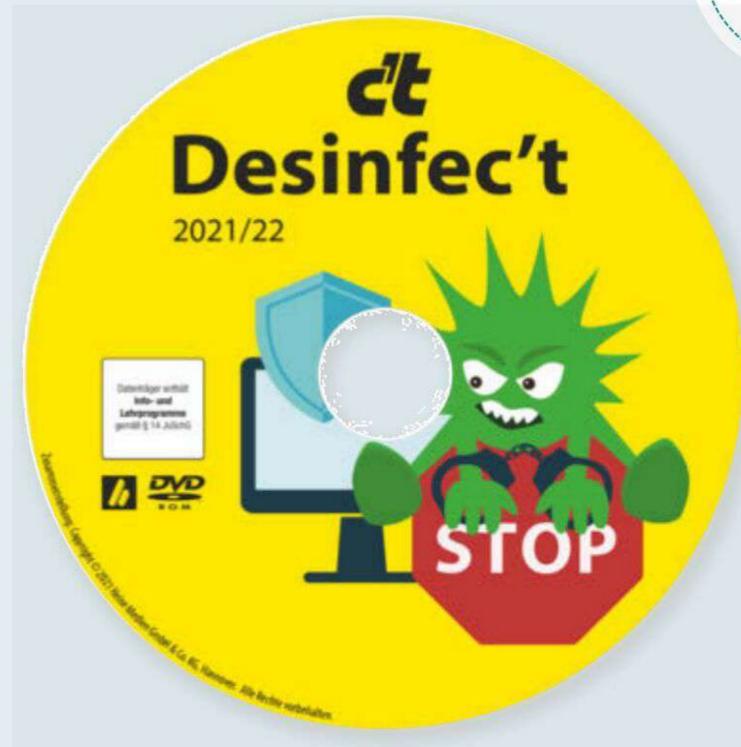
68 Booten aus dem Netz Das Notfallsystem startet nicht nur von DVD oder USB-Stick, sondern auch aus dem Netzwerk. Wir zeigen die nötigen Handgriffe.

Zum Heft

3 Editorial

74 Impressum

Auch als
Download!



Die DVD zum Heft

Mit dem c't-Sicherheits-Tool Desinfec't 2021/22 untersuchen Sie Windows aus sicherer Entfernung auf Trojaner. Das Live-System startet von DVD oder USB-Stick und schaut mit vier Viren-Scannern von Avast, Eset, F-Secure und Sophos 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 beseitigen. Dank diverser Tools bringen Sie mit Desinfec't zudem beispielsweise wichtige Daten in Sicherheit. Wer einen Computer ohne DVD-Laufwerk besitzt, kann das Notfall-System dennoch nutzen. Dafür laden Sie zuerst das ISO-Image von Desinfec't 2021/22 herunter. Anschließend erstellen Sie einen USB-Stick und starten es von dort. Weitere Informationen dazu finden Sie im Kasten auf Seite 13.



Das Anti-Viren-System für alle Fälle

Mit Desinfec't radieren selbst Laien Trojaner aus und bringen wichtige Dateien von Windows-PCs in Sicherheit. Das Sicherheitstool startet direkt von einem USB-Stick und erlaubt ein Jahr lang kostenlose Viren-Signaturupdates.

Von **Dennis Schirmmacher**

Als Familien-Admin ist das Leben manchmal nicht leicht: Als neulich am frühen Abend das Telefon klingelte und meine Mutter sagte, dass irgendetwas mit ihrem Laptop nicht stimmt, ahnte ich bereits Böses. „Da kamen so Meldungen, dass irgendein Trojaner oder so gefunden wurde. Das habe ich nicht verstanden und die Fenster einfach weggeklickt. Jetzt tauchen aber überall so komische Fenster mit Werbung für Erwachsene auf. Kannst du das reparieren?“ Nach einem Facepalm atme ich erst mal tief durch und sage: „Ja, kann ich. Aber wenn das nächste Mal solche Warnmeldungen auftauchen, nimm die bitte ernst und lies sie genau durch, bevor du sie vorschnell wegklickst. Jetzt lass Windows erst mal aus und starte den Desinfec't-Stick, wie ich es dir mal erklärt habe.“ Wenige Minuten später übernehme ich über die Fernwartungssoftware Teamviewer die Kontrolle über den Problem-PC und erfülle gefühlt zum hundertsten Mal meine Rolle als Familien-Admin.

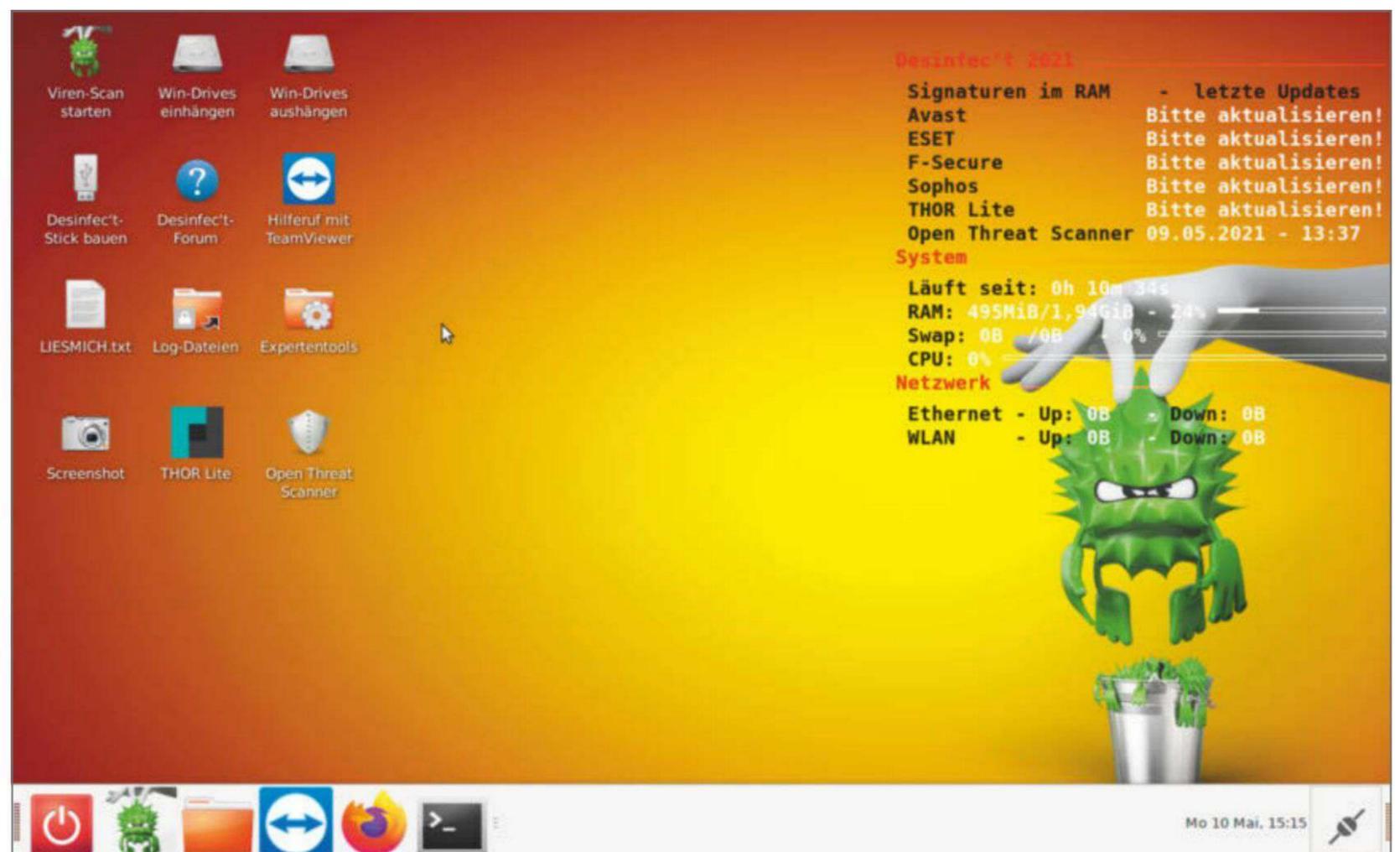
Das kann Desinfec't

Sie kennen Desinfec't bereits? Dann verschwenden Sie keine Zeit und springen direkt zum nächsten

Artikel, der die Nutzung des Systems für Einsteiger und Profis erklärt. Desinfec't 2021/22 richtet sich an Windows-Nutzer und kann Computer von Trojanern befreien. Dafür bringt das langjährig bewährte Sicherheitstool der c't-Redaktion vier Virens Scanner von Avast, Eset, F-Secure und Sophos mit. Damit die Scanner auch für aktuelle Schädlinge gewappnet sind, gibt es ein Jahr lang kostenlose Signaturupdates. Für Profis bringt es noch den Open-Threat-Scanner und das Threat-Hunting-Werkzeug Thor Lite mit, um Computer noch tiefergehender zu untersuchen.

Der Clou an Desinfec't ist, dass es keine Anwendung ist, die unter Windows läuft. Es bringt ein eigenes Live-Betriebssystem auf Linux-Basis mit, das Sie statt Windows direkt von einem USB-Stick booten. Das hat den großen Vorteil, dass Sie ein möglicherweise verseuchtes Windows nicht starten müssen, um es zu untersuchen. Das ist wichtig, da ein Trojaner in einem inaktiven Windows keinen weiteren Schaden anrichten kann. So schauen Sie mit dem Notfallsystem gewissermaßen aus sicherer Entfernung auf das womöglich verseuchte System. Bei der Virensuche müssen Sie keine Angst vor einer erneuten Trojaner-Infektion haben: Da Desinfec't auf

Dank aussagekräftiger Icons und verständlichen Menüs gehen selbst Computer-Neulinge mit Desinfec't auf Trojanerjagd.



Linux basiert, können Windows-Viren dem System nichts anhaben.

Virenjagd für jedermann

Live-System? Linux? Ich verstehe nur Bahnhof. Keine Angst: Von der Oberfläche orientiert sich das Sicherheitstool an Windows und dank verständlich beschrifteter Icons sollten selbst Computer-Laien einen Scan starten können. Wir haben bewusst viele Einstellungsmöglichkeiten und Linux-Funktionen herausgeworfen beziehungsweise versteckt, damit nichts vom eigentlichen Einsatzzweck von Desinfec't ablenkt.

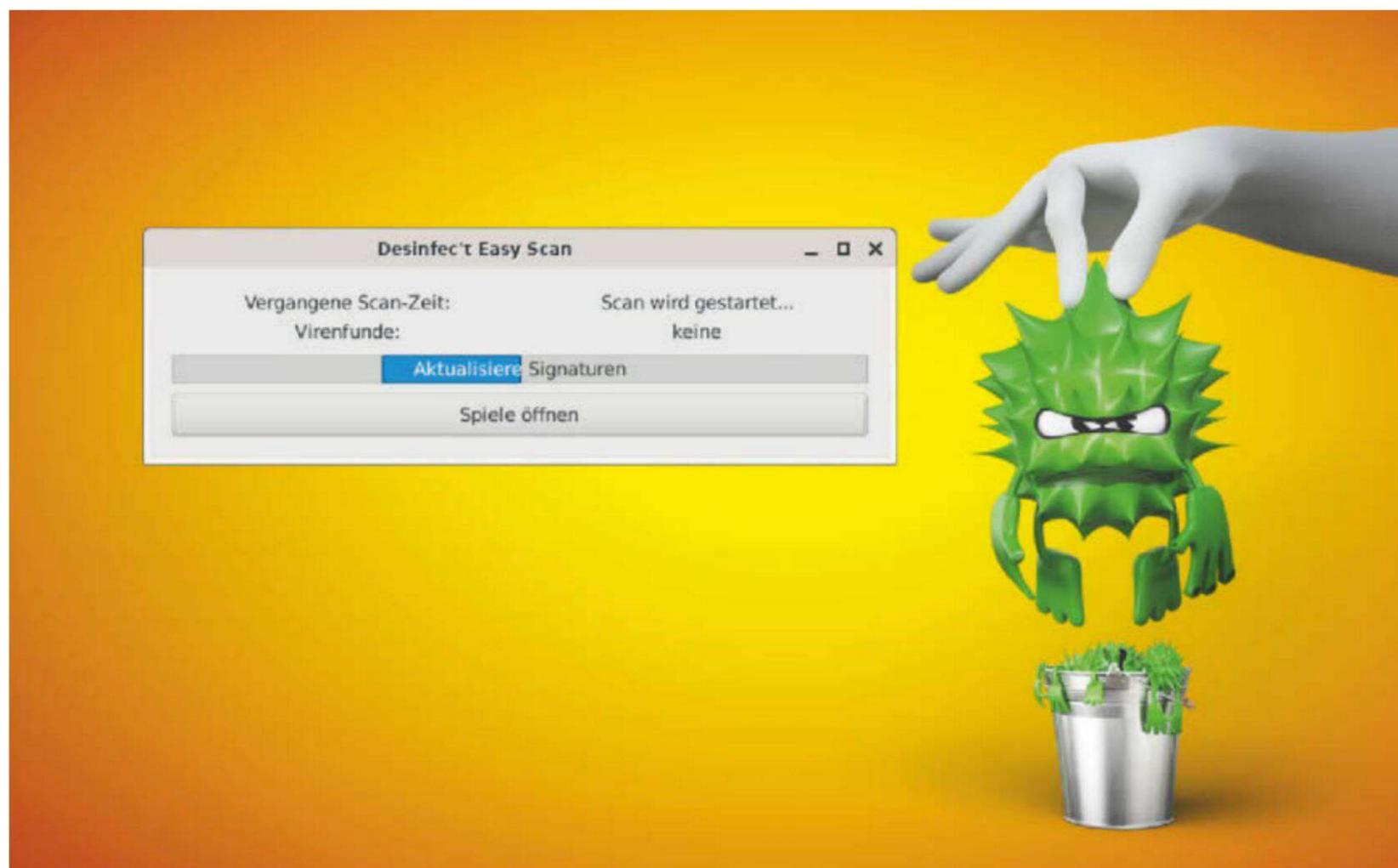
Wer trotzdem überfordert ist, startet einfach den Easy-Scan-Modus. Hier ist die Oberfläche noch weiter heruntergebrochen und das System startet automatisch mit der Trojanerjagd. Dabei schaut sich der Scanner von Avast auf der Windows-Festplatte um.

Doch auch im ausgewachsenen Desinfec't gibt es Hilfestellungen. So kann sich beispielsweise der Familien-Admin über die integrierte Fernwartungssoftware Teamviewer über das Internet auf Problem-PCs umschaun und einen Scan starten.

Voraussetzungen

Um Desinfec't auf einem USB-Stick zu installieren, benötigen Sie ein Exemplar mit mindestens 16 GByte Speicherplatz. Einen Stick erstellen Sie beispielsweise mit unserem Installer direkt unter Windows. Im Anschluss müssen Sie in den Bootoptionen Ihres Computers lediglich den Stick als Startmedium auswählen (siehe Kasten auf S. 14). Das Sicherheitstool läuft auch von einer DVD. Dafür brennen Sie das ISO-Image mit einem Laufwerk auf einen Dual-Layer-DVD-Rohling. Diese Betriebsart ist aber aus mehreren Gründen nicht zu empfehlen: Das System läuft davon wesentlich langsamer und es stockt öfter. Außerdem merkt es sich keine Daten. So müssen Sie etwa die Virensignaturen nach jedem Neustart erneut aktualisieren und Sie können keine Daten von verunfallten PCs in Sicherheit bringen. Von einem USB-Stick gestartet, merkt es sich die Signaturen und kopierten Dateien.

Damit das System läuft, benötigt Ihr Computer mindestens 4 GByte RAM. Wer sich für einen der schlankeren Scanner von Avast oder Eset entscheidet, kann Desinfec't auch auf Computern mit 2 GByte



Wer direkt loslegen will, wählt im Bootmenü den Easy Scan aus. Dieser startet direkt den Viren-Scanner von Avast, der die Windows-Installation untersucht.

RAM nutzen. Im folgenden Artikel finden Sie Tipps und Tricks, wenn Desinfec't nicht startet. In der Redaktion haben wir das System auf vielen älteren, aber auch auf aktuellen Computern erfolgreich getestet. Wir können aber nicht garantieren, dass es mit allen möglichen Hardwarekonfigurationen harmoniert. Gegebenenfalls startet es also auf manchen Computern gar nicht.

Trojaner ausfindig machen

Wenn Sie den Verdacht haben, dass Windows infiziert ist, genügt es für einen ersten Überblick, nur den vorausgewählten Scanner von Avast von der Leine zu lassen. Bei Bedarf können Sie im Scan-Assistenten aber auch alle Scanner auf die Jagd schicken. Standardmäßig prüfen die Scanner die gesamte Windows-Festplatte. Je nach Datenmenge und Leistungsfähigkeit Ihrer Hardware kann das eine ganze Nacht und länger dauern.

Bevor der Scan startet, aktualisiert Desinfec't mit einer aktiven Internetverbindung automatisch die Virensignaturen. Den Kontakt zum Internet stellen Sie per WLAN oder Kabel her. Trotz regelmäßiger Updates kann es vorkommen, dass ein Schädling so neu ist, dass es noch gar keine Signaturen gibt. Es gibt also keine hundertprozentige Sicherheit. Avast, Eset, F-Secure und Sophos bieten bis Oktober 2022 kostenlose Signaturupdates.

Nach dem Scan öffnet das System automatisch eine Ergebnisliste im integrierten Firefox-Browser. Dort finden Sie weitere Informationen zu den Funden. Aus der Liste heraus können Sie Schädlinge direkt aus dem Verkehr ziehen. Doch nicht immer geht die Welt gleich unter, wenn ein Scanner Alarm schlägt. Manchmal weisen legitime und harmlose Dateien Trojanern ähnliche Signaturen auf und werden fälschlicherweise als solche erkannt. Mit verschiedenen Bordmitteln von Desinfec't grenzen Sie Fehlalarme effektiv ein. So laden Sie mit nur wenigen Klicks womöglich gefährliche Dateien auf die Analyseplattform Virustotal hoch. Dort schauen noch mal mehr als 60 Onlinescanner auf die Datei und geben eine Einschätzung ab.

Dass Desinfec't etwas in Windows kaputt macht, ist sehr unwahrscheinlich: Standardmäßig hat das System nur lesenden Zugriff und kann somit nichts auf der Windows-Festplatte verändern. Wenn Sie beispielsweise einen Trojaner unschädlich machen wollen, müssen Sie den Schreibzugriff explizit erlauben.

Neben der Virenjagd können Sie Desinfec't als Notfallsystem nutzen, wenn Windows nicht mehr

startet. So ist es beispielsweise möglich, wichtige Dateien wie Lebensläufe oder private Fotos in Sicherheit zu bringen. Dafür kopieren Sie die Dateien einfach auf den USB-Stick, von dem das System läuft.

Futter für PC-Experten

Wer sich gut mit Computern beziehungsweise Linux auskennt, kann aus Desinfec't noch mehr herausholen. Um noch tiefer nach Schädlingen zu graben, bietet sich der Open-Threat-Scanner an. Ganz neu ist der Thor Lite Scanner. Damit ausgerüstet steigen PC-Profis tief in die Trojanersuche ein. Damit kann man besonders gut hoch entwickelte Schädlinge vom Kaliber Emotet aufspüren. Doch eins darf man nicht vergessen: Desinfec't kann zwar Trojaner unschädlich machen, wenn aber eine Malware bereits zugeschlagen hat, sind oft viele Systemeinstellungen manipuliert. Diese kann das Sicherheitstool nicht gerade biegen. In vielen Fällen bekommt man Systeme nur sauber, indem man Windows komplett löscht und neu installiert.

Desinfec't kann sogar noch mehr: Mit integrierten Expertentools können Sie verloren geglaubte Daten retten. Beispielsweise, wenn Sie versehentlich Fotos von einem USB-Stick gelöscht haben. Außerdem ist es möglich, Kopien von ganzen Festplatten anzufertigen.

Probleme lösen

Wenn das Notfallsystem nicht startet oder Sie andere Probleme mit dem System haben, lesen Sie bitte zuerst den folgenden Artikel. Dort finden Sie Anleitungen, wie man Desinfec't auf einen USB-Stick installiert und es davon startet. Außerdem gibt es Hinweise zu Startproblemen. Viele Probleme lassen sich meist mit relativ wenig Aufwand lösen. Das offizielle Desinfec't-Forum (siehe ct.de/wd3v) ist eine weitere Anlaufstelle, um Probleme aus der Welt zu schaffen. Dort ist neben Nutzern auch die Redaktion und der Desinfec't-Entwickler aktiv. Wer gar nicht weiter weiß, kann sich per Mail an die Redaktion wenden. Um Fehler im System kümmern wir uns in Form von Updates. Diese installieren sich automatisch, sobald das Sicherheitstool am Internet hängt.

Auf dem PC von meiner Mutter habe ich übrigens mehrere Trojaner gefunden und mich deswegen für die sicherste Alternative in Form einer kompletten Neuinstallation entschieden. Die wichtigsten Daten habe ich vorher auf einem Desinfec't-Stick in Sicherheit gebracht.

(des) **ct**

Desinfec't-Forum

ct.de/wd3v



Viren aufspüren und erledigen

Wenn in Windows sprichwörtlich der Wurm drin ist, können Sie diesen mit Desinfec't austreiben. Außerdem retten Sie mit dem Sicherheitstool wichtige Daten aus einem nicht mehr startenden Windows.

Von **Dennis Schirmacher**

Um für den Viren-Notfall gerüstet zu sein, sollten Sie das ISO-Image von Desinfec't am besten sofort herunterladen (siehe Kasten auf Seite 13) und auf einem USB-Stick installieren. Schließlich sollte ein womöglich infizierter Windows-PC ausgeschaltet bleiben, damit ein Schädling im laufenden System nicht noch mehr Unheil anrichten kann. Den Stick bewahren Sie in einer Schublade auf – das gibt ein sicheres Gefühl, falls doch mal was passiert.

USB-Stick erstellen

Damit das System von einem USB-Stick startet, müssen Sie es mit unseren Tools installieren. Bitte benutzen Sie ausschließlich die integrierten Installationsroutinen, damit das Sicherheitstool fehlerfrei läuft. Das bloße Kopieren der ISO-Datei auf einen Stick führt nicht zu einem lauffähigen System. Der Grund dafür ist, dass Desinfec't auf mehrere Partitionen aufbaut, die nur unsere Tools korrekt erzeugen.

Das ist neu in Desinfec't 2021/22

- Gratis Signatur-Updates bis Oktober 2022
- Optionaler Kernel 5.13
- Windows-Registry-Editor Fred 0.2

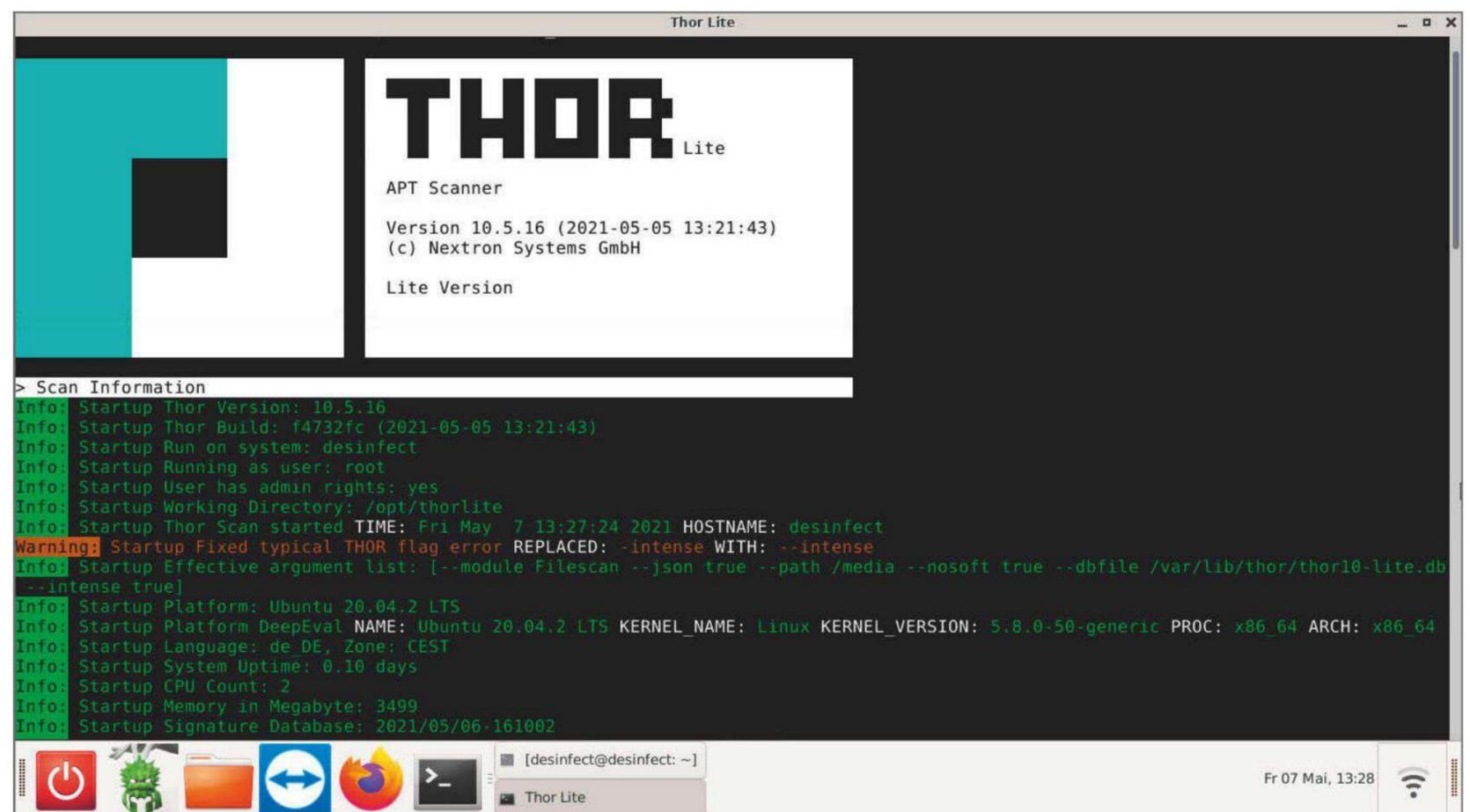
Zwar können Sie das System auch auf einen Dual-Layer-DVD-Rohling brennen, sein volles Potenzial spielt Desinfec't aber erst von einem USB-Stick aus. Nur darauf speichert es aktualisierte Daten wie Viren-Signaturen und gerettete Dateien dauerhaft. Das Erstellen eines Sticks gelingt über mehrere Wege.

Wenn Windows läuft, müssen Sie das heruntergeladene ISO-Image zuerst als Laufwerk im Datei-Explorer verfügbar machen. In der Standardeinstellung von Windows 10 gelingt das mit einem Doppelklick auf die ISO-Datei. Danach taucht Desinfec't als Laufwerk im Explorer auf. Wenn Sie ein DVD-Brennprogramm installiert haben, könnte es an dieser Stelle dazwischenfunken, indem es die Datei auf einen Datenträger brennen will. In diesem Fall klicken Sie

mit der rechten Maustaste auf die Datei und wählen „Öffnen“ oder „Öffnen mit/Windows-Explorer“ aus.

Nun klicken Sie im Explorer auf das Laufwerk mit dem Desinfec't-Logo. Mit einem Doppelklick auf die Datei „Desinfec't2USB_64_Bit.exe“ starten Sie den Installationsvorgang. Jetzt müssen Sie aufpassen: Der Installationsassistent löscht den ausgewählten Datenträger unwiderruflich. Entfernen Sie am besten alle anderen externen Datenträger und stellen Sie sicher, dass sie für die Installation den richtigen USB-Stick ausgewählt haben. Um sicherzugehen, schauen Sie sich den dem Stick zugeordneten Laufwerksbuchstaben im Explorer an und vergleichen diesen mit dem unter „Device“ im Installationsassistenten. Stimmt alles, klicken Sie auf die Schaltfläche „Write“. Im Anschluss beginnt die Installation.

Wenn dieser Vorgang erfolgreich abgeschlossen wurde, können Sie das System starten (siehe Kasten auf Seite 14). Doch bevor es richtig losgeht, muss sich das System noch einmalig richtig an den Stick anpassen. Das gelingt über den Punkt im Desinfec't-Bootmenü „in nativen Desinfec't-Stick umwandeln“. Diese Option müssen Sie auch auswählen, wenn Sie Desinfec't 2021/22 auf einem USB-Stick gekauft haben. Geschieht die Umwandlung nicht, verhält sich das System wie von einer DVD gestartet und speichert keine Daten. Dementsprechend müssten



**Mit dem neuen
Thor-Scanner graben
Profis noch tiefer
nach Malware vom
Schlage Emotet.**

Sie dann Viren-Signaturen nach jedem Neustart erneut herunterladen. Deshalb raten wir sehr dazu, das zu machen; je nach Geschwindigkeit des Sticks ist dieser Vorgang innerhalb weniger Minuten abgeschlossen. Nun merkt sich das Sicherheitstool Daten und Sie können auch beispielsweise Fotos und Videos von verunfallten Windows-PCs in Sicherheit bringen.

Alternativer Weg

Wenn Windows sich bereits seltsam verhält, sollten Sie den Stick nicht auf dem betroffenen Rechner erzeugen. Wenn Sie schon einen Desinfec't-Stick oder eine DVD mit dem Sicherheitstool besitzen, starten Sie es davon und erzeugen anschließend einen Stick. Ist das nicht der Fall, müssen Sie einen Bekannten mit einem sauberen Windows bitten, das System für Sie auf einen Stick zu installieren.

Läuft Desinfec't, müssen Sie zur Stick-Erstellung auf das Icon „Desinfec't-Stick bauen“ auf dem Desktop klicken. Vorsicht: Der Vorgang löscht den ausgewählten Stick ohne Nachfragen. Stimmt alles, können Sie die Voreinstellung so lassen und auf „Anwenden“ klicken. Nach dem wenige Minuten andauernden Installationsvorgang halten Sie einen vollständigen Desinfec't-Stick in der Hand, den Sie direkt nutzen können. Eine Umwandlung ist nicht mehr nötig.

Wenn Sie bei der Erstellung den Punkt „Easy Scan“ auswählen, startet das System ohne Umwege direkt mit einem Komplet-Scan von Windows. Dieser Modus

ist besonders für Freunde und Verwandte interessant, die sich nicht so gut mit Computern auskennen: Nichts lenkt vom eigentlichen Anwendungszweck ab und man kann nichts falsch machen.

Mit der BTRFS-Option erstellte Sticks sind umfangreich modifizierbar. Das Dateisystem hat aber nach wie vor experimentellen Charakter und richtet sich nur an Linux-Profis. Läuft Desinfec't mit dem BTRFS-Dateisystem, kann man es zum Beispiel dauerhaft mit aktuellen Treibern oder Office-Anwendungen erweitern (siehe Artikel auf Seite 28). Dafür benötigen Sie aber einen großen (minimal 32 GByte) und schnellen USB-Stick.

Meldet Desinfec't bei der Installation ein Problem, liegt das zumeist an alten oder fehlerhaften Sticks. Damit die Installation optimal gelingt, prüft Desinfec't den Stick und gibt eine Warnung aus, wenn er beim Lesen und Schreiben zu langsam ist. In so einem Fall können Sie das System trotzdem nutzen, im Betrieb bekommen Sie aber ziemlich sicher Probleme. Vor allem lahme Sticks (Schreibvorgang mit weniger als 3 MByte/s) machen bei Signatur-Updates Ärger. Erkennt die Prüfung bei der Erstellung Fehler, kann Desinfec't den Stick auf Wunsch zurücksetzen. Anschließend können Sie ihn wie gewohnt formatieren und für andere Zwecke nutzen.

Sicherheitstool starten

Wie Sie Desinfec't booten, zeigt der Kasten auf S. 14. Wenn das Starten geklappt hat, haben Sie die

Detection	Details	Relations	Behavior	Community
Ad-Aware	Trojan.GenericKD.36608277	AegisLab	Trojan.MSIL.PowerShell.4!c	
AhnLab-V3	Trojan.Win.AgentTesla.C4398311	Alibaba	Trojan.MSIL/Tnega.Ob157687	
ALYac	Spyware.AgentTesla	SecureAge APEX	Malicious	
Arcabit	Trojan.Generic.D22E9915	Avast	Win32.RATX-gen [Trj]	

Um Fehlalarme effektiv einzugrenzen, laden Sie Funde aus der Ergebnisliste direkt zum kostenlosen Analyse-dienst Virustotal hoch. Dort schauen noch mal 60 Scanner auf die Datei und geben eine Einschätzung ab.

Download von Desinfec't 2021/22

Wer einen Computer ohne DVD-Laufwerk besitzt, kann das Sicherheitstool dennoch nutzen. Dafür laden Sie das ISO-Image von Desinfec't 2021/22 herunter. Anschließend installieren Sie es auf einem USB-Stick und booten es von dort. Alternativ brennen Sie es auf eine Dual-Layer-DVD mit 8,5 GByte Speicherplatz.

Käufer der digitalen Einzelausgabe bekommen mit ihrer Auftragsbestätigung via E-Mail einen Downloadlink für die ISO-Datei.

Auch Kioskkäufer des Heftes können Desinfec't herunterladen. Dafür müssen Sie lediglich

die Website ct.de/desinfect2021-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

Anhand der MD5-Prüfsumme können Sie prüfen, ob das ISO-Image unverändert auf Ihrem Computer gelandet ist. Stimmt der MD5-Wert nicht überein, ist es beim Download zu Fehlern gekommen. Laden Sie die Datei erneut herunter. Prüfsummen kann man mit kostenlosen Tools wie HashCheck erzeugen.

MD5: 3cafab830f9311689ab1226459512fe3

größte Hürde überwunden. Das Problem ist, dass das System aus Speicherplatzgründen nicht alle Treiber für jegliche erschienene Hardware enthalten kann. Wir haben das System aber erfolgreich auf Hardware aus den vergangenen 10 Jahren getestet. Bei Intel haben wir mit i7-CPUs der 2000er-Serie und bei AMD mit A6-APUs begonnen. Bei den Grafikkarten

kamen neben Onboard-Lösungen wie HD3000 von Intel auch aktuelle RTX2000-Modelle von Nvidia zum Einsatz. In unseren Tests startete Desinfec't 2021 problemlos. Außerdem haben wir die Kompatibilität mit NVMe-SSDs gesteigert.

Wenn das System partout nicht startet, können Sie im Desinfec't-Bootmenü den Safe Mode auswählen oder das Booten mit einem alternativen Kernel ausprobieren. Hilfe finden Sie im offiziellen Desinfec't-Forum (siehe ct.de/w41r).

Trojaner-Gefangenschaft vorbereiten

Wenn Desinfec't das erste Mal auf einem Computer gestartet ist, müssen Sie mit dem automatisch auftauchenden Assistenten einen Projektordner anlegen. Dieser Ordner bildet Ihr Arbeitsverzeichnis für diesen Vorfall. Darin speichert das Sicherheitstool beispielsweise Scan-Ergebnisse und vor einem Virus in Sicherheit gebrachte Dateien. Der Ordner ist unter Windows sichtbar. So haben Sie später auch von anderen Windows-Systemen aus Zugriff auf die Dateien. Desinfec't erkennt PCs an individuellen Hardware-IDs und legt für jeden Computer einen neuen Projektordner an. Davon profitieren vor allem Nutzer, die Desinfec't auf vielen verschiedenen Computern einsetzen. Bei der Analyse



Wenn der Viren-Scan läuft, können Sie sich die Zeit mit verschiedenen Mini-Spielen vertreiben.

von Ergebnissen behalten Sie dank aussagekräftigen Ordner-Namen wie „Spiele-PC“ und „Arbeits-Möhre“ den Überblick.

Ist der Projektordner erstellt, können Sie mit dem ersten Viren-Scan beginnen. Führen Sie dafür einen Doppelklick auf das Desktop-Icon „Viren-Scan“ aus. Im Anschluss öffnet sich der Scan-Assistent. Wenn der PC noch nicht mit dem Internet verbunden ist, taucht das WLAN-Fenster auf. Darin können Sie bestätigen, dass sich Desinfec't das WLAN-Passwort merkt. Achtung: Das steht dann im Klartext auf dem Stick. Wenn Sie den verlieren, sollten Sie das WLAN-Passwort also vorsichtshalber ändern. Eine Internetverbindung ist nötig, damit die Scanner von Avast,

Eset, F-Secure und Sophos ihre Signaturen aktualisieren können.

Wählen Sie nun die zu scannende Festplatte aus. Standardmäßig schauen sich die Scanner die gesamte Windows-Installation an. Alternativ können Sie mit der Option ganz unten gezielt einen Ordner oder eine Festplatte beziehungsweise einen USB-Stick scannen. Wenn keine Festplatte im Scan-Assistent auftaucht, machen Sie einen Doppelklick auf das Desktop-Icon „Win-Drives einhängen“. Im Anschluss sollten die Laufwerke im Scan-Assistenten auftauchen.

Nachdem Sie die gewünschte Festplatte oder einen Ordner zum Scannen ausgewählt haben, klicken Sie auf „Vor“. Um eine erste Einschätzung über

Desinfec't starten

Vermuten Sie, dass ein Schädling sein Unwesen auf Ihrem Windows-PC treibt, fackeln Sie nicht lange und fahren Sie den Computer herunter. Schalten Sie ihn 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 das nicht klappt, starten Sie auf Ihrem Smartphone eine Internet-suche und geben neben Ihrem Computer-Modell noch BIOS-Bootmenü ein, um die richtige Taste zu finden.

Erscheint das Menü auf dem Bildschirm, legen Sie die Desinfec't-DVD ein oder schließen einen Stick an. Wählen Sie im Anschluss das Medium mit Desinfec't aus und starten Sie davon. Funktioniert das nicht, müssen Sie den Umweg über das BIOS-Menü gehen. Dieses rufen Sie meist durch das Drücken der Taste Entf oder F2 auf.

Auch an dieser Stelle gilt, dass das Menü über verschiedene Tasten aufrufbar ist.

Dort stellen Sie die Boot-Reihenfolge so ein, dass das Medium mit Desinfec't zuerst startet. Wollen Sie nur einen Routine-Check machen, können Sie den Start von Desinfec't auch direkt aus einem laufenden Windows 8.1 oder 10 anstoßen. Das funktioniert aber nur, wenn das System im UEFI-Modus läuft. Dafür halten Sie die Umschalttaste (Shift) gedrückt ❶ und klicken im Startmenü auf Neustart. Im anschließend auftauchenden Bildschirm bestätigen Sie den Punkt „Ein Gerät verwenden“ ❷. Als Nächstes wählen Sie das Medium mit Desinfec't aus ❸. Nun fährt Windows herunter und bootet automatisch das Notfallsystem. Klappt der Start partout nicht, wählen Sie bitte im Desinfec't-Bootmenü die Option „Safe Mode“ aus.



Verschlüsselte Festplatten scannen

Wer seine Festplatte mit Microsofts Bitlocker verschlüsselt hat, kann Laufwerke direkt aus dem Scan-Assistenten einbinden. Dafür müssen Sie das Laufwerk lediglich auswählen und nach den Scanner-Updates das Passwort für das verschlüsselte Volume eingeben.

Im Test hat das in der Redaktion problemlos mit einer unter Windows 10 20H2 verschlüsselten Systempartition geklappt. Mit kommenden Windows-Updates ist die Kompatibilität aber möglicherweise nicht mehr gegeben. Das Problem ist, dass Microsoft in neuen Windows-Versionen oft 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 Vera-

Crypt-Client. Die Festplatte taucht dann im Scan-Assistent zur Auswahl auf. Haben Sie Ihre Systemplatte voll verschlüsselt, müssen Sie noch die Option „mount partition using system encrypting“ auswählen.



Mit Bitlocker verschlüsselte Laufwerke tauchen direkt im Scan-Assistenten auf und stehen nach der Auswahl für Scans bereit.

den Infektionsgrad eines Computers zu erhalten, genügt es, die Untersuchung mit dem vorausgewählten Scanner von Avast zu starten. Dafür klicke Sie auf „Anwenden“. Umgehend startet der Assistent die Aktualisierung der Viren-Signaturen, damit die Scanner für aktuelle Schädlinge gerüstet sind. Im Anschluss startet ohne weiteres Zutun der Scan.

Im Reiter „Experte“ können Sie den Scan anpassen. Auf Wunsch schauen sich die Scanner Archive und Mailboxen an. Achtung: Diese Option verlängert die Scan-Zeit erheblich und der Computer kann sogar abstürzen. Der Grund dafür: Wenn Desinfec't zur Untersuchung große Archive im Arbeitsspeicher entpackt und scannt, kann das zu Instabilitäten des Systems führen. Wenn Sie nur die Signaturen aktualisieren wollen, ohne einen Scan durchzuführen, wählen Sie die entsprechende Option aus und kli-

cken auf „Anwenden“. Das ist zum Beispiel hilfreich, wenn Sie später einen Computer scannen wollen, der nicht mit dem Internet verbunden ist.

Nach der Untersuchung

Ist der Scan abgeschlossen, erscheint hoffentlich ein Fenster mit der Nachricht, dass kein Trojaner gefunden wurde. Doch Vorsicht: Selbst wenn kein Scanner Alarm schlägt, kann sich dennoch ein Schädling auf dem PC befinden. Das kann passieren, wenn der Trojaner so neu ist, dass es noch keine Signaturen zur Erkennung gibt. Wähnen Sie sich also nicht in hundertprozentiger Sicherheit.

Haben die Scanner hingegen angeschlagen, atmen Sie erst mal tief durch und prüfen Sie die sich automatisch in Firefox öffnende Ergebnisliste mit

Virenfunde

Systemzeit: 2021-05-07 11:37:43 +0200
 Verwendete Scanner:
 Startordner des Scans: /media/B40E-89EE/Test-Viren/für Desinfec't 2021 relevant
 Zum Zeitpunkt des Scans eingebundene Laufwerke:
 • /dev/loop1 auf /media/desinfDATA (vfat)

Vollständigkeit der Logdateien:
 • avast: vollständig
 • eset: vollständig
 • f-secure: vollständig
 • sophos-av: vollständig

Avast	ESET NOD32	F-Secure	Sophos	Open Threat Scanner	Aktion
	/media/B40E-89EE/Test-Viren/für Desinfec't 2021 relevant/2021-03-30/06cbc13be02300d9a718f6c8bafd5e233eaa195d3d261f7d02eae0197189f987			HTML/Phishing.Gen(trojan)	VirusTotal umbenennen
	/media/B40E-89EE/Test-Viren/für Desinfec't 2021 relevant/2021-03-30/0699e84310a1998ee2f9c77c39e3ad13b7e23671e33ff339f5492aa107f2e8da			Win64/Filecoder.Conti.A(trojan)	VirusTotal umbenennen
	/media/B40E-89EE/Test-Viren/für Desinfec't 2021 relevant/2021-03-30/1aa4e7b8481bcd47b508a00f90e0547c40aa2dfe47895c4f199b136cb31e12b			MSIL/TrojanDownloader.Agent.HOV(trojan)	VirusTotal umbenennen
	/media/B40E-89EE/Test-Viren/für Desinfec't 2021 relevant/2021-03-30/0eb9fb0576242164d5b3056606d681bdb28a09a5e370e70b5da12848da3f135a			Win32/PSW.Fareit.A(trojan)	VirusTotal umbenennen
	/media/B40E-89EE/Test-Viren/für Desinfec't 2021 relevant/2021-03-30/10495df99a18c97ac180cf29b32daf92bb67146f5e927f89c2c75432976e379			MSIL/Kryptik.AAFR(trojan)	VirusTotal umbenennen
	/media/B40E-89EE/Test-Viren/für Desinfec't 2021 relevant/2021-03-30/28c0354c264de3750471377896cb7ce958c6540324e9553b16179d3c23b06cd7			Win32/Kryptik.GZNI(trojan)	VirusTotal umbenennen
	/media/B40E-89EE/Test-Viren/für Desinfec't 2021 relevant/2021-03-30/11ddd28c20537bbae6b351a2833152a180a729dc94e8648698d82c5f9cfc7e7			MSIL/Kryptik.AAET(trojan)	VirusTotal umbenennen

In der Ergebnisliste in Firefox finden Sie Infos, wie den Speicherort, von als verdächtig eingestuft Dateien. Über die Schaltfläche „Umbenennen“ machen Sie Trojaner unschädlich.

den Funden. Es ist nicht auszuschließen, dass es sich um Fehlalarme handelt. Um das besser einschätzen zu können, bringt Desinfec't mehrere Methoden mit. Springt beispielsweise nur einer der vier Scanner auf eine Datei an, liegt ein Fehlalarm nahe. Es kann zum Beispiel vorkommen, dass in einer Abschlussarbeit verankerte harmlose Word-Makros einen Alarm auslösen.

Wenn sich der Trojaner-Verdacht dadurch nicht aus der Welt schaffen lässt, laden Sie die verdächtige Datei zum Online-Analysedienst Virus hoch. Dafür klicken Sie auf die Verknüpfung ganz rechts in der Ergebnisliste und anschließend auf „Link öffnen“. Dort schauen über 60 Scanner auf den Fund und geben eine Einschätzung ab. Zusätzlich zu diesen Ergebnissen finden Sie dort oft noch Kommentare anderer Nutzer zu analysierten Dateien. Das ist für eine Einschätzung sehr hilfreich. Ob sie Dokumente mit vertraulichen Inhalten hochladen, müssen Sie selbst entscheiden.

Wenn Sie gar nicht mehr weiterwissen und überfordert sind, rufen Sie mittels Teamviewer jemanden aus der Familie oder dem Bekanntenkreis zu Hilfe. Derjenige übernimmt via Internet die Kontrolle über den Problem-PC und schaut sich auf dem System um. Das Fernwartungstool bringt Desinfec't direkt mit. Auch eine Windows-Version ist mit dabei. Die Nutzung ist aber ausdrücklich nur im privaten Bereich erlaubt.

Echter Trojaner voraus

Auch wenn alle Zeichen auf einen echten Virenbefall hindeuten, lässt Desinfec't Sie nicht im Stich. Mit wenigen Klicks machen Sie Trojaner unschädlich – das gelingt direkt aus der Ergebnisliste. Klicken Sie dafür einfach auf „Umbenennen“ und Link öffnen. Im Anschluss müssen Sie im automatisch auftauchenden Fenster dem Sicherheitstool erlauben, schreibend auf die Windows-Festplatte zugreifen zu dürfen. Das ist standardmäßig nicht erlaubt, damit Desinfec't nichts am System verändern und gegebenenfalls kaputt machen kann. Ist der Schreibzugriff erlaubt, hängt das Skript an den Dateinamen die Endung .VIRUS. Handelt es sich um eine ausführbare EXE-Datei, wird daraus „Ransomware.exe.VIRUS“. Diese Methode ist simpel, aber effektiv: Dadurch ändert sich der Dateityp und Windows kann die Datei nicht mehr ausführen.

Falls bei diesem Vorgang zum Beispiel eine legitime Systemdatei unter die Räder kommt und Windows im schlimmsten Fall nicht mehr startet, können Sie einfach die Dateiendung .VIRUS entfernen und alles ist wieder wie zuvor. Alternativ können Sie das entsprechende Skript im Expertentools-Ordner einsetzen. Das versetzt alle von Desinfec't umbenannten Dateien wieder in den ursprünglichen Zustand zurück.

Für Profis

Der Open Threat Scanner (OTS) und der neue implementierte Thor-Lite-Scanner richten sich an erfahrene Virenjäger, die noch tiefer nach Schädlingen vom Kaliber eines Emotet graben wollen. Beide können Sie direkt über die Icons auf dem Desktop starten. Der OTS setzt auf Yara-Regeln. Dabei handelt es sich um Listen mit Merkmalen von Schädlingen, um diese via Pattern Matching aufzufinden. Die Aktualisierungen holt sich OTS vom GitHub-Repository von Reversing-Labs. Die haben sich eine hohe Erkennungsrate und geringe Fehlalarmquote auf die Fahne geschrieben. Ambitionierte Trojanerjäger können sogar eigene Regeln für den Scanner schreiben und so ihren eigenen Viren-Scanner bauen (siehe Artikel auf Seite 22).

Den Thor APT Scanner von Nextron setzt Desinfec't 2021/22 in der Lite-Version ein. Der Scanner verwendet neben etwa 3000 ständig aktualisierten Yara-Regeln auch weitere sogenannte Indicators of Compromise (IOC), um Anzeichen für aktuelle Bedrohungen aufzuspüren. Die eingesetzten Regeln sind

größtenteils von Hand optimiert, um das Risiko von Fehlalarmen gering zu halten. Wenn jedoch Thor anschlägt, ist es mit dem Umbenennen einer Datei definitiv nicht mehr getan. Die Behandlung der so gefundenen Bedrohungen erfordert solide Kenntnisse der Incident Response. Sowohl Thor als auch OTS sind Werkzeuge für Profis; im Zweifelsfall muss man sich da dann kompetente Hilfe holen.

Im Expertentools-Ordner auf dem Desktop finden Sie weitere Profi-Werkzeuge, etwa um verloren geglaubte Dateien zu retten und ganze Festplatten zu klonen. Mit QPhotoRec rekonstruieren Sie mit etwas Glück versehentlich gelöschte Daten. Das klappt beispielsweise mit Bildern oder Office-Dokumenten. Die Dateien bringen Sie dann auf einem Desinfec't-Stick in Sicherheit. Mit einem weiteren Tool fertigen Sie eine 1:1-Kopie einer Festplatte an. Das kann zum Beispiel für die Wiederherstellung von Windows auf einem anderen Computer hilfreich sein. Aber wie der Name der Werkzeuge schon sagt, sollten sich nur Experten an diese Tools wagen. Andernfalls könnte Windows Schaden nehmen. (des) **ct**

Forum

ct.de/w41r

Make:
KREATIV MIT TECHNIK

DAS KANNST
DU AUCH!



2x Make testen und 6 € sparen!

Ihre Vorteile:

- ✓ **GRATIS** dazu: Arduino Nano
- ✓ Zugriff auf Online-Artikel-Archiv*

Für nur 15,60 Euro statt 21,80 Euro.

* Für die Laufzeit des Angebotes.

- ✓ **NEU:** Jetzt auch im Browser lesen!
- ✓ Zusätzlich digital über iOS oder Android lesen

Jetzt bestellen:

make-magazin.de/miniabo

GRATIS!





FAQ Desinfec't 2021/22

Mit dem Sicherheitstool jagen Sie Trojaner und greifen auf wichtige Daten von nicht mehr startenden PCs zu. Die meisten Probleme bei der Nutzung sind meistens ohne viel Aufwand lösbar.

Von **Dennis Schirmmacher**

USB-Stick-Erstellung schlägt fehl

? Ich will Desinfec't 2021/22 wie im Heft beschrieben unter Windows auf einem USB-Stick installieren. Leider bricht der Vorgang immer mit der Meldung „Error 5“ ab. Was mache ich falsch?

! Das Problem lässt sich oft lösen, indem Sie für die Dauer der Stick-Erzeugung Ihren Virenwächter deaktivieren. Vergessen Sie aber nicht, den Echtzeit-Scanner im Anschluss wieder zu aktivieren, sonst ist Ihr System potenziell gefährdet. Hintergrund dafür ist, dass manche AV-Scanner einen Master-Boot-Record-Schutz (MBR) mitbringen. Der soll verhindern, dass sich ein Trojaner in den ersten 512-Byte-Blocks eines Laufwerks einnistet, verhindert aber auch, dass das Erstellungstool den für Desinfec't nötigen Boot-Manager schreibt.

Desinfec't aktualisieren

? Ich habe gelesen, dass es Updates für Desinfec't 2021/22 gibt. Was machen die und wie installiere ich sie?

! Wir unterstützen jede Desinfec't-Version für ein Jahr. Tauchen Bugs auf, stellen wir Updates in unserem eigenen Repository bereit. Die Aktualisierung geschieht in der Regel automatisch, sobald das System über eine aktive Internetverbindung verfügt. Ob das System aktuell ist, sehen Sie oben rechts im Statusfenster. Steht dort beispielsweise „Desinfec't 2021/22 p1“, ist es auf dem aktuellen Stand. Taucht die Bezeichnung nicht auf, stoßen Sie das Update mit den Befehlen `sudo apt-get update` und `sudo apt-get -y dist-upgrade` an. Nach der Installation eines Desinfec't-Updates ist in der Regel kein Neustart nötig.



Damit Desinfec't 2021/22 noch mehr aktuelle Hardware wie NVME-SSDs erkennt, starten Sie das System über das Bootmenü mit dem Kernel 5.13.

Desinfec't trotz LAN-Kabel offline

? Ich nutze Desinfec't auf einem ziemlich aktuellen Computer mit einem 2,5-Gbit-Netzwerkcontroller und einer NVMe-SSD. Das System startet problemlos. Wenn ich ein LAN-Kabel anschlieÙe, baut sich aber keine Verbindung zum Internet auf. Außerdem sieht der Scan-Assistent meine NVMe-SSD nicht. Wenn ich dann meine andere Festplatte scanne, tauchen andauernd Input-Output-Fehler auf. Kann ich dagegen was machen oder ist Desinfec't nicht mit meinem Computer kompatibel?

! Das klingt so, als könnte der alternative in Desinfec't implementierte Linux-Kernel 5.13 helfen. Dieser ist neuer als der bewährte Standard-Kernel 5.8 und bringt mehr Treiber für aktuelle Hardware mit. Um das System damit zu starten, wählen Sie im Desinfec't-Bootmenü den Eintrag mit Kernel 5.13 aus. In unseren Tests haben wir damit beispielsweise eine bessere Kompatibilität mit NVMe-SDDs erreicht. Erscheint beim Start von Desinfec't mit dem Kernel 5.13 die Fehlermeldung „error: /casper/vmlinuz.55 has invalid signature“, deaktivieren Sie im BIOS/UEFI die Secure-Boot-Option. Hintergrund ist, dass Ubuntu Mainline-Kernel nicht signiert, worüber Secure Boot meckert.

Schrift zu klein: Auflösung dauerhaft umstellen

? Wenn ich Desinfec't auf meinem Laptop mit 4K-Bildschirm starte, kann ich die Schrift aufgrund der hohen Auflösung kaum lesen. Deswegen

lasse ich mir zuerst im Terminal mit dem Befehl `xrandr` die verfügbaren Auflösungen anzeigen. Anschließend stelle ich mit `xrandr -s 1280x800` eine niedrigere Auflösung ein, sodass die Schrift größer wird. Das muss ich aber nach jedem Neustart erneut eingeben. Gibt es eine Möglichkeit, die Auflösung dauerhaft zu ändern?

! Ja, das funktioniert. Dafür müssen Sie lediglich ein vorhandenes Skript mit ein paar Befehlen im Terminal anpassen. Öffnen Sie mit den folgenden Befehlen mit dem integrierten Editor das Skript `autoscan.sh`. Dieses ist namensgebend eigentlich dafür da, um nach dem vollständigen Aufbau des Desktops automatisierte Scans auszuführen. Man kann es aber auch zur dauerhaften Anpassung der Bildschirmauflösung nutzen. Öffnen Sie dazu die Datei im Editor Scite:

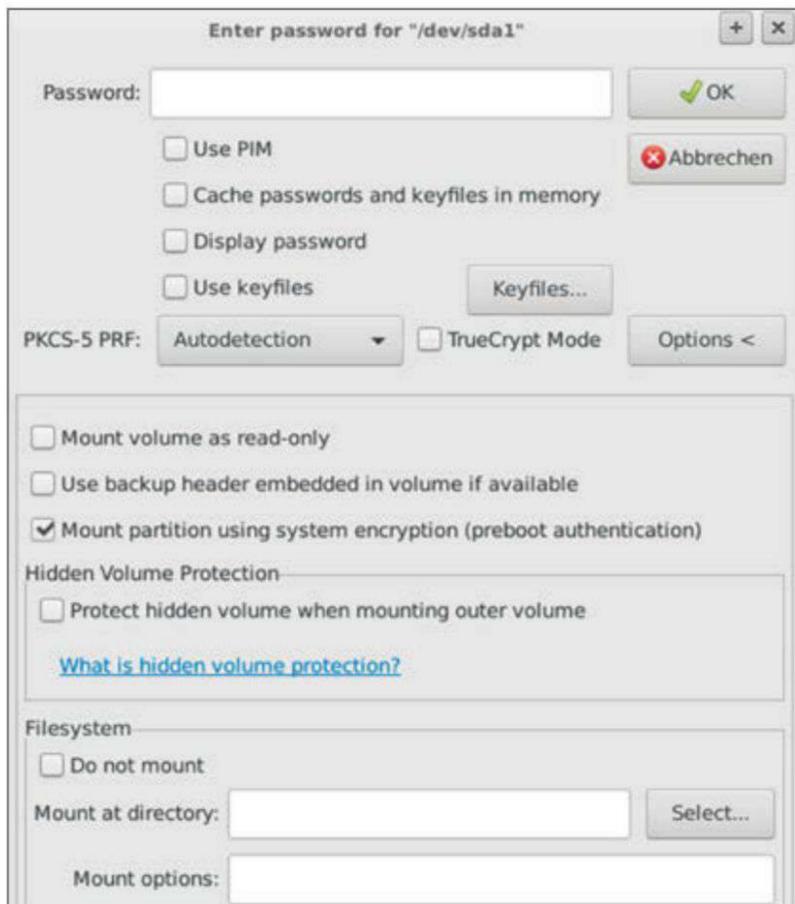
```
sudo scite /opt/desinfect/signatures/autoscan.sh.
```

Nun tragen Sie den folgenden Abschnitt in das Skript ein.

```
xrandr -s 1280x800
killall -9 conky
conky &
```

Wenn Sie den Stick auf mehreren PCs nutzen, können Sie pro Computer eine spezifische Auflösung festlegen. Dafür müssen Sie zuerst mit den folgenden Befehlen die PC-Seriennummer herausfinden und diese notieren.

```
sudo dmidecode |grep UUID
```



Damit VeraCrypt voll verschlüsselte Windows-Festplatten erkennt, müssen Sie die Option „Mount partition using system encryption“ auswählen.

Im nächsten Abschnitt ersetzen Sie XXX mit der Seriennummer des jeweiligen Computers. Für mehrere PCs kopieren Sie die Einträge und passen die UUID-Nummern an. Nach einem Neustart gibt Desinfec't auf dem jeweiligen Computer die eingestellte Auflösung aus.

```
if sudo dmidecode | grep -i XXX ; then
    xrandr -s 1920x1080
    killall -9 conky
    conky &
fi
```

Desinfec't-Stick löschen

? Ich möchte meinen Desinfec't-Stick nun wieder wie einen normalen USB-Stick nutzen. Leider wird unter Windows nach der Formatierung nur noch ein Bruchteil der eigentlichen Speicherkapazität angezeigt. Ist der Stick jetzt kaputt?

! Nein, der USB-Stick ist nicht kaputt. Desinfec't nutzt mehrere Partitionen, die Windows nicht alle erkennt. Dort versteckt sich der vermisste Spei-

cherplatz. Um den Stick vollständig zu löschen, benutzen Sie am besten das Windows-Kommandozeilenprogramm diskpart. Um es unter Windows 10 zu starten, tippen Sie einfach diskpart in das Suchfeld in der Taskleiste ein und drücken die Eingabetaste. Mit den folgenden Befehlen identifizieren Sie den Stick, wählen ihn aus – das „?“ müssen Sie durch die korrekte Ziffer, die Ihren Stick auszeichnet, ersetzen und löschen diesen:

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

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

Desinfec't-Installer infiziert?

? Ich habe das Installationsprogramm Desinfec't 2USB_64_Bit.exe zum Online-Viren-Analyse-dienst VirusTotal hochgeladen und von den über 60 Scannern hat MaxSecure die Datei als einen Trojaner eingestuft. Muss ich mir Sorgen machen?

! Nein. Dabei handelt es sich um einen Fehlalarm.

Verschlüsselte Festplatte nicht sichtbar

? Ich habe meine Windows-Festplatte vollständig mit VeraCrypt verschlüsselt. Leider kann ich die Partition nicht scannen.

! Starten Sie VeraCrypt im Expertentools-Ordner und wählen die verschlüsselte Festplatte aus. Bei einer Vollverschlüsselung von Windows müssen Sie noch den Punkt „Mount partition using system encryption“ aktivieren. Nach der Eingabe des Passworts für die verschlüsselte Platte sollte diese im Scan-Assistenten auftauchen.

Weitere Hilfe

Das Desinfec't-Forum (siehe ct.de/w45t) ist die erste Anlaufstelle, wenn Sie Schwierigkeiten oder sogar Lösungen für Probleme haben. Dort tauschen sich nicht nur Nutzer aus, auch die Redaktion und der Desinfec't-Entwickler sind dort aktiv. (des) **ct**

Desinfec't-Forum

ct.de/w45t

Nur 995 €
im Jahr

Vernetzen, verstehen, umsetzen

Mit heise Security Pro zu mehr IT-Sicherheit.

heise Security Pro liefert Ihnen **Hintergründe, Analysen und vertiefendes Know-how** rund um IT-Sicherheit und **vernetzt IT-Security-Experten**. Werden auch Sie Teil dieser Community und sichern Sie sich jetzt das Profi-Paket für nur 995 € im Jahr*:

-
- | | |
|---|--|
|  Mindestens 4 Security Webinare |  Jährliche heise Security Konferenz |
|  1 Ticket für die secIT |  heise Security Expertenplattform |
|  Wöchentlicher Experten-Newsletter |  1 heise+ und 1 Pur-Lizenz |
-

*Weitere Pakete auf Anfrage bei pro-service@heise.de.



JETZT IT-PAKET SICHERN: heise.de/heisec-pro



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 2021/22 und ist gar nicht schwer.

Von **Mattias Schlenker**

Am 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 Virenscanner 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 2021/22 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-Re-

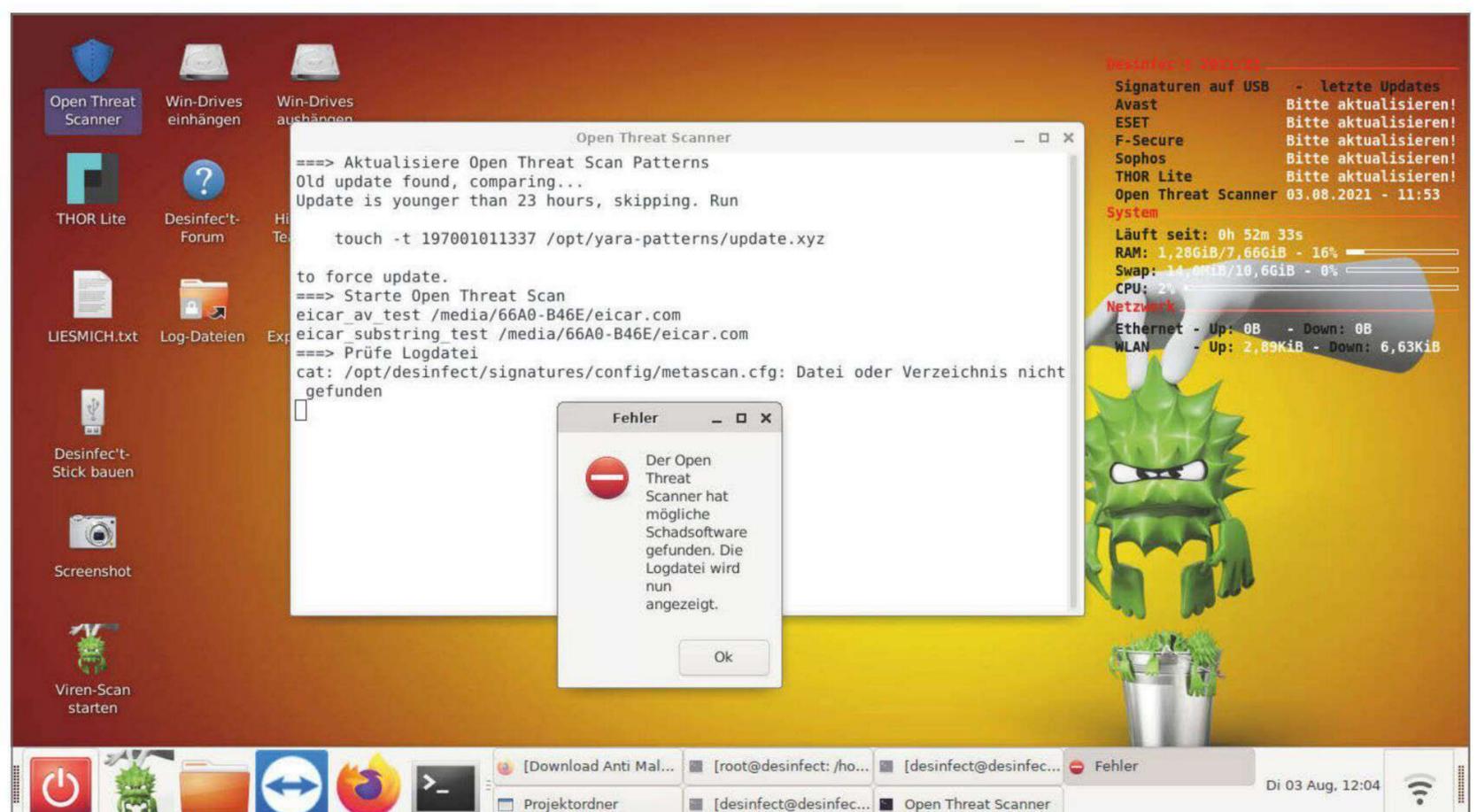
geln. Nach dem Booten von Desinfec't können Sie den OTS direkt starten: Der Scanner aktualisiert sich automatisch und durchsucht Festplatten mit unserem Standard-Yara-Regelsatz.

Ausgangspunkt ist das Skript „/opt/desinfec't/yara-ots-wrapper.sh“. Starten Sie den OTS über den Scan-Assistenten, hängt das Skript zunächst alle Windows-Laufwerke ein. Anschließend startet das automatische Update über das Skript „/opt/desinfec't/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/desinfec't/signatures/desinfec't/yara/emotet.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 als die zu Beginn vom OTS eingesetzte MD5-Methode, bei der wir die Yara-Integration mit den Hashes per Honey-pot „eingefangenen“ Schadsoftware-Samples fütterten. 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.

Das OTS Script mountet Laufwerke und zeigt nach Abschluss des Scans, ob Schadsoftware gefunden wurde.



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 (1DeaDBEefXulubMiRF4311tN1xE1n) enthält.

Damit simulieren Sie eine typische Erpressernotiz. 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 = "1DeaDBEefXulubMiRF4311tN1xE1n"
  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 yar-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 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 verdächtigten 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 oder den Scan-Assistenten starten, sucht der Scanner mit Ihren Regeln. Glückwunsch, Sie haben Ihren ersten eigenen Virenschanner 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 Programme, 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“-Codesequenzen, die in den erzeugten Regelsätzen als Erkennungsmerkmale vermieden werden. Für eine bessere Performance beschränkt das Tool die 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

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 00files.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:
    $s1 = "cmd.exe /c \"%s\" fullword ascii /* score: '36.00' */
    $s2 = "launcher.dll" fullword ascii /* score: '23.00' */
    $s3 = "msvcrt.dll" fullword ascii /* score: '23.00' */
    $s4 = "mssecsv.exe" fullword ascii /* score: '22.00' */
    $s5 = "tasksche.exe" fullword ascii /* score: '22.00' */
    $s6 = "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" fullword ascii /* score: '21.00' */
    $s7 = "C:\\%s\\qeriuwjhrf" fullword ascii /* score: '18.50' */
    $s8 = "BftpI3QdaPuJ8mJwsMVPRLNoZDvMTD9HteHBrxPFR9U8VZkx2Z0f0cKEYCsVTYygtI1L8M85VxaahPKyDa2y0r+SfxdvtfxIIhg18+wT/Q906zU5p"
    $s9 = "C:\\%s\\%s" fullword ascii /* score: '15.50' */
    $s10 = "U/nNqV1y0bXCn602atx6H7k9hHfYx2btG804e9Wyz+KrieA6wXQSAIERL1SDoEq05cCwzoUrrlcYVi+9wdjVuPzY6wN28tmh1Y070+UFFFP/bcJ4FTP"
    $s11 = "vEPaFyH2mXbRyDILYrV/l4GnsWY0asWepqTFZDZMtojz2/yys/dI44M27Zgev93L5zZT+37Ds9Chglw426hFyShgeT5jh1hLu+ejGM150AxxcYQ3"
    $s12 = "IJHTz0ttJ8JnC9fI4zh2DwAc6x/q9kMwN/ftPtPGb77yloLzrHlDh8kTB4RZTHBjTNKVeaDcVYlmlhu+qt/xH5Lw04KfrhsAShjavx/3xkyv9fkywM"
    $s13 = "muJmufSa7mqne1+wRdBNGUIkDwu9doV0S0QMzWSPYHEjff+flSY1IR0u8QtKofBASyCEQ/H1MieJp2eAqorc8gfZy/Xm1Ggpb7hljJoD00p8Klv3I4v0"
    $s14 = "h7RQJszvFX9y28zvzY/rBKNi3Mrxgsjfp7r0pCjMDaEL+m0dLP1bLwPpY5HwTgEtw0rV3ARznLMA9AaxJKuF3n1R131s3k6EahnnfQmkVI6/vJk8f"
    $s15 = "W7ued/BLAuVkbC8L5g5HkS6TStIYpkV4M4M1491ygmH841Xxoas4R25esIE6V14TNYMLYtM/bbZ205kh6XwtgeTN7/eYA7td0HraA9un6Y07MI2WqzVlI"
    $s16 = "R9KUDXyIU8whdEYNVve1MAHt/TJSAZiVoLog3MEfx2qLXZFKmm8ch01PeIpevvpf9xdsPItHzqBL1yk2PVZGSe00j1yo6DysGdE8JHCwqJ1dXARx"
    $s17 = "wE98CXh+wDXpV0rR0uXsT/ex09Fgq3iJa9YrshwDvrNddLhLPZ5jd+r7Vb1N42DLI3TsRC60TWTW/u9CZP50tTLfFSRtGpPRD1w7ATC3MGEX3ec"
    $s18 = "nSng5kSgHtsbeJnUjcju0zvn2nTY9S1breKlBohT1b2pV14XP89N0wVvetwXppn2Jnn00Yzq8eDvYh0LvjB5pyEkBDoG7bgNdJ1ElyBn69WmaSvnG0m"
    $s19 = "a7yIX0BwC5CdVZqK6x0+eefN1Xs1f5rWd+40a/JJmGHTSERUATPC0YvZFL8310lvCuN11eBGetCuavZr00+1gsMg2hJHCWVFPB1oKkp3VFQ+YuuJv7"
    $s20 = "GySx4DGbnqS1LBX7zH4M9YnggehLsqEYBHBH0InG1qiehuSriXaDarh2D1Yd09u2z9A7mdMUrj73sFY57/3s9MbgL0oy00HoSTGYgLS0NKD21404n"

    $op0 = { ff 15 2c 20 00 10 85 c0 59 a3 4c 31 00 10 75 04 }
    $op1 = { 08 52 52 52 68 38 30 00 10 52 66 89 55 dc c7 45 }
    $op2 = { 8b 44 24 08 48 75 09 8b 44 24 04 a3 3c 31 00 10 }
  condition:
    uint16(0) == 0x5a4d and filesize < 1500KB and
    ( pe.imports() == "2e5708ae5fed0403e8117c645fb23e5b" and pe.exports("PlayGame") or ( 1 of ($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 = "yyyytttfffaab" fullword ascii /* score: '8.00' */
    $s5 = "xammmffaaatxx" fullword ascii /* score: '8.00' */

```

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 langsamen 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 dürfte.

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

```

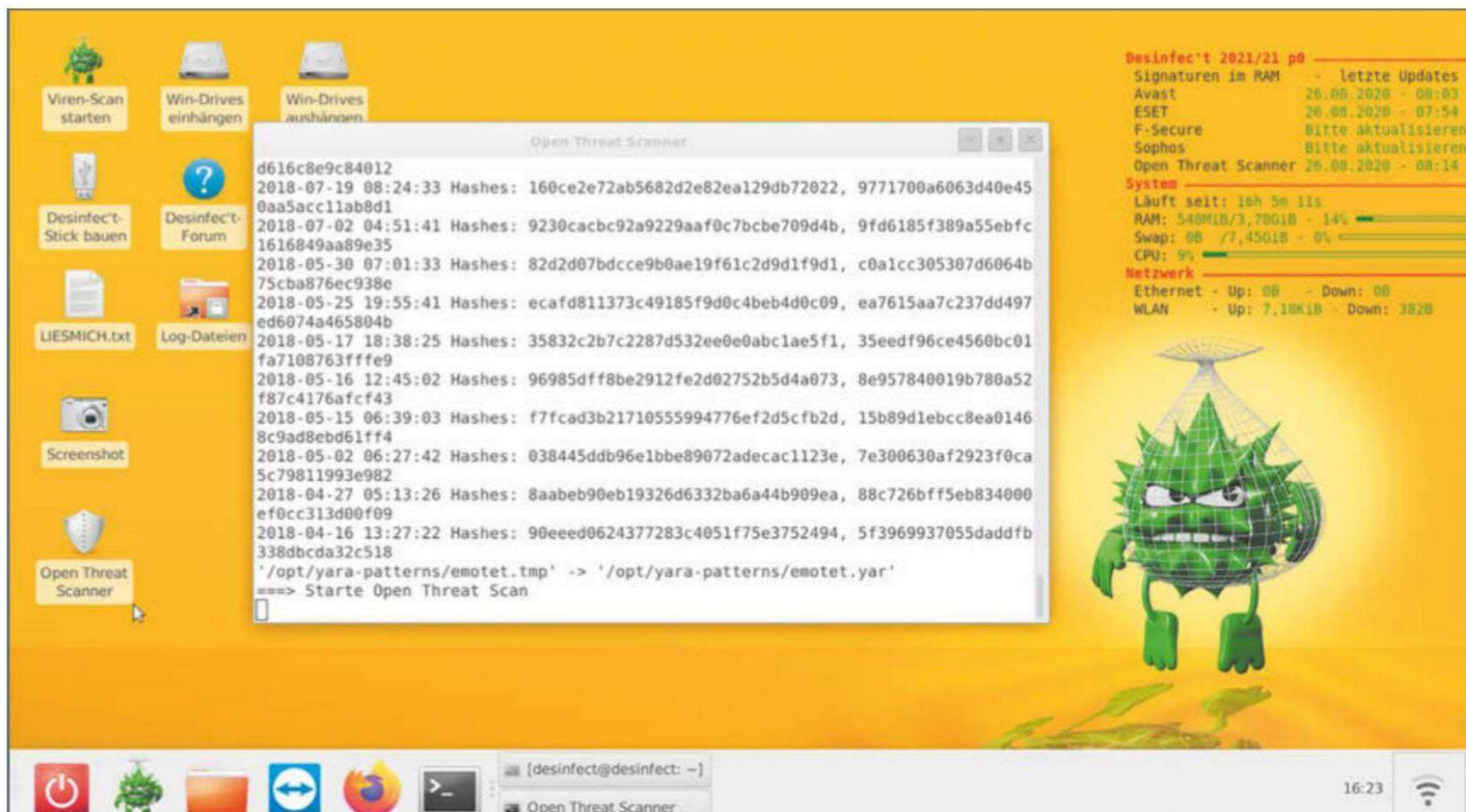
Unter Windows tippen Sie folgenden Befehl in die PowerShell oder die Eingabeaufforderung:

```

python.exe -m pip install pefile
naiveBayesClassifier

```

Anschließend laden Sie yarGen von GitHub (Download via ct.de/w6h1) über „Download ZIP“ herunter.



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

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

```
python3 yarGen.py update
```

Der Vorgang dauert circa zehn Minuten. Zeit für eine Kaffeepause.

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 Git-Hub-Website (siehe ct.de/w6h1). Aber Vorsicht! Es handelt sich um echte Trojaner! Öffnen Sie die Dateien keinesfalls! Wenn Sie mit solchen Dateien unter Windows hantieren, müssen Sie Ihren Virens scanner temporär deaktivieren. Ansonsten funkt 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 vorge-setzte 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. Standard-

mäßig 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 Fehlalarme 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:

```
python3 yarGen.py --opcodes ↵  
↳--score -z 6 -m MalwareEXE
```

Auf der GitHub-Seite des yarGen-Projektes (siehe [ct.de/w6h1](https://github.com/ct-w6h1/yarGen)) 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 Binärcode lesen können und keine Zeit für Analysen haben. Mit der Integration ist Desinfec't die ideale Plattform für schnelle Reaktionen mit eigens erstellten Yara-Regeln.

(des) **ct**

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/w6h1

Es gibt 10 Arten von Menschen. iX-Leser und die anderen.

Jetzt Mini-Abo testen:
3 Hefte + Bluetooth-Tastatur nur **16,50 €**

www.iX.de/testen

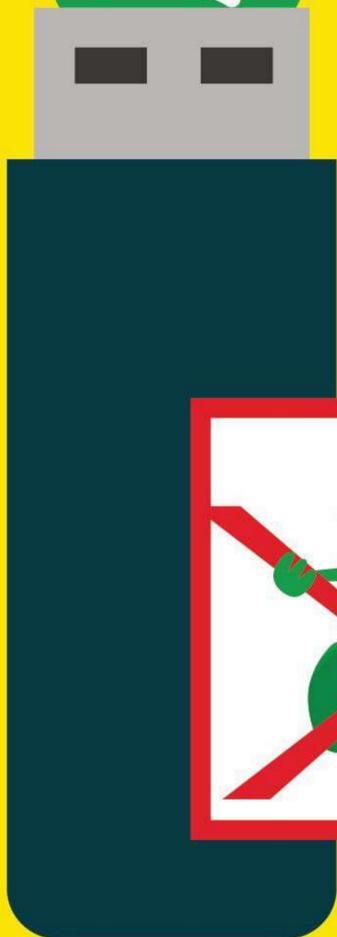
3x als Heft

KI schnell und einfach

Atom, Sublime Text, Visual Studio Code, Vim

MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

www.iX.de/testen 49 (0)541 800 09 120 leserservice@heise.de



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!

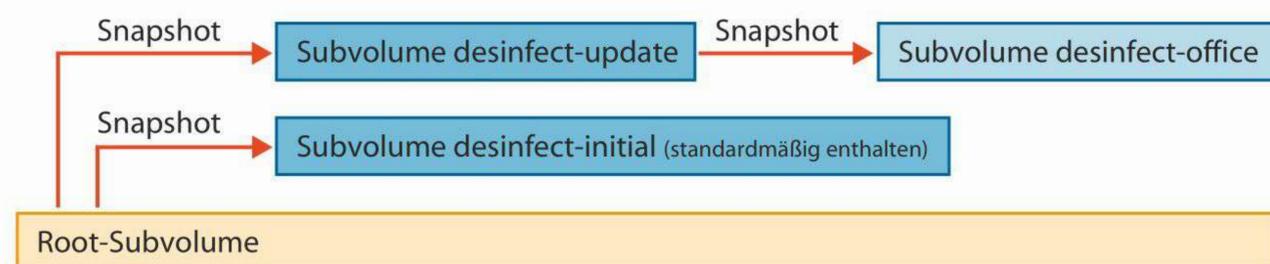
Als erstes Praxisbeispiel aktualisieren Sie Desinfec't und machen das Update persistent. Dafür installieren Sie es zuerst nach der alten Methode, sodass es aus dem RAM läuft. Dann verweben Sie das Update mit einem neu angelegten Subvolume, damit es dauerhaft in Desinfec't integriert ist.

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 2021/22 p1“, hat es geklappt. Steht dort nur „Desinfec't 2021/22“, 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 das Debian-Paket dort:

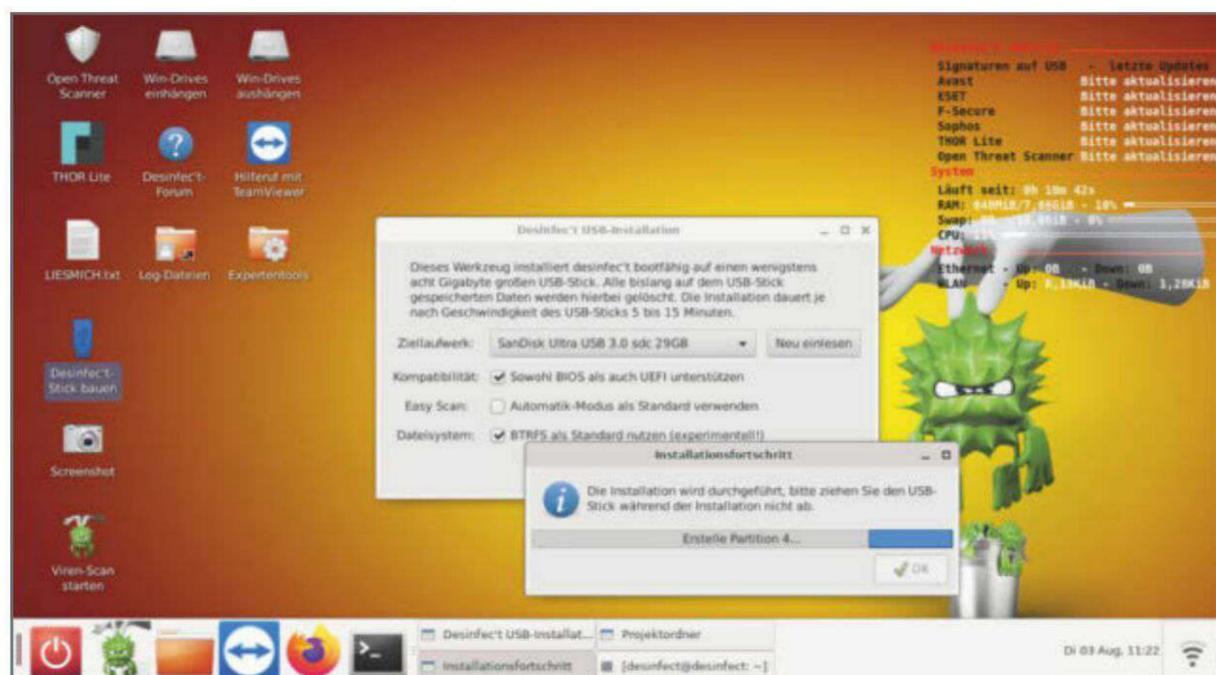
```
sudo chroot /cdrom/desinfect-update/↵
↵.casper/filesystem.dir
dpkg -i /var/cache/apt/archives/↵
↵.desinfect-meta*.deb
```

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 Sicherheitstool 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 Sicherheitstool 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 Vorarbeit 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 Desinfect in einem Rutsch mit LibreOffice aus, aktualisieren Firefox 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 Vorarbeit 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
```

Desinfec't, Btrfs und Windows 10

Bei Desinfec't 2021/22 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 Formatierung

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 2021/22 arbeitet mit versteckten Partitionen. Bisher konnten wir dieses Schema allerdings nicht für einen Btrfs-Stick anwenden – aber wir arbeiten daran.

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 dazwischenfunken. 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:

```
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-Updates nicht standardmäßig auf der Signatur-Partition landen.

Dank der bisherigen Vorbereitungen aktualisieren Sie auch Firefox ganz einfach:

```
apt-get install --reinstall firefox ↵  
↵firefox-locale-de firefox-locale-en
```

Zusätzlich fügen Sie mit dieser Installationsmethode neue Firmware und Treiber hinzu. Das folgende Beispiel statet den in Desinfect 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:

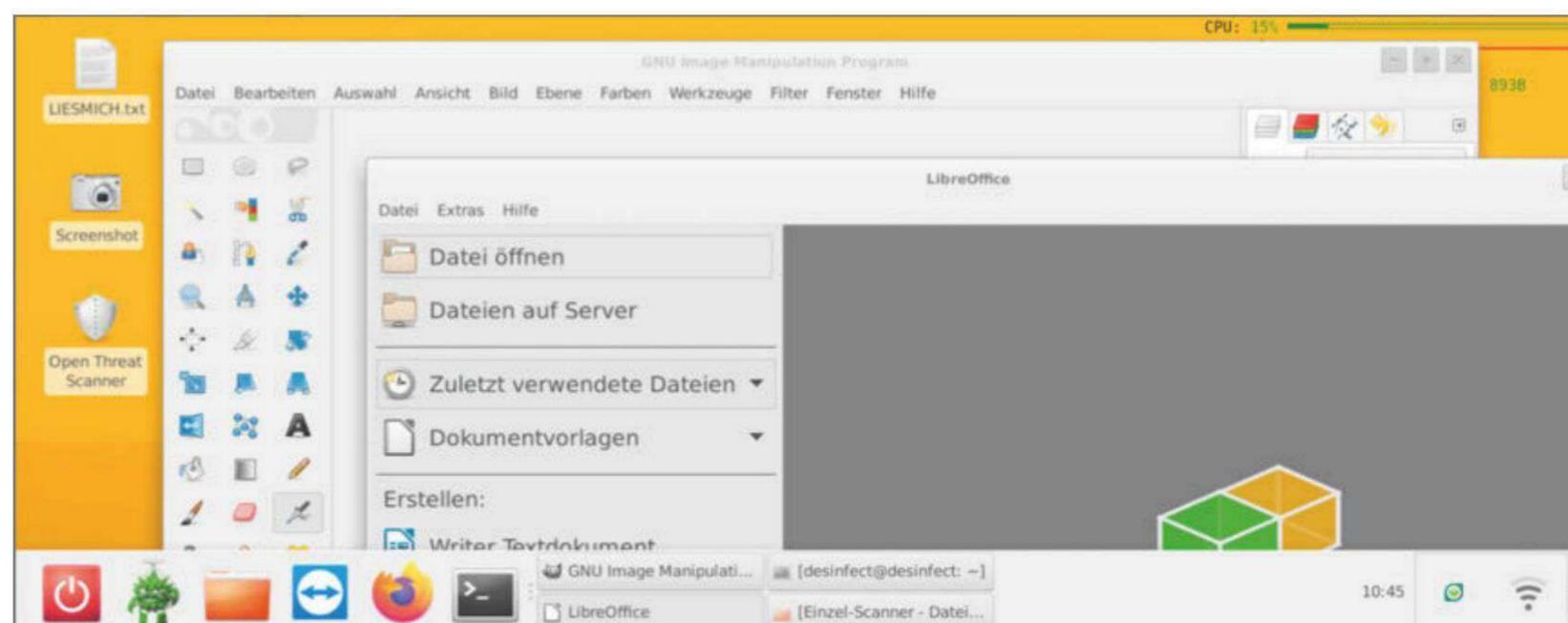
```
sudo apt-get install broadcom-sta-source ↵  
↵broadcom-sta-common broadcom-sta-dkms
```

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
```



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

Mountpoint /cdrom fehlt?

Mit neueren Kernen kann es vorkommen, dass der Mountpoint /cdrom nicht mehr sichtbar ist, nachdem Ubuntu Bootscripte das Rootverzeichnis gewechselt haben. Für diesen Fall haben wir im Bootmenü den Eintrag „Des-

infec'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.

Als Nächstes kommentieren Sie noch die Ubuntu-Repositories via

```
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 wie 4.4 aus dem Jahr 2016 oder 4.19 aus 2018. Ist die Hardware brandneu, müssen aktuelle Mainline-Kernel her – bei Redaktionsschluss war dies 5.14. 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 nachzusehen, welche Mainline-Kernel aktuell sind. Dann kann man direkt im Mainline-Archiv (siehe ct.de/w8yr) 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.58`“ und „`vmlinuz.58`“. 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 zurückzusetzen:

```
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/w8yr) tauschen sich außerdem Tüftler aus. Also keine Angst und viel Spaß beim Basteln!
(des) **ct**

Tipps & Tricks
für Btrfs-Sticks

ct.de/w8yr



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**

Bei 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.

In den Grundlagen-Artikeln 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 Ex-

plorer) gefahrlos umsehen, den Sie über das Ordnersymbol in der Taskleiste erreichen. Die Windows-Laufwerke finden Sie in der Seitenleiste des Dateimanagers 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 Besseren 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 `ntfsclose` oder dem nachinstallierbaren Clonezilla).

Sollten Sie Ihre Windows-Partition nicht finden, etwa weil mehrere kleinteilig partitionierte Festplatten im System stecken, hilft die Laufwerksübersicht 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 ab Seite 10.

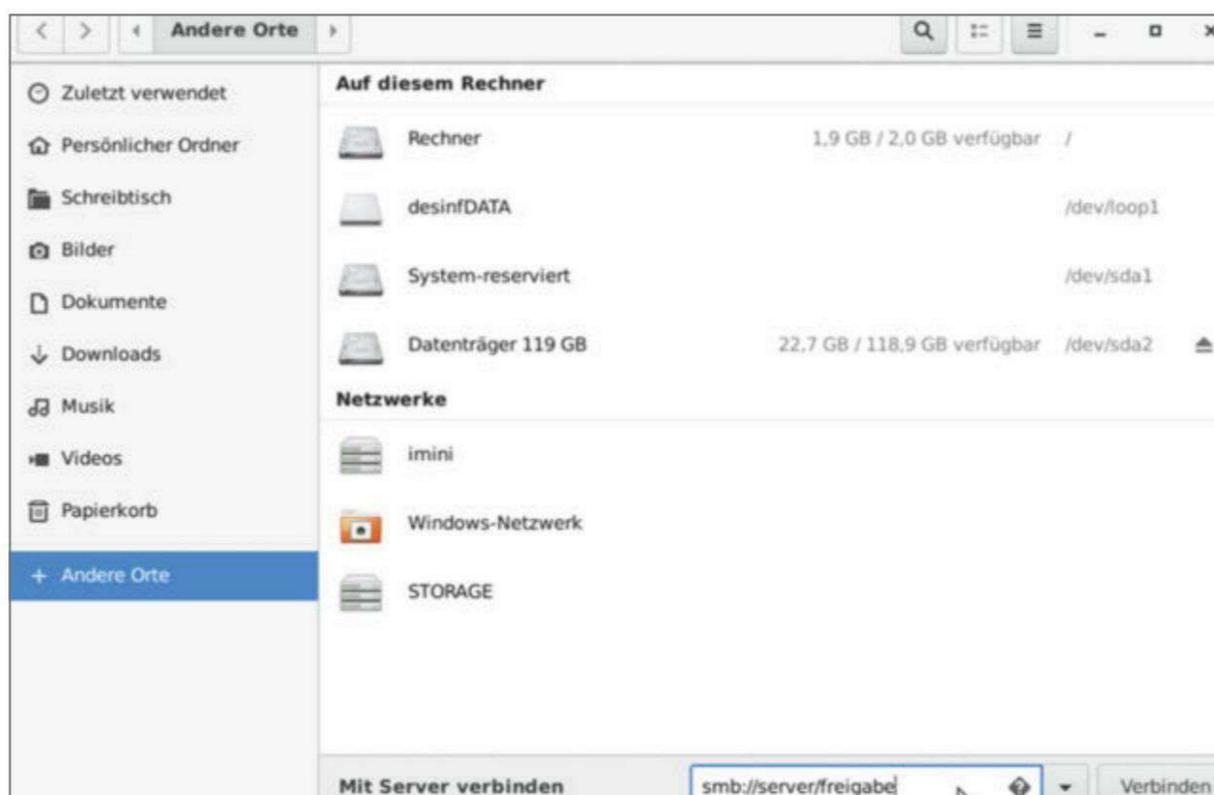
Eine Anmerkung noch zu Windows-Installationen oder Datenplatten, die auf einem Software-beziehungsweise BIOS-RAID gründen: Das hinter dem Symbol auf dem Desinfec't-Desktop „Win-Drives einhängen“ hinterlegte Skript schafft es nicht, die Windows-Partition zu finden und einzuhängen. Benutzen Sie in einem 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: Desinfec't 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 eingehängt haben). Öffnen Sie dann in den Expertentools die Laufwerksübersicht, wählen Sie die Windows-Partition aus und klicken Sie den „Play“-Knopf (das nach rechts gerichtete Dreieck) an. Desinfec't 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 Einhängpunkt 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 cp SAM /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.

Desinfec't 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-

nannten Kniff, das bei der Installation angelegte, aber deaktivierte Konto namens „Administrator“ anklicken 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.

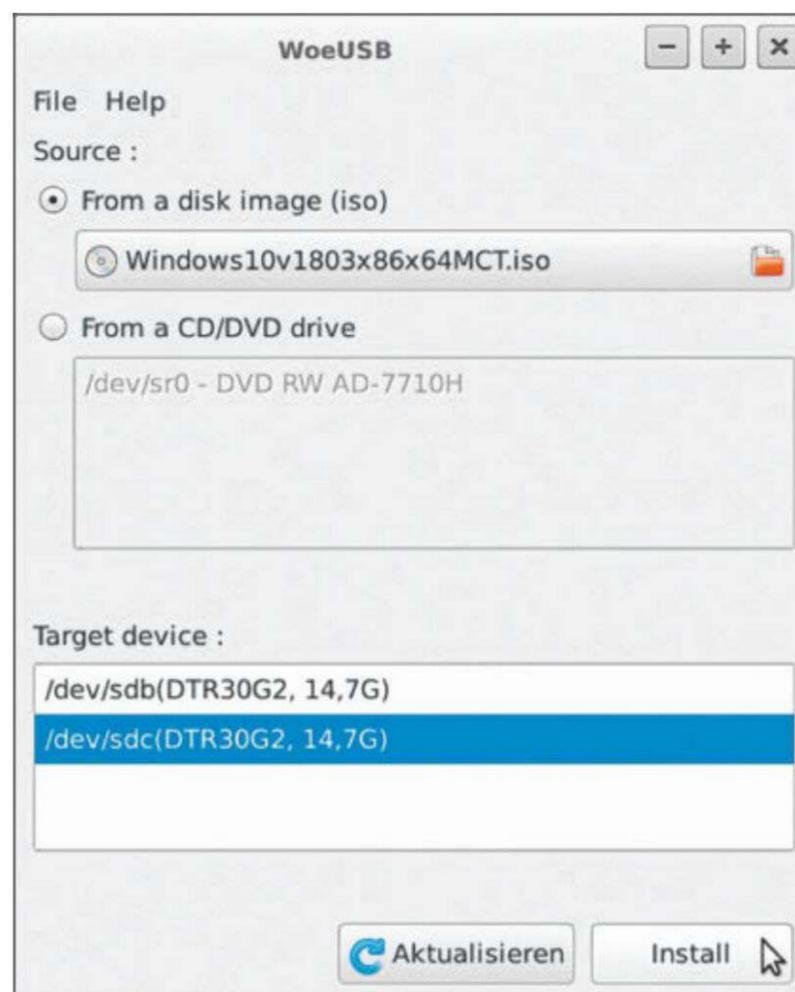
Wenn Windows partout auf das falsche Profil-Verzeichnis zugreift (manchmal legt es die auch einfach unter einem abgewandelten Namen neu an), hilft womöglich ein Eingriff in der Registry. Unter HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList (Datei SOFTWARE im o.g. Verzeichnis) 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.

Weitere Hinweise

[ct.de/w7p7](https://www.ct.de/w7p7)

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 `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 Bionic Beaver 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:

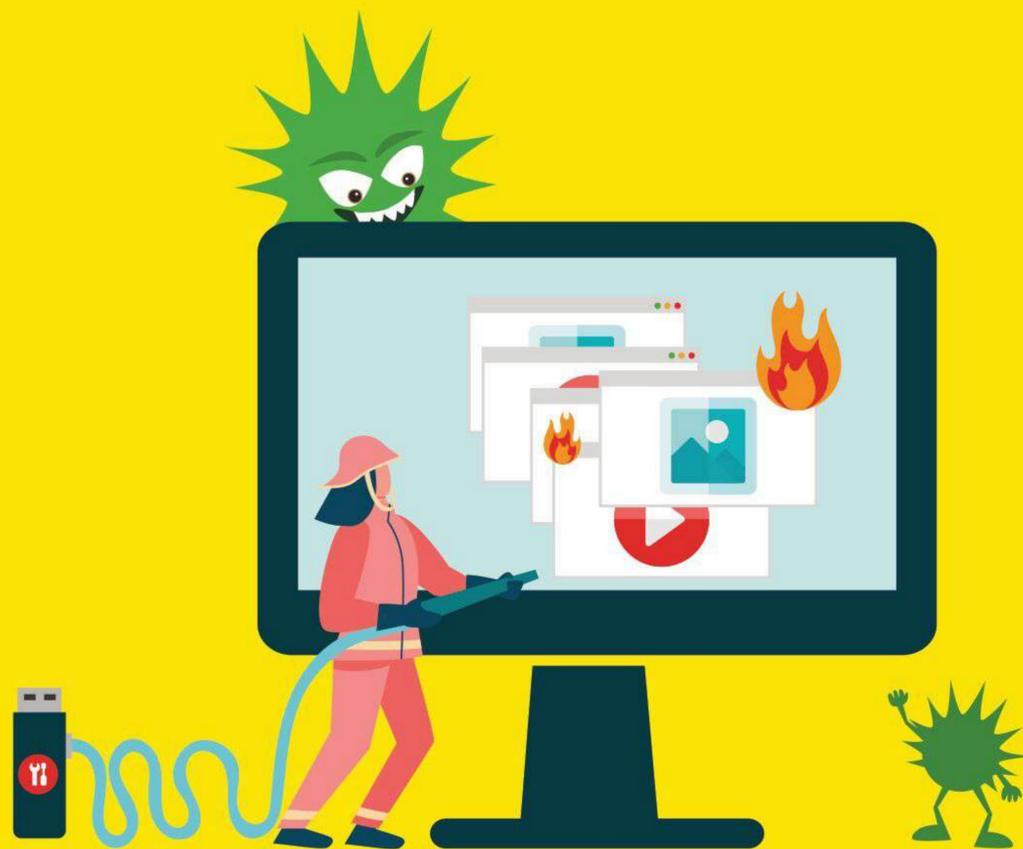
```
sudo cp /var/cache/apt/archives/* ↵  
↵/opt/desinfect/signatures/deb
```

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) **ct**



Fotos und Dateien retten

Hat man versehentlich den falschen USB-Stick formatiert oder die USB-Festplatte vom Schreibtisch gefegt, wird einem oft erst bewusst, welche wichtigen 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 Löt pads 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 zwischen 100 und 250 Euro.

Laut dem deutschen Unternehmen MSS Kupfrian kostet die Datenrettung im Durchschnitt zwischen

800 und 1500 Euro. Das ist für die Rettung einer Schulhausaufgabe sicher zu viel, für die gerade aufgenommenen Hochzeitsfotos, um eine Steuerschätzung des Finanzamts zu verhindern oder um eine Abschlussarbeit termingerecht fertigzubekommen aber wahrscheinlich gerechtfertigt. In diesen Fällen sollten Sie jedoch alle Selbstversuche unterlassen, denn dadurch können die Daten schlimmstenfalls unwiederbringlich zerstört werden.

Physisch, logisch?

Wie gut Ihre Aussichten sind, die Daten in Eigenregie 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 Festplatten und nicht mehr zugreifbare Zellen in Flash-Speichern schnell vermehren, wenn das Medium weiter in Betrieb bleibt. Deshalb gilt es bei Hardware-Defekten, das Medium in einem Durchgang ein letztes Mal auszu-lesen, bevor Sie es außer Betrieb nehmen. Das dabei erstellte Abbild dient Ihnen anschließend als Grundlage für die Datenrettung.

Für diesen Zweck eignet sich Desinfec't besonders gut, da es die wichtigsten Tools zur Datenrettung bereits an Bord hat und die Dateisysteme von Windows, macOS und Linux unterstützt. 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 aufnimmt – ein großer USB-Stick oder eine externe Festplatte sind hierfür gut geeignet. Wie Sie Desinfec't auf einem USB-Stick installieren und booten, haben wir ab Seite 10 bereits ausführlich beschrieben.

Ein erstes Indiz für einen mechanischen Defekt sind veränderte Laufgeräusche und Zugriffsgeräusche der Festplatte. SSDs und andere Flash-Speicher machen natürlich keine Geräusche, sodass Sie hier per Software nach Fehlern fahnden müssen (siehe Seite 44). Für die Diagnose der Hardware eignet sich vor allem die Self-Monitoring, Analysis and Reporting Technology, kurz S.M.A.R.T oder auch Smart genannt. Dabei überprüft sich das Laufwerk in regelmäßigen Abständen selbst und zeichnet außerdem besondere 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 Laufwerksnamen 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 Festplatte 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 Desinfec't-USB-Stick bekommt einen Laufwerksnamen zugeordnet, manchmal sogar `/dev/sda`.

Sofern die Partitionstabelle des defekten Laufwerks noch lesbar war, zeigt `lsblk` neben dem Laufwerksnamen, 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 verständlich zu halten, verwenden wir nachfolgend `/dev/sdb` als Laufwerksnamen. 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 übersichtliche Liste hat numerische IDs am Anfang der Datenzeilen, über die Sie die einzelnen Angaben leicht wiederfinden können.

Bei defekten Laufwerken finden Sie üblicherweise eine hohe Raw Read Error Rate (ID 1), die (korrigierbare) Lesefehler 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 Sektoren 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, ver-

meidet 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
```

Denken Sie daran, dass Sie bei ntfsclone als letzten Parameter die auszulesende Partition und nicht wie bei dd und ddrescue den Laufwerksnamen 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

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, widerspens-

tige 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.

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 verlorengegangene oder versehentlich gelöschte Dateien wiederherzustellen.

Eingehängt

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 `Desinfec't` 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 zwangsläufig 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 -a 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 `Desinfec't` 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.

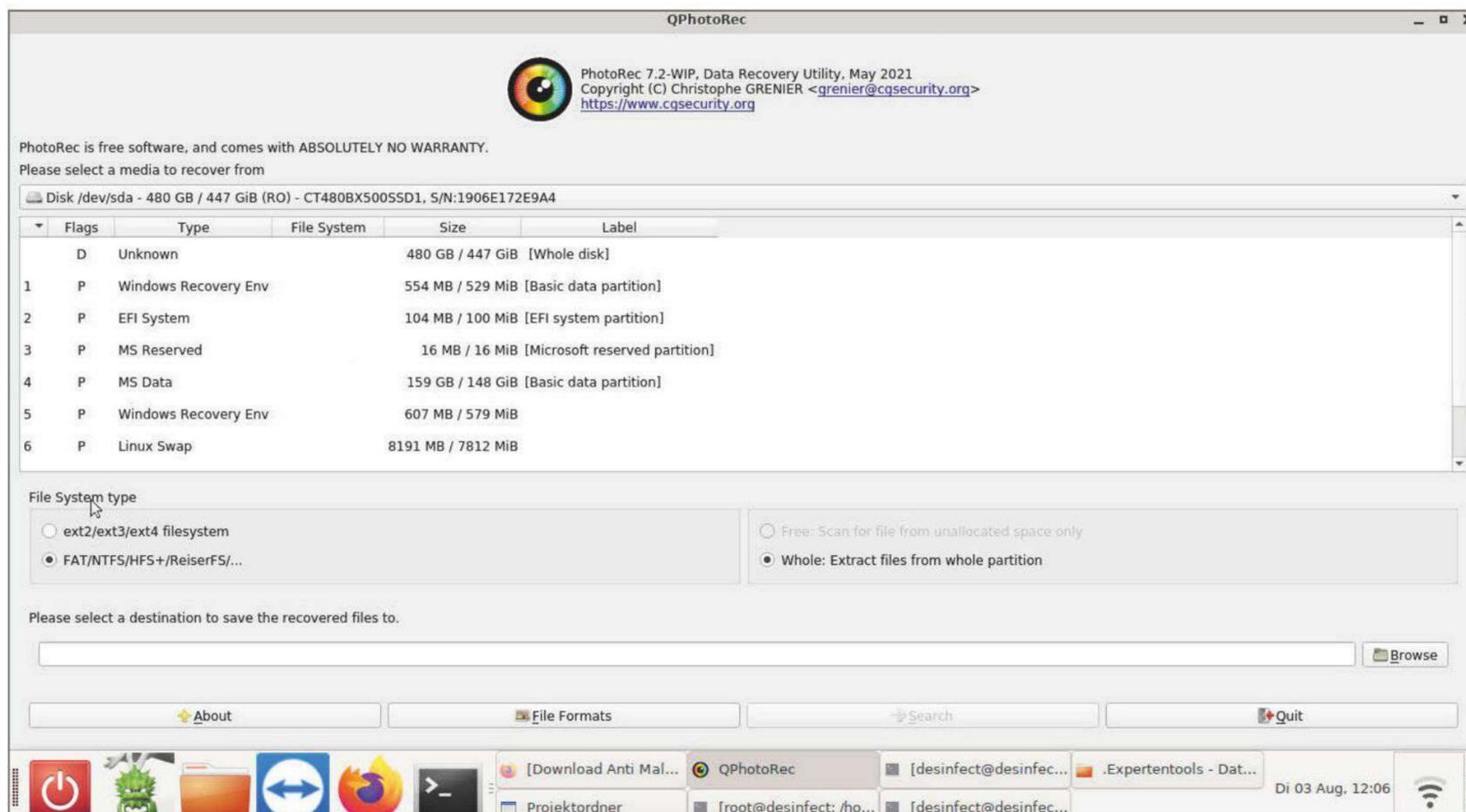
Soll `Photorec` den Datenträger direkt auslesen, etwa weil nur ein logischer Fehler vorliegt, aber die Hardware in Ordnung ist, so müssen Sie `Photorec` beim Aufruf Root-Rechte verschaffen:

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

Arbeiten Sie hingegen mit einem Image, genügen die Standardrechte des `Desinfec't`-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 Verzeichnisbaum von `Desinfec't` hangeln zu müssen:

```
photorec disk.img
```

`Photorec` kommt mit einer rein englischsprachigen Bedienoberfläche und einer ziemlich eigenwilligen Bedienung. Das Menü befindet sich am unteren Rand des Konsolenfensters und wird mit den Cursor-Tasten Links und Rechts ausgewählt, Listen etwa von



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

Laufwerken oder Partitionen finden sich im mittleren Bereich des Fensters und werden mit den Cursor-Tasten Auf und Ab ausgewählt. Um die Auswahl zu bestätigen, verwenden Sie Enter.

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 10 000 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**

Klein – aber oho!

Mit MicroPython spielend leicht Mikrocontroller programmieren

Make Micropython Special

Diese Make-Sonderausgabe zeigt Ein- und Umsteigern, wie man mit MicroPython leicht und schnell eigene Projekte mit dem ESP32 umsetzt. Wie immer in Make Specials geht's sofort in die Praxis mit Audio-Projekten, einer CO2-Ampel und mehr.

Auch als einzelnes Heft erhältlich.

shop.heise.de/make-micropython

Heft + PDF
für nur

19,90 € >



Heft + PDF
mit 29%
Rabatt

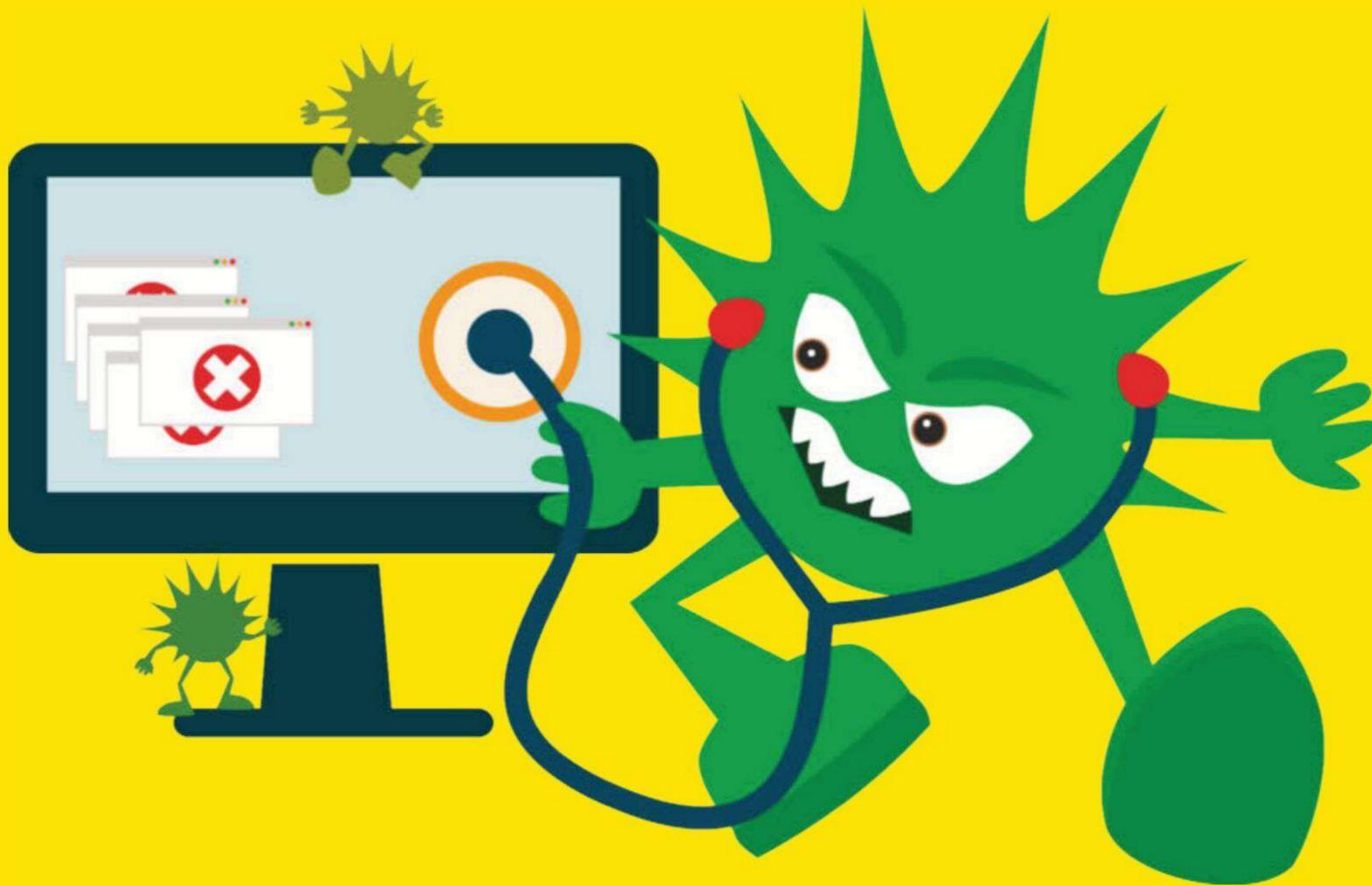


NEU
und exklusiv
im heise shop

 heise Shop

shop.heise.de/make-micropython >

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



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**

Muckt Ihr Betriebssystem? Oder wollen Sie einen fremden, unbekanntem 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 einen damit bespielten USB-Stick booten. Wie das geht, haben wir bereits ausführlich beschrieben (ab Seite 10). Die erwähnten Diagnose-Tools sind übrigens auch Bestandteil anderer Linux-Distributionen, 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 unsauberes 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

```

desinfec't@desinfec't: ~$ sudo lshw -short
H/W-Pfad      Gerät      Klasse      Beschreibung
-----
/0            system     KS2Jr
/0/0         bus        KS2Jr
/0/0         memory     64KiB BIOS
/0/4         processor  Intel(R) Core(TM) i3 CPU          M 350  @ 2.27GHz
/0/4/5       memory     32KiB L1 Cache
/0/4/6       memory     256KiB L2 Cache
/0/4/7       memory     3MiB L3 Cache
/0/41        memory     4GiB Systemspeicher
/0/41/0      memory     4GiB SODIMM DDR3 Synchron 1067 MHz (0,9 ns)
/0/41/1      memory     DIMMProject-Id-Version: lshwReport-Msgid-Bugs-To: FULL NAME <EMAIL@ADDRESS>P0-Revision-Date: 201
/0/41/2      memory     DIMMProject-Id-Version: lshwReport-Msgid-Bugs-To: FULL NAME <EMAIL@ADDRESS>P0-Revision-Date: 201
/0/41/3      memory     DIMMProject-Id-Version: lshwReport-Msgid-Bugs-To: FULL NAME <EMAIL@ADDRESS>P0-Revision-Date: 201
/0/100       bridge     Core Processor DRAM Controller
/0/100/1     bridge     Core Processor PCI Express x16 Root Port
/0/100/1/0   display    Park [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  usbl       bus        EHCI Host Controller
/0/100/1a/1/1 bus        Integrated Rate Matching Hub
/0/100/1a/1/1/2 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 wsl        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 ens5f5     network    JMC250 PCI Express Gigabit Ethernet Controller

```

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

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-Sockel 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-CPU's beispielsweise, wenn Sie auf 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/*
```

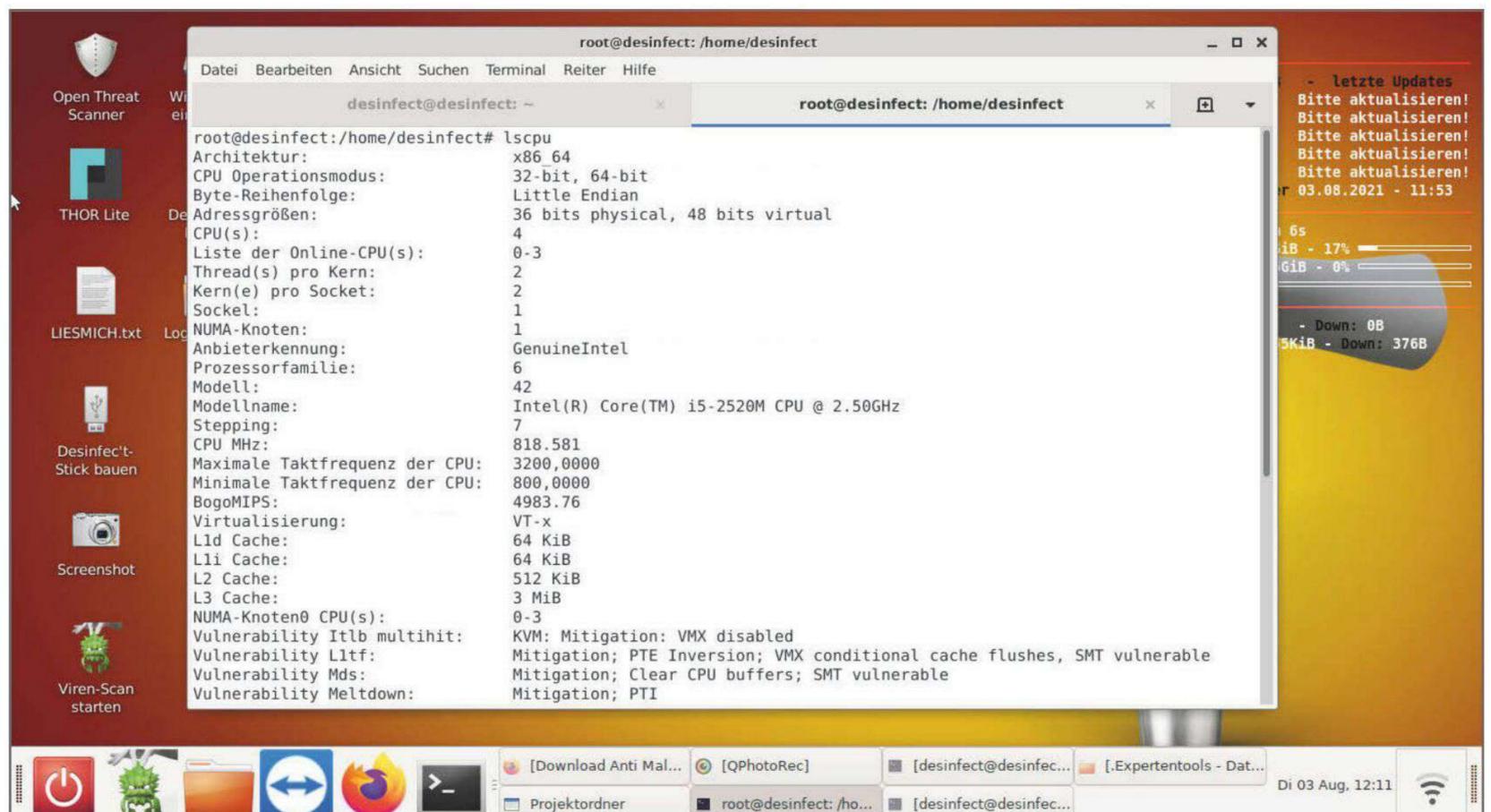
Bei Desinfec't zeigt das den Inhalt von Dateien zu vielen Sicherheitslücken, die seit Anfang 2018 bekannt wurden. Findet sich in den Dateien ein mit „Vulnerable“ oder „Mitigation“ beginnender Text, dann ist Ihr Prozessor für die im Dateinamen genannte Sicherheitslücke anfällig.

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 Prozessorklücken, 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 zwei Dutzend Einträge langen Liste finden sich oft die Grafik- und Netzwerkprozessoren, die Klassenbezeichnungen wie „VGA compatible controller“ oder „Ethernet controller“ kennzeichnen. Die dahinter stehenden 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

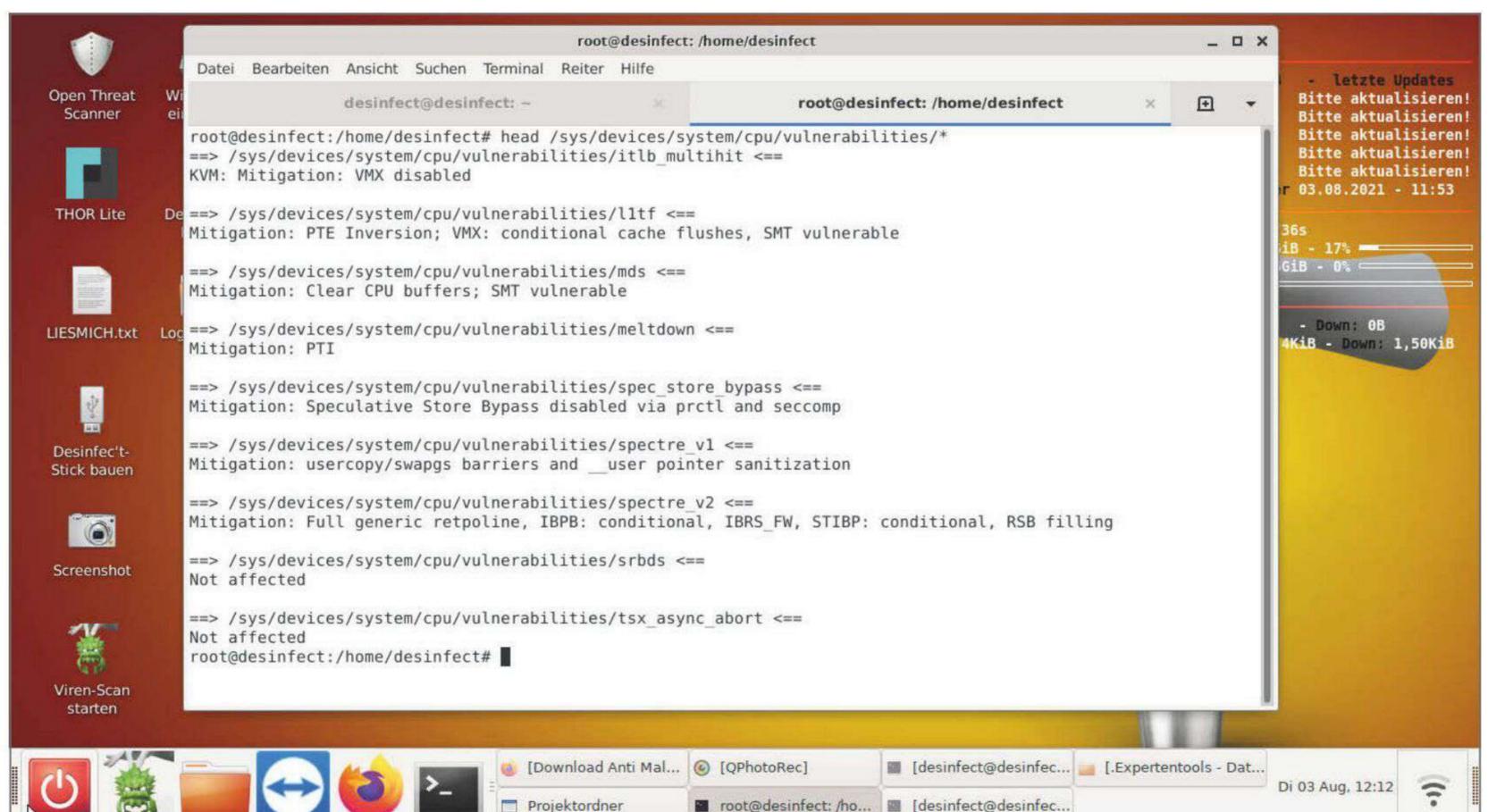
Das Werkzeug **lscpu** nennt die Zahl der CPU-Kerne sowie Minimal- und Turbo-Taktfrequenz.

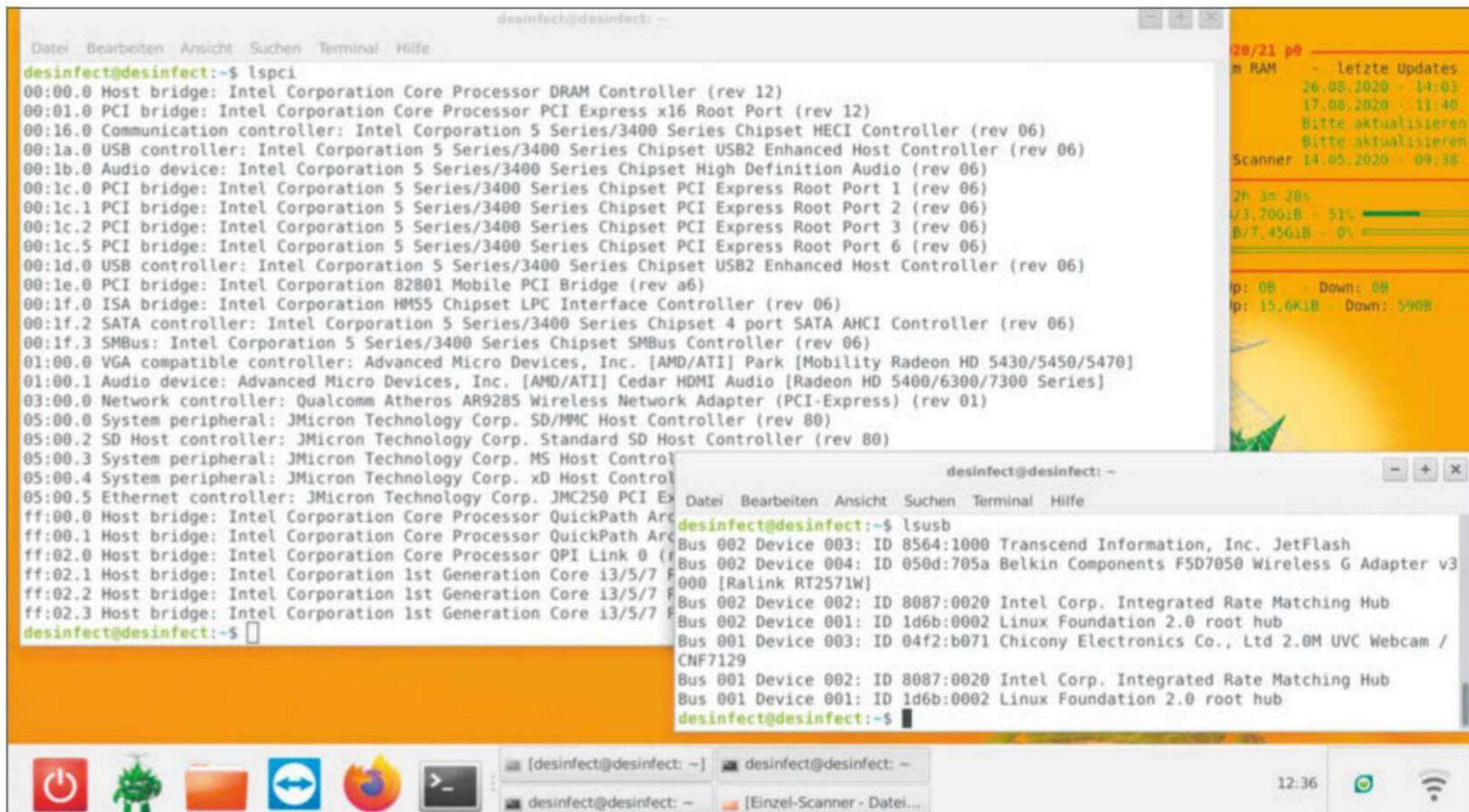


manchmal unter ganz unterschiedlichen Bezeichnungen vertreiben – der Grafikkern eines Intel-Core-i-Prozessors wird daher vielleicht als GPU eines Xeon dargestellt. Da auch das eingangs erwähnte lshw auf solche Daten zurückgreift, sollten

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

Desinfect't klärt, ob Ihr Prozessor für die Sicherheitslücken Meltdown und Spectre anfällig ist.





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

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 Gerätebezeichnungen 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 `lspci` und `lsusb` direkt vom Mainboard und den jeweiligen Hardware-Komponenten. In den Aufstellungen tauchen daher auch Komponenten auf, die der von Desinfec't 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 Desinfec't aber in Einzelfällen nicht – das ist einer von mehreren Gründen, warum Desinfec't 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 Ihrer 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 Gerätebezeichnung. 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 Gerätebezeichnung 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     0x000f   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-Löschfehler (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 auf Seite 38.

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:

```
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 `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 Notebook-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.

Befeuern

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 belasten. Für diese Aufgabe können Sie den Furmark von GpuTest nutzen. Laden Sie dessen Linux-Version via ct.de/wbpr herunter, um es dann wie folgt zu starten:

```
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 nennenswerte 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 halt 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 `lsusb` 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 nur einige der vielen Möglichkeiten, die die erwähnten Programme bieten. Diese liefern meist selbst eine Übersicht über ihr Potenzial, 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) **ct**

Literatur

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

GpuTest herunterladen

ct.de/wbpr



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 aufgebrezelt haben, genügt meist, um sie mit überschaubarem Aufwand zu bergen.

Von **Peter Siering**

Ein 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 hängen: 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 Rettungsplatte 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=noautodetect` 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](S)
        242149440 blocks
md127 : inactive sdb1[1](S)
        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 irreführende 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 herunterzukratzen. Die Produkte der Firma QNAP haben die nicht erfüllt: Aktuelle 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 geschickt, 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 eingerichtet wurde beziehungsweise sein Speicherplatz provisioniert worden ist (thick oder thin). Obendrein gibt es wohl noch eine Legacy-Konfiguration, die kompatibel zu regulären Linux-Techniken bleibt. Ob Ihre QNAP-Platten von einer regulären Linux-Distribution lesbar sind oder nicht, finden Sie beim Suchen nach physischen 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 will sie vorerst beibehalten. Andere Hersteller hingegen werben sogar damit, dass man die Platten ihrer Geräte mit regulären 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 zwangsweisen 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 wz--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 Rettungsdaträger. Bezogen auf die bisherigen Beispiele, also der NAS-Platte als „sdb“ und dann als `/target` eingehängtem Rettungsdaträger, 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 umschiffet. Die Parameter unterscheiden sich vom einfachen `dd`. Details zu `ddrescue` und das Retten von Dateien führen wir im Artikel auf ab Seite 38 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 Rettungsdaträger 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.

Schutzschirm

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/
```

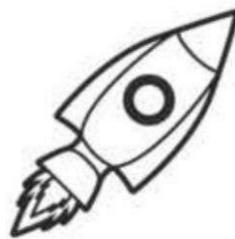
Er bindet das physische Gerät /dev/sdb als neues Gerät unter dem Pfad /fakedev/sdb.dd ein. Daten aus schreibenden Zugriffen, die auf dieses virtuelle Gerät erfolgen, landen in der Datei /target/sdbcache und nicht auf /dev/sdb. Gesetzt den Fall, /dev/sdb enthält wie in den bisherigen Beispielen zwei Partitionen, 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

**MIT
Technology
Review**
Das Magazin für Innovation von Heise

40%
Rabatt



**Die Welt verstehen,
wie sie morgen sein wird.**

2 Ausgaben inklusive Prämie nach Wahl:

mit-tr.de/testen

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.

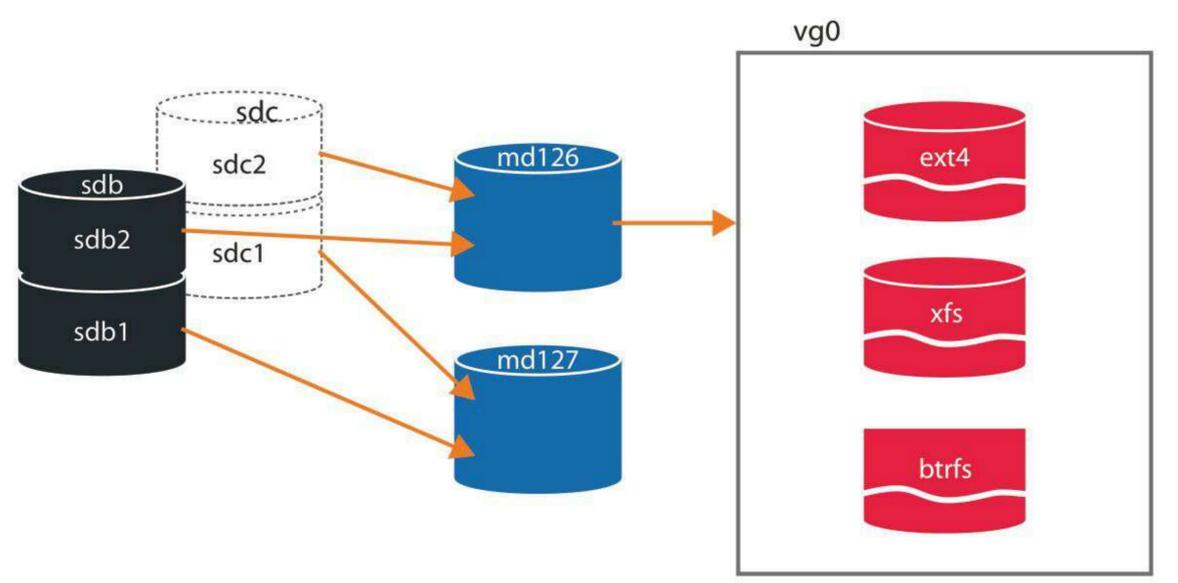
Einfacher ist das Auslesen von NAS-Daten, wenn die Platten direkt mit einem Dateisystem bespielt sind. Das ist etwa bei Platten aus einem Selbstbau-NAS mit FreeNAS als Software der Fall. Die kann Desinfec't von sich aus lesen (dank integriertem ZFS on Linux). ZFS kennt zwar unterschiedliche Feature-Sets, 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: pctest
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:
  pctest          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 pctest -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 logische Volumes. Die kann man in ihrer Größe verändern. Die logischen Volumes versehen sie mit einem Dateisystem (`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 dürften Sie Ihre Daten auf dem größten RAID-Verbund finden.

Die einzelnen RAIDs 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/wpvt 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 zerstören.

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 Elektroschrottsammlung 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 Hersteller spezialisiert, weil die das mit der Offenheit von Linux nicht so ernst nehmen und eben mehr als nur die Frisur ändern. (ps) **ct**

Literatur

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

Ergänzende Hinweise

ct.de/wpvt

Aufrüsten im Homeoffice

Heft + PDF
mit 29%
Rabatt

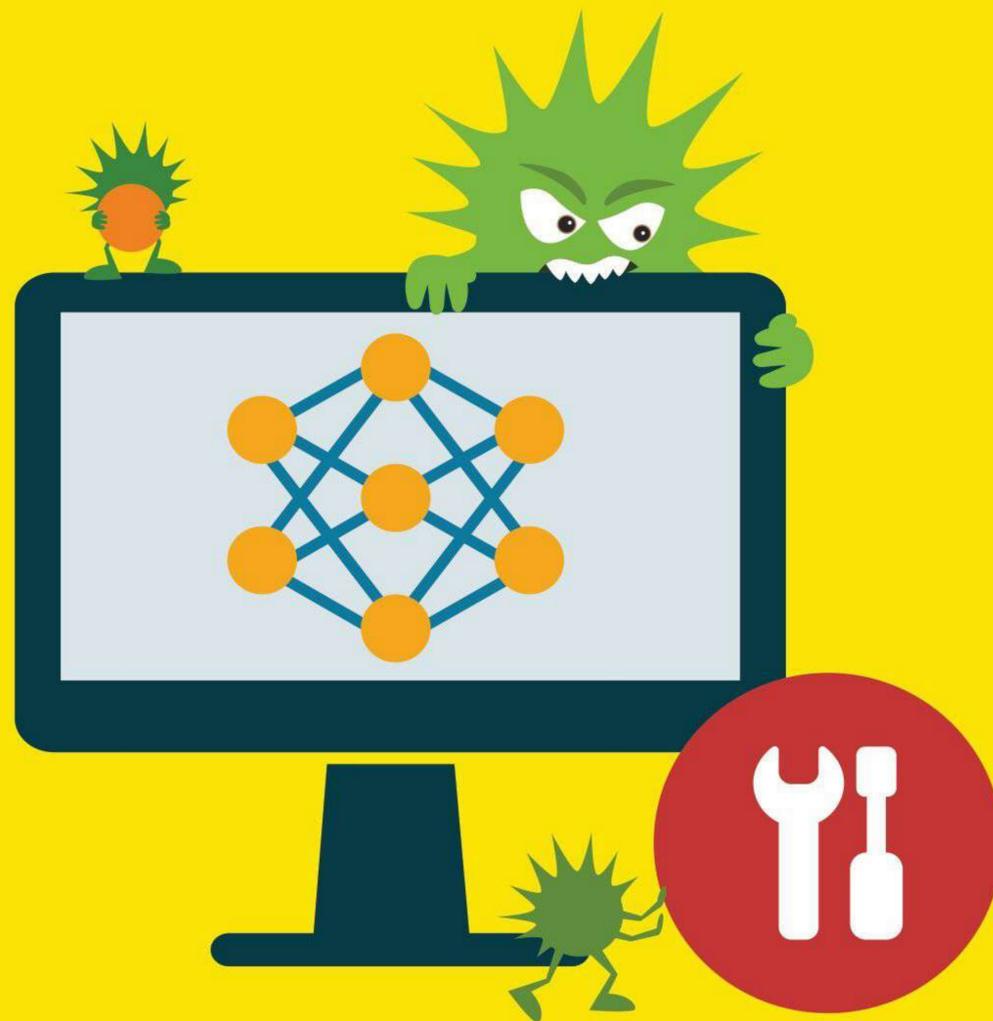


NEU

 heise Shop

shop.heise.de/ct-hardware-ho21

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



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. Wie in

den vorhergehenden Teilen unserer Desinfec't-Artikelreihe 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 nunmal zusetzt, etwa in Form von unerwünschten Browser-Plug-ins, Schädlingen ...

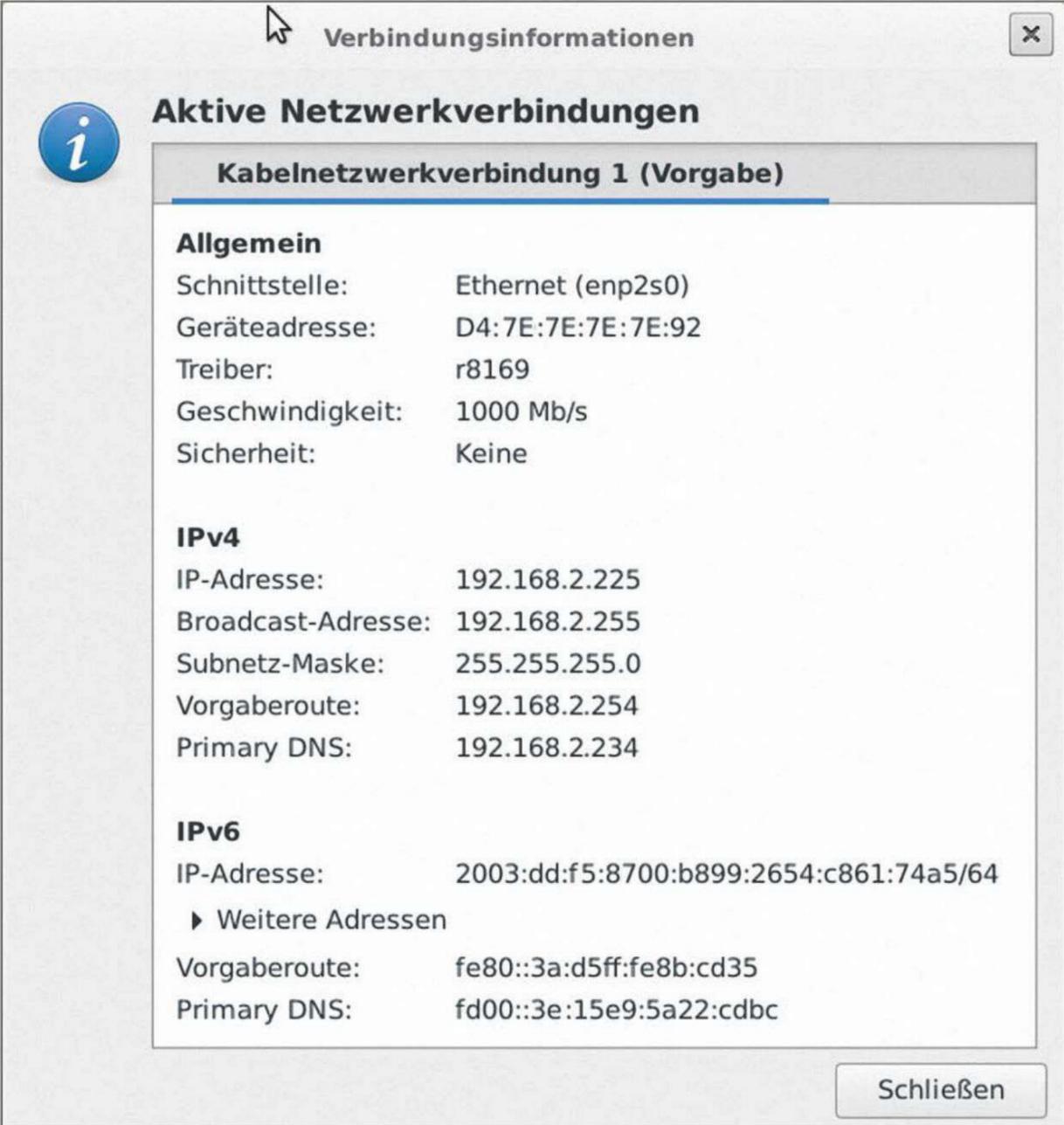
Insofern können Sie Desinfec't auch benutzen, um alltägliche Aufgaben zu erledigen und es in die Fußstapfen seiner nicht mehr weiterentwickelten Geschwister Surfex und Bankix zu setzen: Es eignet sich, um mal eben eine Überweisung im Browser abzuschicken, mal eben zu surfen et cetera - von

der DVD gebootet, muss man keine Änderung an Desinfec't selbst befürchten. Anders als seine igiten 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 Netzwerkd Diagnose.

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 Zugangs-

Der Knopf unten rechts in der Task-Leiste des Desinfec't-Desktop führt in die Netzwerkkonfiguration. Dort lassen sich die aktuellen Konfigurationsdaten einsehen und ändern sowie Schnittstellen ein- und ausschalten.



The screenshot shows a window titled 'Verbindungsinformationen' with a close button in the top right. Below the title bar is a section 'Aktive Netzwerkverbindungen' with an information icon on the left. Underneath, there is a sub-section for 'Kabelnetzwerkverbindung 1 (Vorgabe)'. This section is divided into three parts: 'Allgemein', 'IPv4', and 'IPv6'. Each part contains a list of network parameters and their values.

Allgemein	
Schnittstelle:	Ethernet (enp2s0)
Geräteadresse:	D4:7E:7E:7E:7E:92
Treiber:	r8169
Geschwindigkeit:	1000 Mb/s
Sicherheit:	Keine

IPv4	
IP-Adresse:	192.168.2.225
Broadcast-Adresse:	192.168.2.255
Subnetz-Maske:	255.255.255.0
Vorgaberoute:	192.168.2.254
Primary DNS:	192.168.2.234

IPv6	
IP-Adresse:	2003:dd:f5:8700:b899:2654:c861:74a5/64
▶ Weitere Adressen	
Vorgaberoute:	fe80::3a:d5ff:fe8b:cd35
Primary DNS:	fd00::3e:15e9:5a22:cdbc

At the bottom right of the window is a 'Schließen' button.

daten 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. Surfen 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` 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“ Desinfec't 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 ersatzweise in die Konfiguration von Desinfec't 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-Nameservers anzusprechen: `193.99.144.80` oder `8.8.8.8`. Kommt hier keine Antwort der Gegenseite, probieren Sie es mit der von Desinfec't als „Vorgabroute“ 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 durchexerzierten 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 – unser Artikel in [1] zeigt, wie es richtig geht.

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 Freigabennamen 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.

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.



shop.heise.de/ct-fritzbox21

Router sicher im Griff!

**Heft + PDF
mit 29% Rabatt**

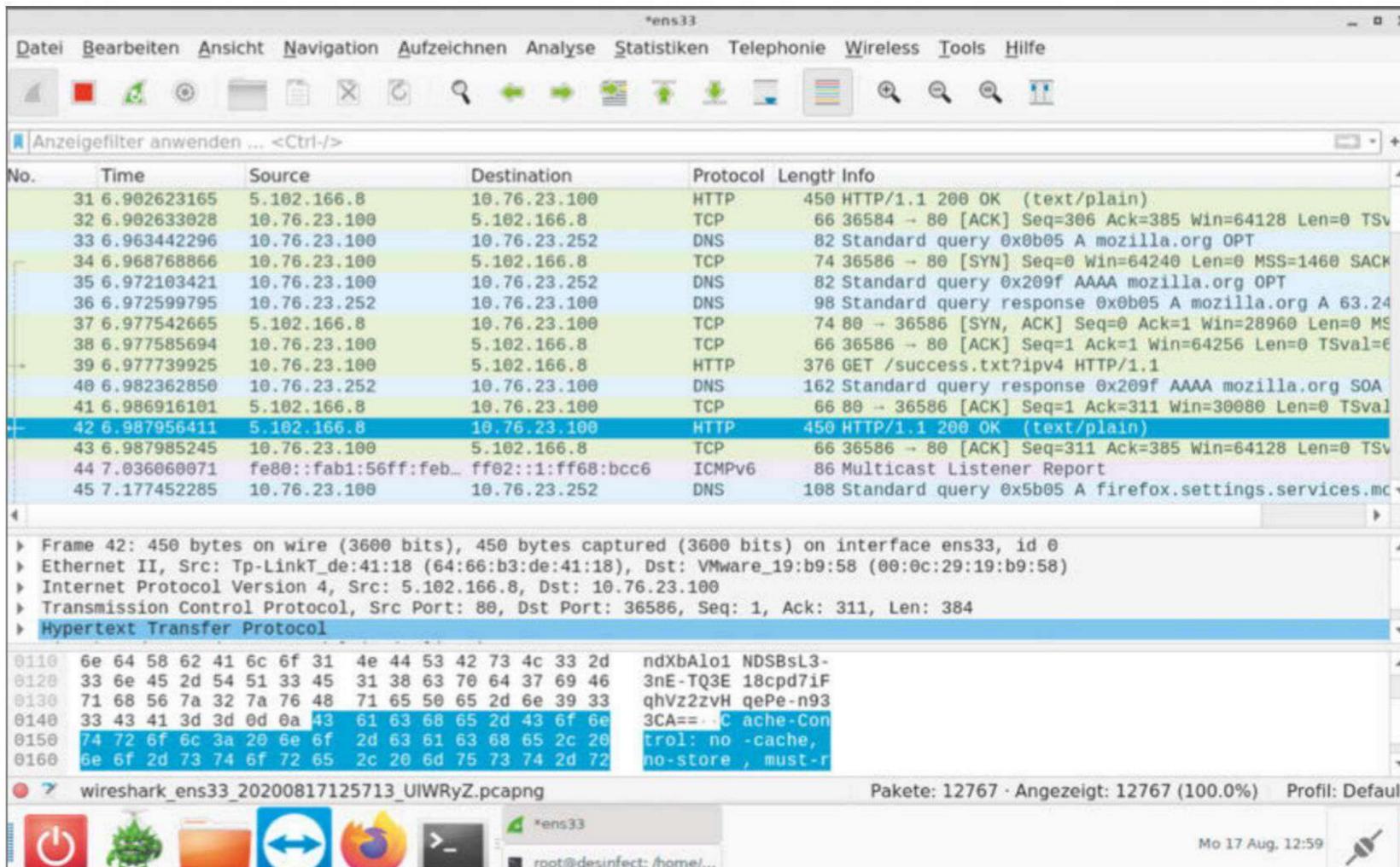


shop.heise.de/ct-fritzbox21

Wappnen Sie Ihre Fritzbox gegen Angriffe von Außen und machen Sie Ihr Smart Home fit mit dem neuen **Sonderheft von c't**:

- ▶ Ihre Fritzbox absichern, erweitern, tunen
- ▶ Über 170 Seiten konzentrierte c't-Expertise
- ▶ Auch im Set mit Fachbuch erhältlich
- ▶ Für Abonnenten portofrei

Heft für 14,90 € • PDF für 12,99 € • im Set 29% günstiger!



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.

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 Netzwerk Dosen 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 wärmte 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 Automaten 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 linsid` das Paket für die

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.

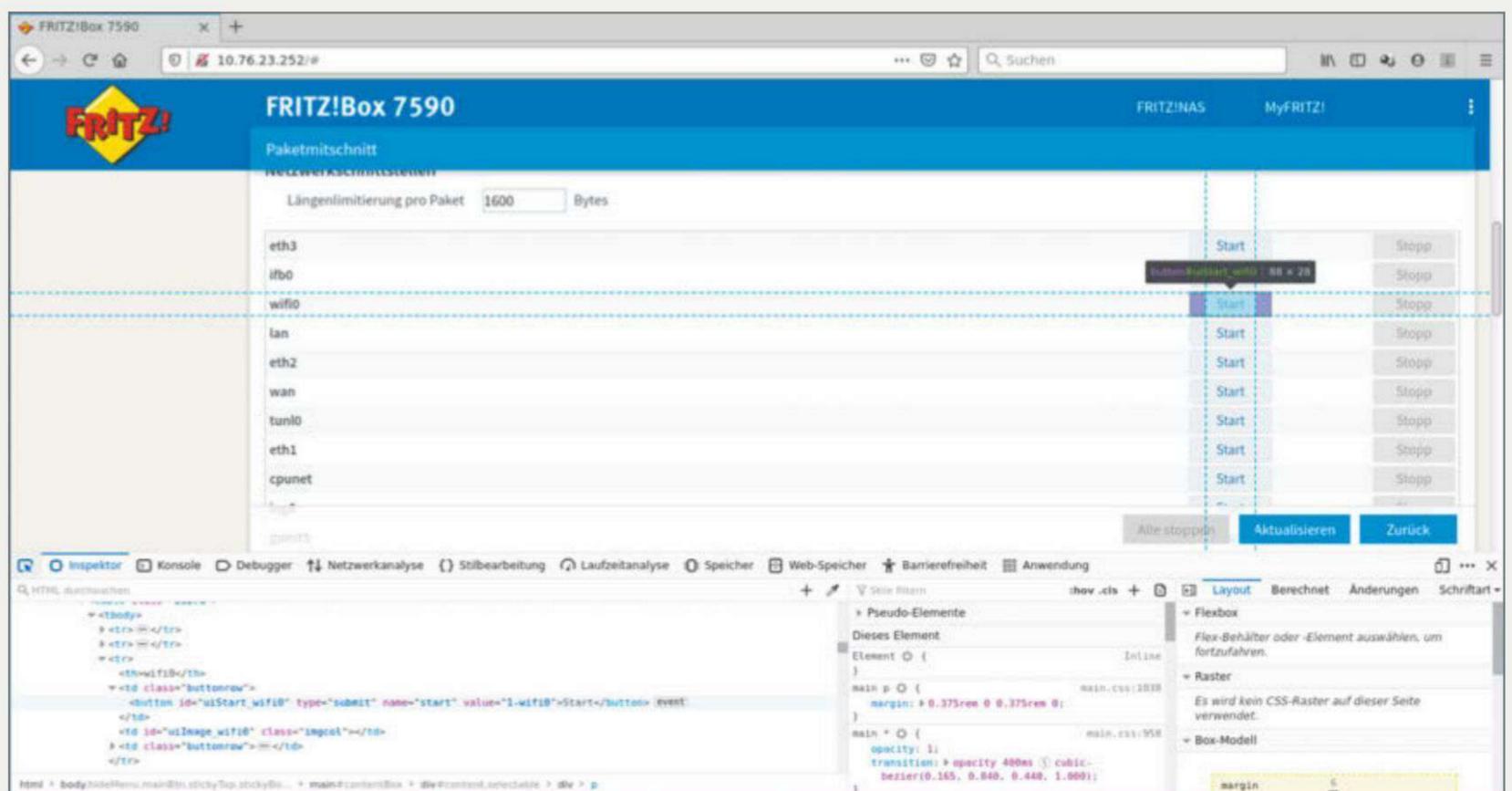
Das Shell-Skript fritzdump.sh automatisiert diese Handgriffe, indem es die Ausgaben direkt an ein Programm weiterleitet, das diese anzeigt - man muss also den Zwischenschritt über eine Datei nicht gehen. Das Skript stammt übrigens von den ntopng-Machern (siehe Kasten auf der folgenden Seite). Nach dem 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 `./fritz-dump.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 erwisch haben.

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



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 20.04 zu nehmen, sondern gleich auf die Pakete zu setzen, die die ntopng-Macher bereitstellen (siehe auch ct.de/w71g). 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-Repositories nachinstallieren kann, und rufen Sie dann folgende Befehle auf (stellen Sie ggf. `sudo` voran):

```
wget http://apt-stable.ntop.org/20.04/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 auf der vorangegangenen Seite 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

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. Hier 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.

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 Desinfec't 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 Fehlersuche oder zum Überprüfen von Geräten, die man der Datenschleuderei verdächtigt.

	Applikation	Protokoll	Client	Server	Dauer	Ausfall	aktuelle Thpt	Total Bytes	Info
Info	VNC	TCP	desinfect 5900	10.76.23.5 57100	01:25	Server	0 bps ↓	8.92 MB	
Info	G+ TLS.GoogleServices	TCP	desinfect :56286	172.217.18.106:https	00:53	Server	0 bps	4.67 MB	safebrowsing.googleapis...
Info	TLS	TCP	desinfect :58468	143.204.202.64:https	00:47	Server	0 bps	1.93 MB	tracking-protection.cdn...
Info	TLS	TCP	desinfect :54130	193.99.144.85:https	01:02	Server	0 bps	746.14 KB	www.heise.de
Info	TLS	TCP	desinfect :53906	193.99.144.85:https	00:54	Server	0 bps	678.34 KB	www.heise.de
Info	TLS.Cloudflare	TCP	desinfect	104.18.164.34:https	00:55	Server	0 bps	322.57 KB	www.mozilla.org

Literatur

[1] Ronald Eikenberg, **Filterbeere**, Schadcode und Werbung mit Raspberry Pi und Pi-hole filtern, c't 11/2018, S. 144

Skripte, Software

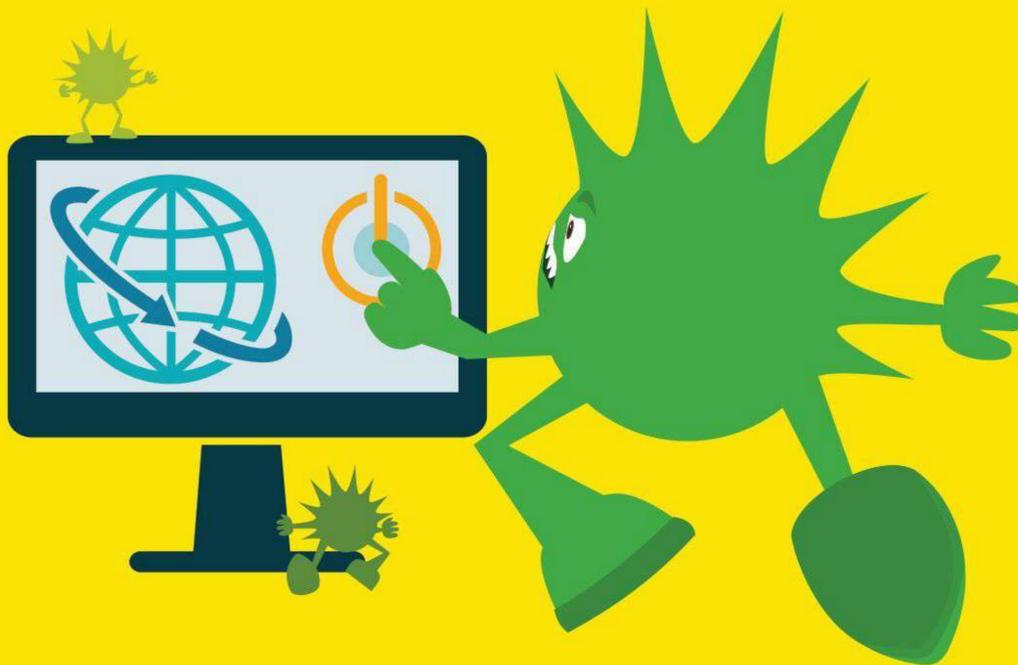
ct.de/w71g

Mit der zusätzlichen Option -1 können Sie netcat anweisen, 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 dieser Seite. 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) **ct**



Desinfec't per PXE booten

Wer häufiger Windows-PCs auf Schadsoftware untersuchen möchte und nicht ständig einen Stick oder eine DVD zur Hand hat, kann Desinfec't komplett aus dem Netz starten. Wie das geht, zeigt dieser Artikel anhand eines Boot-Servers auf Debian-Basis.

Von **Mattias Schlenker**

Wer als Admin in einer Firma PCs schützt, will nicht ständig mit einem Desinfec't-Stick in der Hand zu Kollegen laufen und unter deren Schreibtische krabbeln, um den Stick anzuschließen. Viel bequemer ist es, Desinfec't direkt aus dem Netzwerk zu booten, um anschließend Virencans zu starten. Das Booten auf diesem Weg ist ungemein praktisch.

Für das Einrichten benötigt man nur einen als Boot-Server 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 Onboard-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. Benötigte Dateien für die Einrichtung finden sie im Ordner casper im ISO-Image von Desinfec't 2021/22. 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. So ist es beispielsweise vorstellbar, den DHCP- und TFTP-Server auf einem OpenWRT-Router laufen zu lassen und den NFS-Server auf ein NAS auszulagern – auch der Kleinstcomputer Raspberry Pi kann hier gute Dienste leisten.

Für ein besseres Verständnis empfehlen wir aber, zunächst unsere Musterkonfiguration auf Computern

mit Ubuntu, Debian oder Raspbian nachzustellen und erst dann die Server auf beispielsweise NAS und Router zu verteilen. Unter ct.de/wc9w 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 so aus:

```
INTERFACES="enp2s0"
```

Im folgenden Beispiel bearbeiten Sie die Konfigurationsdatei unter `/etc/dhcp/dhcpd.conf`. Dabei setzen Sie einen DHCP-Server auf, der das Netz `10.76.23.0/24` bedient. In diesem Beispiel hat der Bootserver die Adresse `10.76.23.250`. Gateway und Nameserver sind mit `10.76.23.252` ansprechbar. Der Parameter `O` sorgt dafür, dass dieser DHCP-Server maßgeblich für dieses Netzwerk ist:

```
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";
    }
}
```

```
}
}
```

Nach Erstellung der Konfiguration starten Sie 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 Parameter 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 „Advanced TFTP-Server“ aus dem zu installierenden Paket `atftpd` zum Einsatz. Diesen konfigurieren Sie über die Datei `/etc/default/atftpd`. Passen Sie die IP-Adressen an die in Ihrem Netz verwendeten an und ändern Sie gegebenenfalls den Pfad des Ordners mit den Bootdateien.

```
USE_INETD=false
OPTIONS="--tftpd-timeout 300 ↵
↵--retry-timeout 5 ↵
↵--mcast-port 1758 --mcast-addr ↵
↵10.76.23.0-255 --mcast-ttl 1 ↵
↵--maxthread 100 --verbose=5 ↵
↵/opt/tftpboot"
```

Nun gilt es, das Bootverzeichnis `/opt/tftpboot` zu befüllen. Alle benötigten Dateien sind in der korrekten Ordnerstruktur im Archiv `/cdrom/casper/tftpboot.tgz` enthalten. Sie können diese einfach in Ihren Ordner `/opt/tftpboot` kopieren.

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 übers Netz booten, ist die Differenzierung der Klasse

„pxeclient“ natürlich 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 dieser minimalen Konfiguration:

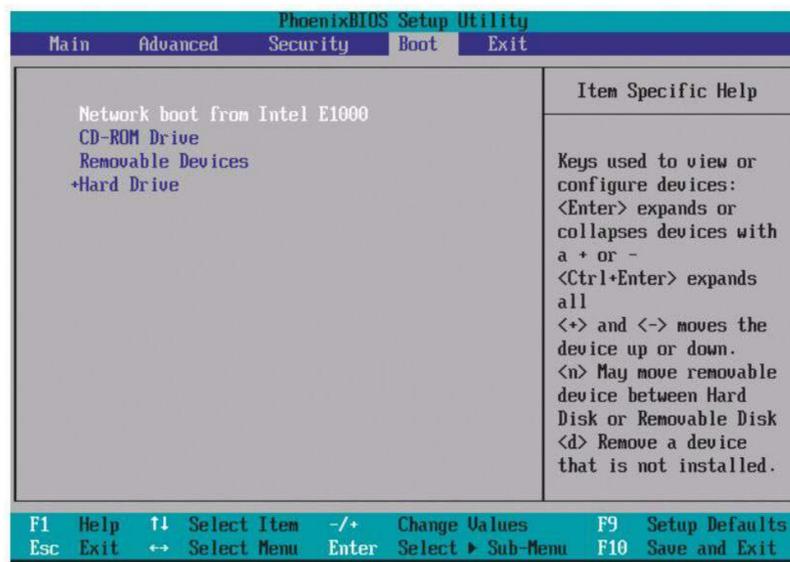
```
set default=0
set timeout=10
menuentry "Start von Festplatte" {
exit
}
```

In beiden Fällen wird der Computer lediglich angewiesen, die PXE-Boot-Umgebung nach 10 Sekunden zu verlassen und mit dem nächsten Bootmedium 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. Der Bootloader PXELINUX erlaubt Konfigurationsdateien für MAC- oder IP-Adresse, die vor „default“ gesucht werden, Details zeigt das Syslinux-Wiki (siehe ct.de/wc9w). Im Falle von GRUB empfehlen viele Tutorials, während des Bootvorgangs auf HTTP zu wechseln, dann kann ein Script auf dem Webserver anhand der IP-Adresse bestimmen, welche Konfiguration ausgeliefert wird.



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.

Der NFS-Server

Nun installieren Sie das Paket nfs-kernel-server und setzen damit den NFS-Server auf. Die Konfiguration geschieht in der Datei /etc/exports. An dieser Stelle müssen Sie folgende Zeile hinzufügen:

```
/opt/nfsboot/desinfect202021 ↵
↵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:

Instant PXE-Server

Desinfec't 2021/22 enthält einen Instant-PXE-Server, den Sie starten können, wenn Ihr Computer über eine Ethernetverbindung verfügt:

```
sudo /opt/desinfect/instant-pxe.sh
```

Das Script erstellt ausgehend von Ihrer aktuellen Netzwerkkonfiguration Konfigurationsdateien für DHCP-, TFTP- und NFS-Server und startet die Dienste. Beachten Sie, dass Sie möglicherweise bei Konflikten mit dem DHCP-Server Ihres DSL-Routers diesen zeitweise deaktivieren müssen. Vergessen Sie aber nicht, ihn wieder anzuschalten, wenn der letzte Client per PXE gebootet wurde.

Das bringt Licht ins Dunkel!



shop.heise.de/ho-beleuchtung

**Heft + PDF
mit 29% Rabatt**



heise online special

Smarte Beleuchtung

Grundlagen, Kaufberatung und Praxis für smartes Licht in Haus & Garten

Licht für Haus & Garten

Wie Sie die passende LED-Lampe finden
Smarte LED-Strips für drinnen und draußen
Terrasse und Balkon perfekt beleuchten

Lichtsysteme im Vergleich

Welcher Funkstandard zu Ihnen passt
Smarte LED-Lampen für E14 und E27 im Test
Smarte Retro-Lampe für Glühbirnen-Feeling
AVM, Ikea & Co.: Datensparsame Lichtpakete

Intelligente Erweiterungen

Leuchten mit Zwischensteckern smart machen
Mit smarten Lichtschaltern Fehlbedienungen verhindern

Cooler Lichtstimmungen

Packendes Gaming- und Fernseh-Erlebnis mit dynamischem Licht
Mit smartem Tageslichtwecker entspannter in den Tag starten



shop.heise.de/ho-beleuchtung

Starten Sie mit dem Thema **Smarte Beleuchtung** in die **neue Heftreihe von heise online**:

- ▶ Smartes Licht in Haus und Garten
- ▶ Auch im Set mit Smart Steckdose zum Sonderpreis
- ▶ Smarte LED-Lampen für E14 und E27 im Test
- ▶ Für Abonnenten portofrei

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

```
mkdir -p /opt/nfsboot/desinfect202021
mkdir /tmp/desinfect202021
mount -o loop desinfect-202021-  
amd64.iso /tmp/desinfect202021
rsync -avHP /tmp/desinfect202021/   
/opt/nfsboot/desinfect202021/
umount /tmp/desinfect202021
```

Falls Sie auch noch die 32-Bit-Version von Desinfect't per PXE bereitstellen wollen, müssen Sie analog mit 32-Bit-Kernel und Ramdisk sowie dem Inhalt des 32-Bit-ISOs verfahren. Starten Sie jetzt den NFS-Server neu:

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

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

Signaturen speichern

Desinfect't 2021/22 bringt die Möglichkeit mit, aktualisierte Signaturen der Virens Scanner auf einem NFS-Share zu speichern. Hierfür legen Sie einen leeren Export-Ordner an, der schreibbar freigegeben ist und eine leere Datei namens „desinfect202021“ enthält:

```
mkdir -p /mnt/archiv/desinfect-signatures
touch /mnt/archiv/desinfect-  
signatures/.desinfect202021
```

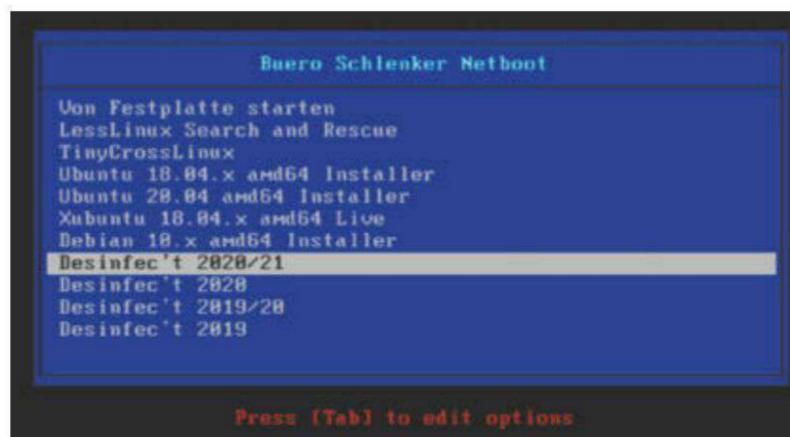
Dieser Ordner enthält den folgenden Eintrag in der Konfigurationsdatei /etc/exports:

```
/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 Desinfect'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 Virens Scanner mit ein paar Minuten Abstand.

Wenn Sie Desinfect't 2020/21 auf einem BTRFS-Stick mit Änderungen versehen haben, können Sie das modifizierte Rootverzeichnis der BTRFS-Partition in den Ordner casper/filesystem.dir/ des exportierten Desinfect'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 mal 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 Desinfect't auf den Grund gehen, beispielsweise indem man das Share manuell einbindet und dabei auf Fehler 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 Desinfect't aussehen. Läuft alles, kann man die Optik noch etwas schicker machen: Im Syslinux-Wiki findet man viele Hinweise, um das PXE-Bootmenü aufzuhübschen (siehe ct.de/wc9w). (des) **ct**

Das Bootmenü des Autors: Neben Desinfect't und TinyCross Linux erleichtern Debian- und Ubuntu-Netinstall-Images die bequeme Installation neuer PCs.

Bootloader PXELINUX, PXE-Bootmenü aufhübschen, PXE-Bootumgebung auf DSL-Router

ct.de/wc9w

Für Maker!

Zubehör und Gadgets

shop.heise.de/gadgets



Raspberry Pi-Kameras

Aufsteckbare Kameras, optimiert für verschiedene Raspberry Pi-Modelle mit 5 Megapixel und verschiedenen Aufsätzen wie z. B. Weitwinkel für scharfe Bilder und Videoaufnahmen.

shop.heise.de/raspi-kameras

ab 18,50 € >

NEUER PREIS!



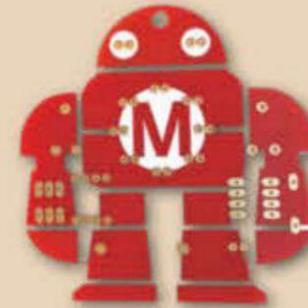
ArduiTouch-Set

Setzen Sie den ESP8266 oder ESP32 jetzt ganz einfach im Bereich der Hausautomation, Metering, Überwachung, Steuerung und anderen typischen IoT-Applikationen ein!

shop.heise.de/arduitouch

~~69,90 €~~

36,90 €



Makey Lötbausatz

Hingucker und idealer Löt-Einstieg: das Maskottchen der Maker Faire kommt als konturgefräste Platine mitsamt Leuchtdiodendie, die den

Eindruck eines pulsierenden Herzens erwecken.

Jetzt neu mit Schalter!

shop.heise.de/makey-bausatz

ab 4,90 € >



NEUER PREIS!

Komplettset Argon ONE Case mit Raspberry Pi 4

Das Argon One Case ist eines der ergonomischsten und ästhetischsten Gehäuse aus Aluminiumlegierung für den Raspberry Pi. Es lässt den Pi nicht nur cool aussehen, sondern kühlt auch perfekt und ist leicht zu montieren. Praktisch: alle Kabel werden auf der Rückseite gebündelt ausgeführt – kein Kabelsalat!

shop.heise.de/argon-set

~~117,60 €~~

99,90 € >



Stockschirm protec'ted

Innen ist Außen und umgekehrt. Dieser etwas andere Regenschirm sorgt für interessierte Blicke auch bei grauem und nassem Wetter. Als Highlight kommt noch das stilvolle und dezente Design in Schwarz und Blau mit der mehr als passenden Aufschrift "Always protec'ted" daher.

shop.heise.de/ct-schirm

22,90 € >



c't Tassen

c't-Leser und -Fans trinken nicht einfach nur Kaffee, sie setzen Statements. Und zwar mit drei hochwertigen Blickfängern, individuell designt für Ihr Lieblings-Heißgetränk: „Kein Backup, kein Mitleid“, „Deine Mudda programmiert in Basic“ oder „Admin wider Willen“. Perfekt für Büro und Frühstückstisch!

shop.heise.de/ct-tassen

ab 12,90 € >

NEU



„No Signal“ Smartphone-Hülle

Passend für Smartphones aller Größen bis 23cm Länge blockt diese zusammenrollbare Hülle alle Signale von GPS, WLAN, 3G, LTE, 5G und Bluetooth, sowie jegliche Handy-Strahlung. Versilbertes Gewebe im Inneren der Tasche aus recycelter Fallschirmseide bildet nach dem Schließen einen faradayschen Käfig und blockiert so alles Signale.

shop.heise.de/no-signal-sleeve 29,90 € >

> Bestellen Sie ganz einfach online unter shop.heise.de oder per E-Mail: service@shop.heise.de

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

heise Shop

shop.heise.de >

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.ct-special.de

Leserbriefe und Fragen zum Heft: 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 Redakteurskürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

Chefredakteur: Jobst-H. Kehrhahn (keh)
(verantwortlich für den Textteil)

Konzeption: Dennis Schirmmacher (des)

Koordination: Ann-Sophie Eikermann (ase),
Angela Meyer (anm)

Redaktion: Mirko Dölle (mid), Angela Meyer (anm),
Dennis Schirmmacher (des), Peter Siering (ps)

Mitarbeiter: Thorsten Leemhuis, Mattias Schlenker

Assistenz: Susanne Cölle (suc), Tim Rittmeier (tir),
Christopher Tränkmann (cht), Martin Triadan (mat)

DTP-Produktion: Lara Bögner, Beatrix Dedek,
Madlen Grunert, Lisa Hemmerling, Natalie Hollstein,
Kirsten Last, Martina Lübke, Steffi Martens,
Marei Stade, Matthias Timm, Ricardo Ulbricht

Produktion: Christine Kreye (Ltg.), Melanie Becker,
Kevin Harte, Martin Kreft, Pascal Wissner

Illustration: Steffi Martens, Ninett Wagner,
www.flaticon.com, www.freepik.com, www.stock.adobe.com

Titel: Steffi Martens

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

Herausgeber: Christian Heise, Ansgar Heise, Christian Persson

Geschäftsführer: Ansgar Heise, Dr. Alfons Schröder

Mitglieder der Geschäftsleitung: Beate Gerold, Jörg Mühle

Verlagsleiter: Dr. Alfons Schröder

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

Anzeigenverkauf: Verlagsbüro ID GmbH & Co. KG,
Tel.: 05 11/61 65 95-0, 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:

VU Verlagsunion KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 145 1800
E-Mail: info@verlagsunion.de

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

Erstverkaufstag: 21.09.2021

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 Verlags 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 Verfügungsrecht des Verlages über. Sämtliche Veröffentlichungen in c't erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes.

Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Hergestellt und produziert mit Xpublisher:
www.xpublisher.com

Printed in Germany.

Alle Rechte vorbehalten.

© Copyright 2021 by
Heise Medien GmbH & Co. KG

Sind Sie sicher?

NEU
im heise shop

Auch als
PDF zum
Download!



IT-Grundschutz-Kompendium des BSI

B1 SYSTEMS Support & Managed Service für Ihre IT-Umgebungen
Linux, Container, Cloud & mehr
info@b1-systems.de | 030 22004 | 030 22005 | 030 22006 | Mehr auf S. 148!

ix KOMPAKT Herbst 2020
Ein Sonderheft des Magazins für professionelle Informationstechnik

IT-SICHERHEIT

- Ende des Privacy Shield: Konsequenzen für Unternehmen
- DSGVO-Fallstricke im IT-Alltag
- Cyberisiken im Griff
- Den Krisenfall meistern
- Pentests vs. Datenschutz
- Notfallmanagement
- Produkte für Endpoint Security
- KI als Angriffsziel und Tatwerkzeug
- Zwei-Faktor-Authentifizierung bedroht
- Pentesting in der Cloud

Awareness: Es mangelt an Gefahrenbewusstsein

Risikofaktor Mensch

Sicherheitsmanagement: ISMS-Tutorial

ix KOMPAKT IT-Sicherheit

Datenschutz umfasst mittlerweile so viel mehr als den Schutz vor Cyberattacken. Nach DSGVO und Ende des Privacy Shield sind auch rechtliche Maßnahmen zu ergreifen. Die neuesten Aspekte rund um den Datenschutz finden Sie zusammengefasst hier im ix Kompakt IT-Sicherheit.

shop.heise.de/ix-sicherheit20

14,90 € >

heise Shop

shop.heise.de/ix-sicherheit20 >

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



**WIR MACHEN
KEINE WERBUNG.
WIR MACHEN EUCH
EIN ANGEBOT.**

ct

ct.de/angebot

Jetzt gleich bestellen:

 ct.de/angebot

 +49 541/80.009 120

 leserservice@heise.de

ICH KAUF MIR DIE c't NICHT. ICH ABONNIER SIE.

Ich möchte c't 3 Monate lang mit 35 % Neukunden-Rabatt testen.
Ich lese 6 Ausgaben als Heft oder digital in der App, als PDF oder direkt im Browser.

**Als Willkommensgeschenk erhalte ich eine Prämie nach Wahl,
z. B. einen RC-Quadrocopter.**

