

# Editorial

---

## Hallo und herzlich willkommen zum Windows-Sonderheft 2023!

---

Das beste Windows ist ein möglichst unauffälliges: keine stressigen Updates, keine Schädlinge und bei Malheurs möglichst einfache Abhilfe. Das ist keine Utopie, denn das System bringt durchaus interessante Funktionen gegen Malware mit und ebenso ein paar Möglichkeiten, um Updates zu steuern.

Weil Windows aber immer noch Windows ist, liegen diese Features brach, solange Sie sie nicht einschalten – und genau dabei hilft Ihnen dieses Sonderheft. Wir erklären, welche Schutzfunktionen was können, wie Sie sich Updates vom Leib halten, wenn es gerade auf Betriebssicherheit ankommt, und wie Sie Programme, denen Sie nicht hundertprozentig vertrauen, in einer abgeschotteten Umgebung stressfrei ausprobieren.

Trotzdem bleibt Vorsorge wichtig. Im Fall der Fälle hilft ein startbereites Notfallsystem. In der 2023er-Version fußt das vom USB-Stick startbare c't-Notfall-Windows erstmals auf dem quelloffenen PhoenixPE-Baukasten. Neben der Bauanleitung finden Sie auch kompakte Anleitungen für die wichtigsten Handgriffe im Notfall-Windows, für die Virensuche und für die PowerShell. Außerdem entwirren wir, warum wir für Systembackups mal zu Drive Snapshot raten – das steckt auch im Notfall-Windows – und mal zu dem von uns entwickelten c't-WIMage. So sind Sie auf alle Eventualitäten vorbereitet.

Viel Erfolg wünscht



Jan Schübler

# Inhalt



## WINDOWS GEGEN ANGRIFFE ABSICHERN

Schon von Haus aus stecken einige interessante Abwehrfunktionen gegen Malware in Windows – aber einige wollen erst eingeschaltet werden. Wenn das nicht reicht, bietet eine Sandbox einen praktischen Extra-Schutzwall für Programme, denen Sie nicht ganz über den Weg trauen.

- 8 So wird Windows angegriffen
- 16 Mehr Sicherheit mit wenigen Handgriffen
- 22 Mehr Schutz dank Smart App Control
- 28 Mit Restric'tor Schädlinge stoppen
- 32 Sandkasten für Windows-Programme



## HILFE FÜR NOTFÄLLE VORBEREITEN

Vorsorge macht das Leben leichter – das gilt auch in der IT. Dazu gehört nicht nur, stets ein aktuelles Backup zur Hand zu haben. Ein nach Ihren Bedürfnissen zusammengebautes c't-Notfall-Windows leistet erste Hilfe bei kleineren und auch größeren PC-Unfällen.

- 38 Das eigene Notfallsystem bauen
- 46 FAQ: c't-Notfall-Windows 2023
- 50 Keine Angst mehr vor Windows-Updates
- 58 Drive Snapshot oder c't-WIMage? Beide!

## WINDOWS-PROBLEME LÖSEN

Im Falle eines Falles ist das vom USB-Stick startende c't-Notfall-Windows Ihr Universalwerkzeug – sei es bei Startproblemen, bei vergurkten Updates oder auch bei Virenbefall.

- 64 Probleme lösen mit dem Notfall-Windows
- 72 Virensuche mit dem Notfall-Windows
- 76 PowerShell fürs c't-Notfall-Windows



## ZUM HEFT

- 3 Editorial
- 6 **Aktion:** heise-Academy-Kurs „Windows-Sicherheit - Der Praxiskurs: Schutzfunktionen richtig einsetzen“
- 71 Impressum
- 82 Vorschau: c't Solarstrom-Guide 2023

**6** **AKTION**  
Videokurs mit über 90% Lesernabatt

**8** **Windows gegen Angriffe absichern**  
So gehen Angreifer vor  
Sicherheit mit wenigen Handgriffen  
Neue Windows-Schutzfunktion nutzen

**38** **Hilfe für Notfälle vorbereiten**  
c't-Notfall-Windows 2023: Überarbeiteter Bausatz mit besserer Bedienung  
Update-Stress vermeiden  
Den richtigen Imager fürs Backup wählen

**64, 72, 64, 76** **Windows-Probleme effektiv lösen**  
Troubleshooting mit dem Notfallsystem  
Viren jagen, Laufwerke klonen  
Notfall-Windows per PowerShell

€ 14,90  
4 252 228 487 10 00  
4 252 228 487 10 00

 heise Academy-Aktion:

# Schutzfunktionen richtig einsetzen

**Abwehr-Werkzeuge inklusive: Microsoft hat in die Pro- und Enterprise-Version von Windows Funktionen integriert, mit denen Sie Ihr Betriebssystem sicherer machen. Wie Sie den optimalen Schutz für private und Unternehmens-Netzwerke herausholen, lernen Sie in diesem Videokurs der heise Academy.**

Von **Markus Richter**

**E**s ist die Schreckensmeldung jedes Anwenders und kann sogar den Ruin für Unternehmen bedeuten, wenn Hacker ein Netzwerk angegriffen haben. Meldungen zu gekaperten Netzwerken, Erpressungsversuchen mit Trojanern, Viren, Würmern und Spyware sind heute an der Tagesordnung. Da gilt es, seine Technik abzusichern.

Microsoft arbeitet ständig daran, das Windows-Betriebssystem sicherer zu machen. Viele der Sicherheitsfunktionen sind aber nicht auto-

matisch aktiv, sondern müssen erst konfiguriert werden. Wie das geht, zeigt IT-Experte Holger Voges im Videokurs „Windows-Sicherheit – Der Praxiskurs“, an dem Sie mit dem Kauf dieses c't-Sonderheftes für 9,90 Euro statt 119 Euro teilnehmen können. Der erfahrene Trainer ist Speaker auf Fachkonferenzen und seit über 20 Jahren Berater namhafter Firmen.

Er zeigt Ihnen, wie Sie die Kennwortsicherheit in Ihrem Netzwerk anpassen.

Lernen Sie, sichere Kennwörter zu definieren und zu erzwingen. Erfahren Sie zudem, welche Alternativen zu Kennwörtern Windows bereits bietet.

Lernen Sie unter Holger Voges' fachkundiger Anleitung, Security-Tools zur Angriffsabwehr wie Bitlocker, Firewall und Defender Antivirus effektiver zu nutzen und Ihr System mit Gruppenrichtlinien abzusichern. Auch können Sie Malware blockieren, indem Sie nur ausgewählte Programme zulassen. Mit AppLocker und Defender Application Control geht das. Schützen Sie sich zudem mit virtualisierungsbasierter Sicherheit vor „Pass-the-Hash“-Attacken und testen Sie Soft-

ware blockieren, indem Sie nur ausgewählte Programme zulassen. Mit AppLocker und Defender Application Control geht das. Schützen Sie sich zudem mit virtualisierungsbasierter Sicherheit vor „Pass-the-Hash“-Attacken und testen Sie Soft-



## Das lernen Sie im Videokurs:

- Windows-Anmeldung sicherer machen
- Zentrale Sicherheitsfunktionen konfigurieren
- Anwendungen zum Schutz vor Malware blockieren
- Festplatten mit Bitlocker verschlüsseln
- Schutz vor „Pass-the-Hash“-Angriffen

Über [shop.heise.de/windows2023](https://shop.heise.de/windows2023) erhalten Sie diesen Videokurs mit dem Rabattcode **Windows2023** einmalig für nur 9,90 Euro, statt 119 Euro\*.

\*Preis- und andere Irrtümer vorbehalten. Das Angebot ist gültig bis zum 31.12.2023 (Stand: März 2023).

ware vorab in einer isolierten Umgebung mit der Windows-Sandbox. Starten Sie jetzt mit neuem Fachwissen in eine sicherere Zukunft.

## IT-Wissen aufbauen mit der heise Academy

Der Videokurs ist Teil des Angebotes der heise Academy. Im Mittelpunkt steht dort, Lernformen von morgen zu gestalten: Wie finden wir das Wissen, das uns wirklich weiterbringt? Und wie kann sich unser Lernangebot an individuelle Bedürfnisse anpassen? Die heise Academy will darauf Antworten liefern.

In einem digitalen Campus finden interessierte Admins, Entwickler, Programmierer und alle weiteren IT-Professionals zeitgemäße und maßgeschneiderte Wissensangebote. Damit können Sie Ihre Skills vertiefen, neue Schwerpunkte in Ihrer Arbeit setzen, Ihre Karriere voranbringen und vor allem: mit Spaß lernen.

Wählen Sie Ihr Thema aus einem Angebot, das ständig wächst und immer aktuell ist. Von Netzwerken und Systemen über IT-Projektmanagement, Softwareentwicklung, Data Science und IT-Security bis hin zu Web- und Cloud-Technologien bietet der digitale Campus jede Menge geballtes Fachwissen für die professionelle Anwendung. Dabei steht die Wissensvermittlung durch ausgewählte Experten im Mittelpunkt. Diese erfahrenen Trainer kommen aus dem gesamten deutschsprachigen Raum und be-

dienen unterschiedliche Schwerpunkte mit starkem Praxisbezug.

Aufgeteilt in übersichtliche Kapitel und Lektionen, bieten die Videokurse spannende Lernpakete für alle Situationen, in denen Weiterbildung angesagt ist – sei es während der Arbeitszeit, nach Feierabend oder von unterwegs.

Die Videokurse schauen Sie in einem von der heise Academy entwickelten Player, der eine komfortable Benutzeroberfläche bietet. So kann das Video jederzeit gestoppt und natürlich an der zuletzt gesehenen Stelle wieder gestartet werden. Durchsuchen Sie den Kurs mithilfe einer Volltextsuche nach Stichworten, hinterlegen Sie persönliche Notizen und testen Sie Ihr neu erworbenes Wissen durch kleine Quizze am Ende jeder Lektion. Mit erfolgreichem Kursabschluss erhalten Sie schließlich Ihr Academy-Zertifikat.

Der Campus bietet aber noch mehr: Sie finden dort unter anderem über 100 Live-Webinare jährlich, die immer am Puls der Zeit sind. Hier wird über Trendthemen diskutiert, an praktischen Fallbeispielen geübt und eine Lösung für jedes IT-Problem angeboten. Möglich ist dazu ein moderiertes Networking mit Fachleuten im Chat. Die Webinare sind direkt anschließend für alle Abonnenten und Einzelkäufer als Aufzeichnung verfügbar.

Alle Infos zu den Angeboten finden Sie unter [www.heise-academy.de](http://www.heise-academy.de). (anm) **ct**

**Wie Sie die Windows-Schutzfunktionen in privaten und Firmennetzwerken richtig einsetzen, erklärt Holger Voges anschaulich in den 82 Lektionen des Videokurses.**

The screenshot shows the heise Academy course player interface. The main video area displays a man (Holger Voges) sitting at a desk with a laptop. The interface includes a navigation menu on the right with 10 lessons, a progress bar at the bottom, and a search bar at the top. The lessons listed in the menu are:

- 1 Einführung in lokale und Domänen-Gruppenrichtlinien
- 01 Herzlich Willkommen zu diesem Kurs
- 02 Intro
- 03 Lokale Gruppenrichtlinien konfigurieren
- 04 Workflow für Gruppenrichtlinien
- 05 Überblick über Domänen-Richtlinien
- 06 Einführung in die Group Policy Management Console
- 07 Gruppenrichtlinien-Objekte verwalten
- 08 Zusammenfassung
- 09 Quiz Lokale und Domänen-Gruppenrichtlinien
- 10 Windows-Kennzeichensicherheit
- 11 Sichere Authentifizierung
- 12 Windows Sicherheitsoptionen anpassen
- 13 Einstellungen mit administrativen Vorlagen erzwingen
- 14 Windows Security Baselines und das Security Compliance Toolkit

# So wird Windows angegriffen

Bild: Andreas Martini

Angriffe auf PC-Systeme sind eine ernstzunehmende Bedrohung. Gut organisierte Banden von Cyber-Erpressern erbeuten Jahr für Jahr Milliarden. Vor allem Windows-Rechner stehen in der Schusslinie – nicht zuletzt, weil sie für Einbrecher häufig offen wie ein Scheunentor sind.

Von **Jürgen Schmidt**



Windows unter Beschuss	8
Mehr Sicherheit mit wenigen Handgriffen	16
Mehr Schutz dank Smart App Control	22
Mit Restric'tor Schädlinge stoppen	28
Sandkästen für Windows-Programme	32

**W**indows ist für Kriminelle das beliebteste Angriffsziel unter den Betriebssystemen. Das liegt vor allem an zwei Dingen: Zum einen ist es das mit Abstand am weitesten verbreitete Desktop-Betriebssystem - mit funktionierenden Angriffen auf Windows erschließt sich dem Angreifer ein riesiges Reservoir an Datenschätzen. Zum anderen macht Windows es Angreifern nach wie vor sträflich einfach, ihre Ziele zu erreichen. Diesen Vorwurf werden wir noch genauer beleuchten, wenn wir die konkret eingesetzten Techniken vorstellen.

Doch zunächst zu den Angreifern und deren Zielen: Das sind in der überwältigenden Mehrzahl aller IT-Sicherheitsvorfälle organisierte Kriminelle, also eine Art Cyber-Mafia, die durch Betrug und Erpressung jährlich Milliarden Schäden verursacht. Insbesondere die Erpressung hat sich als Goldesel der Cyber-Kriminalität erwiesen. Mit überschaubarem Aufwand erbeuten die Kriminellen dabei echtes Geld in rauen Mengen - und das selbst ohne großes Know-how und mit einem vernachlässigbaren Risiko.

In der Folge hat sich in den letzten Jahren rund um Ransomware - der Begriff bezeichnet zur Erpressung genutzte Schadsoftware und stammt vom englischen „ransom“ für „Lösegeld“ - ein ganzes Cybercrime-Ökosystem mit Dienstleistungen aller Art gebildet. Anbieter von „Ransomware as a Service“ (RaaS) liefern auch unerfahrenen Mächtgern-Kriminellen Komplettpakete aus Tutorials mit Anleitungen, einfach zu bedienenden Software-Baukästen und Infrastruktur für Verhandlungen und Geldübergabe.

Die Opfer dieses Treibens sind vornehmlich Firmen, Organisationen und Behörden, deren Abhängigkeit von funktionierender IT ihre Achillesferse wurde. Aber auch Privatanwender befinden sich nach wie vor im Visier der Kriminellen: Zum einen ist in Zeiten von Homeoffice fast jeder Privat-PC ein potenzielles Einstiegstor in die IT des Arbeitgebers seines Besitzers. So lassen sich die auf einem privaten PC gestohlenen Zugangsdaten gut im Untergrund ver-

- den eigentlichen Einbruch (Initial Access),
- das Ausbreiten im Netz (Lateral Movement),
- die Erpressung (Impact)

In diesen Phasen kommen nicht nur unterschiedliche Tricks und Werkzeuge zum Einsatz, es ist auch durchaus üblich, dass dahinter verschiedene Akteure stecken. So gibt es einen eigenen Markt, auf dem Initial Access Broker (IAB) Zugänge zu Systemen verkaufen. Die auf den Einbruch spezialisierten Kriminellen ernten die infizierten Computer ihrer Opfer systematisch ab und stehlen dort insbesondere alle Zugangsdaten, derer sie habhaft werden können.

Außerdem installieren sie noch ein Hintertürprogramm - einen Remote-Access-Trojaner (RAT), der ihnen zukünftig die volle Kontrolle über das System beschert. Diese Aufgabe übernimmt oft ein Cobalt Strike Beacon: Cobalt Strike ist eine kommerzielle Software, die von Sicherheitstestern bei simulierten Angriffen eingesetzt wird. Aber auch echte Angreifer nutzen sie überaus gern. Eine Webseite, die Cobalt Strike-Angriffe und mögliche Abwehrmaßnahmen beschreibt, haben wir unter [ct.de/w51j](https://ct.de/w51j) verlinkt.

Die gestohlenen Passwörter und den Zugang zum RAT verkaufen die Angreifer in speziellen Untergrundforen und -börsen. Es gibt übrigens Dienstleister, die Privatpersonen und Firmen anbieten, diese IAB-Marktplätze zu überwachen und sie zu benachrichtigen, wenn ihre Daten dort auftauchen sollten. Doch das ist in der Regel das Geld nicht wert. Denn die etablierten IAB-Spezialisten haben Geschäftsbeziehungen zu RaaS-Anbietern, denen sie vorab Zugriff auf ihre Ware anbieten. So landen viele der erbeuteten Daten nie in den für solche Dienstleister einsehbaren Foren.

## Einfallstor Office-Dokumente

Zu den wichtigsten Einfallstoren für den „Initial Access“ gehören nach wie vor präparierte Office-Dateien, die bösartige Makros enthalten. Klickt der An-

Lesen Sie mehr in c't Windows-Guide 2023

# Das eigene Notfallsystem bauen

Unser Notfall-Windows hilft seit Jahren, Windows-Installationen von außen auf den Zahn zu fühlen: Vom USB-Stick gebootet, jagt es Schädlinge, klont Festplatten, beseitigt Startprobleme, setzt Passwörter zurück oder prokelt sie aus den Windows-Untiefen heraus und vieles mehr. Wir haben den Bausatz auf ein neues Fundament gestellt und die Bedienung weiter vereinfacht.

Von **Stephan Bäcker und Peter Siering**



Bild: Andreas Martini

Das eigene Notfallsystem bauen	38
FAQ c't Notfall-Windows 2023	46
Keine Angst mehr vor Windows-Updates	50
Drive Snapshot oder c't-WIMage? Beide!	58

**A**m liebsten würden wir Ihnen unser Notfall-Windows als Fertigsystem liefern, doch da steht Microsofts Lizenzpolitik im Weg (siehe Kasten „Hintergründe zum Bausatz“). Aber keine Angst: Auch mit dem Bausatz kommen Sie schnell ans Ziel – und wir haben ihn dieses Jahr sogar nochmal vereinfacht. Die folgenden Absätze erklären, wie Sie ihn benutzen und welche Voraussetzungen erfüllt sein müssen. Am Ende erfahren Sie auch, wie Sie sich helfen können, wenn der Bauversuch nicht auf Anhieb gelingt.

## Bewährtes

Das Grundprinzip ist einfach und seit Jahren bewährt: Sie benötigen zum einen die Zip-Datei ctnotwin23.zip mit der Bauvorlage, die Sie bei uns herunterladen können. Zum anderen möchte der Bausatz einen Installationsdatensatz verarbeiten, sprich die Windows-Originaldateien, die man üblicherweise zum Einrichten des Betriebssystems verwendet („Quelldateien“ genannt). Die stellt Microsoft in Form von Evaluierungsversionen kostenlos zum Download bereit. Alle nötigen Links haben wir unter [ct.de/ww88](http://ct.de/ww88) versammelt.

Wir raten unbedingt dazu, die von Microsoft bereitgestellten ISO-Dateien der Evaluierungsversionen herunterzuladen. Eine eventuell lokal vorhandene Installations-DVD oder eine vom Media Creation Tool erstellte ISO-Datei eignet sich nicht als Quelle, weil diese die vom Bausatz benötigten Dateien in einem Dateicontainer aufbewahren, den der Bausatz nicht verarbeiten kann (ESD statt WIM).

Sparen Sie Zeit und folgen Sie deshalb der Empfehlung.

Wenn Sie Wert auf aktuelle Treiber legen, sollten Sie auf die Evaluierungsversion von Windows 11 22H2 zurückgreifen. Die verträgt sich mit dem Bausatz. Auch ihr Vorgänger Windows 11 21H2 harmonisiert mit der Softwareauswahl. Auf Nummer sicher gehen Sie mit der Evaluierungsversion von Windows 10 in Version 2004. Sie genügt für die meisten Notfalleinsätze, wenn es nicht um hochaktuelle Hardware geht – alle Treiber bringt das Notfallsystem ohnehin nicht mit und man muss gegebenenfalls nachhelfen, entweder temporär, wie der Artikel „Probleme lösen mit dem Notfall-Windows“ ab Seite 64 zeigt oder dauerhaft, wie die FAQ ab Seite 46 erklärt.

Die Links zum Herunterladen finden Sie über [ct.de/ww88](http://ct.de/ww88) und zusätzliche Hinweise auf der ebenda per Link erreichbaren Projektseite. Dort ergänzen und berichtigen wir gegebenenfalls diesen Artikel beziehungsweise die bereitgestellte Software. Außerdem finden Sie dort ein Forum für den Erfahrungsaustausch untereinander und als erste Anlaufstelle für eventuelle Probleme. Gern können Sie sich aber auch per Mail an uns wenden. Richten Sie diese bitte an [notwin23@ct.de](mailto:notwin23@ct.de).

Um den Bausatz auszuführen, benötigen Sie einen PC mit einer von Microsoft noch mit Updates versorgten Windows-Version. Das sind wenige Wochen nach Erscheinen dieser Ausgabe nur noch zwei: Windows 10 und 11 – beide eignen sich gleich gut. Weil der Support für Windows 8.1 im Januar 2023 endet, haben wir es nur flüchtig getestet. Auf das

## Hintergründe zum Bausatz

Lesen Sie mehr in c't Windows-Guide 2023

# Probleme lösen mit dem Notfall-Windows

Bild: Andreas Martini

Dateien verschwunden, Windows bootet nicht, Anmeldekennwort vergessen, Virenalarm: Schon ist der Puls auf 180. Doch fluchen bringt dann nichts. Greifen Sie stattdessen zu unserem Notfallsystem. Das hilft, wenn Windows kränkelt. Unsere Anleitungen leiten Sie Schritt für Schritt durch die jeweils erforderlichen Therapien.

Von **Axel Vahldiek**



Probleme lösen mit dem Notfall-Windows	64
Virensuche mit dem Notfall-Windows	72
PowerShell fürs c't-Notfall-Windows	76

**E**s gilt unverändert: Viele Windows-Probleme lassen sich mit einem simplen Neustart lösen (merke: „Wenns nicht tut, hilft Reboot!“). Doch manchmal reicht das nicht. Dann schlägt die Stunde unseres Notfallsystems (Bauanleitung siehe S. 38). Dabei handelt es sich um eine saubere, bootfähige Rettungsumgebung. Nachdem der PC vom Stick gestartet hat, müssen Sie schon genau hinsehen, um Unterschiede zu einer herkömmlichen Windows-Installation zu entdecken. Einige gibt es aber doch. Dieser Artikel hilft beim Umgang damit und erklärt, wie Sie vom Stick booten, wie Sie sich einen Überblick verschaffen, die Onlineverbindung aktivieren und gegebenenfalls dafür nötige Treiber nachinstallieren, wie Sie BitLocker-geschützte Laufwerke entsperren und so weiter. Weitere Schritt-für-Schritt-Anleitungen helfen Ihnen beim Restaurieren des Bootloaders und beim Zurücksetzen eines vergessenen Windows-Kennworts.

Für viele Probleme bringt unser Notfallsystem passende Werkzeuge mit. Es sind so viele, dass selbst die lange Tabelle in diesem Beitrag nur eine Auswahl bietet. Mitunter ist nicht mal auf den zweiten Blick ersichtlich, was sich damit alles anstellen und reparieren lässt. Sie können sich dennoch einen Eindruck davon verschaffen: Die Literaturliste in die-

sem Beitrag bietet eine Sammlung von c't-Artikeln mit Grundlagen und Praxis rund um das Notfallsystem. Einem unverändert wichtigen Thema widmen wir auch in dieser Ausgabe wieder einen separaten Artikel: der Virensuche mit dem c't-Notfall-Windows (siehe S. 72).

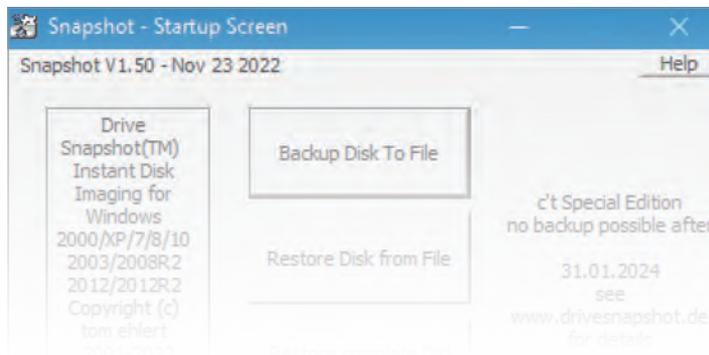
Die Schritt-für-Schritt-Anleitungen in diesen Artikeln kommen Ihnen bekannt vor? Sie täuschen sich nicht. So wie wir unser Notfall-Windows nicht in jedem Jahr komplett neu, sondern stattdessen immer weiter entwickeln, verfahren wir auch mit den Anleitungen: Wir überprüfen und aktualisieren sie Jahr für Jahr und berücksichtigen dabei auch Ihre Rückmeldungen und Wünsche. Die Anleitung zum Reparieren des Bootloaders beispielsweise ist dank eines neuen c't-Skripts nun deutlich kürzer. Verwenden Sie bitte stets die Anleitungen, die zur jeweiligen Version des Notfallsystems gehören.

Tipp für Käufer der digitalen Ausgabe dieses Sonderhefts: Legen Sie das PDF auf den Stick mit dem Notfall-System. Dann haben Sie im Ernstfall alles Nötige auf einem einzigen Stick beieinander.

## Spezialversion Drive Snapshot

Zum Notfall-Windows gehört auch in diesem Jahr wieder eine Spezialversion des Imagers Drive Snapshot. Mit dem können Sie beispielsweise vor Reparaturversuchen Abbilder von Festplatten erzeugen (bis Ende 2023) und später bei Bedarf wiederherstellen (zeitlich unbegrenzt).

Das Verwenden des Imagers ist einfach: Booten Sie das Notfall-Windows und verschaffen Sie sich einen Überblick über die Laufwerke (siehe Schritt-für-Schritt-Anleitung). Rufen Sie anschließend aus dem Startmenü „Drive Snapshot“ auf. Zum Sichern wählen Sie „Backup Disk to File“, die Windows-Partition sowie Ziel und Name der Backup-Datei (am besten auf einer externen Festplatte). Nach einem Klick auf „Start Copy“ beginnt das Sichern. Das Zurückspielen gelingt ähnlich simpel. In Drive Snap-



Lesen Sie mehr in c't Windows-Guide 2023