c't WINDOWS-GUIDE

System absichern · einrichten · reparieren

Windows gegen Angriffe absichern

So gehen Angreifer vor

Sicherheit mit wenigen Handgriffen

Neue Windows-Schutzfunktion nutzen

Hilfe für Notfälle vorbereiten

c't-Notfall-Windows 2023: Überarbeiteter Bausatz mit besserer Bedienung

Update-Stress vermeiden

Den richtigen Imager fürs Backup wählen

Windows-Probleme effektiv lösen

Troubleshooting mit dem Notfallsystem

Viren jagen, Laufwerke klonen

Notfall-Windows per PowerShell

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

4 197665 614904 01

c't WORKSHOP

Themenauswahl 2023

Einführung in GitLab

Dieser Workshop bietet einen Einstieg in den Betrieb einer eigenen Instanz der Entwicklungsplattform. Sie lernen sowohl, wie Sie GitLab initial aufsetzen, als auch wie Sie Ihre GitLab-Instanz konfigurieren und optimal an die eigenen Anforderungen anpassen

Einführung in den Kea DHCP Server

Der Workshop gibt eine vollständige Einführung in die neue Kea-DHCP-Software auf Unix- und Linux-Systemen. Sie lernen, wie man das Kea-DHCP-System installiert, konfiguriert und wartet.

CI/CD mit GitLab

Die Entwicklungsplattform GitLab bietet umfangreiche Continuous-Integration-Funktionen. Der Workshop bietet eine praktische Einführung in die GitLab-CI-Tools und zeigt, wie man damit Softwareprojekte baut, testet und veröffentlicht.

Docker und Container in der Praxis

Der Workshop richtet sich an Entwickler und Administrierende, die neu in das Thema einsteigen. Neben theoretischem Wissen über Container geht es um die Herausforderungen im Alltag und eigene Container-Erfahrungen auf der Kommandozeile.

Sichern Sie sich Ihren Frühbucher-Rabatt:

www.heise-events.de/workshops

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 Schüßler

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.

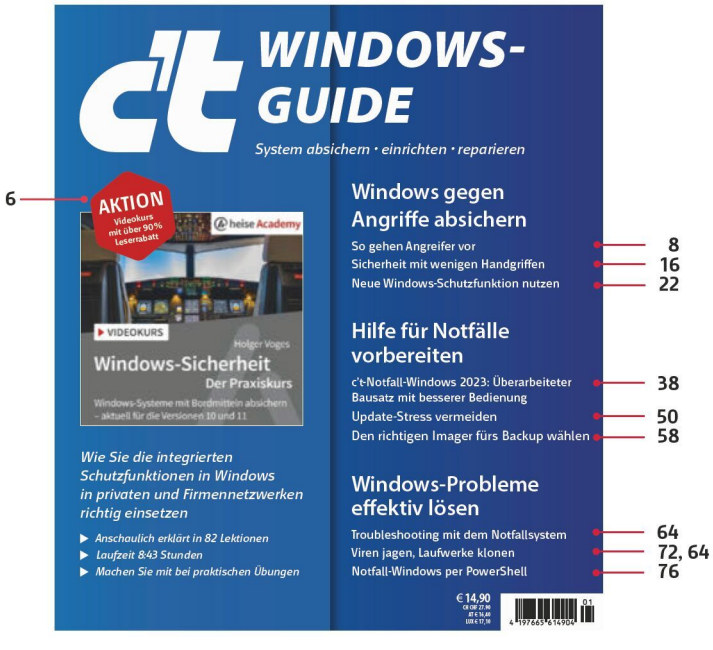
HILFE FÜR NOTFÄLLE VORBEREITEN

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.

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.

ZUM HEFT



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**

Es 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 automatisch 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-

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 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.

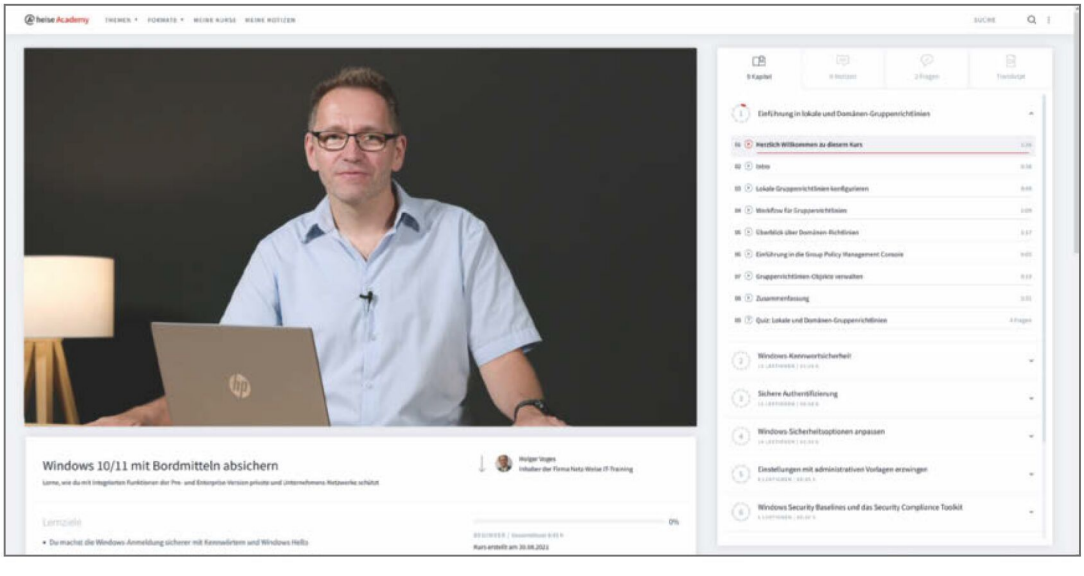
Wählen Sie Ihr Thema aus einem Angebot, das ständig wächst und immer aktuell ist. Von Netzwerken und Systemen über IT-Projektmanagement, Softwareentwicklung, Data Science und IT-Security bis hin zu Web- und Cloud-Technologien bietet der digitale Campus jede Menge geballtes Fachwissen für die professionelle Anwendung. Dabei steht die Wissensvermittlung durch ausgewählte Experten im Mittelpunkt. Diese erfahrenen Trainer kommen aus dem gesamten deutschsprachigen Raum und bedienen 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. (anm) c't



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

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 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 Milliardenschäden 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 Möchtegern-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 verhökern. Zum anderen sind auch Privatanwender oft bereit, beispielsweise für den Zugang zu ihrem verschlüsselten Bilderarchiv mit den Fotos von Geburt, Einschulung und Hochzeit der Kinder erkleckliche Summen zu zahlen – „Kleinvieh macht auch Mist“ gilt auch bei Cybercrime.

Typische Vorgehensweise

Die typische Vorgehensweise bei Einbrüchen in Computer lässt sich in drei Phasen unterteilen:

- 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.

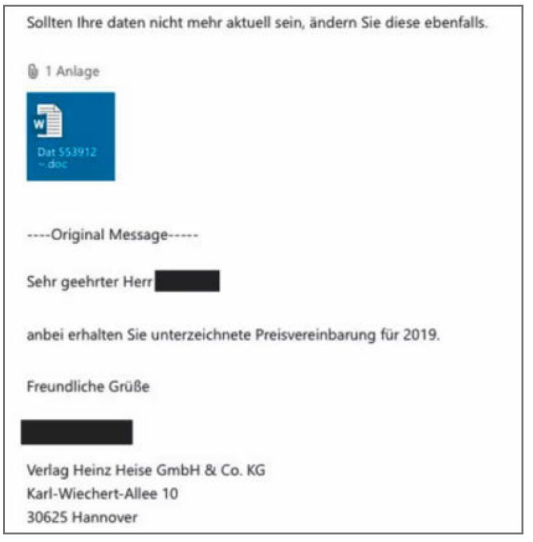
Außerdem installieren sie noch ein Hintertürprogramm – einen Remote-Access-Trojaner (RAT), der ihnen zukünftig die volle Kontrolle über das System beschert. Diese Aufgabe übernimmt oft ein Cobalt Strike Beacon: Cobalt Strike ist eine kommerzielle Software, die von Sicherheitstestern bei simulierten Angriffen 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 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 Anwender beim Öffnen des Dokuments die gelben Balken weg („Inhalt aktivieren“, „Bearbeiten erlauben“), laufen im Hintergrund Befehlssequenzen ab, die etwa eine Datei aus dem Internet nachladen und starten. Das kann dann bereits der oben erwähnte Remote-Access-Trojaner sein, der den Angreifern jederzeit Zugang zum System gibt.

Auf keinem anderen System ist es so einfach, sich mit Schadsoftware aus einer E-Mail zu infizieren, wie bei Windows. Linux, macOS und die Smartphone-Betriebssysteme haben auch ihre Sicherheitspro-


Sollten Ihre daten nicht mehr aktuell sein, ändern Sie diese ebenfalls.

1 Anlage

Dat 553912 ~.doc

----Original Message-----

Sehr geehrter Herr [redacted]

anbei erhalten Sie unterzeichnete Preisvereinbarung für 2019.

Freundliche Grüße

[redacted]

Verlag Heinz Heise GmbH & Co. KG
Karl-Wiechert-Allee 10
30625 Hannover

Mit dieser Mail schaffte es die Emotet-Bande, einen Heise-Mitarbeiter auszutricksen. Die Nachricht zitierte seine eigene E-Mail und sah damit für ihn wie eine ganz normale Geschäfts-Mail aus.

bleme, über E-Mail angelieferte Malware gehört aber nicht dazu. Unter Windows genügen in der Voreinstellung oft ein, zwei unvorsichtige Klicks, damit die Malware aktiv wird, und das Unheil nimmt seinen Lauf. Und mit täuschend echt gestalteten E-Mails und einer überzeugenden Geschichte gelingt es immer wieder, vor allem unerfahrene Anwender davon zu überzeugen, die notwendigen Klicks tatsächlich durchzuführen.

Doch Microsoft steuert endlich aktiv gegen. Immer mehr Office-Installationen blockieren Makros in Dokumenten, die aus dem Internet stammen, sodass sie unbefangene Nutzer nicht mehr ausführen können. Doch das dafür eingesetzte Mark of the Web ist längst nicht so zuverlässig, wie man sich das wünschen würde. Mehr dazu erklärt ein Artikel auf heise Security [1].

Das LNK-Revival

Als Alternative zu Makros experimentieren die IABs mit verschiedenen Tricks. Das führt zu einem Revival der LNK-Dateien: Das sind Verweise auf andere Programme, die beim Öffnen auszuführen sind; Windows verwendet sie zum Beispiel für Desktopsymbole und Startmenüeinträge. Eine einzelne LNK-Datei ist jedoch verdächtig und jedes bessere Mail-Gateway wird sie als potenzielles Schadprogramm blockieren. Stattdessen bekommt ein Anwender deshalb zum Beispiel ein ISO-Image via Mail – optional noch verpackt in ein Zip-Archiv. Diese Image-Datei bindet Windows beim Öffnen netterweise als Laufwerk ein und zeigt ein Fenster mit etwas wie „Umsatz_Report_2022“ an; die verräterische Endung „.lnk“ versteckt der Explorer selbst dann, wenn Sie Windows anweisen, Erweiterungen bei bekannten Dateitypen anzuzeigen.

Beim Klick auf den angeblichen Report passieren je nach Inhalt der LNK-Datei verschiedene Dinge. In einem typischen Szenario startet Windows via rundll32.exe eine Bibliothek, die sich in einem versteckten Ordner des ISO-Image-Laufwerks befindet und den Schadcode der Kriminellen ausführt, also etwa ein Cobalt Strike Beacon nachlädt und installiert. Ein anderes Angriffsszenario lässt Windows den mächtigen Skript-Interpreter powershell.exe starten, der seine Anweisungen aus der Kommandozeile entnimmt. Das Resultat ähnelt letztlich Szenario 1 – der Rechner ist infiziert.

Updates, Updates, Updates!

Vor allem für Firmen sind extern erreichbare Dienste eine große Gefahr. An vorderster Front stehen VPN-Gateways oder fahrlässigerweise aus dem Internet erreichbare RDP-Zugänge. Oft finden Angreifer auch bei Suchmaschinen oder durch Scans ganzer IP- und Port-Bereiche längst vergessene FTP-Server oder ein nur mal testweise eingerichtetes Content Management System, das nicht mit allen Sicherheitsupdates versehen wurde.

Dabei kommt erschwerend hinzu, dass die Lücken nicht nur in den Programmen stecken, die man eigentlich installiert hat. Software besteht heutzutage aus unzähligen fertigen Komponenten, die die Entwickler in ihre Projekte einbinden. Taucht in einer davon eine Lücke auf, sind all ihre Downstream-Apps anfällig. So traf eine Sicherheitslücke in der Java-Bibliothek Log4j Tausende Applikationen, die damit ihre Protokollierung in Log-Dateien erledigten [2].

Nur in seltenen Fällen kommen bei diesen Angriffen unbekannte Sicherheitslücken, auch Zero Days genannt, zum Einsatz. Die große Mehrzahl der Einbrüche erfolgt über bekannte Schwachstellen, gegen die es bereits Updates gäbe. Ein zu spät eingespieltes Sicherheitsupdate bedeutet fast zwangsläufig, dass man ungebetenen Besuch bekommt.

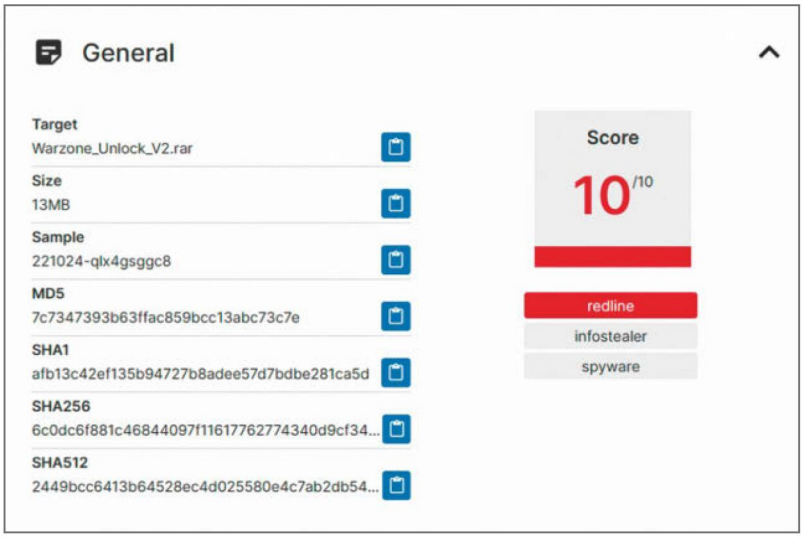
Passwörter als Problem

Ein weiterer wichtiger Einfallsvektor sind kompromittierte Zugangsdaten. Die erlangen Kriminelle häufig über Phishing [3, 4].

Gern jubeln IABs ihren Opfern Infostealer unter. Haben Sie sich schon mal gewundert, wer sich die Mühe macht, gecrackte Versionen von teuren Softwarepaketen zu erstellen und kostenlos im Internet zu verteilen? Oder einen tollen Aim-Bot für den aktuell gehypten First Person Shooter? Das sind nicht selten Initial Access Broker, die mit dem gecrackten Photoshop auch gleich einen maßgeschneiderten Infostealer verteilen. Der sammelt alle auf dem System gespeicherten Passwörter ein, die der IAB danach zu Geld machen kann.

Da schlägt eine weitere Windows-Schwäche zu: Anders als moderne Smartphone-Betriebssysteme schottet Windows die verschiedenen Applikationen, die ein Anwender auf dem System ausführt, so gut wie gar nicht gegeneinander ab. So kann das gecrackte Photoshop auf alle Firefox-Dateien zugreifen. Das funktioniert wohlgemerkt ganz ohne Admin-Rechte, einfach mit Code im Kontext des angemeldeten Benutzers. Auf einem iPhone oder Android-Smartphone wäre das hingegen so nicht möglich. Dort sind alle Apps gegeneinander abgeschottet.

Bild: Hatching Triage



Vorsicht vor gecrackten Spielen! Sie enthalten gern mal Malware wie den hier entdeckten Infostealer „Redline“.

Vereinfacht kann man sich das so vorstellen, dass jede App unter Android einen eigenen Benutzerkontext bekommt und damit die Photoshop-App keinen Zugriff auf Dateien oder gar den Arbeitsspeicher der Firefox-App hat.

Ganz einfach macht es dem Angreifer etwa Microsoft Teams. Dort liegt ein Token im Benutzerverzeichnis, das ein Infostealer nur einsammeln und an seinen Herrn und Meister schicken muss, um diesem den Zugang zum Teams-Account des Opfers zu geben (Details via ct.de/w51j). Im Idealfall verschlüsseln Anwendungen solche Daten deshalb etwa mit dem Data Protection API (DPAPI) von Windows. Damit genügt es nicht mehr, dass der Angreifer die Dateien seines Opfers lesen kann.

Eine große Hürde ist das für einen Infostealer allerdings nicht, jedenfalls wenn er seinen Code bereits im Kontext des jeweiligen Benutzers ausführt: Die DPAPI-Funktion `CryptUnprotectData()` verwendet die Zugangsdaten des aktuell angemeldeten Benutzerkontos als Schlüssel. Immerhin schützt die Verschlüsselung aber Benutzerdaten vor Schnüffelsoftware, die in einem anderen Kontext läuft, etwa unter dem zu einem lokalen Webserver gehörenden Konto.

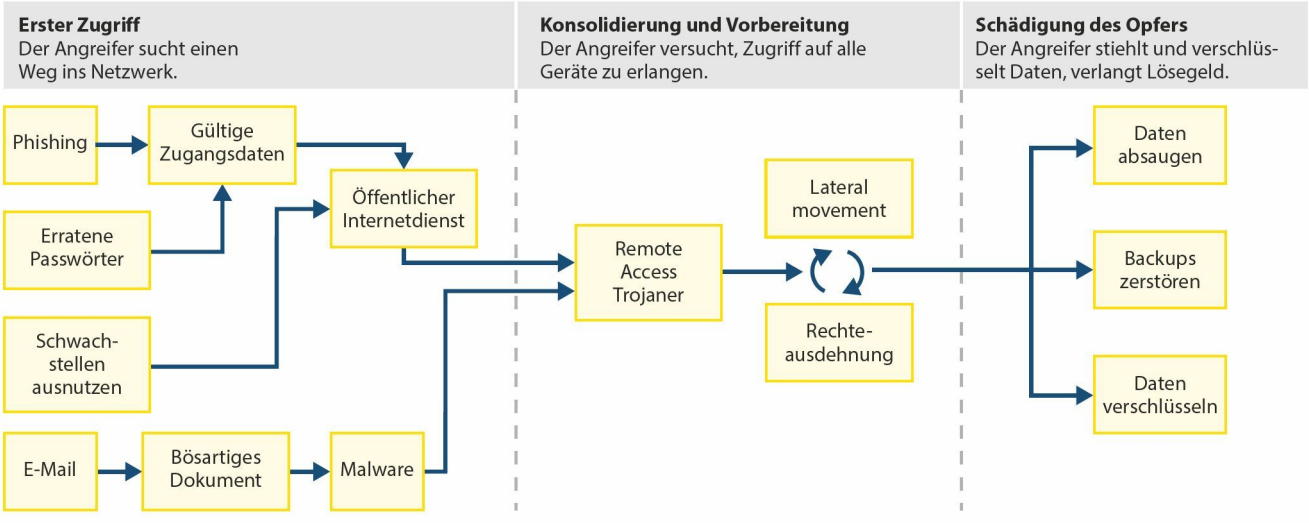
Die Sicherheitsfirma Palo Alto dokumentiert in einem Blog-Beitrag (Link siehe ct.de/w51j) exemplarisch, wie Angreifer gespeicherte Benutzerdaten in Chrome, Firefox, WinSCP, OpenVPN und Git auslesen. Frei verfügbare Tools wie WebBrowserPassView und DataProtectionDecryptor von Nirsoft können das auch. Verhindern ließe sich das, wenn Windows vor dem Entschlüsseln der Passwörter via DPAPI jedes Mal eine Authentifizierung des Anwenders anfordern würde, sei es per Hello-Kamera oder per Fingerabdruck-Scan – macht es aber nicht.

Sie sind drin

Insbesondere die Affiliates von RaaS-Banden – Click-&-Shoot-Kriminelle ohne eigenes Infektions-Knowhow – kaufen Zugangsdaten gerne bei IABs ein. Sie probieren sie systematisch durch, auch bei anderen Diensten. Das nennt sich Credential Stuffing: Irgendwann passt etwa ein im privaten Browser gespeichertes Passwort für den Firmen-Mail-Zugang wegen des Single-Sign-on-Konzepts auch beim VPN-Zugang ins Firmennetz, und sie sind drin. Oder die Affiliates geben etwas mehr Geld aus und kaufen betriebsbereite RAT-Zugänge, um sich auf dem infizierten PC umzusehen. Diese Aktivitäten können durchaus auch ein bis zwei Wochen nach der ursprünglichen

Ablauf eines Ransomware-Angriffs

Einbrüche in Computer laufen typischerweise in drei Phasen ab: Nachdem sich die Angreifer Zugang zu einem ersten System verschafft haben, versuchen sie, ihren Einfluss möglichst unbemerkt auf andere Rechner im Netzwerk auszudehnen. Erst dann verschlüsseln sie Daten oder kopieren sie auf eigene Server, um anschließend ihr Opfer zu erpressen.



Infektion anlaufen, weil die Zugangsdaten zunächst durch mehrere Hände gingen oder sich bei den Banden stauen.

Das weitere Vorgehen unterscheidet sich dann bisweilen nach den vorgefundenen Einstellungen und Programmen. Die Bumblebee-Malware lädt auf Systemen, die Mitglied in einer Arbeitsgruppe wie WORKGROUP sind, einen Infostealer, der den vermuteten Privat-PC nach Passwörtern und Ähnlichem durchsucht. Ist das Opfer hingegen Mitglied in einer Windows-Domäne, wie das typischerweise in Firmen der Fall ist, landet dort sofort ein Cobalt Strike Beacon, über dessen Hintertürfunktion sich recht bald ein Einbrecher persönlich ein genaueres Bild verschafft.

Schadsoftware wird häufig ganz klassisch über Dateien nachgeladen und ausgeführt. Doch es kommen vermehrt auch ausgefeiltere Techniken zum Einsatz. Da holt sich ein Loader den verschlüsselten Schadcode aus dem Internet und dechiffriert ihn im eigenen Arbeitsspeicher. Dann besorgt er sich ein Handle für den Zugriff auf einen laufenden, legitimen Prozess wie den Explorer und reserviert dort Arbeitsspeicher. In den kopiert der Loader den Schadcode und startet ihn als eigenen Thread.

Das hat mehrere Vorteile für den Angreifer: Zum einen sieht es so aus, als ob die Zugriffe auf Dateien und Netzwerk vom Windows-eigenen Explorer stammen, was Sicherheitssoftware beruhigen soll. Zum anderen landet der Schadcode nie auf der Festplatte des Systems. Das reduziert die Gefahr einer Entdeckung durch Wächter wie Antivirensoftware, die gezielt alle Dateien auf Anzeichen von Schadsoftware durchsucht. Außerdem minimiert es die Gefahr, dass der wertvolle Code etwa im Rahmen einer forensischen Analyse in die Hände von Sicherheitsfirmen fällt.

Andererseits birgt diese Methode neue Möglichkeiten, verdächtiges Verhalten zu bemerken. So überwachen Extended Detection & Response Systeme (EDR) die Systemaufrufe aller Prozesse. Bei typischen Malware-Aktivitäten wie dem Zugriff via `WriteProcessMemory()` und `CreateRemoteThread()` auf den Explorer-Prozess terminiert das EDR den Prozess und löst einen Alarm aus. Die Angreifer reagieren darauf, indem sie die EDR-Überwachungs-Hooks deaktivieren oder umgehen. Das Hase/Igel-Rennen ist in vollem Gang.

Eine andere Technik, die verräterische Dateien vermeidet und Windows-eigene Softwaresperren wie Software Restriction Policies (SRP) und AppLocker umgeht, nennt sich Living Off The Land (LOL) – sinngemäß „mit dem arbeiten, was man vorfindet“. Dabei nutzen die Angreifer ganz normale Windows-

Bordmittel – die LOLBins – für ihre Zwecke, also etwa den Download eines Hintertür-Programms via certutil.exe auf der Kommandozeile. Mit LOLBins unterlaufen Angreifer EDR-Systeme, denn es handelt es sich ja um legitime Programme. Eine aktuelle Aufstellung typsicherer LOLBins und wie sie genutzt werden, gibt es unter lolbas-project.github.io.

Quest for Local Admin

Nach dem Einbruch geht es den Einbrechern zunächst darum, den Zugang zum System auszuweiten und sich im Netz zu anderen Systemen weiterzuhangeln (Lateral Movement). Dazu versuchen sie, sich die Rechte eines lokalen Administrators zu verschaffen. Wenn der Anwender, dessen Account gekapert wurde, Mitglied der Gruppe der Administratoren ist und dieser lediglich durch die Benutzerkontensteuerung (User Account Control, UAC) beschränkt wird, haben die Eindringlinge leichtes Spiel. Es gibt reihenweise Demos, wie sich die UAC austricksen lässt, um uneingeschränkte Adminrechte zu ergattern (siehe ct.de/w51j). Etwas schwerer macht man es den Kriminellen, indem man den Regler der Benutzerkontensteuerung (in den Einstellungen nach „UAC“ suchen) ganz nach oben schiebt. Trotzdem sieht auch Microsoft die UAC nicht als zu verteidigende Security-Grenze an. Und Microsoft wird auch erklärtermaßen keine Security-Updates liefern, die UAC-Exploits verhindern könnten.

In Firmennetzen mit administrierten PCs gehören normale Benutzerkonten eher selten zur Gruppe der Administratoren. Deshalb nutzen die Angreifer dort Privilege-Escalation-Lücken. Penibel gepflegte Sicherheitsupdates würden solche Rechteerweiterungen oftmals verhindern, doch dem Angreifer genügt ein einziger, nicht rechtzeitig installierter Patch. Nicht aussterben will auch grottige Software, die noch mit Admin-Rechten läuft, aber bei den Zugriffsrechten auf Dateien und Verzeichnisse schlampt und sich so zum Beispiel eine Malware-DLL unterjubeln lässt. Hat ein Angreifer erst einmal einen Fuß in der Tür, gelingt es ihm erschreckend häufig auch, sich Adminrechte zu verschaffen. Eine erschütternd lange Liste an Tools und Methoden dazu pflegt beispielsweise das GitHub-Projekt „PayloadsAllTheThings“ (siehe ct.de/w51j).

Quest for Domain Admin

Mit den Rechten des lokalen Administrators wird der Rechner erneut auf Zugangsdaten geflöht. Eine zentrale Anlaufstelle dafür ist der Local Security Authority Server Service, kurz LSASS, der alle Anmeldevorgänge durchführt. Dazu hält der LSASS-Prozess die gehashte Version des Passworts im Arbeitsspeicher vor. Dessen Inhalt kann man etwa mit dem – legitimen und von Microsoft bereitgestellten – Werkzeug ProcDump aus der Sysinternals Suite in eine Datei schreiben:

```
procdump64 -ma lsass.exe lsass.dmp
```

Spezielle Tools wie Mimikatz extrahieren aus dieser Datei dann unter anderem die NTLM-Hashes angemeldeter Benutzer. Damit kann sich der Angreifer dann ebenfalls bei allen Diensten im Netz anmelden und sich beispielsweise via RDP von System zu System hangeln. Ist auf einem dieser Systeme ein Domänen-Administrator angemeldet, findet der Angreifer auch dessen NTLM-Hash im Arbeitsspeicher des LSASS-Prozesses. Damit schwingt er sich zum König des Windows-Netzes auf.

Um das zu verhindern, hat Microsoft eigentlich den Credential Guard eingeführt, der den LSASS in eine besonders geschützte virtuelle Umgebung verschiebt, auf die selbst der Administrator oder ein Account mit Systemrechten nicht zugreifen kann. Der Haken dabei ist, dass Credential Guard den teuren Enterprise-Versionen von Windows vorbehalten ist; Heimanwender und auch kleinere Firmen mit Windows-Home- oder -Pro-Lizenzen schauen in die Röhre. Überhaupt setzt sich bei Microsoft immer stärker die Philosophie „Windows ist billig, Security kostet extra“ durch und führt dazu, dass man Sicherheitsfunktionen als Lockmittel für teurere Lizenzen verwendet oder sie sich für viel Geld extra bezahlen lässt [5].

Impact

Mit den erbeuteten Zugängen gehen die Angreifer dann auf Raubzug und exfiltrieren alles an Daten, was ihnen wertvoll erscheint: Dokumente, Datenbank-Dumps und Quellcode landen dabei auf externen Servern. Typischerweise nutzen die Angreifer dazu öffentlich verfügbare Tools wie Rclone, um ganze Verzeichnisbäume in einen speziell dafür angemieteten Cloud-Speicher bei Hostern wie Mega zu kopieren.

Erst wenn sie das Gefühl haben, alles Erreichbare abgeerntet zu haben, kommt die Verschlüsselungssoftware zum Einsatz. Damit die auf möglichst vielen Rechnern im Netz gleichzeitig zuschlägt,

nutzen die Cybercrime-Banden gerne Tools wie psexec, ebenfalls von Sysinternals. So bindet die Ransomware Netwalker mit folgendem Kommando auf allen Systemen der Domain eine Dateifreigabe als Laufwerk Q: ein und startet von dieser aus ein PowerShell-Skript, das letztlich alle wichtigen Daten auf dem Rechner verschlüsselt:

```
C:\psexec.exe @ip-list.txt -d cmd /c "net use q: ↵
↳\\DomainController\DomainName ↵
↳/user:DomainName\administrator Pa$$wOrt &; ↵
↳powershell -EP ByPass -NoLogo -NoProfile ↵
↳-windowstyle hidden -NoExit -File q:\P100119.ps1"
```

Dieses Kommando nutzt keine Sicherheitslücken mehr aus, sondern arbeitet völlig regulär mit den Credentials des Domänen-Administrators. Das gestartete PowerShell-Skript startet die eigentliche Ransomware – ebenfalls von Q: – und hinterlegt anschließend die Lösegeldforderung als neuen Desktop-Hintergrund. In aktuellen Erpressungsversuchen sollen die Opfer häufig gleich zweimal zahlen: erstens für den Schlüssel, mit dem sie ihre Daten wiederherstellen können, und zweitens für die Versicherung der Kriminellen, dass man die kopierten Daten lösche und nicht an Dritte weitergebe.

APT, Hacktivists & Trolle

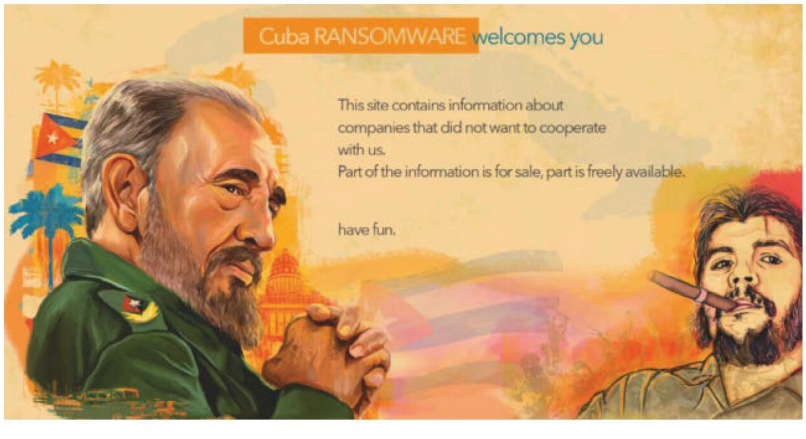
Neben dem organisierten Verbrechen, dem es vor allem um Geld geht, gibt es auch staatlich gesteuerte Angreifergruppen. Die agieren prinzipiell ähnlich, können jedoch auf viel umfangreichere Ressourcen zugreifen und damit auch technisch anspruchsvollere Angriffstechniken einsetzen. Der größte Unterschied ist jedoch in der Zielsetzung begründet: Sowohl für Spionage als auch für gezielte Sabotage am Tag X ist es erforderlich, möglichst unauffällig vorzugehen.

Deshalb agieren diese Advanced Persistent Threats (APT) nicht in die Breite, sondern extrem zielgerichtet und vorsichtig, um keine Alarme auszulösen. Es ist nicht unüblich, dass APT-Gruppen über Monate oder sogar Jahre hinweg unentdeckt im Netz ihrer Opfer agieren. Privatanwender und kleinere Unternehmen haben von APTs in der Regel nur wenig zu befürchten. Außer natürlich, sie haben sich etwa politisch besonders exponiert oder können als Sprungbrett zu den eigentlich anvisierten großen Fischen dienen.

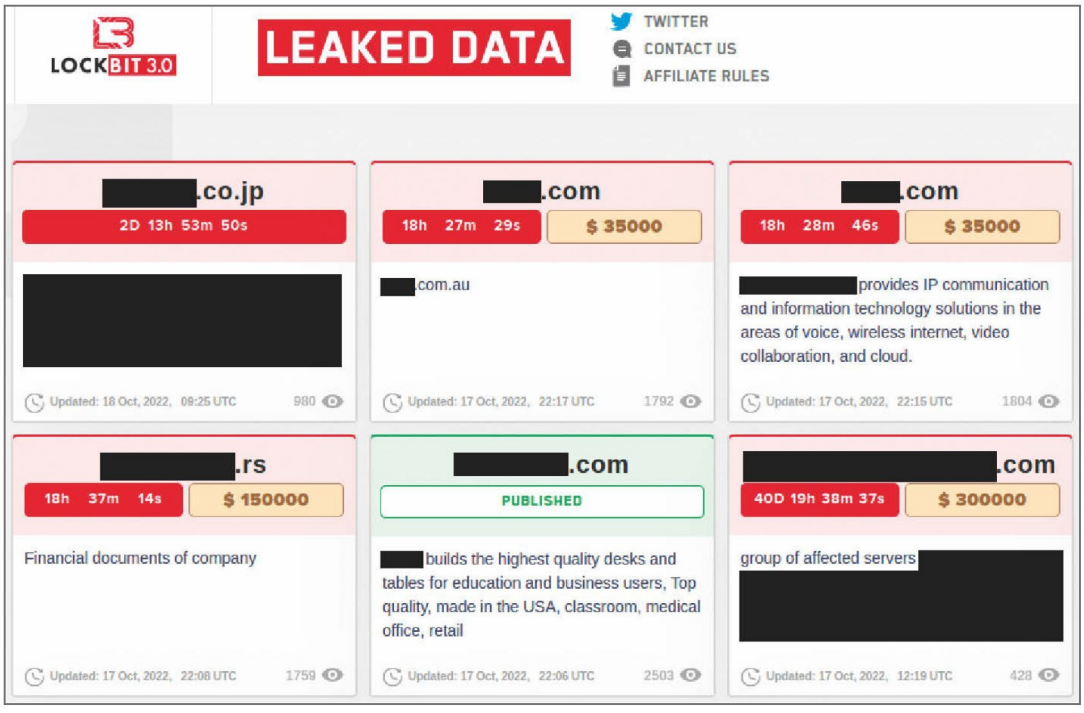
Ferner gibt es auch noch weniger gut organisierte Angreifer, die häufig aus politischen Gründen aktiv werden. Dazu gehören Aktivisten wie die ukrainische IT-Army oder vergleichbare russische Gruppen, die vor allem Dienste mit DDoS-Attacken lahmlegen oder leicht zugängliche Daten stehlen und veröffentlichen.

So schützen Sie sich

Ähnlich, wie die Angriffe mehrstufig erfolgen, sollte auch das Schutzkonzept nicht alles auf eine Karte setzen, sondern in Schichten angelegt sein. Sicherheitsexperten nennen das „Defense in Depth“. Die Grundidee ist, dass auch nach einer Infektion mit Schadsoftware noch nicht automatisch alles verloren ist, sondern man realistische Chancen hat, den Einbrecher zu bemerken und rechtzeitig wieder rauszuwerfen, bevor er ernsten Schaden anrichten kann.



Wer nicht zahlt, wird bloßgestellt: Die Erpresserbande „Cuba Ransomware“ präsentiert erbeutete Datensätze auf einer Webseite im Tor-Netz.



Lockbit ist einer der großen Anbieter von „Ransomware as a Service" und arbeitet mit Doppel-Erpressung. Wer nicht rechtzeitig zahlt (grün), dessen Daten werden auf einer eigenen Leak-Site veröffentlicht.

Der erste Verteidigungswall versucht, es dem Angreifer so schwer wie möglich zu machen, überhaupt einen Fuß in die Tür zu bekommen. Dazu gehören technische Maßnahmen, darunter Sicherheitsupdates zügig einzuspielen und konsequent Zweifaktor-Authentifizierung zu nutzen, aber auch verantwortungsbewusst mit E-Mails umzugehen. Welche Windows-Einstellungen es Eindringlingen so schwer wie möglich machen, lesen Sie im folgenden Artikel „Mehr Sicherheit mit wenigen Handgriffen" ab Seite 16. Und ab Seite 22 nehmen wir „Mehr Schutz dank Smart App Control" unter die Lupe, eine Sicherheitskomponente, die Microsoft im Herbst in Windows 11 eingeführt hat.

Die nächste Verteidigungsschicht soll den Angreifer daran hindern, sich festzusetzen und weiter auszubreiten. Dazu gehören Härtungsmaßnahmen aller Art, also unter anderem die Nutzung von Software Restriction Policies und andere White-Listing-Lösungen. Im Artikel „Mit Restric'tor Schädlinge stoppen" ab Seite 28 erfahren Sie mehr dazu.

Ein wichtiger Baustein ist auch das Monitoring und Alerting, bei dem es darum geht, Angreifer in flagranti zu ertappen. Das muss kein teures Intrusion Detection System sein. Stellen Sie Fallen und Stolperdrähte auf, die ein Angreifer mit seinem Treiben auslöst. Legen Sie dazu zum Beispiel einen ungenutzten Windows-Account auf dem System an, dessen Passwort Sie in Ihrem Arbeitsverzeichnis an passender Stelle speichern. Dann richten Sie alles so ein, dass jeder Login einen Alarm auslöst, und Sie haben Ihren ersten Honeypot gebastelt.

Und schließlich muss man für den Ernstfall vorsorgen. Das beginnt mit guten Backups – kein Backup, kein Mitleid! – und geht bis zu vollständig ausgearbeiteten Notfallplänen. Insbesondere Firmen sollten sich vorab ganz konkret Gedanken machen, wie sie auf – die ganz sicher eintretenden! – Sicherheitsvorfälle reagieren, und das auch dokumentieren. Und zwar tunlichst nicht im Netz, das dann vielleicht schon der Angreifer kontrolliert, sondern ganz klassisch ausgedruckt auf Papier. (hos) c't

Jürgen Schmidt ist Senior Fellow Security bei Heise und baut mit heise Security Pro eine Community für IT-Professionals auf, in der Angriffe, Probleme der täglichen Praxis sowie aktuelle und künftige Technik diskutiert werden: www.heise.de/heisec-pro.

Literatur

[1] Jürgen Schmidt, **MS-Office: So funktioniert der neue Office-Makroschutz,** heise.de/-7164134

[2] Mirko Dölle, **Kleine Ursache, Super-GAU**, Sicherheitslücke Log4Shell: Internet in Flammen, c't 2/2022, S. 10

[3] Ronald Eikenberg, **Gute Mails, böse Mails**, Gefahrloser Umgang mit E-Mails, c't 19/2022, S. 16

[4] Ronald Eikenberg, **E-Mails durchleuchtet**, Phishing-Mails erkennen und abwehren, c't 19/2022, S. 18

[5] Oliver Klarmann, **Microsoft und Emotet: Makroschutz in Office 365 nur für Konzerne,** heise.de/-4664218

Weitere Informationen, Tools zum Download

ct.de/w51j

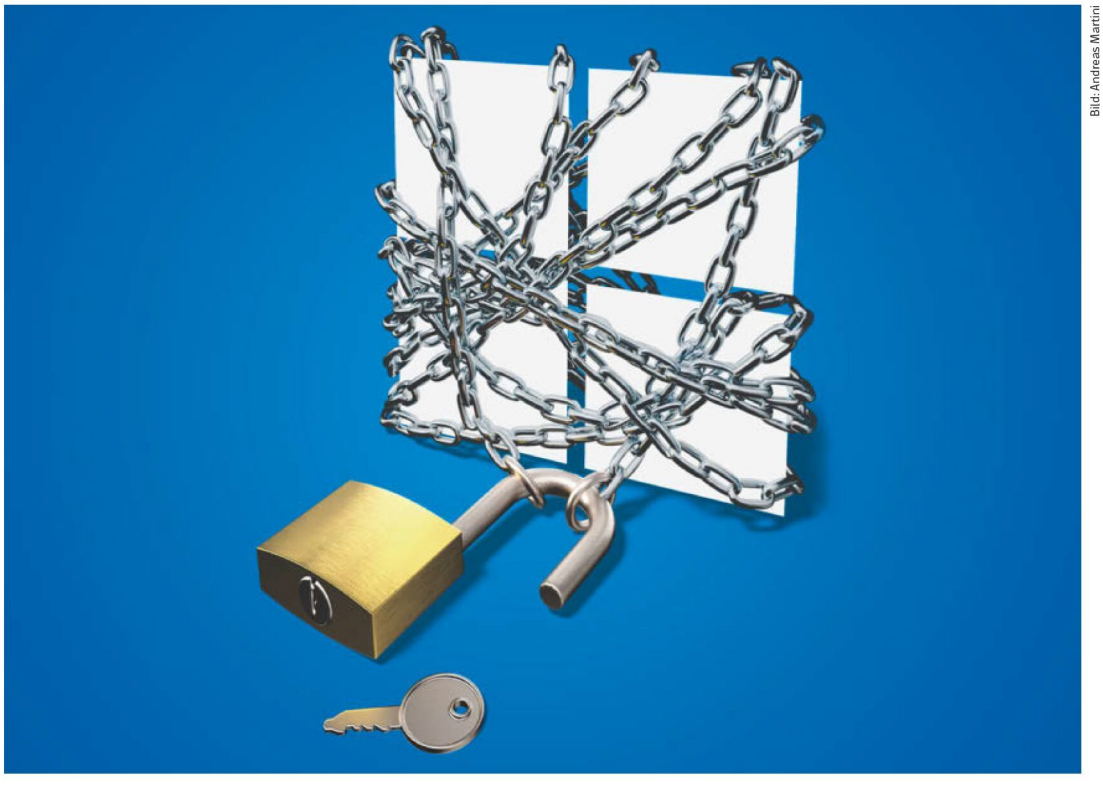


Bild: Andreas Martini

Mehr Sicherheit mit wenigen Handgriffen

Windows ist in seiner Grundkonfiguration nicht einmal halbwegs sicher. Das System bringt einige Funktionen mit, die die Lage bessern – Sie müssen sie aber erst aktivieren. Hier geben wir einen Überblick, welche Funktion eigentlich was macht.

Von **Jan Schüßler**

So mies der Ruf von Windows in Sachen Sicherheit auch ist: Microsoft hat ein paar Funktionen eingebaut, um die inhärenten Sicherheitsprobleme zu entschärfen. Manche wie Virenwächter und Firewall sind immer serienmäßig aktiv, andere nur manchmal – und wieder andere wollen gezielt aktiviert werden oder eignen sich nicht für jeden Nutzer. Auch mit den Bezeichnungen tut Microsoft sich keinen Gefallen: Zuverlässigkeitsbasierter Schutz, SmartScreen, Smart App Control, Manipula-

tionsschutz, Application Guard – wer soll denn da den Überblick behalten? Wir klamüsern das Wirrwarr einmal auseinander.

Das Gros der Sicherheitsfeatures hat Microsoft immerhin zentral in einer App zusammengefasst. Die gibts in Windows 10 und 11 und sie heißt einfach „Windows-Sicherheit“. Die wichtigste Rubrik darin hat den Namen **Viren- und Bedrohungsschutz**. In den „Einstellungen für Viren- und Bedrohungsschutz“ finden Sie vier Schalter: erstens für die Live-Wächterfunktion („Echtzeitschutz“), auch On-Access-Scanner genannt; zweitens für die Cloudunterstützung, die in Verdachtsfällen bei Microsoft anfragt, ob ein Verdacht begründet ist; drittens für die Erlaubnis, unbekannten und verdächtigen Programmcode bei Bedarf zur Analyse an die Microsoft-Cloud zu schicken („Automatische Übermittlung von Beispielen“); viertens für den „Manipulationsschutz“. Der bewirkt, dass zum Abschalten der anderen drei Funktionen Administratorrechte nötig sind. Wir empfehlen, stets alle vier Optionen aktiviert zu lassen. Ausnahme: Wenn Sie Softwareentwickler sind, sollten Sie die automatische Beispielübermittlung abschalten. Anderenfalls könnte jede neue Programmversion, die Sie kompilieren, ungefragt bei Microsoft landen.

Erpressern in den Arm fallen

Außerdem finden Sie unter „Viren- und Bedrohungsschutz“ den „Ransomware-Schutz“, auch „überwachter Ordnerzugriff“ genannt. Nach unserem Eindruck ist diese schon einige Jahre bestehende Funktion zuerst in Verruf und dann in Vergessenheit geraten, weil sie sich mitunter sperrig verhält. Ist sie aktiv, dürfen nur als unschädlich bekannte Prozesse in Ihren Dokumentenordnern schreiben. Wird ein Erpressungstrojaner (Ransomware) aktiv, hindert die Funktion ihn daran, Ihre Dateien zu verschlüsseln.

Wenn Sie den Ransomware-Schutz verwenden, müssen Sie damit rechnen, dass er gelegentlich dazwischengrätscht, wenn Sie eine Datei speichern oder ändern wollen – und zwar dann, wenn Windows das Programm, mit dem Sie arbeiten, (noch) nicht als harmlos erkennt. Das kann bei eher unbekannten oder hoch spezialisierten Programmen passieren, aber auch nach einem Update einer gängigen Software. Sofern Sie sich sicher sind, dass das fragliche Programm harmlos ist, gewähren Sie ihm per „App durch überwachten Ordnerzugriff zulassen“ Schreibrechte. Außerdem können Sie mit einem Klick auf „Geschützte Ordner“ zusätzliche Orte angeben, für die der Ransomware-Schutz ebenfalls greifen soll.

Streng genommen ist diese Funktion kein echter Virenschutz, denn sie hindert den Nutzer nicht daran, schädlichen Code zu starten. Die Idee, beliebige Prozesse nicht kommentarlos in die eigenen Dateien schreiben zu lassen, ist allerdings gut und durchaus eine sinnvolle zusätzliche Schutzschicht. Unsere Empfehlung: Einschalten und schauen, wie sich der Ransomware-Schutz in Ihrem Alltag schlägt. Nutzen Sie nur wenige und stark verbreitete Software, stehen die Chancen gut, dass Sie ihn im Alltag gar nicht bemerken. Nehmen die Arbeitsunterbrechungen durch neue Programmversionen doch überhand, schalten Sie die Funktion einfach wieder ab – einen Versuch war es wert.

Eine Selbstverständlichkeit

Eine Firewall ist ein Grundpfeiler eines sicheren Betriebssystems. Sie schützt das System vor unberechtigten Zugriffen aus dem Netz. Die Windows-Firewall muss im Alltagsbetrieb nicht angefasst werden; nur bei wenigen Programmen fragt sie einmalig, ob Sie der Software die Verbindung mit dem Internet erlauben möchten.

Manuelle Eingriffe in die Firewall-Konfiguration brauchen Sie nur in Spezialfällen, wenn Sie zum Beispiel Netzwerkdienste konfigurieren oder unter bestimmten Bedingungen nur einzelnen Prozessen den Internetzugriff erlauben möchten – ein Beispiel für Letzteres lesen Sie in [1].

Ob die Firewall aktiv ist, sehen Sie in der App „Windows-Sicherheit“ unter **„Firewall und Netzwerkschutz“**. Dort können Sie sie mit einem Klick auf „Standard für Firewalls wiederherstellen“ auch auf Werkseinstellungen zurücksetzen. Das kann praktisch sein, wenn Sie die Einstellungen einmal durch falsche oder zu viele händische Eingriffe kaputtgespielt haben. Hier droht eine Falle: So manche Anwendung, die ganz legitim ein Loch in der Firewall braucht, fragt Sie zwar, ob Sie das zulassen wollen. Doch oft erscheint diese Nachfrage nur bei einer Neuinstallation des Programms. Nach dem Zurücksetzen der Firewall kann es passieren, dass die Anwendung einfach kommentarlos nicht mehr geht. Die Abhilfe ist simpel: fragliche Anwendung erst de- und dann wieder neu installieren.

Funktionsflut

Im Bereich **„App- und Browsersteuerung“** der Windows-Sicherheit-App stecken einige Funktionen, die Sie kennen sollten. Ins Untermenü „Zuverlässig-

keitsbasierter Schutz“ hat Microsoft einen ganzen Schwung von verwirrend ähnlichen und schwammig voneinander abgegrenzten Funktionen hineingestopft. Sie firmieren unter „SmartScreen“ und haben gemeinsam, dass es nicht um klassischen Virenschutz geht, sondern um Schutz vor anderer unangenehmer Software, oft auch „potenziell unerwünschte Apps“ (PUA) genannt, sowie um Betrugs- und Identitätsschutz. Ein typisches Beispiel dafür sind betrügerische Webseiten und Apps zum Zweck von Phishing, Scam und Ähnlichem, aber auch Adware, die häufig in den Installationspaketen von Gratis-Downloads steckt und unerwünschte Zusatzsoftware installiert oder Werbebanner einblendet. Doch der Reihe nach.

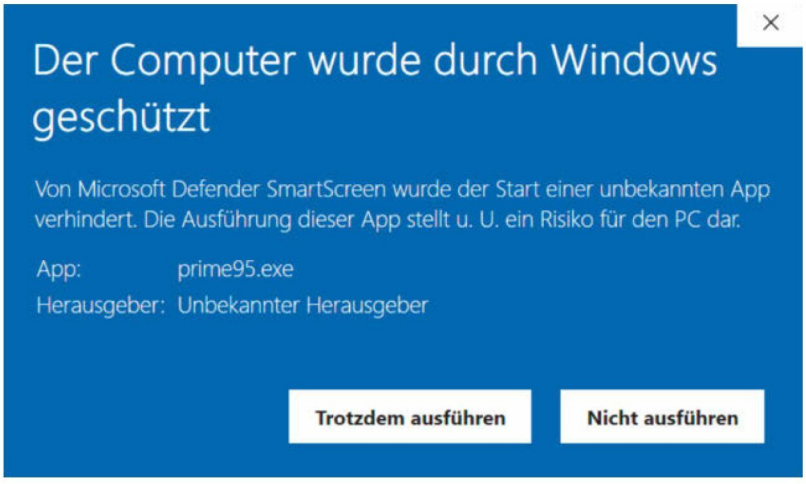
Ist „Apps und Dateien überprüfen“ aktiv, hält SmartScreen auf dem PC nach betrügerischer Software Ausschau; „SmartScreen für Microsoft Edge“ zeigt eine Warnung, wenn Sie mit Microsofts Webbrowser Edge versuchen, eine Phishing-Seite oder Ähnliches aufzurufen. „SmartScreen für Microsoft Store-Apps“ erweitert diesen Schutz analog dazu auf das Verhalten von Apps aus dem Microsoft-Store.

Zudem gibts noch einen weiteren Schalter mit der etwas kantigen Bezeichnung „Potenziell unerwünschte Apps werden blockiert“. Wenn Sie ihn aktivieren, nimmt der Defender nicht nur Betrügerisches ins Fadenkreuz, sondern auch Software, die gar kein Sicherheitsrisiko darstellt, aber zu Stabilitäts- oder Performanceproblemen führen kann – so beschreibt Microsoft das zumindest.

Die Klassifizierung, was nur leistungsschädigend ist und was betrügerisch, bekommt Microsoft aber nicht immer einwandfrei hin. So blockierte SmartScreen etwa zeitweilig das als CPU-Stresstester beliebte Tool Prime95, und zwar selbst dann, wenn „Potenziell unerwünschte Apps werden blockiert“ gar nicht eingeschaltet war. Betrügerisch ist an dem Tool nichts – es lastet bloß die CPU stark aus und führt dazu, dass das System nur noch lahm reagiert, die CPU viel Leistung aufnimmt und die Lüfter hochdrehen. Solche Fehlalarme sind keine große Hürde; mit Klicks auf „Weitere Informationen“ und „Trotzdem ausführen“ können Sie sie übergehen.

Noch mehr Verwirrung gefällig? Unter Windows 11 gibt es im Untermenü „Zuverlässigkeitsbasierter Schutz“ noch einen weiteren Schalter namens „Phishingschutz“. Gemeint ist hier speziell der Schutz Ihres Windows- beziehungsweise Microsoft-Kontokennworts, je nachdem, ob Sie sich mit einem lokalen oder mit einem Microsoft-Konto am Rechner anmelden. Bemerkt Windows, dass Sie Ihr Kennwort irgendwo eintippen, wo es nicht hingehört, grätscht eine Warnung dazwischen. Möglich ist das erstens bei verdächtigen Apps und Webseiten, zweitens, wenn Sie Ihr Kontokennwort in Apps oder auf Webseiten anderer Anbieter wiederverwerten wollen,

Manche Funktionen von „Zuverlässigkeitsbasierter Schutz“ gehen auf Kosten der Bequemlichkeit; trotzdem empfehlen wir, alle einzuschalten.



SmartScreen greift auch mal bei harmlosen Tools ein. Wenn Sie sicher sind, dass das Programm keine Gefahr birgt, können Sie die Warnung aber mit zwei Klicks übergehen.

und drittens, wenn Sie Ihr Kennwort im Klartext in ein Dokument eintippen. Letzteres war in einem kurzen Test nicht gerade verlässlich: Gegen eine Eingabe des Kennworts im Editor (notepad.exe) protestierte die Funktion, in LibreOffice-Dokumente hingegen konnten wir es ungehindert eintippen. Unsere Empfehlung: Schalten Sie alle Funktionen im Untermenü „Zuverlässigkeitsbasierter Schutz“ ein. Der bessere Schutz wiegt schwerer als ein paar übereifrige Warnungen wie bei Prime95.

Im Menü „App- und Browsersteuerung“ der App „Windows-Sicherheit“ gibt es außer dem Abschnitt „Zuverlässigkeitsbasierter Schutz“ noch ein paar weitere Untermenüs. Im „Exploit-Schutz“ finden Sie Optionen, um an Sicherheitsfunktionen von Kernel und Prozessor zu drehen, etwa der Speicherverwürfelung (Address Space Layout Randomization, ASLR) oder der Data Execution Prevention (DEP). Bitte ändern Sie hier nichts – die Werkseinstellungen sind bereits optimal.

Wenn Sie Windows in einer Pro- oder höheren Edition verwenden und das Feature „Microsoft Defender Application Guard“ installiert haben, finden Sie unter „App- und Browsersteuerung“ den Abschnitt „Isoliertes Browsen“. Hier können Sie festlegen, welche Aktionen in einem Edge-Fenster im Application-Guard-Modus erlaubt sind (unten mehr dazu).

In Windows 11 ab Version 22H2 finden Sie unter „App- und Browsersteuerung“ außerdem die neue Funktion „Smart App Control“, die mit einem Mix aus bekannten Ansätzen vor Malware schützen will. Verwendbar ist sie nur auf einem frisch installierten Windows 11 in Version 22H2. Auf Systemen, die diese Version als Upgrade erhalten haben, können Sie Smart App Control erst aktivieren, nachdem Sie Windows auf den Werkszustand zurückgesetzt haben. Sie ist dennoch so interessant, dass wir sie separat im Artikel „Mehr Sicherheit mit weniger Handgriffen“ auf S. 22 erklären.

Hardwarenahe Sicherheitsfeatures

Die Rubrik **Gerätesicherheit** der Windows-Sicherheit-App enthält je nach Ausstattung des Systems bis zu vier Unterpunkte. Drei davon informieren lediglich über bestimmte Sicherheitsfunktionen – nämlich die Untermenüs „Sicherheitschip“ für Infos zu einem eventuellen Trusted Platform Module (TPM), „Sicherer Start“, sofern UEFI Secure Boot in der Gerätefirmware aktiv ist, sowie „Datenverschlüsselung“, wo es um die Laufwerksverschlüsselung BitLocker geht.

Einen Blick wert ist allerdings das Untermenü „Kernisolierung“ mit der Funktion „Speicherintegrität“. Hierbei handelt es sich um eine Funktion für virtualisierungsbasierte Sicherheit (VBS). Die Details zu VBS sind kompliziert, mehr dazu lesen Sie in [2]. Ist die Speicherintegrität aktiv, laufen Windows-Kernelkomponenten und systemkritische Treiber isoliert vom Rest des Systems. Die technische Grundlage dafür ist Microsofts Hyper-V-Hypervisor – deshalb „virtualisierungsbasierte“ Sicherheit.

Eine Voraussetzung, um die Kernisolierung einschalten zu können, ist eine CPU mit Hardware-Virtualisierung. Die allermeisten CPUs aus den letzten zehn Jahren haben diese Funktion; im BIOS muss sie aber eventuell erst aktiviert werden. Meist heißt sie „Intel VT“, „AMD-V“, „Secure VM“ oder ähnlich. Außerdem können Sie die Kernisolierung nicht scharfschalten, wenn in Ihrem Windows ein inkompatibler Treiber mitläuft.

Die Kernisolierung zu verwenden drückt die Systemleistung ein wenig [3]. Unser Tipp: Wenn Sie nicht gerade das letzte Quäntchen Leistung aus Ihrer Hardware herausquetschen wollen, schalten Sie die Kernisolierung ein. Aber: Ist die Funktion nicht verfügbar oder scheitert sie an einem Treiber für eine alte, aber essenzielle Hardware, investieren Sie nicht allzu viel Aufwand. Microsoft möchte zwar die Kern-

isolierung in Windows 11 künftig stets serienmäßig aktivieren und perspektivisch zu einer Selbstverständlichkeit machen. Am wichtigsten bleibt es aber, schon vorher einzugreifen und Malware gar nicht erst auf den PC kommen zu lassen. Sofern auf Ihrem System verfügbar, können Sie HVCI als willkommenes Security-Schmankerl ansehen – lebenswichtig ist es nicht.

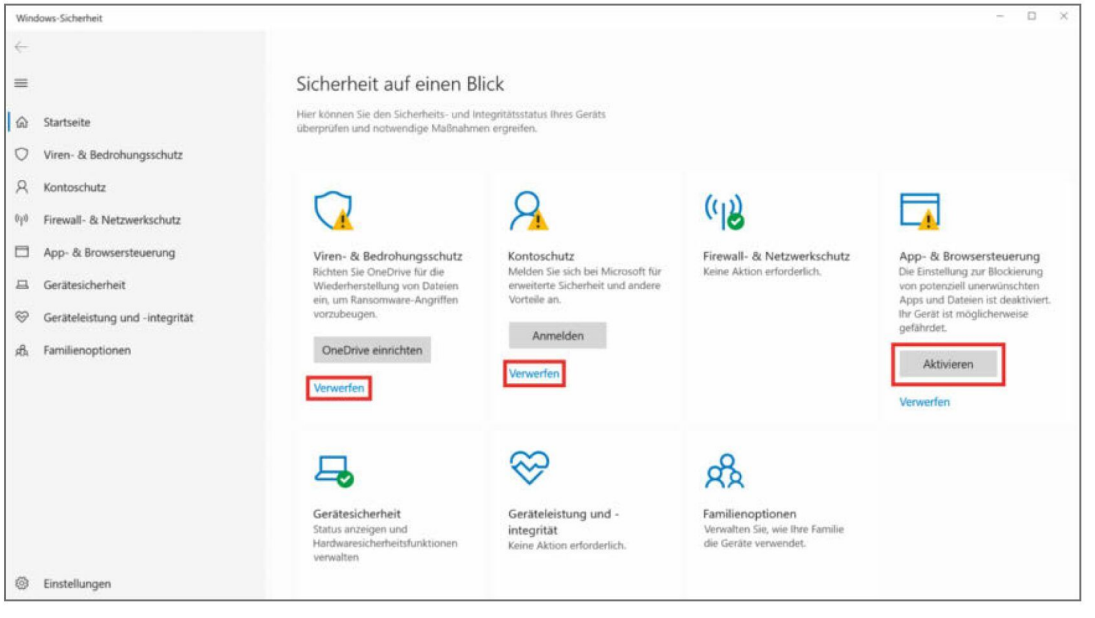
OneDrive für mehr Sicherheit?

Was die App „Windows-Sicherheit" sonst noch bietet, hat mit dem Schutz vor Schadsoftware nur wenig bis gar nichts zu tun. Eine Funktion, die Microsoft allerdings gerne auch als Schutz vor Erpressungstrojanern anpreist, ist die Synchronisierung mit OneDrive unter „Kontoschutz". Wenn Sie die einrichten, hält Windows die Inhalte Ihrer Dokumenten-, Bilder- und sonstigen Datenordner nicht nur stets mit Microsofts Cloudspeicher synchron, sondern versioniert auch alles umgehend, was Sie an Dateien hochladen. Selbst wenn Sie sich einen Erpressungstrojaner einfangen und alle verschlüsselten Dateien ins OneDrive wandern: Über den Versionsverlauf können Sie Ihre Dateien einfach wieder auf den unverschlüsselten Zustand zurücksetzen. Natürlich erst, nachdem Sie den Rechner vom Trojaner befreit haben.

Wer OneDrive nutzen will, muss aber ohnehin schmerzfrei sein, was die offenkundigen Datenschutzdefizite angeht. Zudem muss das OneDrive groß genug für den eigenen Datenbestand sein. Wer mehr als 5 GByte an Dateien besitzt, kommt um ein kostenpflichtiges Abo nicht herum. Unser Tipp: Kein Backup, kein Mitleid – doch Microsofts Cloudspeicher brauchen Sie nicht, um Ihre Daten vor Ransomware zu schützen. Mit dem P2P-Tool Syncthing und einem Raspi als Datenhalde richten Sie Ihre eigene Synchronisierung ein – quelloffen, sicher, datenschutzfreundlich und ebenfalls versionierend [4,5].

Außerhalb der Sicherheits-App

Die Benutzerkontensteuerung (User Account Control, UAC) zwingt Prozesse, die Administratorrechte verlangen, Sie vorher um Erlaubnis zu bitten. Die typischen Abfragen, bei denen der Bildschirm abgedunkelt wird und Sie die Adminrechte mit einer Ja/Nein-Abfrage bestätigen oder verweigern müssen, er-



Nicht allen Vorschlägen von Windows müssen Sie folgen – zu OneDrive gibt es gute Alternativen, und der Login per Microsoft-Konto dient vor allem dem Komfort.

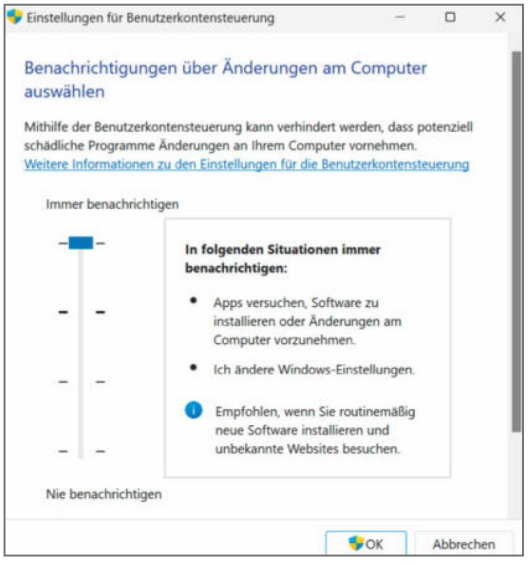
scheint in der Werkseinstellung von Windows nur, wenn Sie Programme installieren wollen, nicht aber beim Verändern von Windows-Einstellungen.

Streng genommen ist es technisch unsauber, UAC als eine Sicherheitsfunktion zu bezeichnen. Malware-Entwickler, die es darauf anlegen, können die Abfrage austricksen, und Microsoft gibt selbst zu, dass UAC keine harte Grenze zieht, sondern vor allem den Anwendern helfen soll, wachsamer zu sein. Dennoch steht die laxe Werkseinstellung seit Langem in der Kritik. Insbesondere kann eine Schadsoftware Module der Microsoft Management Console (Dateiendung .msc) missbrauchen, um eine unbemerkte Rechteausweitung (Privilege Escalation) zu erschleichen – ein Beispiel dafür ist die Ransomware Erebus [6]. Unsere Empfehlung: UAC ist nicht perfekt, doch es spricht nichts dagegen, sie stets auf die höchste Stufe zu setzen. Das klappt im Handumdrehen: Windows-Taste drücken, `uac` eintippen, Eingabetaste betätigen und den Regler ganz nach oben schieben. Die UAC macht Windows zwar nicht im Alleingang sicher, aber die bisherigen Exploits funktionieren dann nach unserem Kenntnisstand nicht mehr.

Pro-Funktionen nutzen

Manch praktische Sicherheitsfunktion bietet Windows erst ab der Pro-Edition an. Der bereits erwähnte **Microsoft Defender Application Guard** richtet sich zwar in erster Linie an Admins von Firmennetzen, kann aber auch auf Einzelplatzrechnern sinnvoll sein. Die Funktion müssen Sie zunächst über „Windows-Features aktivieren oder deaktivieren“ einschalten. Nach einem Neustart des Rechners können Sie im Webbrowser Edge rechts oben im Dreipunktmenü auf „Neues Application Guard-Fenster“ klicken. Nach wenigen Sekunden öffnet sich eine Edge-Instanz, die abgeschottet in einer virtuellen Umgebung läuft – praktisch etwa, um Webseiten aufzurufen, von deren Unbedenklichkeit Sie nicht überzeugt sind.

Ähnlich hilfreich ist die **Windows Sandbox**. Sie aktivieren sie ebenso wie den Application Guard per „Windows-Features aktivieren oder deaktivieren“. Die Sandbox ist ein schlank vorkonfiguriertes virtuelles Windows, das auf halbwegs modernen Rechnern innerhalb weniger Sekunden startet. Schließt man das Sandbox-Fenster, werden sämtliche Änderungen an der VM verworfen. Damit eignet sich die Funktion prima, um Software in Ruhe auszuprobieren, ohne sie nativ auf einem Produktivsystem zu installieren.



Schieben Sie den Regler an den oberen Anschlag, haben es Trojaner schwerer, sich unbemerkt an Ihnen vorbeizuschleichen.

Fazit

Windows kommt mit einigen serienmäßig inaktiven Features, die zu aktivieren Ihnen helfen kann, die Security-Misere des Systems zu entschärfen. Nicht alle davon sind für jedermann geeignet, doch es lohnt sich, sie auszuprobieren und aktiv zu lassen, wenn sie keine Probleme bereiten. So können Sie pauschal alles einschalten, was Windows im Bereich „zuverlässigkeitsbasierter Schutz“ bietet und die Benutzerkontensteuerung mit einem Handgriff verbessern. Der wenig bekannte Ransomware-Schutz „überwachter Ordnerzugriff“ fristet sein Schattendasein nach unserer Einschätzung zu Unrecht – vor allem auf Systemen, auf denen keine exotische Software läuft, sollten Sie ihm eine Chance geben.

Andere Funktionen sind nett, sofern Sie verfügbar sind, etwa die Kernisolierung und die ab der Pro-Edition enthaltenen Abschottungsfunktionen. Zeigt Ihr Windows sie nicht, müssen Sie sich aber kein Bein ausreißen, um sie zu bekommen. Erwähnt haben wir in diesem Artikel bereits die neue Funktion „Smart App Control“. Sie könnte sich auf Dauer als komfortablerer Ersatz für den Ransomware-Schutz erweisen – wie sie das macht, lesen Sie im folgenden Artikel. (jss) c't

Literatur

[1] Jan Schüßler, **Sparsam im Grünen**, Wie Sie unter Windows das Inklusiv-Volumen Ihres Mobilfunkvertrags schonen, c't 11/2021, S. 150

[2] Christof Windeck, **Harter Schnitt**, Wie Sie erkennen, ob ihr PC die Hardware-Anforderungen für Windows 11 erfüllt, c't 22/2021, S. 22

[3] Axel Vahldiek, **Und los!**, Windows 11: Erste Messergebnisse, c't 24/2021, S. 50

[4] Jan Schüßler, **Ding zum Sichern**, Plattformunabhängiges Backup mit Syncthing, c't 14/2021, S. 140

[5] Jan Schüßler, **Synchrone Kopien**, Raspi als zentraler Backupserver mit Syncthing, c't 14/2021, S. 144

[6] Dennis Schirrmacher, **Erpressungs-Trojaner Erebus umgeht erfolgreich UAC-Abfrage von Windows**, heise Security, via heise.de/-3619820

Bild: Andreas Martini

Mehr Schutz dank Smart App Control

Die mit dem 2022er Update eingeführte Schutzfunktion Smart App Control soll Windows 11 endlich sicher machen. Das Konzept könnte aufgehen, doch wer von dem neuen Schutz profitieren will, muss Einschränkungen in Kauf nehmen.

Von **Ronald Eikenberg**

Mit der Sicherheitsfunktion Smart App Control hat Microsoft die größte Änderung am Schutzkonzept von Windows seit der Einführung des Virenschutzprogramms Windows Defender vorgenommen. Die Schutzfunktion soll verhindern, dass das System von aktuellen und künftigen Schädlingsgenerationen befallen wird – und schützt den Anwender dabei im Wesentlichen vor sich selbst: Ist die neue Schutzfunktion aktiv, darf man nur noch ausführen, was Microsoft für unbedenklich hält.

Das Konzept dürfte insbesondere Apple-Kunden bekannt vorkommen. Die Mobilbetriebssysteme iOS und iPadOS führen seit jeher ausschließlich Apps aus, die aus dem App Store stammen und von Apple überprüft und digital signiert wurden. Das kurbelt

nicht nur den Umsatz des App Store an, es sorgt auch dafür, dass iPhones und iPads bislang weitgehend virenfrei sind. macOS ist nicht ganz so streng: Das Desktopbetriebssystem warnt zwar vor unsignierten Apps, per Rechtsklick und „Öffnen“ kann man sie jedoch trotzdem starten.

Unter Windows genießen Anwender indes alle Freiheiten und dürfen installieren und starten, was immer sie möchten. Das hat nicht nur positive Seiten, aus Security-Sicht ist das sogar höchst problematisch. Denn nicht jeder Windows-Nutzer ist dazu in der Lage, das Risiko, das von einer Datei ausgeht, angemessen zu bewerten, bevor er sie ausführt. Dies ist jedoch gerade unter Windows unerlässlich, denn das Betriebssystem steht wie kein anderes unter Beschuss der Cyberganoven. Das Resultat: Tagtäglich werden unzählige Windows-Systeme mit Malware infiziert, darunter auch kritische Ziele wie Energieversorger, Krankenhäuser und Stadtverwaltungen. Es genügt ein unbedarfter Klick und alle Räder stehen still.

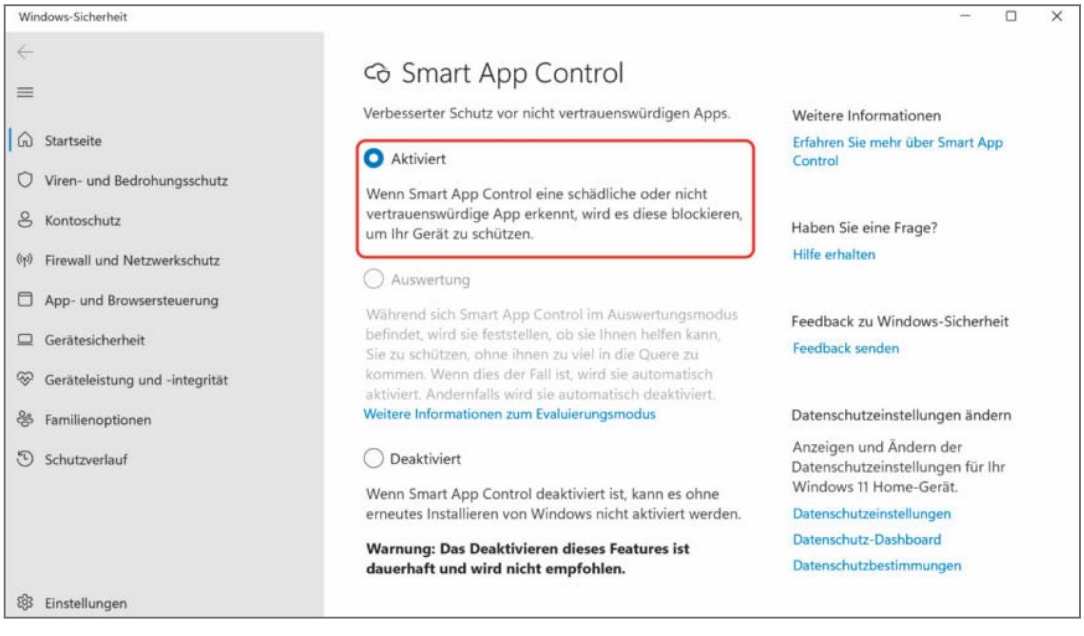
Zwickmühle Windows

Microsoft steckt hier in einer Zwickmühle. Um das Problem zu lösen, wären weitreichende Änderungen nötig. Doch Windows ist historisch gewachsen und läuft auf mehr als einer Milliarde Rechner weltweit. Es ist undenkbar, auf all diesen Rechnern nachträglich etwa den Microsoft Store zur einzigen Bezugsquelle für Software zu erklären, auch wenn es der Sicherheit zuträglich wäre. Der auf manchen Rechnern beim Kauf aktive S-Modus von Windows, der genau das umsetzt, erfreut sich aufgrund solcher Einschränkungen keiner großen Beliebtheit.

Mit Smart App Control (SAC) beschreitet der Windows-Hersteller nun einen flexibleren Mittelweg: Die neue Schutzfunktion erlaubt es den Anwendern weiterhin, Programme aus beliebigen Quellen zu beziehen. Ausführen darf man sie jedoch nur, wenn SAC zu dem Urteil kommt, dass die Datei unbedenklich ist.

Das ist ein wichtiger Unterschied zu Virenschutzprogrammen: Diese schreiten ein, wenn sie vermuten, dass eine Datei bösartig ist – SAC hingegen blockiert alles, was nicht unbedenklich ist. So kann Smart App Control auch Schädlinge abwehren, die noch nicht auf dem Radar des Virenwächters auftauchen. SAC ergänzt den Virenschutz und arbeitet mit beliebigen Antivirenprogrammen zusammen, da es nicht an den Windows Defender gekoppelt ist.

Doch welche Dateien sind eigentlich unbedenklich? Um das herauszufinden, befragt Smart App Control die Microsoft-Cloud. Dort läuft ein KI-Modell, das laut Microsoft täglich mit 43 Milliarden Informationshäppchen gefüttert wird. Es ist darauf trainiert,



Sie können Smart App Control auch manuell einschalten. Knipsen Sie die Schutzfunktion aber wieder aus, bleibt sie dauerhaft deaktiviert.

Angreifer nutzen aktuell gerne Dateiformate wie ISO zur Verbreitung von Malware. Smart App Control blockiert solche Dateien grundsätzlich, wenn sie aus dem Internet stammen.

die Vertrauenswürdigkeit von Dateien zu bewerten, und liefert in Echtzeit ein aktuelles Ergebnis. Darüber hinaus überprüft SAC die digitalen Signaturen der Dateien. Weist eine Datei eine gültige Signatur auf, kann man sie auch dann ausführen, wenn die Cloud-KI kein grünes Licht gibt.

Damit sich Malware-Entwickler dieses Schlupfloch nicht zunutze machen, muss die digitale Signatur mit einem Zertifikat erstellt worden sein, das den Ansprüchen von Microsofts Authenticode-Verfahren genügt. Solche Zertifikate sind mit einem aufwendigen Verifizierungsprozess verbunden und kosten normalerweise mehrere hundert Euro im Jahr. So soll sichergestellt werden, dass legitime Hersteller wie Adobe oder Mozilla ein passendes Zertifikat bekommen, nicht aber die Entwickler von Schadsoftware. Aufwand und Kosten sind allerdings auch für zahlreiche Entwickler zu hoch – wer kein Geld mit seiner Software verdient, wird eher davon absehen, ein teures Zertifikat zu erwerben.

Trotz Cloud-Intelligenz und Signaturcheck kann es vorkommen, dass SAC die Ausführung einer legitimen Datei verhindert. Besonders groß ist die Wahrscheinlichkeit bei wenig verbreiten Programmen, selbst kompilierten Binaries oder Tools, die sich theoretisch auch für Angriffe missbrauchen lassen. In diesem Fall steht man vor einem echten Problem, denn derzeit gibt es keinen Weg, die Datei trotzdem zu starten – es ist nicht vorgesehen, eine Ausnahme zu definieren.

Mark of the Web

Smart App Control nimmt auch die aktuellen Angriffstrends ins Visier, etwa Vireninfektionen durch Verknüpfungsdateien (.lnk) oder ISO-Container (siehe „So wird Windows angegriffen“ ab Seite 8). Es führt eine Liste potenziell gefährlicher Dateitypen und blockiert das Öffnen grundsätzlich, sofern die Dateien aus dem Internet stammen. Die folgenden 39 Dateitypen stehen auf der schwarzen Liste: .appref-ms, .appx, .appxbundle, .bat, .chm, .cmd, .com, .cpl, .dll, .drv, .gadget, .hta, .iso, .js, .jse, .lnk, .msc, .msp, .ocx, .pif, .ppkg, .printerexport, .ps1, .rdp, .reg, .scf, .scr, .settingcontent-ms, .sys, .url, .vb, .vbe, .vbs, .vhd, .vhdx, .vxd, .website, .wsf und .wsh.

Ob eine Datei aus dem Internet stammt, liest SAC an der Mark of the Web (MotW) ab. Dabei handelt es sich um eine Textmarkierung in den Alternate Data Streams (ADS) einer Datei, die von dem Programm gesetzt wird, das die Datei heruntergeladen hat – üblicherweise der Browser oder der Mailclient.

Ob das MotW bei einer Datei gesetzt ist, können Sie leicht selbst überprüfen: Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie „Eigenschaften“. Befindet sich unten auf dem Registerreiter „Allgemein“ der Abschnitt „Sicherheit“ mit dem Hinweis „Die Datei stammt von einem anderen Computer. Der Zugriff wurde aus Sicherheitsgründen eventuell blockiert“, dann ist die Markierung gesetzt.

Wenn Sie einen Blick hinter die Kulissen werfen möchten, könnten Sie den passenden ADS einsehen, indem Sie den folgenden Befehl in die Eingabeaufforderung oder ins Terminal tippen: `notepad.exe DATEINAME:Zone.Identifier`.

Ist das MotW gesetzt, öffnet sich der Editor mit dem folgenden Inhalt:

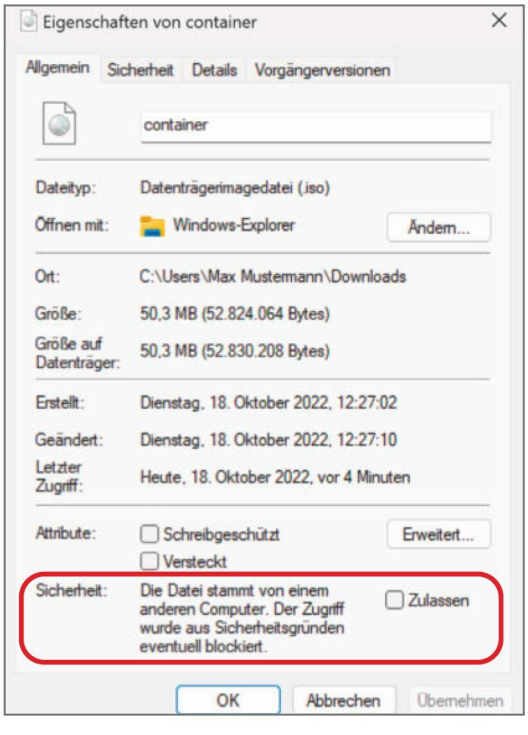
```
[ZoneTransfer]
ZoneId=3
```

Die ZoneId 3 steht für das Internet. Fragt der Editor, ob er eine neue Datei erstellen soll, dann existiert kein ADS namens Zone.Identifier und das Mark of

the Web ist somit auch nicht gesetzt. Alternativ kann man sich auch mit dem PowerShell-Befehl `get-item * -Stream Zone.Identifier -ErrorAction SilentlyContinue | select FileName` alle Dateien auflisten lassen, die das MotW tragen.

Das MotW existiert bereits seit vielen Jahren, es wurde jedoch erst vor kurzem von Microsoft wiederentdeckt: Nach einem Update für MS Office warnt die Büro-Suite sehr deutlich vor Makros, wenn anhand des MotW erkennbar ist, dass das Dokument aus dem Internet stammt [1]. Seitdem werden Office-Anwender mit einem roten Warnhinweis über die möglichen Gefahren aufgeklärt, bevor die Makros ausgeführt werden können.

Das zielt auf den wichtigsten Verbreitungsweg von Ransomware ab: Cyberganoven verschicken vor allem mit Makros gespickte Office-Dokumente, die den eigentlichen Schädling aus dem Internet nachladen und ausführen. Ist Smart App Control aktiv, können auch andere, potenziell gefährliche Dateitypen nicht mehr so leichtfertig ausgeführt werden. Ein zuverlässiger Schutz ist das MotW allerdings nicht: Mitunter geht es beim Entpacken oder Kopieren der heruntergeladenen Dateien verloren, etwa wenn das Entpackprogramm die Markierung bei den extrahierten Dateien nicht setzt.



Ob eine Datei aus dem Internet stammt und damit potenziell gefährlich ist, liest Smart App Control an der Dateimarkierung „Mark of the Web" ab. Erscheint der rot markierte Abschnitt in den Dateieigenschaften, ist sie gesetzt.

Nicht für jeden

Das Konzept von Smart App Control klingt schlüssig und könnte tatsächlich dazu beitragen, dass Ihr Windows von der nächsten Virenwelle verschont bleibt. Die Sache hat jedoch einige Haken. Einen davon haben wir oben schon erwähnt: Wenn SAC eine Datei blockiert, gibt es keine Möglichkeit, sie auf eigenes Risiko trotzdem auszuführen. Vermutlich möchte Microsoft so verhindern, dass der Rechner infiziert wird, wenn die Schutzfunktion mal kurz nicht hinschaut. Die einzige Ausnahme sind Dateien, die ausschließlich aufgrund ihres MotW blockiert wurden: Das kann man leicht entfernen, indem man in den Dateieigenschaften unter „Allgemein" ganz unten das Häkchen „Zulassen" setzt.

Ob das Schutzkonzept für Sie aufgeht, hängt von Ihrem individuellen Nutzungsverhalten ab: Wenn Sie mit Windows hauptsächlich surfen oder arbeiten und weit verbreitete Software wie Google Chrome, Microsoft Office oder Photoshop nutzen, werden Sie von den Einschränkungen wahrscheinlich nichts mitbekommen, weil die Schutzfunktion ohnehin alles durchwinkt. Sind Sie hingegen ein Windows-Poweruser und probieren gerne brandneue oder exotische Tools aus, dann werden Sie mit Smart App Control möglicherweise nicht glücklich, weil es sich Ihnen immer mal wieder in den Weg stellt. Dasselbe gilt für Entwickler.

Grundsätzlich steht SAC nur nach einer Neuinstallation von Windows 11 Version 22H2 zur Verfügung. Wer ein Upgrade von einer vorhandenen Windows-Installation macht, muss das Betriebssystem zunächst über die eingebaute Reset-Funktion zurücksetzen – was einer Neuinstallation nahekommt.

SAC ist erstmal nicht eingeschaltet, sondern läuft still im Auswertungsmodus mit. In diesem Modus beobachtet es Ihr Nutzungsverhalten und versucht herauszufinden, ob die Schutzfunktion für Sie geeignet ist. In diesem Fall – und nur dann – schaltet es sich nach einiger Zeit automatisch ein. Das ist durchaus clever: So verhindert Microsoft einerseits, dass die Poweruser von Smart App Control gestört werden, andererseits erreicht die Schutzfunktion durch die Automatik jene Nutzer, die sich so gar nicht um die Sicherheit Ihres Systems kümmern und den Extraschutz deshalb am nötigsten haben.

Wer nicht abwarten möchte, bis Windows SAC einschaltet, kann auch selbst aktiv werden: Suchen

Halt, Stopp: Wenn Smart App Control eine Datei blockiert, gibt es keine Möglichkeit, sich darüber hinwegzusetzen.

Sie im Startmenü nach „Smart App Control" und drücken Sie die Eingabetaste. Klicken Sie anschließend auf „Aktiviert", um den Schutz scharf zu schalten. Dieser Schritt sollte allerdings wohlüberlegt sein, denn anschließend kommen Sie nicht mehr zurück in den Auswertungsmodus.

Sie können SAC zwar jederzeit durch einen Klick auf „Deaktiviert" abschalten, aber dieser Schritt ist endgültig. Danach können Sie die Schutzfunktion erst wieder aktivieren, nachdem Sie Windows zurückgesetzt haben.

Ausprobiert

Wir haben Smart App Control einem Praxistest unterzogen, um herauszufinden, wie sich die Einschränkungen im Alltag auswirken. Begonnen hat unser Test bereits mit einer Insider-Vorschauversion von Windows 11 22H2, also noch bevor SAC eine große Verbreitung hatte. Zu diesem Zeitpunkt stießen wir häufiger auf harmlose Dateien, die wir nicht ausführen durften.

Die Situation verbesserte sich, nachdem die Windows-Version fertig war und an die breite Masse verteilt wurde. Offenbar profitierte die KI in der Cloud von der größeren Nutzer- und damit auch Datenbasis. Zudem dürfte die Veröffentlichung der neuen Version so manchen Software-Entwickler zum Einsatz digitaler Signaturen motiviert haben.

Dennoch stießen wir auf manche Problemfälle: So durften wir zum Beispiel das Tool gwt.exe aus dem Bausatz des c't-Notfall-Windows partout nicht starten, weil es laut Smart App Control persönliche Daten stehlen, beschädigen oder verschlüsseln könne. Ferner könne die Datei unser „Gerät verwenden, um die Geräte anderer Personen anzugreifen".

Solange SAC aktiv war, war es schlicht nicht möglich, die Datei auszuführen. Versuchsweise signierten wir die Datei mit unserem Zertifikat, das wir eigentlich für Software nutzen, die wir selbst herausgeben. So konnten wir das Tool schließlich doch starten – offenbar hat die digitale Signatur eine höhere Gewichtung als die Einschätzung der Microsoft-Cloud.

Die Wahrscheinlichkeit, dass Sie zufällig ein solches Zertifikat herumliegen haben, ist nicht sehr groß. Sie können sich in solchen Fällen jedoch behelfen, indem Sie die blockierte Datei in einer isolierten Windows-VM oder in der Windows Sandbox der Pro-Edition [2] ausführen. So halten Sie das Hauptsystem sauber und können darauf auch weiterhin die meisten Programme mit dem Segen von SAC ausführen. Die Verdachtsfälle öffnen Sie einfach in der abgeschotteten Umgebung ohne SAC, in der sie keinen Schaden anrichten können.

Smart App Control ist eng mit dem Windows Defender Application Guard (WDAC) verwandt, einer Schutzfunktion für Windows in verwalteten Unternehmensnetzen. Anders als WDAC, das der Admin konfigurieren muss, kommt SAC mit einem festen Satz an Regeln (Policies), die automatisch aktiv sind und vor den gängigen Bedrohungen schützen sollen.

Hinter den Kulissen ist die Einführung von SAC allerdings schuld daran, dass die bisher auch in der Home-Edition inoffiziell verfügbaren Software Restriction Policies (SRP) nicht länger greifen – auch dann nicht, wenn die neue Schutzfunktion abgeschaltet ist. Über SRP war es bislang möglich, sehr detailliert vorzugeben, was auf dem System gestar-

tet werden darf und was nicht – ein effektiver Schutz vor Schädlingen aller Art. Unser Schutz-Tool Restric'tor (siehe Artikel „Mit Restric'tor Schädlinge stoppen“ auf S. 28), das die SRPs komfortabel nutzbar macht, funktioniert mit der aktuellen Version 22H2 mitunter nicht mehr verlässlich.

Ist Windows vor einem Upgrade auf Windows 11 Version 22H2 mit SRP konfiguriert, greifen die Policies in manchen Fällen auch nach dem Upgrade. Zudem kursieren Registry-Hacks, um die SRP unter Version 22H2 ans Laufen zu kriegen. Doch auch wenn die SRP aktiv bleiben, sollte man sich nicht länger blind auf sie verlassen. Es besteht die Gefahr, dass ein zukünftigtes Update oder Upgrade die Schutzfunktion heimlich wieder kaputtmacht – fatal, weil Sie das mit etwas Pech erst dann bemerken, wenn Malware den Rechner schon befallen hat.

Hopp oder top

Smart App Control ist Microsofts Versuch, die Sicherheit von Windows auf die Höhe der Zeit zu bringen, ohne es sich dabei mit den Powerusern zu verscherzen. Wenn man sich darauf einlässt, ist das Risiko einer Vireninfektion deutlich geringer. Dafür muss man sich darauf einstellen, im Zweifel eine bestimmte Datei nicht öffnen zu können, die von SAC kein grünes Licht bekommen hat.

Ob die neue Schutzfunktion für Sie geeignet ist, müssen Sie individuell entscheiden. Grundsätzlich spricht wenig dagegen, sie einfach mal einzuschalten und zu schauen, wie weit Sie damit kommen. Dieses Experiment ist jedoch nur einmal möglich: Schalten Sie es anschließend ab, bleibt es dauerhaft aus.

Auch wenn Smart App Control für Sie persönlich nicht infrage kommt, sollten Sie es im Hinterkopf behalten: Wenn Sie ein Familien-Admin sind, kann es Ihnen noch mal gute Dienste leisten. Schalten Sie es doch einfach mal ein, wenn Sie den nächsten Surf- oder Office-Rechner für die Verwandtschaft einrichten. Die Wahrscheinlichkeit, dass Ihnen dadurch so mancher durch Trojaner bedingte Notfalleinsatz erspart bleibt, ist groß. (rei) c't

Literatur

[1] Ronald Eikenberg, **E-Mails durchleuchtet**, Phishing-Mails erkennen und abwehren, c't 19/2022, S. 18

[2] Peter Siering, **Enter Sandbox**, Windows-Sandbox am Beispiel des c't-Notfall-Windows, c't 6/2022, S. 166

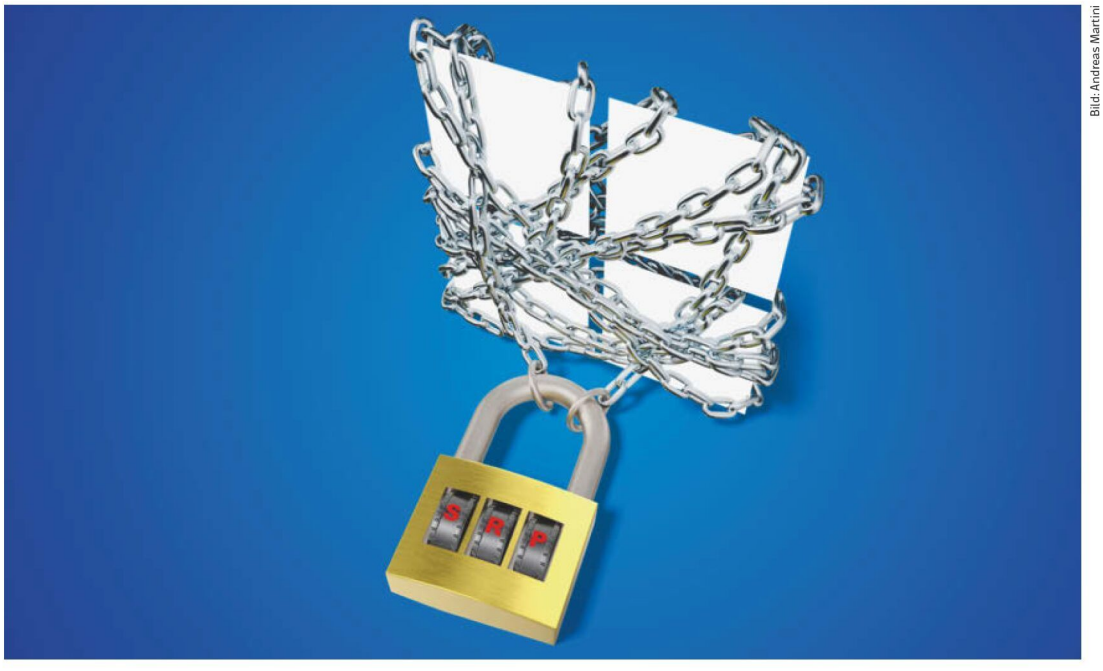


Bild: Andreas Martini

Mit Restric'tor Schädlinge stoppen

Viele Schädlinge nisten sich als ausführbare Datei in einer Windows-Installation ein. Sie können aber nicht mehr starten, wenn man per Software Restriction Policies (SRP) einschränkt, welche Dateien Windows überhaupt ausführen darf. Das ist ein wirksamer Schutz, der dem Nutzer allerdings einige Arbeit aufbürdet. Ob die lohnt, lernen Sie hier.

Von **Peter Siering**

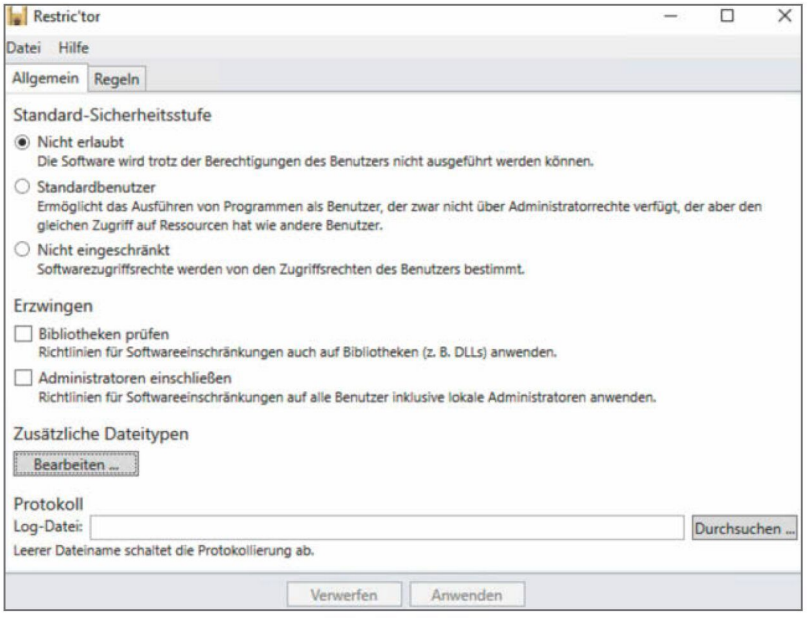
Die Software Restriction Policies (SRP) stecken in jeder Windows-Version. Sie geben dem PC Regeln vor, welche Programmdateien er überhaupt ausführen darf. Wenn man die Funktion aktiviert, blockiert sie in der von Microsoft vorgegebenen Standardeinstellung alle Programmdateien mit wenigen Ausnahmen: Programme, die in regulären vertrauenswürdigen Programmverzeichnissen liegen, die aus Sicherheitsgründen nur für Administratoren beschreibbar sind, bleiben zugelassen.

Schadsoftware, die der Nutzer als E-Mail-Anhang erhält und per versehentlichem Doppelklick aufruft, startet bei aktiven SRP erst gar nicht. Einen Schädling, der sich irgendwo in den Dokumentenverzeich-

nissen des Nutzers niedergelassen und in die Autostarts gemogelt hat, wird Windows dann ebenfalls nicht mehr ausführen. In der Praxis ist all das etwas komplizierter und die Standardeinstellung von Microsoft nicht perfekt. Das Folgende hilft, den Schutz zu perfektionieren.

Totgesagtes

Leider stehen die Software Restriction Policies (SRP) schon seit vielen Jahren auf Microsofts Abschussliste. Bislang störte das nicht, doch in der aktuellen Windows 11 Version 22H2 ist es erstmals anders: Dort streikt nach einer Neuinstallation die Schutzfunktion komplett; einzelne Benutzer berichten auch von Ausfallerscheinungen nach einem Update auf 22H2. Ob das mit voller Absicht geschah oder nur ein Seiteneffekt der Einführung von Smart App Control (siehe Artikel „Mehr Schutz dank Smart App Control“ auf S. 22) ist, kommentiert Microsoft bis heute nirgends offiziell. Die Dokumentation, die SRPs offiziell beschreibt, enthielt bis Redaktionsschluss keinen Hinweis auf eine endgültige Einstellung dieser Schutzmechanismen.



Im Datei-Menü des Restric'tors steckt die Funktion „c't-Empfehlung laden“. Nach dem Anwenden schützen die SRP die Windows-Installation wirksam vor Schadcode, der in ausführbaren Dateien daherkommt.

SRP in Aktion: Wenn nach Konfiguration der Schutzfunktion unerwünschte Programme starten, kommt diese spröde Meldung.

Auf allen älteren Windows-Versionen (8.1, 10, 11 in Version 21H2) wirken die SRPs weiterhin. Die SRPs funktionieren sogar in der Home-Edition von Windows, obwohl sie eigentlich für Firmennetze mit Active Directory erfunden wurden und über die dort nutzbaren Gruppenrichtlinien auf die Client-PCs gelangen. Da der Home-Version passendes Werkzeug zur Konfiguration fehlt, hat c't 2017 eine Software entwickelt, den Restric'tor. Er erzeugt die Registry-Einträge, die SRPs steuern. So greifen die Schutzmechanismen auch auf den eigentlich nicht vorgesehenen Windows-Editionen und sind auch auf den anderen bequem und ohne Active Directory nutzbar.

Der Restric'tor liefert obendrein Schützenhilfe beim Erstellen des Regelwerks. Er generiert zum einen einige aus unserer Sicht sinnvollen Basisregeln, damit Sie sich nicht selbst aussperren. Zum anderen hilft er dabei, die neuralgischen Punkte im Dateisystem zu finden: Die Rechte in einer Windows-Installation sind oft so gesetzt, dass Schädlingen Tür und Tor offen stehen. Sie könnten in diversen ungeschützten Verzeichnissen zusätzlichen Programmcode ablegen und starten. Mit dem Restric'tor finden Sie solche Verzeichnisse und bringen dort mit einem Klick passende Schutzmaßnahmen in Stellung.

Das Einrichten ist leider keine einmalige Aktion: Viele moderne Programme torpedieren den SRP-Ansatz, etwa weil sie in den Verzeichnissen des Benutzerprofils residieren wollen, die sich nicht sinnvoll vor Schreibzugriffen schützen lassen. Für solche Fälle sehen die SRPs spezielle Ausnahmen für einzelne Programmdateien vor, die anhand einer Prüfsumme (eines Hashes) unabhängig vom Speicherort eines Programmes das Ausführen erlauben. Auch hierbei unterstützt Sie der Restric'tor, doch den Anstoß dazu müssen Sie jeweils selbst geben.

Da sich seit der Einführung des Restric'tors die nötigen Schritte zum Einrichten im Wesentlichen nicht geändert haben, machen wir unsere vormals dazu veröffentlichten Artikel kostenlos zugänglich; Sie finden diese über ct.de/restrictor oder ct.de/wa5j.

Die folgenden Hinweise fassen das Wichtigste zusammen und gehen auf einige wenige Neuerungen ein, die die ursprünglichen Artikel noch nicht berücksichtigen. Wenn der Restric'tor für Sie neu ist, empfehlen wir nicht nur diesen Artikel zu lesen, sondern auch die kostenlos zugänglichen Artikel, besonders wenn Sie sich zum dauerhaften Einsatz entschließen.

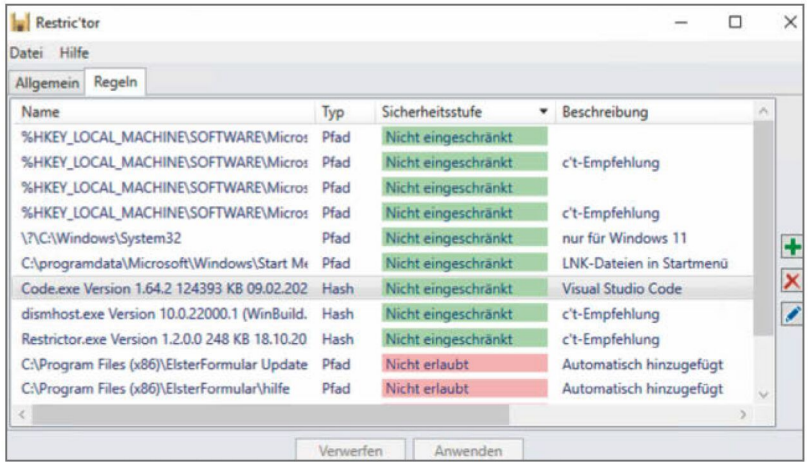
Wenn Sie das Zip-Paket mit dem Restric'tor via ct.de/wa5j heruntergeladen und entpackt haben, kopieren Sie die enthaltene EXE-Datei am besten in ein Verzeichnis „Tools" unterhalb von „C:\Programme". Das werden Sie durch eine UAC-Abfrage bestätigen müssen. Anschließend können Sie Restric'tor starten, was erneut die UAC auf den Plan ruft, denn er benötigt Administratorrechte.

Testen statt tasten

Unsere damalige Empfehlung für den Einstieg bestand darin, zunächst nur das Protokoll einzuschalten, um zu einer Liste der aufgerufenen Programme zu kommen. Aus heutiger Sicht raten wir dazu, direkt loszulegen: Wählen Sie im Menü „Datei" den Punkt „c't-Empfehlung laden" aus, betätigen Sie den Knopf „Anwenden" und starten Sie Windows neu (nicht immer wirken Änderungen an den SRPs sofort, gehen Sie auf Nummer sicher). Anschließend wird Ihr PC nur noch Programme ausführen, die in den einschlägigen Ordnern einer Windows-Installation liegen, also in C:\Windows, C:\Programme und C:\Programme (x86).

Wenn Sie die SRP-Blockade für ein Programm übersteuern wollen, können Sie es mit der rechten Maustaste im Menü „Als Administrator ausführen". Den Restric'tor können Sie ohne diesen Kniff aufrufen, er trägt für sich selbst eine Ausnahmeregel mit einem Hash ein, sodass er auch aus jedem beliebigen Verzeichnis noch startet. Anschließend sollten Sie testen, ob alle für Sie essenziellen Programme noch starten. Meist zeigt SRP eine Fehlermeldung, wenn es eingreift, aber nicht immer.

Hilfreich ist es deshalb, die Ereignisanzeige zu starten und dort eine benutzerdefinierte Ansicht einzurichten, die alle Meldungen aus der Quelle „SoftwareRestrictionPolicies" im Anwendungsprotokoll anzeigt. Nur dort finden Sie wirklich heraus, wo Windows wegen der für die SRP hinterlegten Einstellungen einschreitet. Längst nicht jede Intervention wirft überhaupt die typische Fehlermeldung aus, mit der Windows klarmacht, dass ein Programm blockiert ist.



Für dauerhaften Einsatz sollten Sie das Regelwerk verfeinern. Wir empfehlen über die als „nicht eingeschränkt" markierten Regeln hinaus, die Windows-Verzeichnisse auf beschreibbare Ordner zu überprüfen und als „nicht erlaubt" zu ergänzen.

Nach einer Weile werden Sie dort allerhand Warnungen finden, weil die regelmäßig automatisch gestarteten Update-Helfer von Programmen scheitern. Dazu kommt es, wenn sie nicht in den einschlägigen Ordern für Programme liegen, sondern in den Verzeichnissen des Benutzerprofils (in der Regel in AppData). Dort führt Windows bei aktiven SRPs sicherheitshalber keine Programme aus: Die Updates finden also nicht statt. Wenn Programme keine Option bieten, um sie in die einschlägigen Verzeichnisse zu installieren, bleibt als Behelf nur eines: Starten Sie das Programm dann und wann als Administrator, damit sein Updater zum Zuge kommen kann.

Tun und lassen

Apropos Installation: Software, die in einer MSI-Datei daherkommt, startet unter Aufsicht der SRPs nicht per Doppelklick den Installer: Sie müssen sich zunächst als Administrator anmelden, etwa in einer Eingabeaufforderung oder im Windows-Terminal, und dort den Windows-Installer aufrufen, indem Sie den Dateinamen der MSI-Datei eingeben; zuvor müssen Sie gegebenenfalls ins Verzeichnis wechseln, in dem die Datei liegt. Ein Eintrag im Kontextmenü für MSI-Dateien in der Art „Als Administrator installieren" hielt Microsoft nicht für nötig.

In den Artikeln zum Restric'tor 2017 hatten wir noch behauptet, dass LNK-Dateien, also die Verknüp-

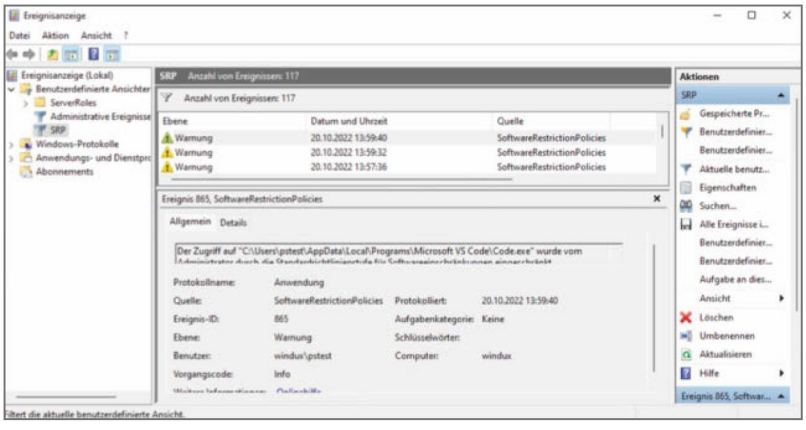
fungen im Windows-Explorer ungefährlich seien. Das stimmt so längst nicht mehr: Malware-Autoren haben sie als Weg entdeckt, um Schadcode einzuschleusen. Insofern empfiehlt es sich heutzutage, dem Vorschlag Microsofts zu folgen und LNK-Dateien über den Restric'tor als Typ für ausführbaren Code auf die SRP-Blacklist zu setzen.

Wenn Sie das tun, sollten Sie aber unbedingt auch eine Pfad-Regel für das Verzeichnis vorsehen, aus dem Windows einen Teil der systemweit, also für alle Nutzer sichtbaren Einträge des Startmenüs zusammenpuzzelt. Tragen Sie dort mit der Sicherheitsstufe „Nicht eingeschränkt" den folgenden Pfad ein: „C:\ProgramData\Microsoft\Windows\Start Menu\". Nun sind die meisten per Verknüpfung realisierten Einträge im Startmenü auch benutzbar. Das ist unbedenklich, weil das Verzeichnis nur für Administratoren beschreibbar ist.

Seit der Veröffentlichung des Restric'tors hat Microsoft an vielen Stellen in Windows gedreht. Dabei ist bezogen auf SRPs nur ein uns bekanntes Detail kaputtgegangen: Unter Windows 11 (bis Version 21H2) öffnet sich nach dem ersten Aktivieren der SRPs mit der c't-Empfehlung die Einstellungsseite für „Viren & Bedrohungsschutz" nicht mehr. Wenn Sie jedoch eine spezielle Pfad-Regel eintragen, zeigt auch Windows 11 diese Einstellungen wieder an: Fügen Sie dazu den Pfad „\?\C:\Windows\System32\" im Restric'tor über den Reiter „Regeln" als „Nicht eingeschränkt" hinzu.

Kostenlos zugängliche, vertiefende Artikel zu Restric'tor und SRP

ct.de/wa5j



Ein Filter in der Windows-Ereignisanzeige, der die Events der Software Restriction Policy filtert, zeigt, wo Sie eventuell mit Regeln im Restric'tor nachsteuern müssen.

Folgende Funktionen des Restric'tors empfehlen sich tendenziell nicht: Wenn „Bibliotheken prüfen" gesetzt ist, würden die SRPs sich nicht nur um direkt ausführbare Dateien (EXE, BAT, CMD …) kümmern, sondern auch um DLLs. Das erhöht die Sicherheit zwar erheblich, verlangsamt Windows aber unter Umständen, verursacht bei einigen Programmen Update-Schluckauf und ist so nur für Paranoiker interessant. Geradezu gefährlich ist „Administratoren einschließen" – wenn es dumm läuft, sperren Sie sich damit aus Ihrem PC aus und können sich nur über holprige Umwege wieder Zutritt verschaffen (die alten via ct.de/wa5j kostenlos erhältlichen Artikel vertiefen die nötigen Maßnahmen).

Rück- und Ausblick

SRPs tun sich schwer mit der neuesten Softwaremode, sprich Programmen, die Browsertechnik als Basis nutzen und sich in den Benutzerprofilverzeichnissen installieren wollen, also unter C:\Users in den AppData-Verzeichnissen. Die Schutztechnik stammt eben aus einer anderen Zeit, in der Softwareentwickler Anforderungen bezüglich der Programmverzeichnisse noch ernster nahmen. Insofern eignen sich die SRPs vor allem für PCs, die mit Software bestückt werden, die sich in den eigentlich vorgesehenen Verzeichnissen daheim fühlt.

Je weniger der Nutzer installiert, desto besser dichtet der Mechanismus ab. Für betreute Benutzer, die ohnehin selbst keine Software einrichten, ist er ideal; mit jeder Software klappt das leider nicht, weil unter Umständen die Updates versiegen. Gegen alle Gefahren schützt er nicht: Code, der über Sicherheitslücken in Viewern mit den Daten auf den PC gelangt, können die SRPs nicht erkennen. Das heißt auch, dass es weiterhin wichtig bleibt, regelmäßig Updates zu installieren. Wer viel Software mal eben ausprobiert, selbst entwickelt oder Skripte schreibt, wird mit den SRP eher selten glücklich.

Dass Microsoft in der neuesten Windows 11 Version 22H2 mit der Einführung von Smart App Control bei Neuinstallationen die SRP-Schutzfunktion endgültig ruiniert hat, bestätigt die verbreitete These, dass die Home- und Pro-Edition von Windows nur zweitklassigen Sicherheits-Support erhalten. Unterm Strich ist das sehr ärgerlich, weil damit eine alternativlose Schutzfunktion fällt – all die neuen zauberhaften Techniken wie Device Guard, AppLocker & Co. setzen schon die Enterprise-Edition voraus, und das moderne Smart App Control erlaubt dem Nutzer keinerlei Eingriffe. (ps) c't

Bild: Albert Hulm

Sandkasten für Windows-Programme

Unter Windows haben Programme viele Befugnisse – und nutzen das nicht selten schamlos aus. Sandboxie-Plus schränkt die Zugriffsrechte aufs Nötigste ein, um Kryptotrojaner zu stoppen und Datenmüll zu verhindern. Im Test konnte Sandboxie sogar ungewollte Zugriffe auf den Arbeitsspeicher verhindern.

Von **Ronald Eikenberg**

Schädlinge haben unter Windows leichtes Spiel, weil sie alles dürfen, was der angemeldete Benutzer darf: Dateien lesen und schreiben, auf den Arbeitsspeicher zugreifen, Daten ins Internet schicken und Vieles mehr. Ein modernes Sandbox- und Berechtigungskonzept, wie man es von Smartphone-Betriebssystemen kennt, sucht man vergeblich.

Ein Virenschutzprogramm wie der Windows Defender hilft nur bedingt, da es prinzipbedingt nicht jeden gefährlichen Code erkennen kann. In einer Sandbox kann solcher Code jedoch keinen Schaden anrichten. Auch wenn Software den Rechner nicht gleich verseucht oder Daten abgreift, hat das Ausführen häufig lästige Folgen: Viele Programme hinterlassen Datenmüll auf dem Rechner, den ihre Deinstallationsroutine nicht beseitigt. Laufen sie in einer Sandbox, verschwindet der Müll nach dem Beenden automatisch.

Mit Sandboxie-Plus kann man den Aktionsradius von Prozessen aufs Nötigste reduzieren. Es führt sie in einer transparenten Sandbox-Umgebung mit ein-

geschränkten Zugriffsrechten aus. Was erlaubt ist, stellt man präzise ein. Die Prozesse bekommen davon nichts mit: Sie können weiterhin auf die Platte schreiben, ihre Dateien landen jedoch nicht am eigentlichen Bestimmungsort, sondern fein säuberlich davon getrennt im Sandbox-Ordner. Beim Lesezugriff reicht Sandboxie-Plus die Dateien von dort einfach weiter.

Eingeschränkte Zugriffsrechte

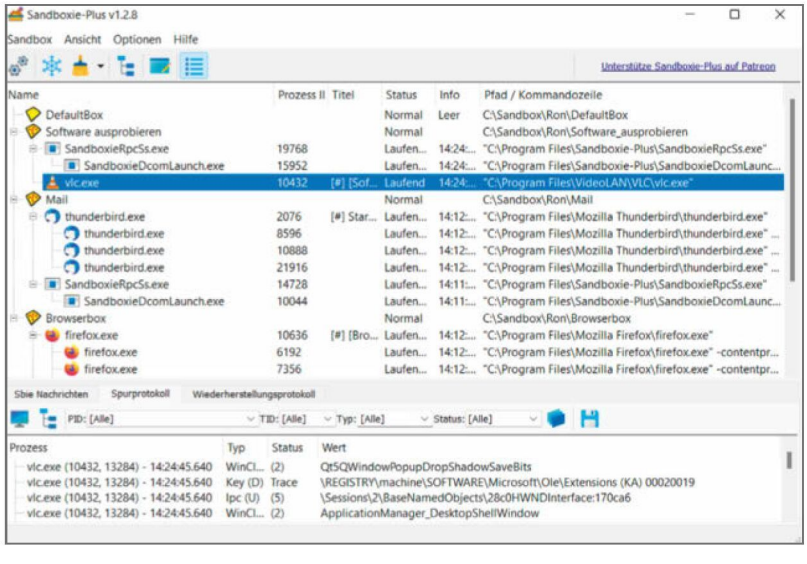
Hinter den Kulissen startet Sandboxie-Plus die Programme mit einem stark eingeschränkten Windows-Benutzer, der eigentlich keine ausreichenden Zugriffsrechte für die Nutzung hat. Damit die isolierten Programme trotzdem funktionieren, lenkt Sandboxie-Plus Windows-Standardfunktionen der Systembibliothek ntdll.dll durch Hooking zu seinem Treiber SbieDrv.sys um, der den Zugriff auf Ressourcen ermöglicht, die für den eingeschränkten Nutzer eigentlich unerreichbar sind. Der Treiber stellt dabei sicher, dass nur Zugriffe innerhalb der vom Anwender definierten Sandbox-Bedingungen erlaubt sind. So kann Sandboxie-Plus beispielsweise das Schreiben einer Datei abfangen und in einen anderen Ordner umlenken oder verhindern, dass der isolierte Prozess den Arbeitsspeicher anderer Prozesse ausliest.

Bei Sandboxie-Plus handelt es sich um eine erweiterte Version der Sandbox-Software Sandboxie [1], die bereits im Jahr 2004 als Schutzschicht für den Internet Explorer das Licht der Welt erblickt hat. Seitdem hat sich viel getan: Das Tool kann seit Langem auch andere Prozesse als den Browser absichern und es gab zwei Besitzerwechsel. Der letzte Besitzer, die britische Security-Firma Sophos, hat Sandboxie im Jahr 2020 als Open Source freigegeben und unter die GPLv3 gestellt. Dies verschaffte dem Programm neuen Auftrieb und legte den Grundstein für eine Weiterentwicklung durch die Community.

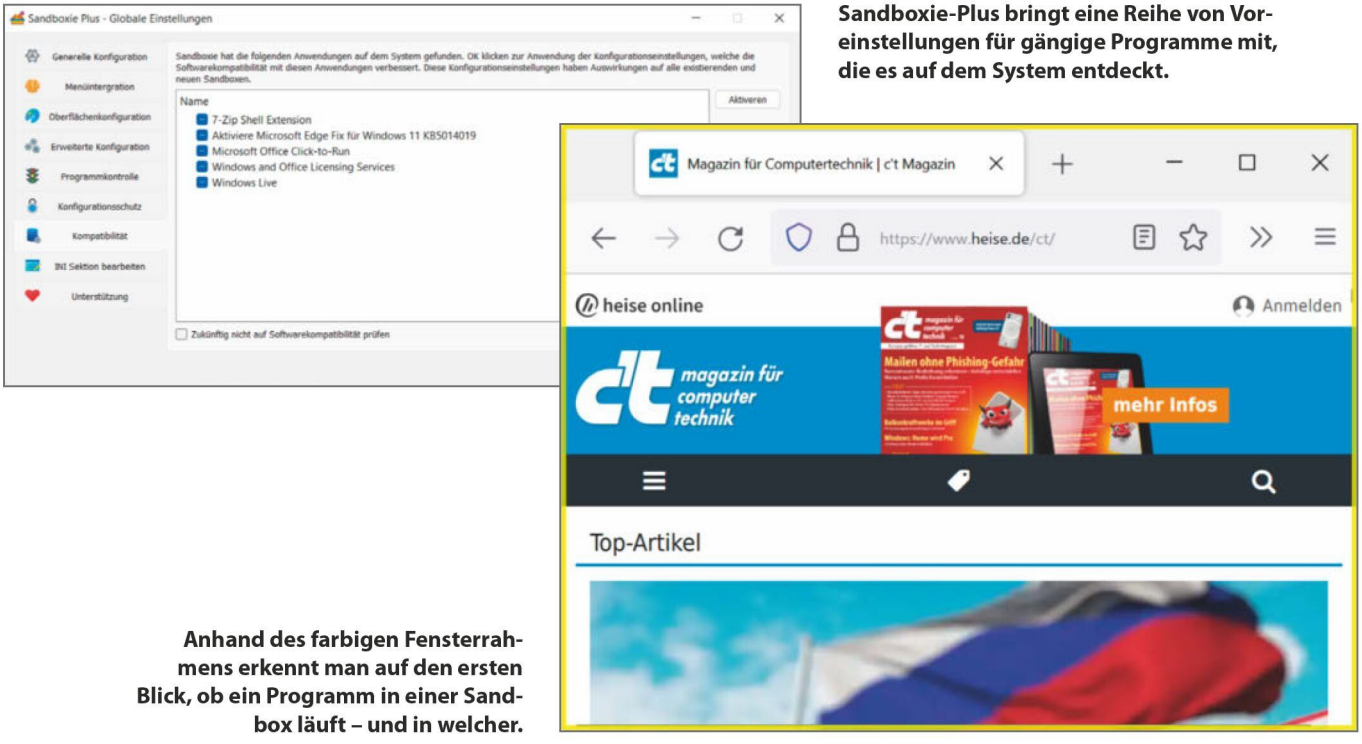
Der Entwickler David Xanatos nutzt das GPL-Projekt als Unterbau für sein Sandboxie-Plus, das eine moderne Qt-Oberfläche namens SandMan und viele neue Funktionen mitbringt. Während der Sandboxie-Kern weiterhin unter GPLv3 steht, handelt es sich bei der neuen Verwaltungsoberfläche um eine kommerzielle Software, deren Code jedoch bei GitHub einsehbar ist (siehe ct.de/wqz1). Die meisten der neuen Funktionen sind für private Zwecke kostenlos nutzbar, für die anderen Funktionen benötigt man eine Lizenz. Privatnutzer zahlen dafür ab 20 Euro im Jahr, eine Lizenz für den Einsatz in Unternehmen kostet 40 Euro pro Jahr und Rechner. Alternativ kann man den Entwickler über Patreon unterstützen (ab 1 Euro/Monat), um die Funktionen freizuschalten.

Frischer Sand

Sandboxie-Plus ist mit wenigen Klicks installiert. Nach dem Einrichten schlägt es für verbreitete An-



Über die neu entwickelte Qt-Oberfläche von Sandboxie-Plus hat man die Prozesse in den abgeschotteten Umgebungen gut im Griff.



Sandboxie-Plus bringt eine Reihe von Voreinstellungen für gängige Programme mit, die es auf dem System entdeckt.

Anhand des farbigen Fensterrahmens erkennt man auf den ersten Blick, ob ein Programm in einer Sandbox läuft – und in welcher.

wendungen wie Microsoft Office, die es auf dem System entdeckt, vorgefertigte Konfigurationsprofile vor. Das soll die Kompatibilität verbessern und bewirken, dass die Programme problemlos in den geschützten Umgebungen starten.

Wie schon früher bei Sandboxie gibts zum Start eine Default-Sandbox für die ersten Schritte. In dieser kann man bereits die ersten Programme starten, doch dazu gleich mehr. Über „Sandbox/Neue Box erstellen“ lassen sich leicht beliebig viele weitere Sandboxen für jeden Zweck anlegen. Diese sind erst einmal leer und belegen keinen Platz auf der Platte. Erst wenn ein Prozess gestartet wird und Änderungen an Dateisystem oder Registry vornimmt, wird ein Ordner für die Box angelegt. Standardmäßig befinden sich die Sandbox-Ordner unter C:\Sandbox\Benutzername\Sandboxname.

Wirft man mit dem Windows Explorer einen Blick hinein, stößt man auf einen Ordner namens drive mit Unterordnern für die einzelnen Laufwerke und einen Ordner users für das Benutzerverzeichnis. Zudem gibt es eine Datei namens RegHive mit der Registry der Sandbox. Über die Sandboxie-Plus-Oberfläche sind diese Daten auch durch einen Rechtsklick auf die Box und dann auf „Boxinhalt anzeigen“ erreichbar. Dort kann man den Registrierungseditor von Windows auch direkt mit der Box-Registry öffnen.

Beim Erstellen einer Box bietet Sandboxie-Plus neben dem Standardprofil noch fünf weitere mit erhöhter oder reduzierter Sicherheit an. Diese aktivieren jedoch kostenpflichtige Funktionen, die ohne Freischaltung nur zeitlich eingeschränkt nutzbar sind. Aktiviert man sie im Gratismodus für eine Sandbox, werden die in der Box gestarteten Prozesse jeweils nach fünf Minuten beendet. Das reicht aus, um die Funktionen zu testen und gelegentlich mal einen verdächtigten Prozess damit zu starten. Wer kein Geld ausgeben möchte, kommt aber auch mit den umfangreichen Gratisfunktionen sehr weit, auf die sich dieser Test beschränkt.

Nach einem Doppelklick auf eine Sandbox öffnen sich die umfangreichen Einstellungen, über die man detailliert festlegt, was die Programme innerhalb der Box dürfen und was nicht. Premiumfunktionen sind hier mit einem kleinen Siegel gekennzeichnet.

Programme isoliert starten

Um ein Programm in der Sandbox zu starten, klickt man beispielsweise im Sandbox-Manager mit rechts auf eine Box und wählt „Starten“. Anschließend bietet Sandboxie-Plus die Programme aus dem Startmenü der Box, die Windows-Eingabeaufforderung und Abkürzungen zu Standardprogrammen wie Browser und Mailclient zur Auswahl an.

Nach dem Start erscheinen die isolierten Prozesse im Sandbox-Manager in einer Baumstruktur unterhalb der Sandbox. Über einen Rechtsklick auf einen dort aufgeführten Prozess beendet man ihn unter anderem oder legt eine Verknüpfung auf dem Hauptsystem an, um ihn beim nächsten Mal bequem zu starten.

Wir konnten die meisten Anwendungen problemlos in Sandboxen starten und nutzen. Merkliche Geschwindigkeitseinbußen konnten wir dabei nicht feststellen. Für Ausnahmefälle, für die man spezielle Zugriffsrechte freigeben muss, findet man häufig Konfigurationstipps im Netz.

Die Fenster der abgeschotteten Programme sind durch einen gelben Rahmen gekennzeichnet, zudem fügt Sandboxie-Plus die Markierung [#] in den Fenstertitel ein. Auf Wunsch erscheint hier auch der Name der dazugehörigen Sandbox, darüber hinaus ist die Farbe des Rahmens wählbar. So ist auf den ersten Blick erkennbar, in welcher Umgebung ein Programm läuft – ähnlich wie bei dem hochsicheren Betriebssystem Qubes OS [2].

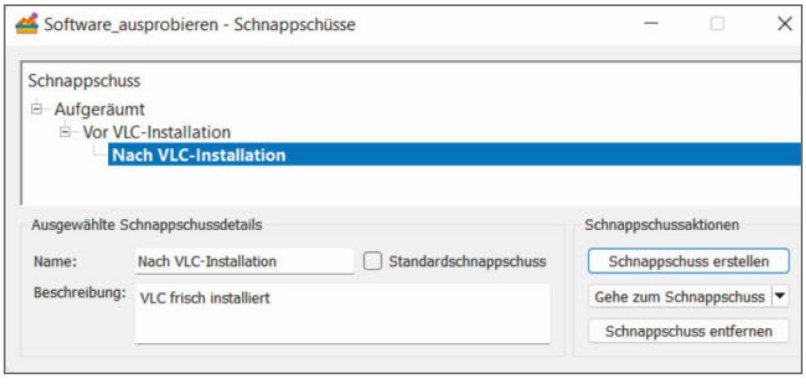
Nach dem Start in der Standardbox ändert sich für das Programm erst einmal wenig, da es weiterhin auf die meisten Ressourcen zugreifen kann. Spannend wird es, wenn das Programm aufs System schreibt: Sandboxie leitet die Schreibzugriffe transparent in den Sandbox-Ordner um. Neue Dateien und Registry-Einträge werden also nicht wie gewohnt im System verstreut, sondern sind fein säuberlich davon getrennt. Das hat den positiven Nebeneffekt, dass man detailliert nachvollziehen kann, wo sich ein Programm im System breit macht – oder besser gesagt: breit gemacht hätte.

Wird eine bereits vorhandene Datei des Hauptsystems geändert und gespeichert, wird nicht das Original überschrieben, sondern eine Kopie im Sandbox-Ordner erzeugt. Der isolierte Prozess bekommt davon nichts mit: Öffnet er die Datei wieder, reicht Sandboxie-Plus die Kopie an ihn weiter. Würde ein Kryptotrojaner auf dem Rechner wüten und versuchen, die Dateien seines Opfers mit verschlüsselten Kopien zu überschreiben, könnte er in der Standard-Sandbox zwar die Dateien lesen, aber nicht das Original überschreiben oder löschen. Die verschlüsselten Varianten der Dateien würden einfach im Sandbox-Ordner aufschlagen.

Sandboxie überwacht innerhalb der abgeschotteten Umgebung ein paar Ordner wie Downloads und Dokumente. Sobald es dort neue Dateien entdeckt, bietet es an, diese über die etwas missverständlich benannte Dateiwiederherstellung aus der Sandbox aufs Hauptsystem zu kopieren. Diese recht aufdringliche Funktion ist in den Sandbox-Einstellungen abstellbar.

Auf Wunsch leert Sandboxie-Plus die Boxinhalte automatisch, wenn keine Prozesse mehr innerhalb der Box laufen. So kann man immer wieder in einer sauberen Umgebung starten. Nützlich ist auch der Schnappschussmanager, der sich unter „Sandboxwerkzeuge“ befindet. Er konserviert den aktuellen Zustand der Box, indem er den Sandbox-Ordner klont. Das klappte im Test flott und reibungslos.

Auch zur Installation neuer Programme sind die Sandboxen bestens geeignet. Führt man den Installer direkt in einer Sandbox aus, zum Beispiel, indem man im Dateiexplorer von Windows mit rechts draufklickt und „Open Sandboxed“ wählt, landen die Programmdateien im Unterordner „drive\c\Program Files\“ des Sandbox-Ordners. Falls die installierte Software doch nicht den Vorstellungen entspricht, löscht man die Sandbox einfach oder beseitigt die Änderungen mit dem Eintrag „Inhalte löschen“ im Kontextmenü – ganz ohne Deinstallation und inklusiver etwaiger Dateileichen, die das Deinstallationsprogramm übersehen könnte. Vorher



Der Schnappschussmanager konserviert den aktuellen Zustand der Sandboxes und erlaubt die spätere Rückkehr dorthin.

sollte man allerdings alle Dateien, die man innerhalb der Sandbox angelegt hat und behalten möchte, aus der Sandbox aufs Hauptsystem übertragen haben (zum Beispiel über die Dateiwiederherstellung).

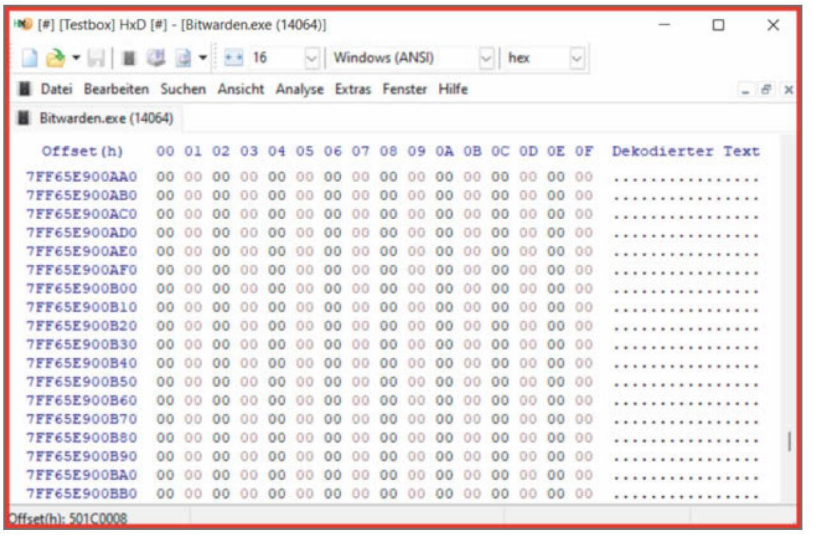
Speicherschutz

Standardmäßig schirmt Sandboxie-Plus auch den Arbeitsspeicher ab: Ein Prozess innerhalb einer Sandbox kann nicht auf die Speicherbereiche von Prozessen zugreifen, die in einer anderen Sandbox oder direkt auf dem Hauptsystem laufen. Das konnten wir mit dem Hexeditor HxD verifizieren. Bei Zugriffsversuchen aus der Sandbox heraus bekam das Programm nur Nullen geliefert. Das ist ein erheblicher Sicherheitsgewinn, denn eine Schadsoftware kann sich normalerweise beliebig im Speicher umsehen und findet dort auch Klartext-Passwörter, die ein Passwort-Manager oder Browser abgelegt hat. Läuft der Schädling in einer eigenen Sandbox, ist das nicht länger möglich.

Für noch mehr Sicherheit kann man über die umfangreichen Einstellmöglichkeiten der Sandboxen sorgen. Unter „Ressourcenzugriff“ etwa lässt sich gezielt der Lesezugriff auf bestimmte Ordner abstellen. Auch der Netzwerkzugriff ist über die Einstellungen regelbar – Programme, die nichts zwangsläufig eine Internetverbindung benötigen, sollten auch keinen Zugriff darauf haben.

Wer sich ein wenig mit den Windows-Interna auskennt und sich in Sandboxie-Plus hineinfuchst, kann die Sicherheit der Sandbox über die Einstellungen noch weiter optimieren – etwa durch das Blockieren des Lesezugriffs auf die Zwischenablage oder weitere Zugriffseinschränkungen.

Anzumerken ist, dass es sich bei Sandboxie-Plus nicht um eine echte Virtualisierung handelt. Anders als bei einer virtuellen Maschine, die etwa mit Hyper-V oder VirtualBox ausgeführt wird, isoliert Sandboxie die Prozesse nicht vollständig vom Hauptsystem. Zudem können Prozesse leicht herausfinden, dass sie in einer Sandboxie-Umgebung ausgeführt werden und sich in diesem Fall unauffällig verhalten – in der Hoffnung, dass sie dann außerhalb des Sandkastens spielen dürfen. Zur Analyse hartnäckiger Schädlinge ist Sandboxie-Plus somit ungeeignet. Im Vergleich zu virtuellen Maschine hat Sandboxie-Plus aber auch einen entscheidenden Vorteil: Der Ressourcenverbrauch ist äußerst gering, es läuft auch auf Systemen mit wenig Speicher rund.



Prozesse in der Sandbox, hier der Hexeditor HxD, können nicht auf den Speicher von Programmen zugreifen, die außerhalb der Sandbox laufen. In diesem Beispiel hat Sandboxie-Plus den Zugriff auf den Speicher eines Passwortmanagers erfolgreich verhindert.

Fazit

Sandboxie-Plus holt den Klassiker Sandboxie in die Neuzeit und ergänzt ihn durch eine moderne Oberfläche und clevere Funktionen. Schon mit der Gratisversion schränkt man die Datenzugriffe von Programmen weitreichend ein. Das dämmt zum Beispiel den Schaden ein, wenn doch mal ein Trojaner durch alle Kontrollen schlüpft. Der Schutzwall ist zwar nicht ganz so robust wie beim Einsatz einer virtuellen Maschine, dafür ist Sandboxie durch den geringeren Ressourcenverbrauch alltagstauglicher. Auch zum Ausprobieren von Software ist das Tool eine gute Wahl, da es danach gründlich aufräumt und Datenspuren löscht, die der Uninstaller liegen lässt. (rei) c't

Sandboxie-Plus

Sandbox-Programm	
Hersteller, URL	David Xanatos, sandboxie-plus.com
Systemanf.	Windows 7 oder höher
Preis	kostenlos für nicht-kommerzielle Nutzung

Literatur

[1] Gerald Himmelein, **Auf der Isolierstation**, Sandboxie schottet Anwendungen vom Betriebssystem ab, c't 20/2013, Seite 168

[2] Knut von Walter, **Von Snowden empfohlen**, Das sicherheitsorientierte Betriebssystem Qubes OS im Test, c't 11/2022, Seite 94

Download von Sandboxie-Plus

ct.de/wqz1

Es gibt 10 Arten von Menschen.

iX-Leser und die anderen.

3 × als Heft

Jetzt Mini-Abo testen:
3 Hefte + Bluetooth-Tastatur
nur 19,35 €

www.iX.de/testen

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

Am 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 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 harmoniert 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 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.

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

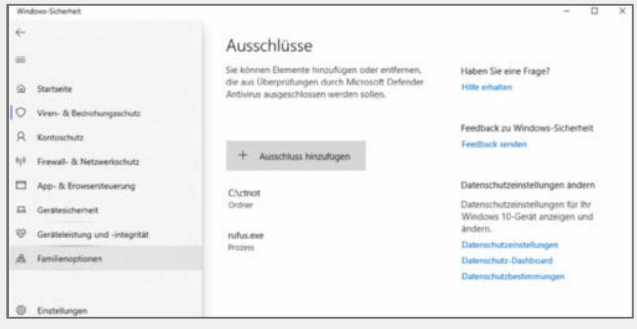
Hintergründe zum Bausatz

Seit jeher bedauern wir, dass wir ein auf Windows aufbauendes Notfallsystem nur als Bausatz bereitstellen können. Leider lizenziert Microsoft das als Grundlage verwendete Windows PE (Preinstallation Environment) nicht. PE als Minimalfassung von Windows hilft unter anderem bei jeder Windows-Installation. Es dient auch als Basis für die Wiederherstellungsumgebung (auch Windows RE genannt), die in einer separaten Partition auf einem PC schlummert und die Windows automatisch im Reparaturfall startet.

Rund um PE sind verschiedene Projekte für Bausätze mit angereichertem Werkzeugsatz entstanden. Die Projekte tun im Grunde alle das Gleiche: Sie bohren Microsofts PE-Umgebung auf. Dazu verwenden sie zumeist dieselbe Skriptsprache, die auf eine Software namens WinBuilder zurückgeht. Wir schauen uns diese Projekte intensiv an und nehmen das aus unserer Sicht attraktivste als Basis für unser Notfall-Windows. Die Skripte lassen wir schon länger nicht mehr von WinBuilder ausführen, sondern von der Open-Source-Software PEBakery.

Erste Etappe: Bauen vorbereiten

- Lesen Sie den Artikel komplett, um die Voraussetzungen zu kennen und für eventuelle Probleme gewappnet zu sein.
- Laden Sie eine ISO-Datei mit einer 64-Bit-Evaluierungsversion von Windows 10 oder 11 herunter (zwischen 3 und 5 GByte). Auf der Projektseite (siehe ct.de/ww88) finden Sie direkte Download-Links.
- Erstellen Sie ein Verzeichnis, in dem der Bauvorgang vonstattengehen soll, zum Beispiel C:\ctnot; nutzen Sie nur Buchstaben im Namen und vermeiden Sie lange, verschachtelte Pfade.
- Definieren Sie in Ihrem Virenscanner eine Ausnahme für dieses Verzeichnis. Windows Defender beispielsweise nennt die „Ausschlüsse“; auf Nachfrage richtet der Bausatz solche für den Defender selbständig ein.
- Laden Sie via ct.de/ww88 das Zip-Archiv mit dem Bausatz (ungefähr 200 MByte) in dieses Verzeichnis herunter.
- Entpacken Sie erst jetzt das Zip-Archiv in diesem Verzeichnis. Ohne Ausnahme würde Ihre Antivirus-Software womöglich einzelne Dateien „wegfressen“ und der Bau würde misslingen.
- Binden Sie per Doppelklick die ISO-Datei als virtuelles Laufwerk ein. Es erhält einen Buchstaben, etwa F:.



Virenschutz- und andere Sicherheitssoftware müssen Sie zügeln, damit die nicht in den Bauprozess eingreift und Dateien wegfischt – Programme, die ein Notfallsystem sinnvoll ergänzen, können in anderem Kontext eine Gefahr darstellen.

längst überholte Windows 7 haben wir uns überhaupt nicht mehr eingelassen.

Für die herunterzuladenden Dateien und als Arbeitsbereich sollten vor Beginn rund 20 GByte Speicherplatz verfügbar sein. Der Bauplatz sollte auf jeden Fall auf einer SSD liegen. 8 GByte RAM genügen zum Bauen. Der USB-Stick, auf dem das fertige Notfallsystem landen wird, sollte mindestens 8 GByte Platz bieten. Sie tun sich einen Gefallen, den Stick eines renommierten Flash-Speicherherstellers zu nutzen – Baumarktgurken kosten nur Nerven und Zeit.

Geändertes

Für die Neuauflage haben wir entschieden, dass der Bausatz ausschließlich 64-Bit-Notfallsysteme herstellt: Quelldateien einer x86-Windows-Version verarbeitet er nicht. Meist kein Problem: Ein 64-Bit-Notfallsystem kann 32-Bit-Installationen behandeln, von einer Einschränkung abgesehen (mehr dazu im Artikel „Probleme lösen mit dem Notfall-Windows“ auf Seite 64). Als Bausystem darf weiterhin eine 32-Bit-Installation dienen; allerdings nutzen die maximal 4 GByte RAM und so geht denen beim Bauen schnell der Speicher aus – das haben wir bei exzessiven Experimenten und mehreren Starts des Build-Prozesses erlebt.

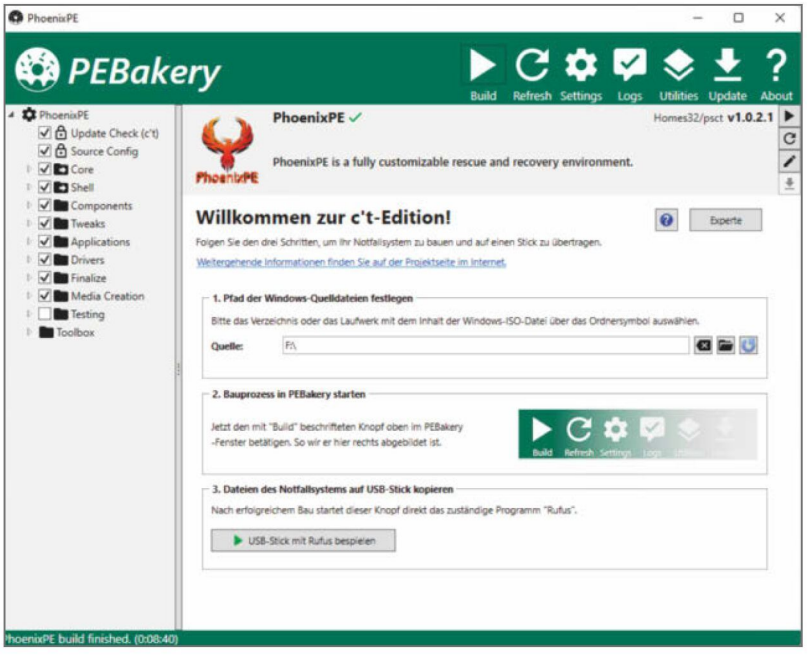
Sie sollten den Bausatz in ein Verzeichnis entpacken, das am besten im Wurzelverzeichnis eines Laufwerks liegt, also zum Beispiel C:\ctnot. Ein Verzeichnis auf dem Desktop stellt eine gefährliche Wahl dar, weil ein dort platzierter Ordner ctnot beispielsweise letztlich in C:\Users\Eugen-Ergün Mustermann\Desktop\ctnot landet und die Skripte des Bausatzes mit Bindestrichen, Leerzeichen und vielen weiteren Sonderzeichen ihre liebe Not haben (und vermutlich nur einen Teil der Varianten abfangen).

Ihrer Virenschutzsoftware müssen Sie abgewöhnen, dieses Verzeichnis zu schützen. Für den Windows-Defender rufen Sie „Windows-Sicherheit“ auf und klicken sich dann über „Viren- & Bedrohungs-

schutz“ durch zu „Einstellungen verwalten“. Rollen Sie dort hinunter bis „Ausschlüsse“ und klicken Sie auf „Ausschlüsse hinzufügen oder entfernen“. Mit „Ausschluss hinzufügen“ fügen Sie den Ordner C:\ctnot und dann den Prozess „rufus.exe“ hinzu (die Texteingabe genügt hier, einen Pfad müssen Sie nicht angeben). Fertig. Falls Sie das versäumt haben, fragt der Bausatz im Fall des Defenders nach, ob er die Ausschlüsse einrichten soll.

Der Aufwand ist nötig, weil Programme, die der Bausatz selbst einsetzt, und einige der Programme, die er verarbeitet, für Sicherheitssoftware eine latente Gefahr darstellen. Mit der Ausnahmeregel funken Defender und seine Artgenossen nicht mehr dazwischen. Was wir aus Leseranfragen gelernt haben: Nicht jede Sicherheitssoftware hält sich an festgelegte Ausnahmen. Mitunter hilft nur, sie kurzzeitig ganz abzuschalten.

Mit dem angelegten Bauplatz C:\ctnot, dorthin entpacktem ctnotwin23.zip-Archiv und der Ausnahmeregel für die Sicherheitssoftware müssen Sie noch die Windows-Quelldateien verfügbar machen. Doppelklicken Sie die heruntergeladene ISO-Datei der Evaluierungsversion, dann wird Windows diese als neues virtuelles Laufwerk einbinden. Wenn sich andere Software ISO-Dateien greift, sollte ein Rechtsklick auf die Datei und die Auswahl von „Bereitstellen“ das Gleiche erledigen.



Drei über die Willkommensseite anstoßbare Schritte genügen, um den Bauvorgang zu starten und einen Stick mit dem fertigen Bausatz zu bespielen.

Loslegen

Im Ordner C:\ctnot finden Sie die Datei PEBakeryLauncher.exe. Starten Sie diese per Doppelklick. Die Benutzerkontensteuerung wird nachfragen, ob Sie das Programm starten wollen – es benötigt Admin-Rechte, stimmen Sie bei einem regulären Windows-Konto also der UAC-Nachfrage bitte zu. Nach einer kurzen Gedenkzeit erscheint die Oberfläche von PEBakery. Das ist das Programm, das die Baupläne in Handlungen umsetzt.

Es kann sein, dass PEBakeryLauncher zunächst empfiehlt, eine aktuelle Version der Windows Desktop Runtime einzurichten. Folgen Sie der Empfehlung, ohne geht es nicht. Auf ganz frisch installierten PCs könnten auch die Visual C++-Bibliotheken fehlen (PEBakery scheitert dann an einer fehlenden „zlibwapi.dll“). Sie finden das Installationspaket für die Visual C++-Bibliotheken ebenfalls unter ct.de/ww88.

Auf der Willkommensseite von PEBakery werden Sie gebeten, den Pfad der Windows-Quelldateien festzulegen. Das kann ein Laufwerk oder ein Verzeichnis sein, wo die Originaldateien des Windows-Datenträgers zu finden sind, also die Inhalte der heruntergeladenen ISO-Datei und nicht die ISO-Datei selbst. Erscheint der gewählte Pfad in dem Feld hinter „Quelle“, eignen sich die Dateien für den Bausatz. Ungeeignetes Ausgangsmaterial erkennen die Skripte nach Auswahl des Laufwerks und melden das.

Wenn PEBakery mit der Auswahl der Quelldateien zufrieden war, betätigen Sie den mit „Build“ beschrifteten großen Knopf in der grünen Dachzeile von PEBakery und starten so den eigentlichen Bauprozess. Zu Beginn prüft der Bausatz jetzt, ob wir Updates veröffentlicht haben. Ist das der Fall, stoppt der Prozess, nachdem er die Updates eingespielt hat, und fordert Sie auf, PEBakery erneut zu starten – nur so können wir sicherstellen, dass Updates auch an alle Stellen gelangen.

Je nachdem, welche Komponenten wir aktualisieren mussten, kann es sein, dass Sie erneut den Pfad der Windows-Quelldateien setzen müssen. Wie lang der Bauprozess dauert, hängt von Ihrem PC und der Bandbreite der Internetverbindung ab. Der Bausatz muss allerlei Dateien herunterladen und verarbeiten. Ein moderner PC mit SSD und 100-MBit-DSL

Zweite Etappe: Bauprozess starten

- Rufen Sie im zuvor angelegten Verzeichnis, etwa C:\ctnot, das Programm PEBakeryLauncher.exe auf.
- Windows zeigt Warnungen an, dass das Programm heruntergeladen wurde, erbittet Administratorrechte und startet bei Bedarf den Browser, um die Windows Desktop Runtime herunterzuladen. Erlauben Sie all das bitte.
- Drei Bedienschritte genügen, um das Notfallsystem zu bauen; die angezeigte Bedienoberfläche in der rechten Fensterhälfte hilft Ihnen hindurch.
- Wenn Sie das erste Mal den Build-Knopf drücken, kann es sein, dass PEBakery zunächst Updates für den Bausatz einspielt. Es fordert Sie dann auf, das Programm erneut zu starten. Tun Sie das und starten Sie wieder bei Punkt 1.
- Nach einem erfolgreichen Baulauf zeigt PEBakery kurz eine Erfolgsmeldung an und aktiviert den Knopf, um Rufus zu starten. Bevor Sie das tun, müssen Sie den Stick einstecken.
- Achtung: Sobald Sie den Startknopf in Rufus betätigen, löscht das Programm den USB-Stick. Achten Sie also darauf, dass das richtige Laufwerk mit dem Stick ausgewählt ist und sich keine wichtigen Daten mehr darauf befinden.

baut das Notfallsystem in unter zehn Minuten zusammen – jedenfalls, solange alle angesteuerten Quellen auch erreichbar sind.

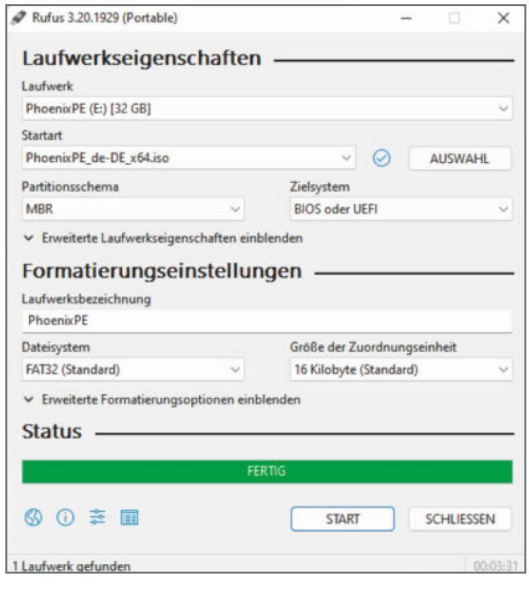
Ein erfolgreicher Baulauf schaltet den Knopf „USB-Stick mit Rufus bespielen“ scharf. Das Programm Rufus erzeugt startfähige USB-Datenträger. Damit Rufus den Stick sieht, müssen Sie ihn anstecken, bevor Sie den Knopf drücken. Achten Sie nach dem Start von Rufus darauf, dass es auch den richtigen Stick als Ziel ausgewählt hat. Die übrigen Felder lassen Sie bitte, wie sie sind – alles ist fertig voreingestellt.

Wenn Rufus den Fortschrittsbalken komplett grün anzeigt und „Fertig“ darin steht, hat das Programm Ihren Stick komplettiert. Sie können ihn jetzt über die üblichen Mechanismen auswerfen und einen PC versuchsweise davon booten.

Weitere Hinweise für den Einsatz der auf dem Stick enthaltenen Werkzeuge geben die Artikel in der Rubrik „Windows-Probleme lösen“ ab Seite 64. Eine Warnung dazu an dieser Stelle: Viele der Tools sind nicht ohne, Sie sollten diese nur mit Bedacht auf einem Produktiv-PC nutzen.

Umwege

Da der Bausatz etliche Programme herunterlädt, ist nicht auszuschließen, dass der Bau im ersten Anlauf nicht gelingt, weil mal ein Server streikt. Es genügt dann erfahrungsgemäß, einige Minuten zu warten und einen neuen Anlauf zu starten. Alles, was PEBakery bis dahin schon erfolgreich heruntergeladen hat, verwendet es dann direkt und kommt so schneller an die Stelle, an der es nicht geklappt hat.



Nach erfolgreichem Bau stecken Sie den Ziel-USB-Stick an und starten dann Rufus – es ist fertig konfiguriert, achten Sie aber darauf, dass wirklich das richtige Laufwerk ausgewählt ist.

Das kann trotzdem nerven, weil bis dahin unter Umständen schon eine erkleckliche Zahl von Schritten auszuführen wäre. Sie können das abkürzen, indem Sie in dem Baum links in PEBakery das zuständige Skript lokalisieren, wahrscheinlich unter „Applications“, und mit einem Klick auf den Namen im rechten Fensterbereich öffnen. Dort finden Sie direkt unterhalb der grünen Kopfleiste von PEBakery einen Knopf, um das Skript allein auszuführen („Run Script“). Probieren Sie das, bis das Skript einmal erfolgreich durch läuft.

Den Erfolg erkennen Sie daran, dass der „Logs“-Knopf in der grünen PEBakery-Kopfleiste nicht orangefarben, sondern weiß ist. Was schiefläuft, verrät ein Klick auf den orangefarbenen Knopf. Wählen Sie dann das Buildlog aus. Wird offensichtlich eine Datei heruntergeladen, aber nicht korrekt weiterverarbeitet, sollten Sie sich den Inhalt der Datei ansehen. Sie finden diese üblicherweise unter C:\ctnot\Workbench\Programs\<Name>.

Mitunter landen als Inhalt in der Datei erweiterte Fehlermeldungen des Webservers, der eigentlich das Programm beziehungsweise eine Installationsdatei dafür liefern sollte. Die Datei können Sie trotz der Endung zum Beispiel mit Notepad öffnen, indem Sie sie per Drag & Drop in ein geöffnetes Notepad-Fenster fallen lassen. Wenn sie eine Fehlermeldung enthält, sollten Sie die jetzt lesen können.

Meist genügt es aber, eine solche „Programmleiche“ durch Löschen zu entsorgen. Die verarbeitenden Skripte können sie nicht von der eigentlich erwarteten Datei unterscheiden. Sie versuchen sich trotzdem daran, sie zu verarbeiten, fallen dabei auf die Nase und der Bauvorgang bricht ab. Mit erneutem Start des Skripts sollte die korrekte Datei vom Server kommen und alles seinen geplanten Gang gehen.

Wenn eine Komponente partout nicht erhältlich ist, können Sie das zuständige Skript für den Baulauf deaktivieren. Entfernen Sie dazu das Häkchen vor dessen Namen in der linken Fensterhälfte. Im Fall

Neues Fundament: PhoenixPE

Die letzten Fassungen des Notfall-Windows verwendeten als Fundament das Win10XPE-Projekt von ChrisR. Für den aktuellen Bausatz sind wir auf PhoenixPE als Basis umgestiegen, eine als Open Source entwickelte Alternative unter MIT-Lizenz.

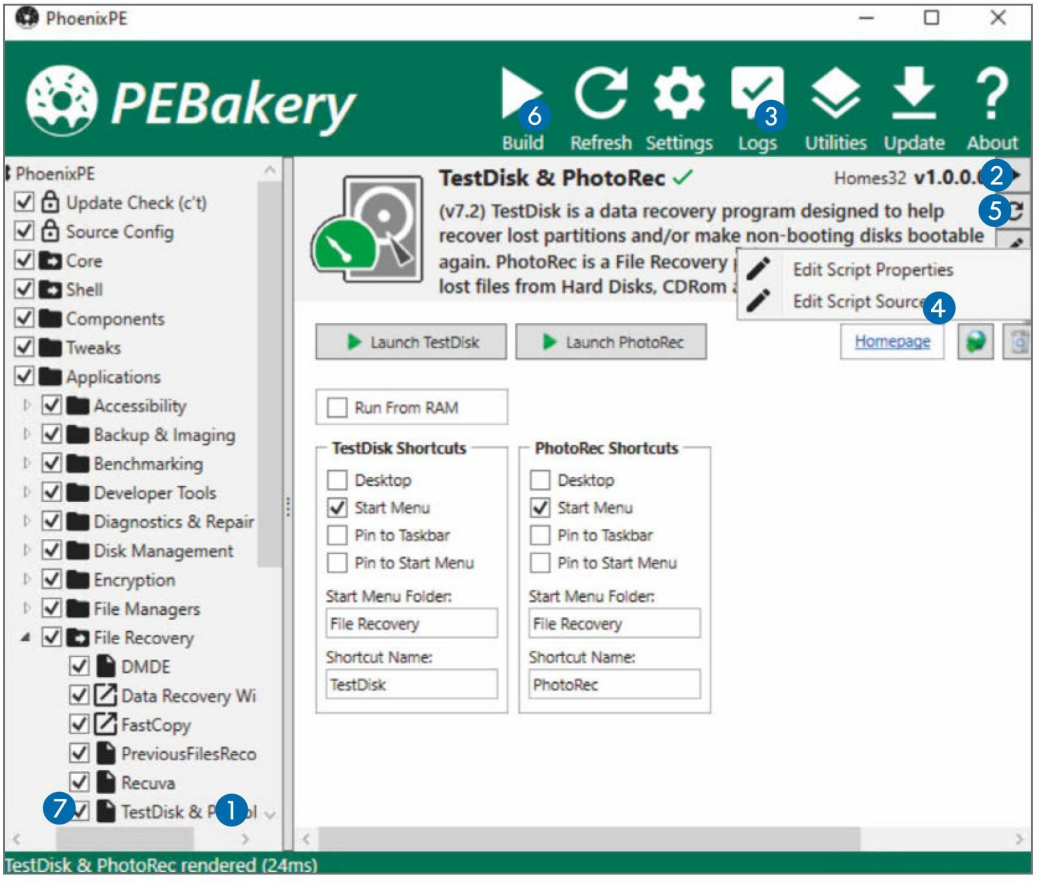
Die Herkunft anderer PE-Projekte ist weniger klar. Sie werden meist in pseudonymreichen Foren von vielen seit Langem engagiert agierenden Kräften, aber auch ein paar sehr eigensinnigen Charakteren entwickelt. Der Quelltext einzelner Komponenten wurde nie offengelegt, vielleicht ist er sogar schon verschollen. Insofern war für uns PhoenixPE eine gute Wahl.

Hinter PhoenixPE steht vor allem Jonathan Holmgren, der unter dem Pseudonym „Homes32“ schon lange zu PE-Projekten beiträgt. Er hat ein zukunftsgewandtes, offenes Projekt auf die Beine gestellt und auf GitHub veröffentlicht. Der offene Ansatz erleichtert es, langfristig mit lästigen Altlasten aufzuräumen. Wir hoffen, mit unseren Erfahrungen und Ergänzungen dazu beitragen zu können.

Im ersten Aufschlag haben wir PhoenixPE für das Notfall-Windows 2023 wie folgt verändert: Wir ergänzen Werkzeuge, die sich in vorherigen Notfallsystemen bewährt hatten, aber im Original noch fehlten, etwa den Windows Defender Offline. Wir bauen eine Jahreslizenz von Drive SnapShot ein, die uns die Firma Tom Ehlert Software freundlicherweise bereitstellt.

Wie auch schon bei den anderen PE-Projekten konfigurieren wir PhoenixPE so, dass sich eine sinnvolle Softwareauswahl ergibt, und supporten sie im kommenden Jahr. Wir haben die Bedienoberfläche für den Bausatz stark vereinfacht; alle Schritte sind nun auf einer Seite zusammengefasst. Außerdem erhielt das Endprodukt einige Polituren: Die Startmenüstruktur ist anders und auf die Artikel abgestimmt.

Unter der Haube haben wir uns weniger vom Originalprojekt entfernt, als das bisher der Fall war. Es wird für erfahrene Nutzer mit PE-Ambitionen perspektivisch möglich sein, zwischen der c’t-Edition von PhoenixPE und dem Original zu wechseln. Dabei gehen dann allerdings einige der Dinge verloren, die wir vereinfacht haben. Die FAQ (siehe Seite 46) enthält Hinweise, wie Experten die verborgenen PhoenixPE-Bestandteile freilegen.



Pannenhilfe, wenn Downloads fehlschlagen: Rufen Sie die Seite für das betroffene Skript links im Projektbaum durch einen Klick auf den Eintrag (hier TestDisk & PhotoRec) auf 1. Lassen Sie das Skript mit etwas zeitlichem Abstand laufen 2. Schauen Sie in das Log, ob der Download geklappt hat 3, oder in den Ordner für das Programm in C:\ctnot\Workbench\PhoenixPE\Programs\TestDisk. Sollte sich die Versionsnummer geändert haben, können Sie über das Stiftsymbol 4 die Versionsnummer oder URL im Skript in einem Texteditor ändern. Bevor Sie das Skript mit 2 erneut starten, muss PEBakery das Skript neu einlesen 5. Bei Erfolg starten Sie das Gesamtprojekt neu 6. Wenn es partout nicht klappt, können Sie das Skript vom Bau ausnehmen 7.

von Programmen aus dem Bereich „Applications“ geht das gefahrlos. Bei anderen Abteilungen ist damit zu rechnen, dass kein startfähiges Notfallsystem entsteht. Schauen Sie auf die Projektseite und ins Forum.

Happy End

Dieser Artikel thematisiert aus gutem Grund eventuelle Schwierigkeiten, die beim Bauen auftreten können. Aus mehreren Jahren aktivem Support für das Projekt können wir aber auch sagen: Die meisten Probleme entstehen dadurch, dass unsere Hinweise nicht beherzigt worden sind – wir wissen freilich auch, dass die nie perfekt sind.

Viele Standardsituationen überprüft der Bausatz und warnt vor dem Start, etwa bei aktiver Antivirus-Software oder zu Windows-Konfigurationseinstellungen, die den Bau behindern. Wenn ein Problem länger anhält, nehmen Sie bitte mit uns Kontakt über die oben genannte E-Mail-Adresse oder im Forum auf. Die neue Version sichert die Bauprotokolle hochkomprimiert im Logs-Verzeichnis (etwa in C:\ctnot\logs). Schicken Sie die Datei gern mit.

Das fertige Notfallsystem als ISO-Datei finden Sie im Ordner Output (etwa in C:\ctnot\output). Wenn Sie diese Datei in einer virtuellen Maschine als DVD-Laufwerk einbinden, können Sie das System erforschen. In Details verhält es sich aber beim Betrieb von einem nicht beschreibbaren Medium etwas anders. Für den Praxiseinsatz sollte das Notfallsystem vom Stick starten, zumal Sie darauf auch Dateien kopieren können.

Bleibt uns nur, viel Erfolg beim Bauen zu wünschen. Berichten Sie auch gern, wie Ihnen das Notfallsystem geholfen hat. (ps) c't

Downloads, Projektseite, Forum
ct.de/ww88

Minds Mastering Machines

Die Heise-Konferenz zu Machine Learning und Künstlicher Intelligenz

9. – 11. Mai 2023 in Karlsruhe

Die Konferenz zu Machine Learning und KI

Die Minds Mastering Machines ist die Konferenz für Fachleute, die Machine-Learning-Projekte in die technische Realität umsetzen.

Das Programm bietet an zwei Tagen 36 Vorträge unter anderem zu folgenden Themen:

- Resilientes Machine Learning
- Komplexität in ML-Projekten reduzieren
- Kontinuierliches Training mit Active-Active-Architekturen
- Large Language Models auf eigene Daten anwenden
- Data-Science-Teams mit Kubeflow skalieren
- Föderiertes Lernen
- MLOps mit Argo und Kubernetes
- Erkennen von Bildmanipulationen

www.m3-konferenz.de

Jetzt Tickets sichern!

Veranstalter

iX Magazin für professionelle Informationstechnik · heise Developer · dpunkt.verlag

c't Notfall-Windows 2023

Unser Notfallsystem auf Windows-Basis erfuhr einige Neuerungen: So dient als Fundament jetzt PhoenixPE. Dadurch sind zum Beispiel die nötigen Schritte zur dauerhaften Treiberintegration einfacher geworden. Viele häufig gegebenen und hier aufgefrischten Support-Antworten gelten aber auch weiter.

Von **Peter Siering**

Scanner findet Viren

? Beim Ausprobieren habe ich einen Virenscanner das Notfallsystem selbst untersuchen lassen und der hat Viren gefunden. Was ist da los?

! Viele Werkzeuge im Notfall-Windows leben in der Grauzone zwischen nützlich und gefährlich. Die Nirsoft-Programme zum Auslesen von Passwörtern beispielsweise sind nützlich, um auf einem nicht mehr startenden System dort hinterlegte Zugänge zu E-Mail-Konten auszulesen, wenn die nur (noch) dort gespeichert sind.

Für ein produktiv genutztes System hingegen stellt ein solches Programm eine mögliche Gefahr dar, besonders wenn nicht der Benutzer selbst es dorthin verbracht hat. Ein Eindringling könnte es mitgebracht haben, um Zugangsdaten auszuspähen. Sicherheitssoftware stuft solche Programme dann als „Possible unwanted application" (PUA) ein, zu Deutsch also „möglicherweise unerwünschte Software".

Wir untersuchen sowohl den Bausatz als auch das Ergebnis jedes Jahr sorgfältig daraufhin, ob Schädlinge enthalten sind. Auf der Projektseite dokumentieren wir alle Dateien, die aus unserer Sicht als im Kontext des für Notfalleinsätze gedachten Systems als „falsch-positiv" eingeschätzt werden, siehe ct.de/wegr.

Keine Tastatur, kein Touchpad, kein Netz

? Nach dem Starten des Notfallsystems kann ich einen All-in-One-PC nicht bedienen, weder Tastatur noch Touchpad reagieren. Was kann ich tun?

! Sehr wahrscheinlich nutzt Ihr PC für diese Peripherie spezielle Treiber, die in Windows selbst nicht enthalten sind. Typisch ist das auch für moderne Surface-Geräte von Microsoft. Sie haben zwei Möglichkeiten: Entweder Sie integrieren passende Treiber ins Notfallsystem (siehe „Integration von Treibern beim Bauen") oder Sie behelfen sich mit separat an den PC angeschlossener USB-Tastatur und -Maus.

Je gängiger solche USB-Geräte sind, desto größer ist die Chance, dass das Notfall-Windows sie ohne weitere Treiber benutzen kann. Das gilt auch für USB-Netzwerkadapter und USB-Hubs, um all die Geräte gleichzeitig überhaupt an Kompaktgeräte mit nur wenigen USB-Ports anschließen zu können. Beachten Sie aber: Das Booten eines USB-Sticks an einem Hub gelingt nicht mit jedem PC und an jedem USB-Port.

PhoenixPE-Komponenten deaktiviert

? Ich habe ein wenig im Bausatz gestöbert und entdeckt, dass ihr im c't-Notfall-Windows viele PhoenixPE-Komponenten gar nicht aktiviert habt. Warum?

! Die meisten PE-Projekte, so auch PhoenixPE, wollen sich breit aufstellen und bieten deshalb eine möglichst große Ausstattung an. Wir trimmen unser Notfallsystem eher auf die typischen Einsatzszenarien und eine möglichst langzeitstabile Mischung, die wir für rund ein Jahr bau- und benutzbar halten.

Wir haben Anfang November angefangen, dabei nahezu alle Optionen in PhoenixPE aktiviert und konnten das System bauen. Wir haben aber nicht alle Programme auf Lauffähigkeit getestet, sondern

nur jene, die aus unserer Sicht eine gute Mischung für das Notfallsystem ergeben.

Aufgrund von Softwareupdates kann es inzwischen aber durchaus sein, dass sich weniger Programme aus der PhoenixPE-Auswahl aktuell noch erfolgreich bauen lassen. Die meisten Programme lädt der Bausatz herunter und sobald sich Versionsnummern ändern, kann der Download scheitern (leider stellt mancher Programmautor nur die jeweils aktuelle Fassung bereit).

PhoenixPE-Apps sichtbar machen

? Wie kann ich die Apps aus PhoenixPE sichtbar machen, die der c't-Notfall-Windows-Bausatz standardmäßig deaktiviert?

! Die wegen häufiger Fehlbedienungen versteckten Programme sind schnell wiederhergestellt. Beachten Sie aber bitte, dass nicht alle Skripte in PhoenixPE fehlerfrei durchlaufen. Zum Teil fehlt Software, zum Teil setzen die Skripte auf Software, die auf dem Bau-PC installiert sein muss, und manche sind auch nur wenig getestet.

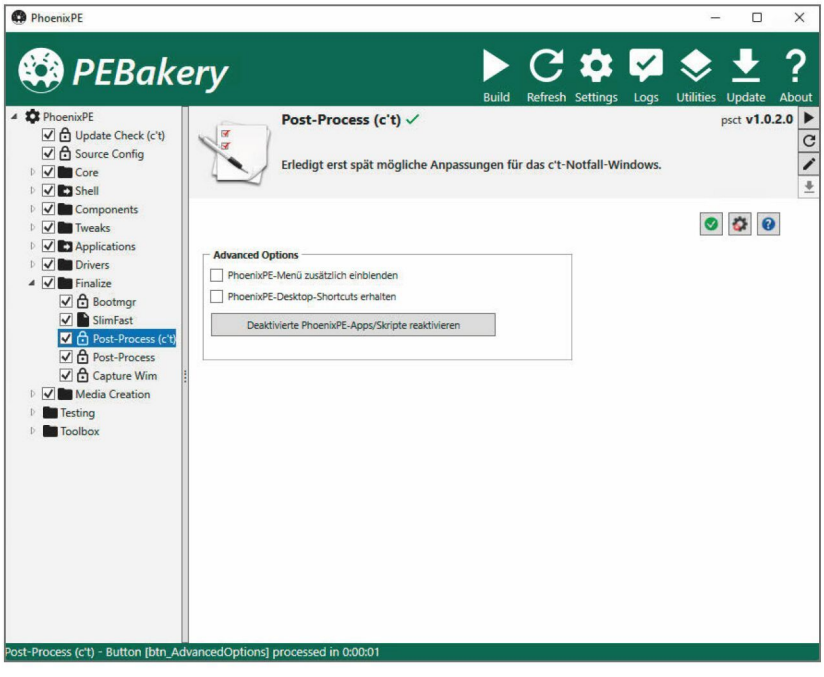
Auf eigene Gefahr und Rechnung können Sie die PhoenixPE-Skripte aktivieren. Selektieren Sie in PEBakery links im Konfigurationsbaum das Skript „PhoenixPE\Finalize\Post-Process (c't)“. Klicken Sie dann in der rechten Fensterhälfte auf das Zahnradsymbol für die erweiterten Einstellungen („Advanced Options“). Sie sehen dann drei Optionen, die bei der Integration von PhoenixPE-Apps/Skripten in das c't-Notfall-Windows helfen. Der Knopf „Deaktivierte PhoenixPE-Apps/Skripte reaktivieren“ tut, was er verspricht. PEBakery liest die Skripte dann neu ein und zeigt auch die „verschwundenen Skripte“ an.

Die Option „PhoenixPE-Menü einblenden“ lässt im Startmenü einen Eintrag „zzz_PhoenixPE“ auftauchen, der die Menüeinträge zeigt, wie PhoenixPE sie betückt. Die Option „PhoenixPE-Desktop-Shortcuts erhalten“ lässt auch die Symbole der Programme auf dem Desktop erscheinen, bei denen das im jeweiligen Skripten aktiviert ist.

Eigene Programme ins Startmenü

? Ich hätte gern, dass hinzugefügte Programme auch im Startmenü erscheinen. Was muss ich dazu tun?

! Wenn Sie Programme dauerhaft ins Startmenü einbinden wollen, können Sie von Hand Ein-



Spezielle Optionen legen zusätzliche PhoenixPE für Experten frei und integrieren die automatisch generierten Einträge aus dem PhoenixPE-Startmenü in das des c't-Notfall-Windows.

träge in der Datei erzeugen, die die Startmenüstruktur und -Einträge des c't-Notfall-Windows beschreibt. Sie finden diese in C:\ctnot\Custom\pecmd_links.ini. Die Datei wird beim Bauen verarbeitet.

Um dauerhaft an das Startmenü angepinnte Einträge für ein Programm zu erzeugen, brauchen Sie das Programm nircmdc.exe. Es erzeugt Verknüpfungen (.LNK-Dateien), die Sie dann im Ordner C:\ctnot\Custom\StartPin_x64 abwerfen. Einen Verweis auf die .LNK-Datei tragen Sie dann in C:\ctnot\Custom\pecmd_pins.ini ein. Beim Start trägt PECMD das Programm dann ins Menü ein.

USB-Stick funktioniert nicht mehr

? Ich habe das System erfolgreich gebaut, auf einen USB-Stick gespielt und ausprobiert. Nachdem der Stick einige Zeit in der Schublade lag, startet er jetzt nicht mehr. Verschleißt das System auf dem Stick?

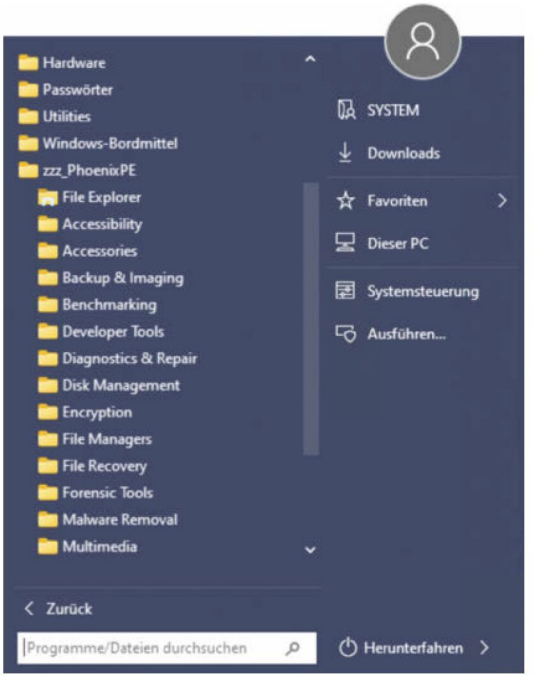
! Das System verschleißt nicht, aber Sticks leider. Viele Probleme beim Kopieren des Notfallsystems auf Sticks oder beim Start später ergeben sich durch unzuverlässige Hardware. Wir haben gute Erfahrungen mit Sticks gängiger Markenanbieter von Flash-Medien gemacht. Probieren Sie es im Zweifelsfall mit einem anderen Stick aus. Beim Wechsel auf einen anderen PC kommen auch allerlei andere Probleme infrage – mehr dazu in unserer FAQ zum Booten von USB-Laufwerken (siehe ct.de/wegr).

Integration von Treibern beim Bauen

? Nach dem Starten fehlen Treiber, wie kann ich solche dauerhaft ergänzen?

! Wenn Sie das Notfallsystem erfolgreich gebaut haben, auf Ihrem PC aber offensichtlich Treiber fehlen, wie das auf dem Surface Laptop oder Surface Pro 9 der Fall ist, können Sie weitere Treiber einbauen lassen. Das ist am einfachsten auf dem betroffenen Gerät selbst, wenn es bereits einen erfolgreichen Baulauf in Standardeinstellung absolviert hat.

Öffnen Sie im PEBakery-Fenster auf der linken Seite den Baum mit den einzelnen Skripten unter „Drivers“. Klicken Sie auf „Driver Integration“. In der rechten Fensterhälfte erscheinen dann die Optionen. Mit einem Klick auf den Knopf „Export Host Drivers“ exportiert PEBakery alle auf dem Host vorhandenen Treiber in das weiter unten in den Eingabefeldern genannte Verzeichnis. Dorthin können Sie auch Dateien kopieren, die Sie auf einem anderen System exportiert haben.



Mit gesetzter Option tauchen die Programme im Startmenü zusätzlich in der von PhoenixPE vorgegebenen Struktur auf – für alle, die gern weitere Programme ausprobieren und nicht im Dateisystem suchen wollen. Aber: Benutzung auf eigene Verantwortung.

Zusätzlich gibt der Bausatz aus, wie umfangreich die ergänzten Treiber ausfallen; auf einem Surface Pro 9 sind das über 1 GByte – das vergrößert die WIM-Datei und damit den vom Notfallsystem „verbratenen“ Hauptspeicher. Wenn Sie das gelbe Ordnersymbol hinter dem Eingabefeld für die x64-Treiber anklicken, sehen Sie Dateien, die beim Export aufgelaufen sind. Sie können dort gefahrlos Verzeichnisse für einzelne Treiber löschen, die nicht in das Notfallsystem sollen.

Der oberste, skriptspezifische Knopf „Run Script“ (direkt unterhalb des PEBakery-About-Knopfes) baut die ausgewählten Treiber in den Arbeitsbereich für das Notfallsystem ein. Wenn Sie anschließend analog von Hand die Skripte „Capture Wim“ unter „Finalize“ und „Create ISO“ unter „Media Creation“ ausführen, übernimmt der Bausatz die Treiber in das fertige ISO.

Danach wechseln Sie auf die Eingangsseite zurück (Klick auf „PhoenixPE“ im Baum links) und können dort den USB-Stick mit dem ergänzten Notfallsystem bespielen. Die Größe der ISO-Datei und der Platzbedarf auf dem Stick wachsen entsprechend mit der Menge der auf diese Weise integrierten Treiber.

Kaputtes Menü zur Auflösungsumschaltung

Im Menü, über das man die Bildschirmauflösung umschaltet, und im angezeigten Bestätigungsdialog erscheinen Hieroglyphen. Lässt sich das reparieren?

Zurzeit scheint es keine Korrektur zu geben, die diese kaputten Ausgaben gerade zieht. Das für die Ausgaben zuständige Programm PECMD hat offenbar in allen verfügbaren Versionen Probleme an dieser Stelle. Ein entsprechender Fehler in PhoenixPE ist auf den GitHub-Seiten des Projekts in Ticket #8 dokumentiert und weiterhin offen.

Notfallsystem stürzt ab

Wenn ich während der Virensuche Browser-Tabs öffne, bleibt meine Test-VM mit dem Notfall-Windows einfach irgendwann stehen. Ist da noch ein Bug drin?

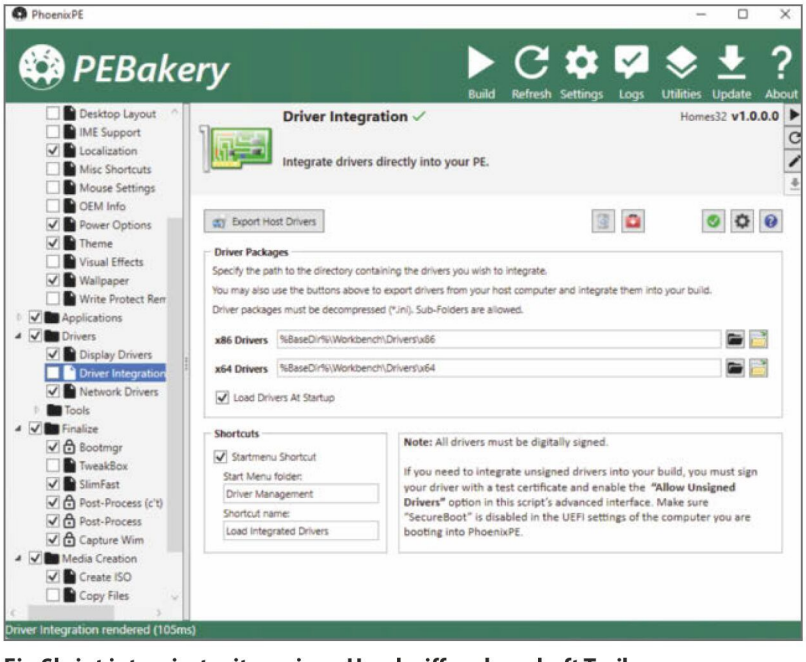
Vermutlich haben Sie der VM nicht allzu viel RAM spendiert. Das Notfallsystem benötigt für die RAM-Disk, in der das System liegt, allein ein GByte Hauptspeicher. So groß ist die WIM-Datei, aus dem es startet. Bei der Integration zusätzlicher Treiber kann sie sogar noch stark anwachsen.

Das heißt, in VMs oder auf Systemen mit nur 4 GByte RAM sollten Sie das Notfallsystem eher mit spitzen Fingern bedienen: Nur ein Programm starten und nutzen und nicht nebenher YouTube-Videos schauen. Zum Zeitvertreib und für eventuell nötige Recherchen empfiehlt sich ein zweites Gerät, etwa ein Notebook oder Smartphone.

Wenn Sie es darauf anlegen, schaffen Sie es auch, mit mehr Hauptspeicher ausgerüstete PCs im Notfall-Windows in einen Absturz zu treiben. Anders als in einer regulären Installation von Windows steht unter Windows PE kein Auslagerungsspeicher zur Verfügung, der den Adressraumhunger von Browserprozessen stillen könnte.

Projekt und weitere Artikel

ct.de/wegr



Ein Skript integriert mit wenigen Handgriffen dauerhaft Treiber aus dem Bestand des PCs, der zum Bauen verwendet wird.

Spracheinstellung blockiert ersten Klick

Beim ersten Start des Notfallsystems erscheint rechts unten über der Taskbar eine Art Menü zur Sprachauswahl. Ein Klick darauf oder an eine andere Stelle auf dem Desktop lässt den Dialog verschwinden. Was ist das?

Das ist ein Artefakt, dessen Ursache wir bisher nicht ergründen konnten. Es tritt nur auf, wenn Sie auf Basis von Windows 11 Version 22H2 das Notfallsystem bauen. Negative Auswirkungen auf die Funktionsweise sind uns keine bekannt – vom zusätzlichen Klick abgesehen.

GWT.EXE fehlt

Beim Starten des Bauprozesses erscheint die Meldung, dass die Datei GWT.EXE fehlt. Ich finde sie auch nicht in C:\ctnot. Ist der Bausatz unvollständig?

Nein, diese Datei ist im bereitgestellten Zip-Archiv enthalten, wird aber häufig von Sicherheitssoftware schon beim Auspacken als gefährlich erkannt und in Quarantäne verbannt. Sie sollten die Protokolle Ihrer Sicherheitssoftware ansehen, dort werden Sie mit großer Wahrscheinlichkeit Hinweise auf solche Aktivitäten finden. Die Datei ist wichtig, ohne gelingt das Bauen nicht. Sorgen Sie bitte dafür, dass sich die Sicherheitssoftware nicht einmischt. (ps) c't

Bild: Albert Hulm

Keine Angst mehr vor Windows-Updates

Updates sind unter Windows ein steter Quell von Fragen und Problemen. Die Auswirkungen der Probleme reichen dabei von ärgerlich bis fatal. Mit unserem Leitfaden wissen Sie, was zu tun ist, wenn mal wieder ein Update aus der Reihe tanzt.

Von **Jan Schüßler**

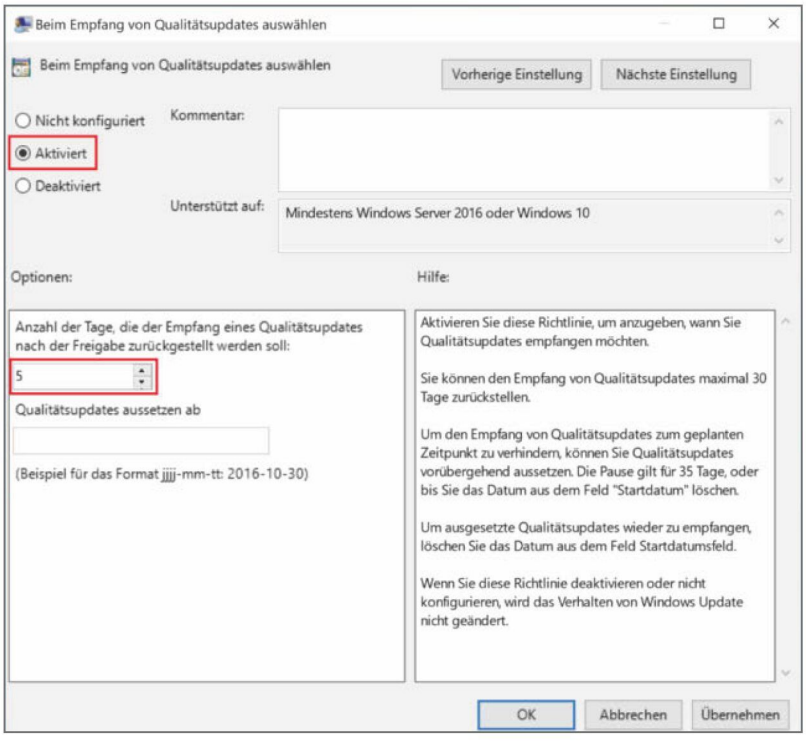
Unter den Fragen, die unsere Leser an uns richten, sind solche zum Thema Windows Update recht häufig – nicht nur, weil sie immer wieder Probleme bereiten, sondern auch, weil es schwierig ist, Updates einigermaßen sinnvoll zu steuern.

Mit ein paar Handgriffen sind Sie besser auf Update-Miseren vorbereitet. Zunächst einmal sollten Sie einen bootfähigen USB-Stick mit einer Windows-Rettungsumgebung griffbereit haben. Ideal dafür ist das c't-Notfall-Windows; für die in diesem Artikel beschriebenen Tipps reicht allerdings auch ein nor-

maler Windows-Setup-Stick, den Sie einfach per Media Creation Tool erstellen (siehe ct.de/w12h). Zweitens: Fertigen Sie regelmäßig Backups des Systems an, um die Betriebsfähigkeit wieder herstellen zu können, wenn gar nichts mehr geht – c't-WIMage ist dafür prädestiniert (ct.de/wimage).

Und drittens: Ist Ihr Systemlaufwerk mit Windows' bordeigener Verschlüsselungssoftware BitLocker gesichert, heben Sie den Wiederherstellungsschlüssel an einem sicheren Ort auf. Sie brauchen ihn womöglich, wenn Windows nach einem Update nicht mehr startet – oder wenn der PC ihn nach einem Neustart unvermittelt verlangt, weil ein Update das Trusted Platform Module beeinträchtigt hat, mit dem das Systemlaufwerk beim Starten sonst automatisch entriegelt wird. In Pro- und höheren Editionen öffnen Sie dazu die BitLocker-Einstellungen per Windows-Taste, tippen `bitlocker`, bestätigen per Eingabetaste und klicken bei Laufwerk C: auf „Wiederherstellungsschlüssel sichern". In der Home-Edition existiert BitLocker offiziell nicht, dafür gibt es eine „Geräteverschlüsselung", die auf BitLocker-Technik fußt und bei Verwendung eines Microsoft-Kontos meist automatisch aktiv wird. In diesem Fall finden Sie den Wiederherstellungsschlüssel im Microsoft-Account (siehe ct.de/w12h).

Um Fehler und Updates einzuordnen und aufzuspüren, ist es unerlässlich, sich mit Microsofts Supportdatenbank (Knowledge Base, KB) zu befassen. Sie enthält detaillierte Listen aller Windows-10- und -11-Versionen und der kumulativen Updates (siehe ct.de/w12h). Die meisten Updates haben einen Eintrag in der Knowledge Base und eine dazugehörige KB-Nummer – darüber finden Sie auch Informationen zu eventuell bekannten Problemen, die ein Patch bereiten kann. Zusätzlich haben wir auf den Seiten 54 und 55 ein Glossar angefügt, das gängige Begriffe erklärt, die oft im Zusammenhang mit Updates für Windows auftauchen.



Wenn Ihnen der Schutz vor fehlerhaften Windows-Patches wichtiger ist als das schnelle Schließen von Sicherheitslücken, können Sie die Updates um ein paar Tage verzögern – sofern Sie keine Home-Edition verwenden.

Pause einlegen

Windows bietet verschiedene Möglichkeiten, die Installation von Updates zu verhindern oder hinauszuzögern. Den Bezug von Updates temporär auszusetzen ist hilfreich, um ungestört an Zeitkritischem zu arbeiten – wie einer wichtigen Präsentation oder Abschlussarbeit. Eine solche Updatepause erlauben alle zur Zeit unterstützten Editionen und Versionen von Windows 10 und 11 mit Ausnahme von Enterprise 2015 LTSB.

In Windows-Update-Einstellungen unterbinden Sie mit der Schaltfläche „Updatepause" (Windows 10) beziehungsweise „Updates aussetzen" (Windows 11) die Suche nach neuen Updates für eine bis maximal fünf Wochen. Lediglich Signatur-Updates für den Virenwächter Defender kommen weiterhin – aber eben nichts, was einen Neustart des Rechners erfordern oder Instabilitäten verursachen könnte. Nach Ablauf der Pause wird Windows allerdings zwingend neue Updates suchen und installieren, um in puncto Sicherheit nicht allzu weit zurückzufallen.

Nicht so schnell!

In allen Editionen außer Home und Enterprise LTSB 2015 lassen sich sowohl Sicherheitsupdates als auch Funktionsupdates über Gruppenrichtlinien in Ein-Tages-Schritten hinauszögern. Diese Möglichkeit

richtet sich zwar vor allem an Admins von Firmennetzwerken, funktioniert auf Einzelplatzrechnern aber ebenso. Die Optionen finden Sie im Gruppenrichtlinien-Editor (Windows-Taste, `gpedit.msc`, Eingabetaste) in Windows 10 in der Abteilung „Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Windows Update/Windows Update für Unternehmen“; in Windows 11 heißt der Unterordner „Vom Windows Update angebotene Updates verwalten“.

Um die monatlichen Sicherheitsupdates zu verzögern, doppelklicken Sie auf die Richtlinie „Beim Empfang von Qualitätsupdates auswählen“. Setzen Sie sie auf „Aktiviert“, tragen Sie im Feld „Anzahl der Tage ...“ einen Wert zwischen 1 und 30 Tagen ein und bestätigen Sie mit OK. Anders als die Updatepause gilt diese Richtlinie nicht einmalig, sondern so lange, bis Sie sie wieder deaktivieren. Updates auf diese Weise eine halbe bis eine Woche zu verzögern, ist vor allem dann sinnvoll, wenn Ausfallsicherheit wichtiger ist als Sicherheitslücken schnellstmöglich zu stopfen. Problematische Patches fallen nach ihrer Veröffentlichung in der allgemeinen Nutzerbasis rasch auf – mit einer Updateverzögerung ersparen Sie sich den Stress, gemeinsam mit der Community von Microsoft als Betatester missbraucht zu werden. Bis die Patches auf dem PC landen, hatte Microsoft im besten Fall ausreichend Zeit, um ein fehlerhaftes Update zu reparieren.

Neue Features warten lassen

Funktionsupdates werden seit ein paar Jahren nicht mehr sofort nach ihrem Release zwangsinstalliert, sondern einige Monate lang optional angeboten. Weil es für Admins größerer Firmenumgebungen wichtig ist, Funktionsupdates möglichst genau vorauszuplanen, gibt es auch dafür eine Gruppenrichtlinie. Auch auf Einzelplatzrechnern kann ihr Einsatz sinnvoll sein – etwa um zu verhindern, dass Mitbenutzer des PCs das Update anstoßen.

Die Richtlinie heißt „Zeitpunkt für den Empfang von Vorabversionen und Funktionsupdates auswählen“. In Windows 11 müssen Sie sie nur aktivieren und eine Verzögerung von 1 bis 365 Tagen einstellen. In Windows 10 steuert die Richtlinie verwirrenderweise auch die Teilnahme am Betatestprogramm Windows Insider, daher müssen Sie dort auch das „Windows-Bereitschaftsniveau“ auf „Semi-Annual Channel“ festlegen. Außerdem ist die Richtlinie auch in den Langzeitsupport-Editionen LTSB und LTSC enthalten, hat dort aber keine Wirkung – der Clou dieser Editionen ist ja gerade, dass Sie generell keine Funktionsupdates bekommen. Achtung: Sobald die Verzögerung abgelaufen ist, wird Windows das Funktionsupdate nicht erst als optional anbieten, sondern direkt zwangsinstallieren. Dieses Verhalten ist ausdrücklich erwünscht, denn nur so können Administratoren größerer Netzwerke die Updates verlässlich planen – wobei die Verteilung in solchen Fällen auch meist über eine WSUS-Infrastruktur erfolgt (siehe Glossar).

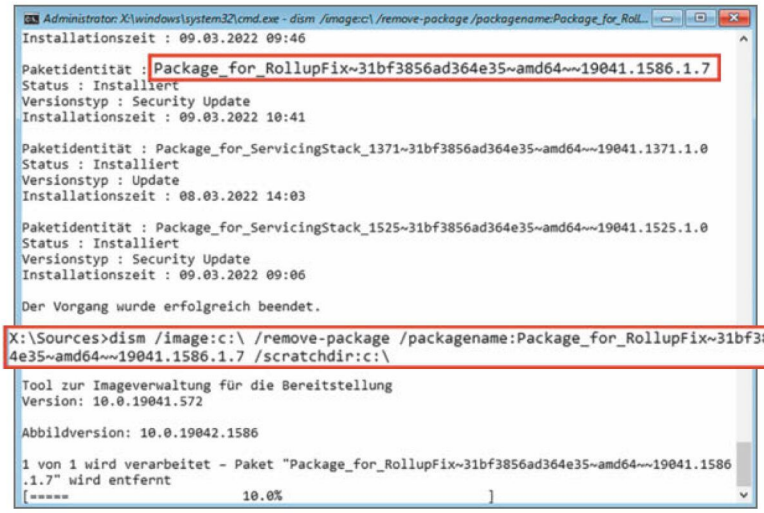
Wenn Sie ein Funktionsupdate auf ein bestimmtes Zieldatum terminieren wollen, müssen Sie auch das Datum kennen, an dem Microsoft die neue Version veröffentlicht hat – diese Daten listet Microsoft in den Versionsübersichten für Windows 10 und 11 auf (siehe ct.de/w12h). Wie viele Tage zwischen Microsofts Veröffentlichung und Ihrem Wunschtermin liegen, errechnet Ihnen die „Datumsberechnung“ des Windows-Taschenrechners.

Windows Downdate

Bereitet der Rechner nach einem kumulativen Update Probleme, ist es einen Versuch wert, das Update zu entfernen, um zu prüfen, ob es schuld am Fehlverhalten ist. Wie einfach das geht, hängt davon ab, ob Windows noch in den Desktop bootet. Wenn ja, öffnen Sie die Seite „Windows Update“ in der Einstellungen-App, dort den „Updateverlauf“ und die Funktion „Updates deinstallieren“. Die folgende Liste ist nach Datum sortiert. Markieren Sie das jüngste Update und klicken Sie auf „Deinstallieren“ – nach einem Neustart sollte das Update verschwunden sein, was Sie leicht per Abgleich der Ausgabe von `winver` mit Microsofts Updateverlauf nachprüfen können (siehe ct.de/w12h). Pausieren Sie vorher die Updates, damit der gleiche problematische Patch nicht sofort wieder installiert wird.

Bootet Windows nicht mehr, wirds etwas kniffliger. Lassen Sie den PC zunächst von einem USB-Stick booten, auf dem die Setup-Umgebung Windows PE oder die davon abgeleitete Reparaturumgebung Windows RE läuft (Tipps dazu in [1]). Das kann zum Beispiel das c’t-Notfall-Windows sein; aber ein einfacher Windows-Setup-Stick ist ebenso ausreichend. Sobald der PC vom Stick gebootet hat, öffnen Sie eine Eingabeaufforderung per Umschalt+F10.

Als erstes ermitteln Sie, welchen Buchstaben Ihr Systemlaufwerk hat – C: ist zwar naheliegend, allerdings sortiert Windows PE die Laufwerksbuchstaben mitunter anders als Ihr installiertes Windows. Um den passenden Buchstaben herauszufinden, können



Wenn Windows nach einem Update nicht mehr richtig startet, können Sie das Update trotzdem entfernen – mit einem Umweg über einen vorher erstellten bootfähigen USB-Stick.

Sie den Texteditor zweckentfremden. Öffnen Sie ihn per `notepad.exe` in der Eingabeaufforderung, klicken Sie auf Datei/Öffnen und dann auf „Dieser PC“. Das Systemlaufwerk sollten Sie nun leicht anhand von Größe und Inhalt erkennen.

Ist das Laufwerk mit BitLocker oder der „Geräteverschlüsselung“ der Home-Edition verschlüsselt, müssen Sie es entriegeln. Dafür brauchen Sie die 48-stelligen Wiederherstellungsschlüssel. Der Befehl

```
manage-bde -unlock c: -rp 633763-669898-077518-↵
↳335323-431232-154685-218939-183336
```

entriegelt das Laufwerk. Der Schlüssel ist ein Beispiel – setzen Sie Ihren eigenen ein. Haben Sie Laufwerk C: erfolgreich entsperrt, listet Ihnen der Befehl

```
dism /image:c:\ /get-packages /scratchdir:c:\
```

die installierten Updatepakete auf; ersetzen Sie dabei `c:\` bei Bedarf durch den zuvor ermittelten Buchstaben. Die Liste ist recht lang, weil sie nicht nur kumulative Updates enthält, sondern auch eine Reihe Windows-eigener Komponenten. Das gesuchte kumulative Update erkennen Sie anhand der Zeile „Paketidentität“. Der Name beginnt entweder mit „Package_for_KB“ und nennt direkt die KB-Nummer, oder aber mit „Package_for_RollupFix“ – dann können Sie zwar nicht die KB-Nummer ablesen, wohl aber die Build-Nummer, auf die Windows durch das Update angehoben wurde (siehe auch Microsofts Update-Listen via ct.de/w12h). Markieren Sie die komplette Paketidentität und kopieren Sie sie per Strg+C in die Zwischenablage; also beispielsweise `Package_for_RollupFix~31bf3856ad364e-35~amd64~~19041.1586.1.7`. Der Befehl

```
dism /image:c:\ /remove-package /packagename:↵
↳Package_for_RollupFix~31bf3856ad364e35~amd64↵
↳~~19041.1586.1.7 /scratchdir:c:\
```

deinstalliert das Update; beim Eintippen können Sie den Paketnamen einfach bequem per Strg+V einfügen. Abschließend starten Sie den Rechner per `wpeutil reboot` neu.

Glossar: Windows Update

Die **Build-Nummer** lässt sich einfach per Windows-Taste, `winver`, Eingabetaste auslesen. Sie besteht aus zwei Zahlen, getrennt durch einen Dezimalpunkt. Die erste, stets fünfstellige Zahl nennt die Windows-Version, so entspricht etwa 19042 Windows 10 Version 20H2; 22000 ist Windows 11 Version 21H2. Die zweite Zahl fällt ein- bis vierstellig aus und nennt das Patchlevel, sprich: den Update-Stand des Systems. Microsoft hat sowohl Versionsnummern als auch Patchlevel in ausführlichen Listen für Windows 10 und 11 dokumentiert (siehe ct.de/w12h).

DISM.exe ist ein Kommandozeilenwerkzeug zum Bearbeiten von Windows-Abbildern, also etwa Installationsabbilder im WIM-Format, aber auch bestehende Windows-Installationen.

Ein **Funktionsupdate** bringt Windows auf eine neue Version, also etwa von 20H2 auf 21H1. Oft werden sie auch Feature- oder Versionsupgrades beziehungsweise -updates genannt. Microsoft spricht stets von „Updates“, obwohl es sich technisch auch um ein Upgrade handeln kann. Der Unterschied: Bei einem Upgrade kommt ein kompletter Windows-Setup-Datensatz auf die Festplatte. Dann wird die bestehende Windows-Installation in einen Backup-Ordner geschoben, die neue installiert und sämtliche Einstellungen, Nutzerkonten, Dateien und Programme dort hinein übernommen. Der Vorgang wird auch als In-Place-Upgrade bezeichnet. Kommt eine neue Windows-Version hingegen als Update, werden die – dann meist nur wenigen – Neuerungen zunächst mit einem regulären kumulativen Update auf den Rechner gebracht, bleiben aber unsichtbar. Das, was in Windows Update dann etwa als „Funktionsupdate auf Version 21H2“ auftaucht, ist in Wahrheit nur ein Enablement Package, das die schon eingespielten Neuerungen nur noch aktiviert. Funktionsupdates, die als kumulatives Update plus Enablement Package kommen, installieren im Regelfall schneller und stressärmer als solche, die als Upgrade auf den PC gelangen.

Die **KB-Nummer** bezieht sich auf einen Eintrag in Microsofts Knowledge Base, also die Supportdatenbank, in der Microsoft alle Updates dokumentiert.

Kumulative Updates sind die übliche Form, in der Microsoft Fehlerkorrekturen verteilt, und zwar sowohl sicherheitskritische als auch nicht sicherheitskritische. Kumulativ („anhäufend“) bedeutet, dass in den Update-Paketen nicht nur die im jeweiligen Monat neuen Fehlerkorrekturen stecken, sondern alle, die seit Veröffentlichung der betreffenden Windows-Version erschienen sind.

Im **Microsoft Update Catalog** stehen die meisten Updates als eigenständige Installationspakete zum Download bereit.

Mit der **Nutzungszeit** in den Windows-Update-Einstellungen legen Sie ein Zeitfenster von maximal 18 Stunden fest, innerhalb dessen Windows den PC nach einem Update nicht automatisch neu starten darf.

Optionale Updates sind nicht sicherheitskritisch und werden nur auf Wunsch des Anwenders installiert. Im Regelfall handelt es sich um kumulative Updates, die unkritische Fehler in Windows beheben sollen. Sie erscheinen meist am dritten oder

Rolle rückwärts

Funktionsupdates, die per Upgrade-Installation auf den Rechner kommen, lassen sich bis zu zehn Tage nach ihrer Installation rückabwickeln. Nach Ablauf dieses Zeitraums löscht Windows das alte, beim Upgrade ins Archiv verschobene System, um Laufwerksspeicher freizugeben. Diese Rollback-Funktion befindet sich in der Einstellungen-App: Bei Windows 10 unter „Update und Sicherheit/Wiederherstellung“, bei Windows 11 unter „System/Wiederherstellung“.

Kommt eine neue Windows-Version hingegen als Update, dessen Neuerungen bloß per Enablement Package scharfgeschaltet wurden, führt der Weg wie bei kumulativen Updates über den Updateverlauf und „Updates deinstallieren“. Der Eintrag hat einen Namen im Stil von „Feature Update to Windows 10 21H2 via Enablement Package“ – nach einem Neustart sollte sich Ihr System per `winver` wieder als Vorversion ausgeben.

Es will nicht?

Ein häufiges Leid besteht darin, dass Updates fehlschlagen und im besten Fall einen nicht sonderlich aussagekräftigen Fehlercode im Updateverlauf hin-

vierten Dienstag des Monats und firmieren auch als Vorschau-Updates. Sofern bei jenen Anwendern, die solch ein Update freiwillig installieren, keine Probleme auftauchen, landen die Änderungen am Patchday des Folgemonats auf dem PC.

Mit dem **Patchday** ist im Microsoft-Universum der zweite Dienstag im Monat gemeint. An diesem Tag veröffentlicht Microsoft ein sicherheitskritisches kumulatives Update und im Regelfall auch weitere Updates, etwa für .NET-Komponenten und ein neues „Windows-Tool zum Entfernen bösartiger Software“, das den Rechner auf aktuelle Schädlinge untersucht. Zudem veröffentlicht Microsoft am dritten oder vierten Dienstag des Monats gelegentlich optionale, nicht sicherheitskritische kumulative Updates. Bei besonders schweren Problemen behält sich Microsoft allerdings vor, jederzeit ein Update außer der Reihe zu veröffentlichen („Out Of Band“).

Service Packs waren Sammel-Updates, die Microsoft für Systeme bis einschließlich Windows 7 veröffentlicht hat – es waren Pakete, in denen alle bis dato erschienenen Einzelupdates zusammengefasst wurden. Der Begriff wurde mit Windows 8 abgeschafft, wenngleich Microsoft dafür noch zwei Update-Pakete veröffentlicht hat, die als Service Pack durchgehen könnten – nämlich das Update auf Windows 8.1 sowie dafür ein „Oktober-2014-Update“, das die bis dato angefallenen Patches in einem Paket gebündelt hat.

Der **Servicing Stack** ist die Softwarekomponente, die Updates einspielt. Hin und wieder braucht der Servicing Stack selbst ein Update, um künftige Updates einspielen zu können. Bis vor rund einem Jahr wurde er als eigenständiges Paket verteilt, seit Februar 2021 sind eventuelle Servicing-Stack-Updates mit dem jeweiligen kumulativen Update gebündelt.

Sicherheits- und Qualitätsupdates ist eine andere Bezeichnung für kumulative Updates und eventuelle weitere sicherheits- oder stabilitätsrelevante Patches.

Mit der **Übermittlungsoptimierung** verteilen Windows-PCs Fragmente von Update-Downloads untereinander – in der Standardeinstellung nur im Heimnetzwerk und nicht via Internet.

Windows PE (Preinstallation Environment) ist ein schlankes, von Wechselmedien startendes Windows; es ist mit einigen Verwaltungs- und Setup-Werkzeugen ausgestattet. Es bildet zum Beispiel die Grundlage der Setup-Umgebung, die Sie sehen, wenn Sie Windows von einem USB-Stick sauber neu installieren. Auch die Recovery-Umgebung **Windows RE** fußt auf Windows PE.

winver.exe zeigt Windows-Version und Build-Nummer an, Sie starten es per Windows-Taste, `winver`, Eingabetaste.

Mit **WSUS**, kurz für Windows Server Update Services, können Administratoren in Netzwerken mit Windows Server eine eigene, lokale Update-Infrastruktur bereitstellen und die Verteilung der Patches an die Desktop-PCs und Server steuern und überwachen. WSUS lädt die Updates von Microsoft herunter, um sie im internen Netzwerk anzubieten.

terlassen. Leider haben wir kein Patentrezept dagegen – immerhin bietet Microsoft inzwischen Listen mit einigen Fehlercode-spezifischen Tipps (siehe ct.de/w12h). Führen die ins Leere, gibt es zumindest noch ein paar allgemeine Handgriffe, die auszuprobieren sich lohnt.

Eine davon ist die bordeigene Problembehandlung für Windows Update, zu finden in den Einstellungen in Windows 10 unter „Update und Sicherheit/Problembehandlung/Zusätzliche Problembehandlungen“ und in Windows 11 unter „System/Problembehandlung/Andere Problembehandlungen“. Das Tool prüft einige Grundeinstellungen, etwa ob der Update-Server erreichbar ist, ob der Update-Dienst läuft und Ähnliches.

Fruchtet das nicht, können Sie versuchen, das betreffende Update als eigenständiges Paket herunterzuladen und zu installieren. Notieren Sie sich dafür die KB-Nummer und tippen Sie sie ins Suchfeld von Microsofts Update-Katalog ein – das ist ein Verzeichnis, in dem Microsoft die allermeisten Patches auch als eigenständige Pakete zum Download anbietet (siehe ct.de/w12h). Laden Sie das zu Ihrer Windows-Version und -Architektur passende Paket herunter und starten Sie die Installation per Doppelklick.

Zudem gibt es ein paar Tipps, die nach unserer Erfahrung nicht allzu oft, aber in manchen Fällen dann doch Probleme beseitigen, weswegen es nicht schaden kann, sie auszuprobieren: etwa der Befehl

```
dism /online /cleanup-image /restorehealth
```

sowie

```
sfc /scannow
```

in einer Eingabeaufforderung mit Administratorrechten. Beide finden und reparieren beschädigte Systemkomponenten – `sfc` (für System File Check) versucht lediglich, schadhafte Dateien aus lokalen Kopien wiederherzustellen; `dism` ist in der Lage, beschädigte Komponenten notfalls per Windows Update nachzuladen.

Ein weiterer Trick, der hin und wieder zum Erfolg führt, ist das Leeren des kompletten Windows-Update-Cache – allerdings geht dabei der gesamte bisherige Updateverlauf verloren (nicht aber die Updates als solche). Wenn Sie das nicht stört: Öffnen Sie eine PowerShell mit Administratorrechten und beenden Sie zunächst die Dienste „Windows Update“ und „Intelligenter Hintergrundübertragungsdienst“ per

```
net stop bits
net stop wuauserv
```

Leeren Sie dann den kompletten Update-Cache mittels

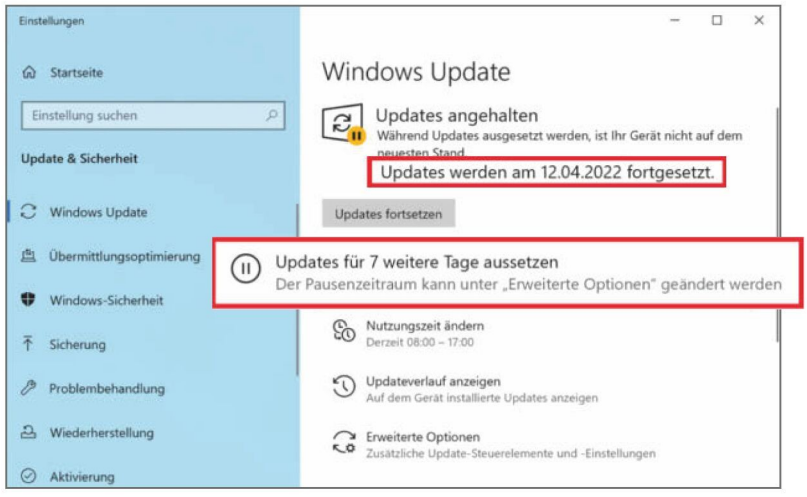
```
rm c:\windows\softwaredistribution\*
```

Bestätigen Sie die Abfrage mit der Taste A, schalten Sie die Dienste mit den zwei Befehlen

```
net start bits
net start wuauserv
```

wieder ein und probieren Sie aus, ob sich die anstehenden Updates nun installieren lassen.

Abschließend noch eine besonders rabiate Methode: Leser berichten uns immer mal, dass ein „Drüberinstallieren“ der aktuellen Windows-Version helfen kann. Dazu erstellen Sie mit dem Media Creation Tool (siehe ct.de/w12h) einen Setup-USB-Stick für Windows 10 beziehungsweise 11, und starten danach das Programm „setup.exe“ aus dem Stammverzeichnis des Sticks. Wichtig: Lassen Sie den PC nicht vom Stick booten, sondern starten Sie das Setup aus dem regulären, laufenden Windows heraus. Achten Sie in den Installationsoptionen darauf, dass Ihre Apps und Dateien beibehalten werden sollen und passen Sie die Einstellung bei Bedarf an.



Mit ein paar Klicks verschaffen Sie sich bis zu fünf Wochen Ruhe vor Windows-Updates und Problemen, die sie verursachen könnten.

Technisch gesehen stoßen Sie damit eine Funktionsupgrade-Installation an, nur dass Sie statt einer neueren einfach die gleiche Windows-Version nochmal installieren. Der Vorgang ist identisch: Zunächst wird ein neues Windows neben das vorhandene installiert. Von der Setup-Umgebung Windows PE aus wird dann die alte gegen die neue Installation ausgetauscht und sämtliche Programme, Dateien, Konten und Einstellungen in die neue übernommen. Um ein komplett festgefahrenes Windows-Update-System wieder auf die Spur zu bringen, ist diese Methode vergleichsweise vielversprechend, birgt aber wie andere Upgrade-Installationen auch das Risiko, dass danach irgendetwas nicht mehr funktioniert. Daher gilt auch hier: vorher ein Backup erstellen!

Fazit

Windows-Updates sollen Probleme beheben, doch hin und wieder bewirken sie genau das Gegenteil. Mit unseren Tipps vermeiden Sie nicht nur Querschläger, sondern sind auch darauf vorbereitet, falls dieser doch einmal auf Ihrem Rechner großen Schaden anrichtet. (jss) c't

Literatur

[1] Axel Vahldiek, **FAQ: Booten von USB-Laufwerken**, Antworten auf die häufigsten Fragen, c't 24/2018, S. 172

Alle Listen und Links
ct.de/w12h

Von Hackern lernen

+ GRATIS Videokurs im Wert von 129,- €

Ganz gleich, ob Sie nur die Sicherheit Ihrer eigenen Websites abklopfen möchten oder beruflich mit IT-Sicherheit zu tun haben. Wer die schmutzigen Tricks der Hacker kennt, kann sich besser davor schützen. Anfänger und Profis lernen in diesem c't-Sonderheft die Grundlagen des Hackens und erfahren wie Hacker ticken.

- ► Hacking ausprobieren Schritt für Schritt
- ► Informationen gewinnen mit OSINT
- ► Malware-Tricks verstehen
- ► Recherche- und Analyse-Tools anwenden
- ► Inkl. heise-Academy-Kurs: „Angriffsszenarien im Netzwerk“
- ► Auch als Heft inkl. PDF-Download mit 29 % Rabatt erhältlich

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

shop.heise.de/ct-hackingpraxis23

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

heise Shop

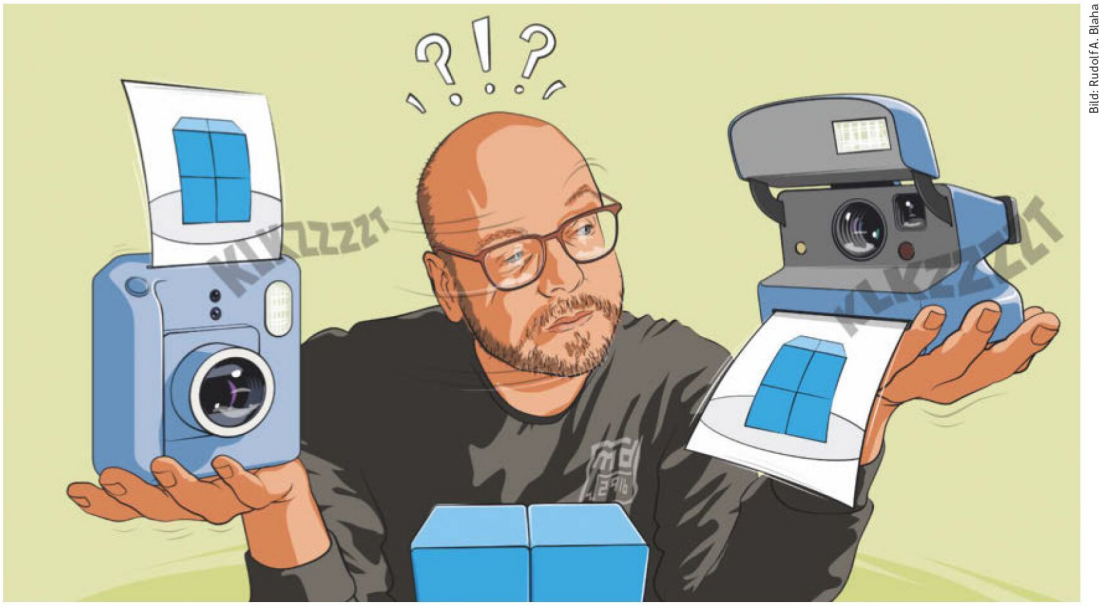


Bild: Rudolf A. Blaha

Drive Snapshot oder c't-WIMage? Beide!

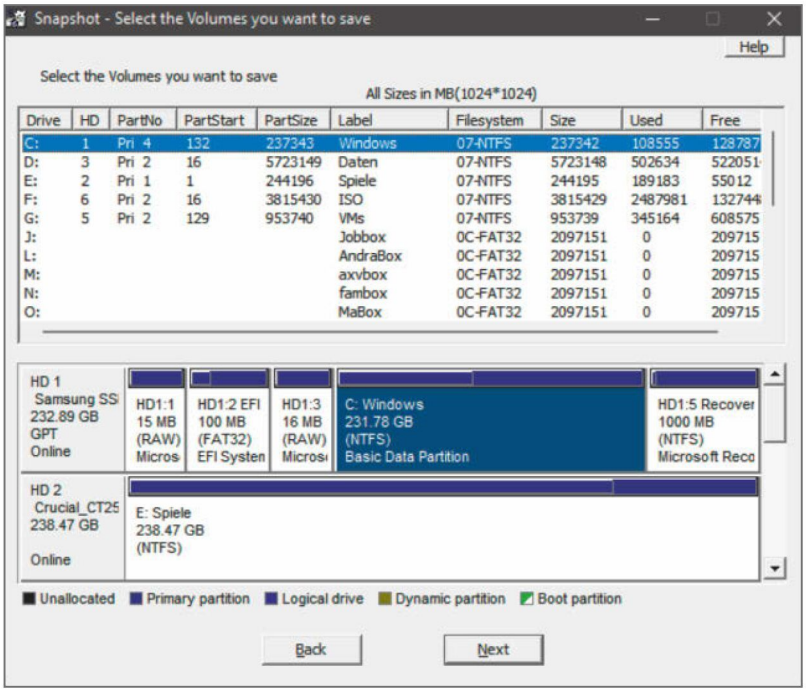
Ob Windows streikt, auf einen anderen PC umziehen soll oder Sie ein Sicherungsnetz für Datenrettungsversuche brauchen: Ein Imager hilft. Einerseits liegt es nahe, Drive Snapshot aus dem c't-Notfall-Windows zu verwenden, andererseits empfehlen wir auch dauernd c't-WIMage. Warum? Weil die beiden unterschiedliche Stärken haben. Dieser Beitrag erläutert sie.

Von **Axel Vahldiek**

Diese c't-Empfehlung ist nun wirklich nicht neu: Fertigen Sie von Windows ein Image an, also eine Sicherheitskopie von Laufwerk C:. Sollte Windows danach mal streiken, können Sie den PC einfach durch Zurückspielen dieses Backups wieder in einen funktionstüchtigen Zustand zurückversetzen. Als Leserservice stellen wir Ihnen sogar einen passenden Imager zum Erstellen solcher Sicherungskopien zur Verfügung. Genauer gesagt, und da liegt das Problem: Wir liefern sogar zwei. Während wir in vielen c't-Artikeln auf das von uns entwickelte Sicherungsskript c't-WIMage verweisen, steckt im c't-Notfall-Windows das Programm „Drive Snapshot". Doch warum können sich die c't-Autoren nicht endlich mal auf einen Imager festlegen? Nun, wir könnten schon, wollen aber nicht, und zwar in Ihrem Interesse: Imager kommen in verschiedenen Szenarien zum Einsatz, mal passt der eine besser und

mal der andere. Wir haben es aber zugegebenermaßen bislang versäumt, das detailliert zu begründen. Hier holen wir das nach.

Zunächst eine Vorstellungsrunde: Drive Snapshot ist ein bewährter Imager von Tom Ehlert, der unter so ziemlich allen Windows-Versionen läuft (ab NT4 SP6). Das Programm erzeugt Abbilder Ihrer Windows-Installation mitsamt Bootloader und allem, was sonst noch dazu gehört, etwa aller NTFS-Besonderheiten wie Zugriffsrechte, Reparse Points, EFS-Dateiverschlüsselung und so weiter. Drive Snapshot läuft ohne Installation, sichert schnell und stellt eine Windows-Installation in genau dem Zustand wieder her, in dem sie sich während des Sicherns befand. Dank Tom Ehlerts Erlaubnis und Mithilfe stecken in unserem c't-Notfall-Windows schon seit Langem jährlich frische Spezialversionen von Drive Snapshot. Diese können ein Jahr lang sichern und zeitlich unbeschränkt wiederherstellen (eine dauerhafte Lizenz ist ab 39 Euro erhältlich, siehe https://drivesnapshot.de).



Drive Snapshot erstellt 1:1-Kopien von Partitionen oder kompletten Datenträgern. Mit einer rechtzeitig angelegten Sicherung können Sie einen PC sogar in seinen Auslieferungszustand zurückversetzen.

Auf der anderen Seite: c't-WIMage. Unser Sicherungsskript braucht mindestens Windows 8.1 und arbeitet technisch zwar ganz anders als Drive Snapshot, doch entscheidend ist ja, was hinten rauskommt. Und das ist auch bei c't-WIMage ein Abbild Ihrer Windows-Installation mitsamt aller NTFS-Besonderheiten, das Sie bei Bedarf bootfähig wiederherstellen können. Das Skript selbst, alle Anleitungen sowie ein Forum finden Sie unter ct.de/wimage.

Was gesichert wird

Drive Snapshot und c't-WIMage sichern beide gleichermaßen Ihre Windows-Installation, also das, was auf Laufwerk C: liegt (genauer: auf dem durch die Umgebungsvariable `%HomeDrive%` bezeichneten Laufwerk). Die Unterschiede liegen beim Drumherum.

Zusätzlich zu Laufwerk C: enthält ein interner Datenträger normalerweise weitere Partitionen. In einer steckt der Bootloader, in einer anderen ein Windows-eigenes Rettungssystem namens „Windows RE“ (Recovery Environment [1]).

Drive Snapshot sichert sowohl die Boot- als auch die RE-Partition auf Wunsch vollständig mit. Es vermag also anders als c't-WIMage auch weitere Partitionen mitzusichern, etwa solche für Ihre persönlichen Dateien. Was das Dateisystem dieser Partitionen anbelangt, ist Drive Snapshot flexibel: Es kennt NTFS, FAT16/32 und ReFS ebenso wie EXT2/3/4, ReiserFS und XFS.

c't-WIMage hingegen ignoriert alles außer der Windows-Partition selbst. Nicht einmal der Inhalt der Boot-Partition landet im Image. Einzige Ausnahme ist die RE-Partition. Die bleibt zwar ebenfalls ungesichert, doch c't-WIMage verschiebt ihren Inhalt vor dem Sichern auf C: (und danach wieder zurück). Daher landet Windows RE trotzdem im Backup. Kurzum: Drive Snapshot kann ein Abbild des kompletten Datenträgers mitsamt aller Partitionen erstellen, c't-WIMage hingegen sichert abgesehen von den Inhalten der RE-Partition nur das, was auf C: liegt.

Wiederherstellen

Weil Drive Snapshot den kompletten Datenträger sichern kann, ist es in der Lage, ihn genau so wiederherzustellen. Das ist praktisch, wenn Sie beispielsweise einen neuen Computer vor sich haben. Mit Drive Snapshot können Sie ein Backup ziehen, bevor Sie die Installation an Ihre individuellen Bedürfnisse anpassen. Das erlaubt es, bei Bedarf und nach dem Wegsichern Ihrer persönlichen Daten den Aus-

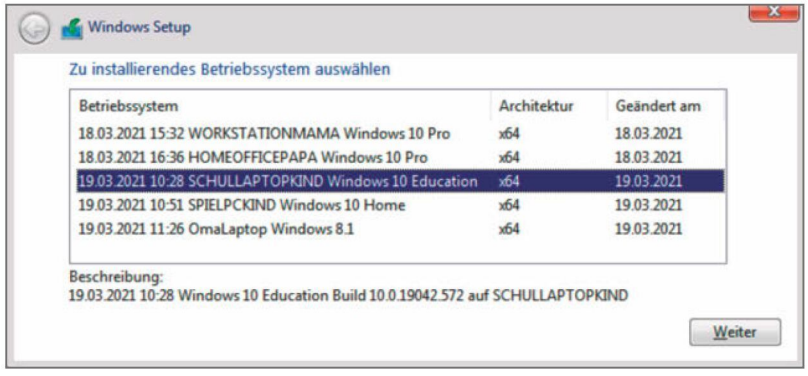
lieferungszustand wiederherzustellen, falls der neue Computer später mal zum Support-Fall wird. So finden weder Händler noch Hersteller einen Grund, nach einem Blick auf das Betriebssystem den Support zu verweigern.

c't-WIMage ist dafür ungeeignet, weil es keine Eins-zu-Eins-Kopien des kompletten Datenträgers anfertigt. Es stellt die Images nicht mal selbst wieder her: Der entscheidende Trick unseres Skripts ist, diese Aufgabe stattdessen dem Windows-Setup-Programm zu überlassen. Das ist kein böser Hack, sondern von Microsoft ausdrücklich so vorgesehen. Wenn Sie wie in unseren Anleitungen empfohlen c't-WIMage auf einem USB-Laufwerk einrichten (Stick oder besser USB-SSD), dient dieses anschließend nicht nur zur Aufnahme der Sicherungen, sondern auch als bootfähiges Wiederherstellungsmedium.

Es verhält sich dann genau so, wie Sie es von einem beispielsweise mit Microsofts Media Creation Tool (MCT, siehe ct.de/wub9) eingerichteten USB-Laufwerk gewohnt sind: Davon bootet das Windows-Setup-Programm. Das installiert ein frisches Windows auf den internen Datenträger, versieht es mit einem neuen Bootloader und erzeugt und befüllt eine RE-Partition. Nur installiert das Setup-Programm bei einem c't-WIMage-USB-Laufwerk kein frisches Windows, sondern das Image Ihrer Windows-Installation. Das wiederhergestellte Image verhält sich direkt wieder so, wie Sie es gewohnt sind; die bei einer Neuinstallation fälligen Fragen nach Sprache, Konto, Netzwerk und so weiter entfallen allesamt.

Der Vorteil: Weil das Setup-Programm nicht einfach den bislang genutzten Bootloader wiederherstellt, sondern einen neuen erzeugt, kann es diesen an die vorhandene Hardware anpassen. Das kann sogar auf demselben PC nützlich sein, etwa nach dem Tausch von Mainboard oder SSD. Auch Änderungen am Bootmodus verlieren so ihren Schrecken: Ein PC kann zum Booten klassische BIOS- oder moderne UEFI-Mechanismen nutzen [2], doch Windows bootet nur dann, wenn der Bootloader auf den richtigen Mechanismus eingerichtet ist. Dabei geht es nicht nur um die Dateien des Bootloaders, sondern auch um die korrekte Partitionierung des Datenträgers [3].

Ein mit c't-WIMage erzeugtes Image wird daher nach dem Wiederherstellen auch bei Änderungen des Bootverfahrens oder sogar auf komplett anderer Hardware starten, sofern der PC die grundlegenden Windows-Anforderungen erfüllt und mit der Architektur Ihrer Windows-Installation (32 oder 64 Bit) zurechtkommt. Auch in einer mit Hyper-V erstellten virtuellen Maschine (VM) lässt sich Ihre Sicherung ruckzuck wiederherstellen [4]. Das Testen eines Images wird so sehr einfach.



c't-WIMage schiebt seine Sicherungskopien dem Windows-Setup-Programm unter. Das merkt gar nicht, dass es kein frisches Windows installiert, sondern die Sicherungskopie wiederherstellt.

Speicherziel

Beide Imager speichern Ihre Sicherungen jeweils in Containerdateien, doch hier enden dann die Gemeinsamkeiten. Drive Snapshot erstellt für jede Sicherung eine eigene Datei, für die Sie jeweils individuelle Namen vergeben können. Die Datei teilt es auf Wunsch in mehrere auf, um Begrenzungen der maximalen Dateigröße von Dateisystemen wie FAT32 zu umgehen. Das Verwalten der Images ist bei Drive Snapshot einfach: Veraltete Images beispielsweise lassen sich leicht identifizieren und durch Löschen der entsprechenden Datei(en) entsorgen. Auf Wunsch erzeugt der Imager auch differenzielle Sicherungen, bei denen nur der Unterschied zur vorigen Sicherung gespeichert wird.

c't-WIMage sichert stattdessen grundsätzlich alles in einer einzigen Datei im WIM-Format [5]. Weil die WIM-Datei im Laufe der Zeit sehr groß werden kann, ist ein Dateisystem erforderlich, das mit so großen Dateien auch umgehen kann. Zudem muss es während der Wiederherstellung für das Setup-Programm lesbar sein. Anders formuliert: Die WIM-Datei liegt grundsätzlich auf einem NTFS-Laufwerk. Das Löschen nicht mehr benötigter Images aus einer WIM-Datei ist zwar möglich, aber anspruchsvoll [6]. Einfacher ist, alle paar Monate die WIM-Datei vom Backup-

Medium von Hand woanders hin zu verschieben. c't-WIMage erstellt dann beim nächsten Sichern eine neue. Veraltete WIM-Dateien können Sie so irgendwann entsorgen. Dass c't-WIMage so vorgeht, mag im ersten Moment als Nachteil erscheinen, entpuppt sich aber als Vorteil, und zwar dann, wenn es darum geht, wie viel Platz das Backup-Medium bieten muss.

Platzbedarf

Zum Sichern einer einzelnen Installation ist bei beiden Imagern grob gleich viel freier Platz erforderlich. Wie groß der ist, hängt im Wesentlichen davon ab, wie groß die zu sichernde Installation ist und wie gut sich die Daten komprimieren lassen. Denn beide Imager verwenden Kompression, um die Images möglichst klein zu halten. Ebenso überspringen beide zwecks Platzsparen beim Sichern die Auslagerungsdatei Pagefile.sys und die Ruhezustandsdatei Hiberfil.sys. Diese beiden Dateien enthalten nur vorübergehend erforderliche Daten, und wenn eine der Dateien fehlt, erstellt Windows sie einfach neu. Schließlich sichern beide Imager mehrfach vorhandene Dateien nur einmalig.

Dennoch arbeitet c't-WIMage platzsparender, und zwar spätestens ab der zweiten Sicherung. Denn während Drive Snapshot für die zweite Sicherung standardmäßig eine neue Container-Datei anlegt, landen die Daten für das zweite Image bei c't-WIMage in jener WIM-Datei, in der auch schon die erste Sicherung steckt. Und hier spielt das Verfahren seinen Vorteil aus: Es sichert das zweite Image inkrementell, wobei es aber nicht nur innerhalb eines Images mehrfach vorhandene Dateien berücksichtigt, sondern über alle Images. Drastisches Beispiel: Wenn Sie zweimal dieselbe, unveränderte Installation nacheinander sichern, belegt die zweite Sicherungsdatei bei Drive Snapshot genauso viel Platz wie die erste, der Platzbedarf verdoppelt sich also. Anders bei c't-WIMage: Weil in diesem Fall schlicht alles, was beim zweiten Anlauf gesichert wird, auch schon beim ersten gesichert wurde, wächst die Containerdatei lediglich um wenige MByte für Metadaten.

c't-WIMage prüft nicht nur, ob Dateien mehrfach vorhanden sind, sondern zerlegt zuerst alles in 32 KByte kleine Blöcke. Anschließend prüft es bei jedem Block, ob er schon vorhanden ist. Dadurch wächst der Platzbedarf bei veränderten Dateien nur um die Änderungen, aber nicht um die unveränderten Bestandteile. Das klappt sogar über Windows-Grenzen hinweg: Auch wenn Windows 11 Pro und Windows 8.1 Home dem Namen nach zwei grundverschiedene Betriebssysteme zu sein scheinen, stecken doch jede Menge Gemeinsamkeiten drin. Sichern Sie beide in dieselbe WIM-Datei, wächst der Platzbedarf bei der zweiten Sicherung daher wieder nur um die Differenz zwischen den beiden. Selbst Images unterschiedlicher Windows-Installationen von verschiedenen Computern können Sie gemeinsam und platzsparend in eine einzige WIM-Datei stopfen.

Tempo

Die unterschiedlichen Verfahren zum Platzsparen haben deutliche Auswirkungen aufs Tempo, mit dem die beiden Imager arbeiten. Drive Snapshot ist in der Standardeinstellung sehr fix, allein schon, weil es dann die aktuelle Sicherung nicht mit älteren abgleichen muss. c't-WIMage geht deutlich langsamer zu Werke.

In beiden Fällen hängt das Tempo aber nicht nur von der Software, sondern auch von vielen anderen Faktoren ab: zu sichernde Datenmenge, Geschwindigkeit des Backup-Mediums, ein alles überwachender Virenscanner und so weiter.

Diese Faktoren fallen bei c't-WIMage schwerer ins Gewicht, weil das Sichern an sich schon länger dauert – da wirkt jede zusätzliche Bremse besonders stark. Vor allem das USB-Laufwerk spielt bei c't-WIMage eine wesentliche Rolle: USB-Sticks bieten oft nur geradezu erbärmliche Schreibraten, daher die Empfehlung zu einer externen SSD. Zum Vergleich: Das Sichern einer frischen Windows-Installation dauert bei deaktiviertem Virenscanner von einem halbwegs aktuellen PC auf eine externe SSD keine zehn Minuten. Doch bei großen Installationen, lahmer Hardware und bremsendem Scanner kann sich das Sichern über viele Stunden hinziehen.

Ein weiterer Nachteil der Langsamkeit von c't-WIMage: Manche USB-Laufwerke verursachen bei stundenlangem Betrieb Probleme, die bei kürzerem Einsatz nicht auftreten. Dafür kann c't-WIMage zwar nichts, doch fallen die Probleme oft erst damit auf. Abhilfe: Verwenden Sie andere USB-Komponenten. Tauschen Sie also das Kabel, das externe Gehäuse und notfalls das USB-Laufwerk und stöpseln Sie das USB-Laufwerk an einem anderen Anschluss an. Garantiert funktionierende Kombinationen können wir leider nicht nennen, allein schon, weil beispielsweise USB-Laufwerke trotz absolut identischer Typenbezeichnung unterschiedliche Firmwareversionen haben können oder der Hersteller plötzlich andere Flash-Bausteine einbaut.

Einzelne Dateien wiederherstellen

Bei beiden Imagern ist es möglich, einzelne Dateien aus einem Image herauszuholen, und zwar ohne das Image dafür wiederherstellen zu müssen. Drive Snapshot bindet das Image dafür als virtuelles Laufwerk mit eigenem Laufwerksbuchstaben im Explorer ein.

c't-WIMage bietet keine eigene Funktion für einzelne Dateien, das ist aber auch nicht nötig. Das für die Sicherungen genutzte Dateiformat WIM ist nämlich auch dem Open-Source-Packprogramm 7-Zip bekannt. Es öffnet WIM-Dateien ebenso wie ZIP-Archive, sodass Sie damit bequem einzelne Dateien und Ordner herauspicken können. Jedes Image steckt in der WIM-Datei in einem Ordner, deren Namen mit 1 beginnend fortlaufend durchnummeriert sind. Welche Nummer zu welchem Image gehört, entnehmen Sie der Datei Backupliste.txt, die c't-WIMage beim Sichern auf das USB-Laufwerk schreibt.

Im Ernstfall

Falls der Crash bereits passiert ist, schlägt die Stunde von Drive Snapshot, weshalb dieser Imager statt c't-WIMage im c't-Notfall-Windows steckt. Denn es kann eine Windows-Installation sichern, die gerade nicht läuft. Das ist praktisch, um später aus der havarierten Windows-Installation wenigstens noch einzelne Dateien herauspulen zu können. c't-WIMage sichert hingegen grundsätzlich nur die gerade laufende Installation.

Ein weiterer Unterschied zwischen den Imagern: c't-WIMage sichert alles dateiweise, seine Arbeitsweise ähnelt also der von Packprogrammen wie 7-Zip. Das erlaubt es, von c't-WIMage angelegte WIM-Dateien genauso wie die frischer Windows-Installationen noch vor dem Wiederherstellen zu bearbeiten, etwa durch das Hinzufügen weiterer Dateien [7]. Drive Snapshot hingegen sichert die vom Dateisystem als belegt markierten Sektoren, interessiert sich also nicht für einzelne Dateien und Ordner. Der Clou: Auf Wunsch kann es auch als unbelegt markierte Sektoren sichern. Dabei kommen Images heraus, die so groß wie die Quell-Partition sind (meist also riesig).

Nützlich ist das in zwei Fällen: Erstens kann Drive Snapshot auf diese Weise Partitionen sichern, deren Dateisystem es nicht kennt und von denen es folglich nicht wissen kann, welche Sektoren belegt sind. So erhalten Sie selbst von solchen Partitionen eine Sicherungskopie für spätere Wiederherstellungsversuche.

Zweitens: Wenn Sie unter Windows eine Datei löschen, verschwindet sie keineswegs im Nirgendwo. Stattdessen markiert das Dateisystem die von der Datei bislang belegten Sektoren als frei, obwohl der ursprüngliche Inhalt immer noch derselbe ist. Er verschwindet erst, wenn er mit neuem Inhalt überschrieben wird. Das nutzen Datenrettungsprogramme, die in den als frei markierten Sektoren nachschauen, ob sie Daten enthalten. Wenn die wie eine Datei oder zumindest wie ein Dateifragment aussehen, stellen die Datenretter sie wieder her. Es besteht während solcher Rettungsversuche aber stets die Gefahr, dass dabei vom Betriebssystem, einer Anwendung oder von was auch immer ausgerechnet das überschrieben wird, was Sie gerade retten wollen. Ausweg: Sie sichern die Installation inklusive aller Sektoren, die das Dateisystem für frei hält, dann können Sie dieses Image vor weiteren Rettungsversuchen bei Bedarf restaurieren.

Fazit

Letztlich beginnt die Antwort auf die Frage, ob Sie besser zu Drive Snapshot oder zu c't-WIMage greifen, wie so oft mit einem entschiedenen „Kommt drauf an".

Wenn es darum geht, eine derzeit funktionierende Windows-Installation so zu konservieren, dass Sie sie selbst nach einem Totalschaden des PCs auf irgendeinem anderen Computer weiternutzen können, dann sind Sie bei c't-WIMage richtig. Das gilt erst recht, wenn Sie sich nicht nur um eine Installation kümmern, sondern um mehrere, etwa als (Familien-)Admin, denn dann sparen Sie mit c't-WIMage sehr viel Platz. Auch das Testen, ob das Image erfolgreich erstellt wurde, ist einfach, weil ein quasi beliebiger echter PC oder eine Hyper-V-VM dafür ausreicht.

Drive Snapshot hingegen ist schnell, stellt den Ausgangszustand eines Datenträgers eins zu eins wieder her und hilft selbst dann bei der Datenrettung, wenn vor dem Crash noch gar kein Image erstellt wurde. Zudem sichert es auch ältere Windows-Versionen und sogar Partitionen mit unbekannten Dateisystemen.

Kurzum: Beide Imager haben ihre Berechtigung und wir empfehlen, dass Sie beide verwenden: je nach Einsatzszenario mal den und mal den. So sind Sie für alle Fälle bestens gerüstet. (axv) c't

Literatur

[1] Axel Vahldiek, **Wo ist sie, und wenn ja, wie oft?**, Windows RE und die Recovery-Partition, c't 18/2021, S. 162

[2] Axel Vahldiek, **Pfadfinder**, UEFI oder BIOS? Windows-Bootmodus erkennen, c't 20/2022, S. 168

[3] Axel Vahldiek, **Vielfach unterteilt**, Die Partitionierung moderner Windows-PCs, c't 5/2018, S. 146

[4] Axel Vahldiek, **VM-Generator**, c't-Skript erstellt Windows-VMs in Hyper-V, c't 20/2020, S. 162

[5] Axel Vahldiek, **FAQ: Windows Image-Format WIM**, c't 18/2018, S. 176, auch kostenlos online lesbar unter ct.de/-4133050

[6] Axel Vahldiek, **Werkzeug-Tuning**, Tipps und Tricks zu c't-WIMage, c't 11/2021, S. 162

[7] Axel Vahldiek, **Noch vor dem Startschuss**, Windows-Installation im Voraus anpassen, c't 1/2019, S. 164

Media Creation Tool

ct.de/wub9

building IoT

Die Konferenz zu (I)IoT

26. und 27. April 2023
in München

Jetzt Tickets sichern!

Software entwickeln für das (I)Iot

Die Fachkonferenz building IoT ist seit 2016 der Treffpunkt für diejenigen, die Softwareanwendungen und digitale Produkte im Internet der Dinge und im Industrial Internet of Things entwickeln.

Das Programm bietet an zwei Tagen in drei Tracks 36 Vorträge unter anderem zu folgenden Themen:

- Datenanbindung und -analyse für das IIoT
- Edge-Computing mit Kubernetes
- Eclipse Sparkplug in Action
- Zeitreihendatenbanken für das IoT
- Maschinenbau trifft auf agile Softwareentwicklung
- Rust auf dem Mikrocontroller
- IoT Cybersecurity: EU-Normen-Update

www.buildingiot.de

Veranstalter

iX Magazin für professionelle Informationstechnik

heise Developer

dpunkt.verlag

Goldsponsor

WAGO

Bronzesponsor

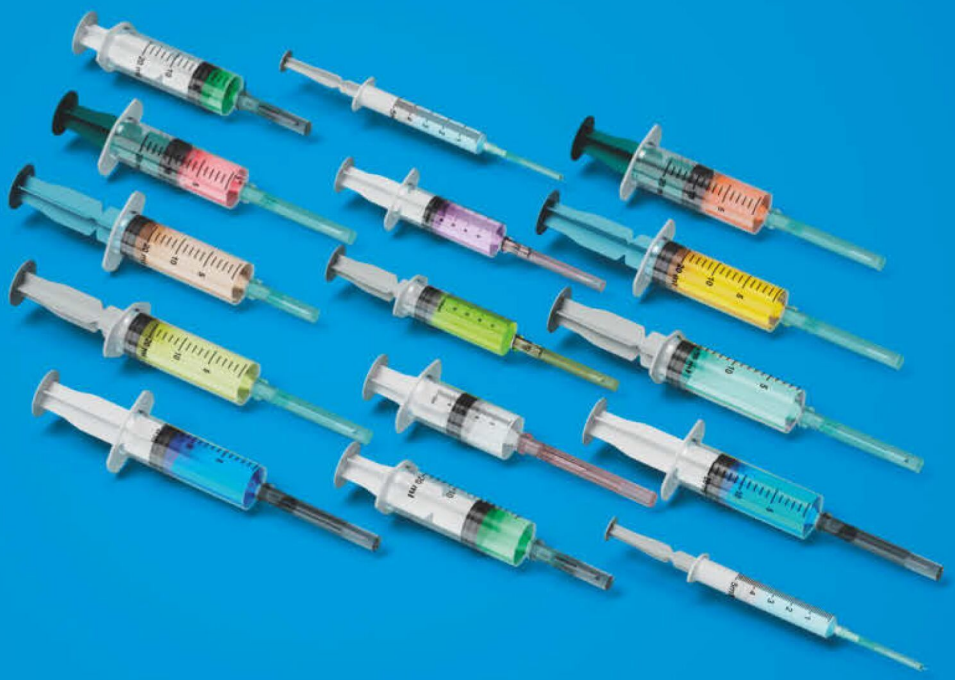
MAIBORNWOLFF

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**

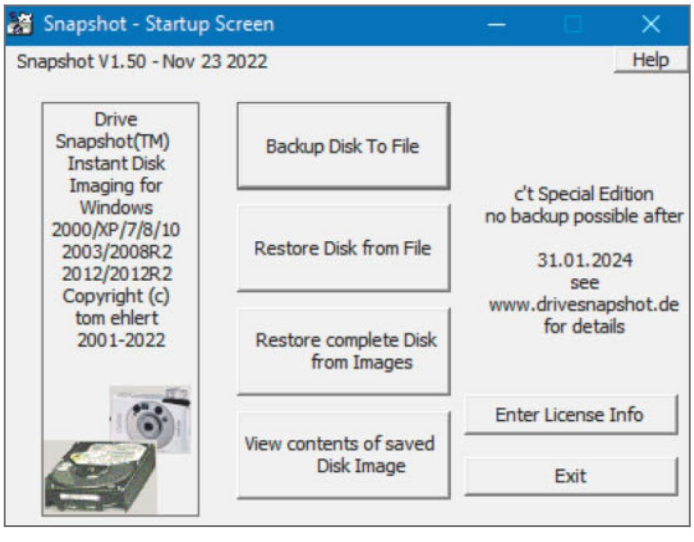


Es gilt unverändert: Viele Windows-Probleme lassen sich mit einem simplen Neustart lösen (merke: „Wenns nicht tut, hilft Reboot!“). Doch manchmal reicht das nicht. Dann schlägt die Stunde unseres Notfallsystems (Bauanleitung siehe S. 38). Dabei handelt es sich um eine saubere, bootfähige Rettungsumgebung. 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 diesem 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.



Auch in diesem Jahr ist wieder eine Spezialversion von Drive Snapshot an Bord. Damit erstellte Images sind auch dann nützlich, wenn bei einem Reparaturversuch etwas schiefging.

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 Snapshot „Restore Disk from File“ anklicken, die Backup-Datei und die Ziel-Partition auswählen und Sicherheitsnachfrage bestätigen. Schon startet die Wiederherstellung.

Voraussetzung für den Einsatz von Drive Snapshot ist zwar das Bauen des Notfall-Windows mit unserem Bausatz. Anschließend läuft der Imager aber nicht nur unter dem gebooteten Notfall-Windows. Wenn Sie das auf dem internen Datenträger installierte Windows starten und den Stick mit dem Notfallsystem anstecken, finden Sie das Programm darauf im

Gilt auch für Reparaturversuche: Backup!

Wenn Sie eine defekte Windows-Installation reparieren, kann es passieren, dass Windows anschließend noch kaputter ist. Und das muss keineswegs an Fehleinschätzungen oder Fehlbedienungen Ihrerseits liegen. So testen wir unser Notfallsystem zwar stets mit vielen Kollegen und noch mehr Testrechnern zeitaufwendig und intensiv. Doch trotzdem kann es passieren, dass uns etwas durchrutscht.

Bei der letztjährigen Version des Notfall-Windows übersahen wir einen geradezu fatalen Fehler. Es stellte sich erst im Nachhinein heraus, dass nach dem Analysieren eines Offline-Systems mit Autoruns die Registrierung der untersuchten Systeme Schaden nahm. Die auf der Windows-Partition auf dem internen Datenträger in \Windows\System32\Config liegenden Dateien hatten nach der Analyse die Länge 0 und die Windows-Installation startete nicht mehr. Hintergrund: Zum Analysieren lädt Autoruns die Registry-Hives des zu durchsuchenden Systems. Bis zur Version 13 (die nun wieder im Notfall-Windows steckt) entlädt es sie korrekt wieder, ab Version 14 aber nicht mehr. Wir sprachen schon im Januar 2022 mit Programmautor Mark Russinovich über den Bug (er ist Technikchef für Azure bei Microsoft). Offenbar enthält aber selbst die aktuelle Autoruns-Fassung weiterhin keinen Fix.

Daher der Hinweis: Seien Sie sich stets bewusst, dass Sie mit unserem Notfall-Windows nicht nur diverse Probleme lösen, sondern womöglich auch neue produzieren können, wobei Bugs wie der von Autoruns zum Glück die Ausnahme sind. Gegen Fehlbedienungen hilft die Lektüre der Anleitungen, gegen Fehleinschätzungen eine gründliche Vorabrecherche, die aber zugegebenermaßen nicht jedermanns Sache ist und für die im Ernstfall oft auch die nötige Ruhe fehlt. Was in allen Fällen hilft: ein Backup. Haben Sie ein Image der noch funktionierenden Installation, ist das Zurückspielen der Problemlöser schlechthin. Doch selbst ein Image einer defekten Installation hilft, wie Sie es mit Drive Snapshot aus dem Notfall-Windows heraus erzeugen können. Denn dann kommen Sie zumindest zum Ausgangspunkt Ihrer Reparaturbemühungen zurück.

Es sei noch ein weiterer Hinweis gestattet: Wir versuchen zwar, Bugs im Notfall-Windows schnellstmöglich zu beheben. Doch das Identifizieren eines Bugs ist nicht immer trivial. Als Folge vergeht oft einige Zeit von der ersten Meldung bis hin zur Erkenntnis, dass etwas faul ist. Schauen Sie daher bitte am besten direkt vor einem Reparaturversuch auf unsere Projektseite und am besten auch dort ins Forum. Dort finden sich Hinweise auf Bugs oft zuerst und wir reagieren dort auch zuerst.

Login Unlocker

Das Programm „Windows Login Unlocker“ kann Windows-Konten aufsperren, die mit einem Microsoft-Konto verknüpft sind. An dieser Aufgabe scheitert das bewährte und im Notfall-Windows enthaltene „NTPWEedit“. Zur Bedienung des „Windows Login Unlocker“ gibt es wenig zu sagen, dafür mehr zu seinen Fähigkeiten und zur Herkunft: Den Login Unlocker sollten Sie nur in Notfällen einsetzen. Die Software stammt aus einem russischen Forum, die Weiterentwicklung wurde schon lange aufgekündigt. Wir haben dem Programm auf die Finger gesehen und nichts Bedenkliches entdeckt.

Seiteneffekte müssen Sie in Kauf nehmen: Beim Aufsperren eines per Microsoft-Konto gesicherten Benutzerkontos wandelt das Programm dieses Profil in ein lokales ohne Passwort um. Das heißt, die Verbindung zu dem Online-Konto geht verloren. Wie auch bei NTPWEedit lassen sich anschließend mit NTFS-Hilfe verschlüsselte Dateien (EFS) nicht mehr lesen. (ps)

Weitere Werkzeuge des c't-Notfall-Windows (Auswahl)

Ans Startmenü angeheftet	
Defender, Eset, McAfee, Trend Micro	Virenscanner, siehe Artikel „Virensuche mit dem Notfall-Windows“
Drive Snapshot	Imager: Erstellt Abbilder der Festplatte und spielt sie wieder zurück (Spezialversion: Erzeugt Images bis Ende 2023 und spielt sie zeitlich unbegrenzt zurück.)
Analyse	
Autoruns	Autostart-Analyse, siehe Artikel „Virensuche mit dem Notfall-Windows“
Blue Screen View	Analyse von Bluescreens
FullEventLogView	Ereignisanzeige der Installation auf dem internen Datenträger einsehen [5]
Windirstat / WizTree	Datenträger-Füllstandsanalyse. WinDirStat ist bewährt, WizTree ist schneller [6]
Daten retten [7]	
BrowserDownloadsView	zeigt die Downloads eines Browsers (Taste F9 drücken zum Anpassen der Pfade)
BrowsingHistoryView	zeigt die History eines Browsers (Taste F9 drücken zum Anpassen der Pfade)
DMDE	Disk-Editor und Datenretter
DRW	EaseUS Data Recovery Wizard, Datenretter
FastCopy	Kopierprogramm
HDDRawCopy	erstellt vollständige Abbilder der Festplatte inklusive jener Sektoren, die das Dateisystem für leer hält
ImgBurn	Brennprogramm
Linux Reader	liest Laufwerke, die mit den Linux-Dateisystemen Ext2/Ext3/Ext4 und ReiserFS sowie Mac-Laufwerke, die mit HFS und HFS+ formatiert sind
Recuva / PhotoRec /TestDisk	Datenrettung: Daten / Bilder / Partitionen
ShadowCoyView	Versucht Daten aus Schattenkopien zu retten
Unstoppable Copier	Kopierprogramm, setzt auch bei Lesefehlern fort
Hardware [8]	
CPU-Z / GPU-Z / PCI-Z / SSD-Z	Informationen zu Prozessor und Arbeitsspeicher / Grafikchip / PCI-Anschlüssen / SSDs
Crystal Disk Info	Informationen über die Datenträger
h2testw	prüft Integrität von Speichermedien (USB-Sticks)
HDTune	liest Smart-Werte von Festplatten/SSDs aus, enthält simplen Benchmark und Oberflächentest
HWinfo	Übersicht über die gesamte erkannte Hardware
HWMonitor	CPU-Überwachung
Prime95	CPU-Stresstest: „Torture Test“ erzeugt sehr hohe Prozessorlast, wahlweise auch auf nur einem Kern (Turbo-Test)
Speccy	Übersicht über die gesamte erkannte Hardware sowie zu einigen Windows-Details
Passwörter	
Keyfinder	liest Produktschlüssel aus
MailPassView	liest Zugangspasswörter von Mail-Clients aus
NTPWedit	setzt neue Windows-Passwörter (siehe Anleitung „Windows-Kennwort vergessen“)
PassReset	entfernt Windows-Passwörter (siehe Anleitung „Windows-Kennwort vergessen“)
SecurityQuestionsView	liest die hinterlegten Sicherheitsfragen zum Passwort aus
Windows Login Unlocker	sperrt Benutzerkonten auf, die mit einem Microsoft-Konto verbunden sind (siehe Kasten)
Utilities	
7-Zip	packt und entpackt diverse Archiv-Formate
AgentRansack	flexible Dateisuche
Alles mounten (ctmountall.bat)	Bindet in den Explorer des Notfall-Windows alle Volumes ein, die bislang keinen Laufwerksbuchstaben haben (siehe Anleitung „Fehlende Laufwerke einbinden“)
AnyDesk	Fernwartung
Bootice	Bootloader, MBR, UEFI-Einträge und mehr bearbeiten
Everything	schnelle Dateisuche auf NTFS-Laufwerken
FreeCommander	Dateimanager
HxD Editor	Hex-Editor
Macrium Reflect	Imager, taugt auch zum Klonen von Windows-Installationen [9]
MiniTool Partition Wizard	Partitionierer
VeraCrypt	Verschlüsselungsprogramm [10]
WinMerge	vergleicht Dateien und Ordner

Ordner „Programs/Snapshot“. Sie können die Datei „Snapshot.exe“ direkt starten oder auf ein Backup-Laufwerk kopieren, um das Programm von dort zu starten und im Ernstfall mit dem Image zusammen parat zu haben. Es läuft ohne Installation. Alternativ können Sie zum Sichern unser Sicherungsskript c't-WIMage verwenden (ct.de/wimage). Eine Entscheidungshilfe, wann welches der beiden Werkzeuge das Richtige für Sie ist, finden Sie im Artikel „Drive Snapshot oder c't-WIMage? Beide!“ ab Seite 58.

Booten

1. Stick an den PC stöpseln, alle anderen USB-Laufwerke abziehen, PC starten. Im Idealfall bootet das Notfall-Windows ohne weiteres Zutun. Voraussetzungen: Der PC muss über mindestens 4 GByte RAM verfügen. Weil unser Notfallsystem eine 64-Bit-Architektur besitzt, muss der PC zudem in der Lage sein, ein 64-Bit-Betriebssystem zu starten. Das können aber seit mindestens zehn Jahren alle PCs bis auf extrem seltene Ausnahmen. Ob auf dem PC eine 32- oder 64-Bit-Installation von Windows läuft, spielt keine Rolle.
2. Falls der PC nicht vom Stick bootet, versuchen Sie es über das BIOS-Bootmenü (englisch „BIOS Boot Select“, BBS). Es erscheint üblicherweise nach dem Drücken einer Taste (oft Esc, F2, F8, F9, F10, F12 oder Entf). Mitunter erscheint ein Hinweis auf die richtige Taste direkt nach dem Einschalten auf dem Bildschirm. Falls ein großes Herstellerlogo die BIOS-Meldungen überdeckt, werden Sie das oft mit Esc oder in den BIOS-Einstellungen los.
3. Ignoriert der PC Ihre Tastendrücke und bootet direkt die Windows-Installation vom internen Datenträger, fahren Sie diese nicht wieder herunter! Wählen Sie stattdessen „Neu starten“. Während jener Zeit, in der Windows bereits heruntergefahren ist, aber noch nicht wieder hochfährt, sollte der PC auf Tastendrücke wieder reagieren.
4. Falls der Stick im BBS doppelt auftaucht, ist das kein Fehler: Er kann sowohl per UEFI als auch klassisch (Legacy BIOS) booten. Achten Sie im Bootmenü auf das, was zusätzlich zum Namen des Sticks in der gleichen Zeile steht, beispielsweise „EFI“ oder „UEFI“. Andersherum steht „CSM“ (Compatibility Support Module) für die klassischen BIOS-Mechanismen. Für Rettungseinsätze spielt es keine Rolle, welchen Eintrag Sie auswählen. Scheitert das Booten bei einem der beiden, versuchen Sie den anderen. Anders als bei manch anderen vom Stick bootenden Betriebssystemen spielt es für unser Notfall-Windows übrigens keine Rolle, ob Secure Boot aktiv ist oder nicht – es startet dank signiertem Loader in beiden Fällen anstandslos.
5. Viele weitere Tipps rund um das Booten von USB haben wir in einer FAQ zusammengestellt [1], die Sie auch vollständig online unter ct.de/-4209809 lesen können.

Übersicht über die Laufwerke verschaffen

1. Vorab: Die Laufwerksbuchstaben können sich von den gewohnten unterscheiden, denn jede Windows-Installation vergibt die Buchstaben selbst [2]. Das gilt auch für das Notfall-Windows. Normale Installationen merken sich die Zuordnung in ihrer jeweiligen Registry, das Notfall-Windows vergisst sie beim Neustart. Es bindet zudem zur Laufzeit eigene Laufwerke ein.
2. Explorer öffnen (via „Dieser PC“ auf dem Desktop, Explorer-Icon neben dem Startknopf oder Tastenkombination Windows+E).
3. Das Notfallsystem benutzt B: als RAM-Disk, X: als Systemlaufwerk und Y: für das Bootmedium. Achtung: Das Programm Macrium Reflect zum Klonen oder Sichern der Windows-Installation verwürfelt manchmal die Buchstaben. Ordnung lässt sich ohne Neustart wieder herstellen. Dazu Windows-Taste drücken und eintippen: `LetterSwap.exe /Auto /BootDrive Y:`
4. Ein Blick im Explorer auf die Dateien und Ordner hilft beim Identifizieren der Windows-Partition.

Fehlende Laufwerke einbinden

1. Die Windows-eigenen Partitionen, die den Bootloader sowie die Wiederherstellungsumgebung „Windows RE“ [3] enthalten, bindet unser Notfallsystem standardmäßig nicht ein (macht Windows auch nicht). Im Startmenü finden Sie unter „Alle Programme/Utilities“ ein Skript namens „Alles mounten (ctmountall.bat)“. Es versieht alle Partitionen mit einem Laufwerksbuchstaben (genauer: die darauf liegenden Volumes), die bislang

Literatur

[1] Axel Vahldiek, **FAQ: Booten von USB-Laufwerken**, c't 24/2018, S. 172, auch kostenlos online lesbar unter ct.de/-4209809

[2] Axel Vahldiek, **Sortieren Sie selbst**, Tipps zu Laufwerksbuchstaben unter Windows, c't 7/2019, S. 134

[3] Axel Vahldiek, **Wo ist sie, und wenn ja, wie oft?**, Windows RE und die Recovery-Partition, c't 18/2021, S. 162

[4] Axel Vahldiek, **Fehlende Laufwerksbuchstaben bei Windows-11-Setup**, c't 2/2022, S. 176, auch kostenlos online lesbar unter ct.de/-6302150

[5] Jan Schüßler, **Ereignisreich**, Die Ereignisanzeige als Wegweiser bei Windows-Problemen nutzen, c't 20/2016, S. 104

[6] Hajo Schulz, **Schnellmesswerk**, c't 18/2021, S. 80

[7] Hajo Schulz, **Die Zeit zurückdrehen**, Datenrettung mit dem c't-Notfall-Windows, c't 22/2019, S. 24

[8] Christof Windeck, **Was ist kaputt?**, So nutzen Sie das c't-Notfall-Windows für die Hardware-Diagnose, c't 2/2022, S. 24

[9] Axel Vahldiek, **Copy & Save**, Windows-Installationen als Klon übertragen oder als Image sichern, c't 22/2019, S. 20

[10] Jan Schüßler, **Dicht und frei**, Windows-Partition mit VeraCrypt verschlüsseln, c't 17/2020, S. 162

[11] Axel Vahldiek, **Mit der Brechstange**, Störrische Windows-Updates wieder deinstallieren, c't 11/2018, S. 168

[12] Axel Vahldiek, **Plattenteiler**, Partitionieren mit Windows-Bordmitteln – Teil 1: Datenträgerverwaltung, c't 2/2018, S. 154

[13] Axel Vahldiek, **Tipp-Schnippler**, Partitionieren mit Windows-Bordmitteln – Teil 2: Diskpart, c't 3/2018, S. 144

[14] Axel Vahldiek, **Vielfach unterteilt**, Die Partitionierung moderner Windows-PCs, c't 5/2018, S. 146

[15] **Titelthema: Windows entschlacken**, Endlich wieder Platz auf der Windows-Partition, c't 8/2018, 5 Artikel ab S. 66

[16] Axel Vahldiek, **Wenn sonst nichts mehr geht**, Probleme lösen mit dem Mini-Betriebssystem Windows PE, c't 10/2018, S. 162

im Explorer nicht zu sehen waren. Das Skript nimmt keinerlei Einfluss auf die Installation auf dem internen Datenträger.
2. In Windows 11 Version 21H2 hatte Microsoft einen Bug eingebaut [4]: Wenn Sie es frisch installiert und dabei dem Setup-Programm das Partitionieren des internen Datenträgers überlassen haben, kann es passieren, dass die Windows-Partition im Explorer des Notfall-Windows nicht auftaucht. Auch hier hilft das Skript „Alles mounten".

Netzwerk verbinden

1. Ist der PC per Kabel mit einem Router verbunden, stellt das Notfallsystem die Verbindung vollautomatisch her.
2. Alternativ können Sie sich auch per WLAN mit dem Netz verbinden, sofern dazu die Eingabe eines Passworts reicht – einen zusätzlichen Nutzernamen können Sie leider nicht eingeben.
3. Für eine WLAN-Verbindung klicken Sie in der Taskleiste im Bereich neben der Uhr auf das Netzwerksymbol.
4. Wählen Sie aus der Liste das gewünschte WLAN zum Verbinden aus.
5. Falls der Treiber für den WLAN-Adapter fehlt, den von der Festplatte nehmen (siehe unten „Treiber nachinstallieren").

Netzlaufwerk verbinden

1. In der Taskleiste doppelt auf das Netzwerksymbol neben der Uhr klicken.
2. Es öffnet sich der „PE Netzwerk Manager". Darin links „Netzlaufwerke" auswählen.
3. Laufwerksbuchstabe wählen, Pfad im Format `\\Server\Freigabe`, Benutzername und Kennwort eintippen, oben auf „Verbinden" klicken.

Treiber nachinstallieren

1. Vorab: Klappt nicht immer und nur mit Treibern, die ohne Neustart installierbar sind.
2. Im Startmenü unter „Alle Programme/Windows-Bordmittel" den „Geräte-Manager" öffnen, unter „andere Geräte" das Gerät ohne Treiber oder eines mit einer Warnmarkierung ansteuern.
3. In dessen Kontextmenü auf „Treibersoftware aktualisieren" klicken, danach „Auf dem Computer nach Treibersoftware suchen". Den vorgegebenen Pfad („C:\Windows\System32\DriverStore\FileRepository") können Sie belassen, klicken Sie auf „Weiter". Fehlt das Laufwerk C:, hilft die Schritt-für-Schritt-Anleitung „Fehlende Laufwerke einbinden".
4. Falls keine Treiber gefunden werden, das Ganze noch mal von vorn, aber mit anderen Pfaden: „C:\Programme", „C:\Programme (x86)", „C:\Windows", „C:<Herstellername>", … Sind Parallelinstallationen vorhanden, können Sie es entsprechend auch mit „D:\Windows" und so weiter probieren (Laufwerksbuchstaben anpassen).
5. Nach einem Neustart des Notfallsystems ist die Prozedur erneut erforderlich, weil es die Änderungen nicht speichert.

BitLocker-Laufwerk entsperren

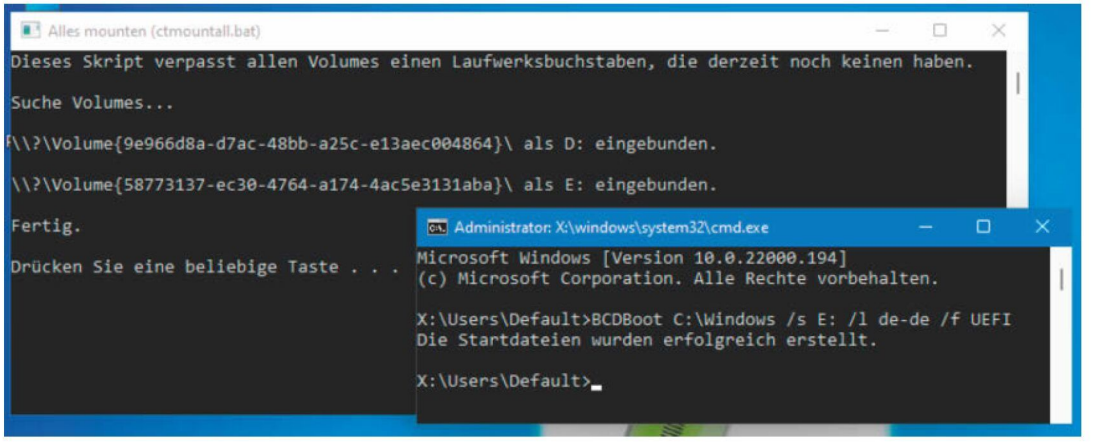
1. Im Explorer im Kontextmenü des Laufwerks auf „Laufwerk entsperren" klicken und das Passwort eingeben.
2. Alternativ: Eingabeaufforderung öffnen (Icon neben dem Startknopf in der Taskleiste). Dort `manage-bde -unlock c: -pw` eingeben (Laufwerksbuchstaben anpassen). Lassen Sie sich nicht davon irritieren, dass beim Eingeben des Kennworts weder Buchstaben noch Sternchen angezeigt werden noch sonst etwas. Das Kennwort mit Enter bestätigen.
3. Bei Bedarf liefert der Aufruf `manage-bde -unlock c: -?` alternative Mechanismen für das Entsperren.

Programme nachrüsten

1. Vorab: Geeignet sind die meisten Programme, die es als portable Version gibt. Solche lassen sich einfach herunterladen und entpacken; sie laufen dann ohne Installation.
2. Booten Sie das Notfall-Windows, starten Sie den Browser Firefox und laden Sie das nachzurüstende portable Programm herunter.
3. Entpacken Sie es auf den Stick mit dem Notfallsystem in den Ordner „Programs". Starten Sie es testhalber. Das entpackte Programm bleibt auch über einen Neustart des Notfallsystems hinweg erhalten.

Windows-Kennwort vergessen

1. Warnung: Sofern Sie Dateien mit der Windows-eigenen NTFS-Dateiverschlüsselung EFS verschlüsselt haben, lassen sich diese nach dieser Prozedur aus Sicherheitsgründen nicht mehr ent-



Bootloader defekt? Ein c't-Skript bindet bei Bedarf mit einem simplen Doppelklick die Partition mit dem Bootloader ein, ein einzelner Kommandozeilenbefehl erzeugt einen neuen Bootloader, und schon startet Windows wieder.

schlüsseln. Falls Sie kein Backup davon haben, sind die Daten dann verloren.

2. Nach dem Booten des Notfallsystems im Startmenü unter „Alle Programme/Passwörter“ das Programm NTPWEdit starten. Achtung: Das Programm entsperrt nur herkömmliche, lokale Konten (für Microsoft-Konten siehe Kasten „Login Unlocker“).
3. Vorausgewählt ist die erste auf dem internen Datenträger erkannte Windows-Installation. Ein Klick auf „Open“ zeigt die Kontonamen.
4. Konto auswählen, „Change password“ klicken, neues Passwort vergeben und bestätigen. Anschließend klicken auf „OK“ und „Save Changes“.
5. Um das Kennwort eines Kontos einer anderen Installation zu ändern, muss deren SAM-Datenbankdatei ausgewählt werden, die jeweils unter \Windows\system32\config zu finden ist. Der Auswahldialog öffnet sich nach einem Klick auf die drei Punkte neben der Pfadangabe.
6. Die Schnell-und-schmutzig-Alternative: PassReset (unter „Alle Programme/Passwörter“) entfernt kurzerhand die Passwörter ausgewählter Konten, vergibt aber keine neuen. Zum Anmelden an ein solches Konto reicht dann das Drücken der Entertaste.

Windows-Bootloader reparieren

1. Aus dem Startmenü unter „Alle Programme/Utilities“ den Eintrag „Alles mounten (ctmountall.bat)“ aufrufen. Das Skript verpasst allen Volumes einen Laufwerksbuchstaben, die derzeit noch keinen haben. Es verwendet dabei von C: über D:, E: und so weiter jeweils das, was frei ist.
2. Starten Sie den Explorer und durchsuchen Sie die Laufwerke. Identifizieren Sie die Windows-Partition und merken Sie sich deren Laufwerksbuchstaben (zum Beispiel C:).
3. Identifizieren Sie im Explorer das Laufwerk mit dem Bootloader. Finden Sie eines, auf dem im Wurzelverzeichnis bloß ein Ordner namens EFI mit Unterordnern namens „Boot“ und „Microsoft“ liegt, merken Sie sich dessen Laufwerksbuchstaben (beispielsweise E:) sowie „UEFI“. Achtung: Bei Linux-Parallelinstallationen können weitere Ordner auf diesem Laufwerk vorhanden sein. Entdecken Sie stattdessen ein Laufwerk mit dem Ordner „Boot“ und der Datei „bootmgr“, merken Sie sich dessen Buchstaben (auch hier diene E: als Beispiel) und „BIOS“.
4. Eingabeaufforderung öffnen (Icon neben dem Startknopf in der Taskleiste).
5. Der Befehl

```
BCDboot C:\Windows /s E: /l de-de /f UEFI
```

restauriert den Bootloader, sodass Windows wieder startet. Passen Sie `C:\Windows` und `E:` (Bootloader-Laufwerk) an. Tauschen Sie gegebenenfalls `UEFI` gegen `BIOS`. Obacht: Linux-Bootloader gehen bei dem Prozedere eventuell verloren und müssen dann ebenfalls restauriert werden. (axv) c't

IMPRESSUM

Redaktion

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

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 Redakteurs-Kürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

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

Konzeption: Jan Schüßler (jss)

Koordination: Pia Ehrhardt (piae), Angela Meyer (anm)

Redaktion: Ronald Eikenberg (rei), Angela Meyer (anm), Jürgen Schmidt (ju), Hajo Schulz (hos), Jan Schüßler (jss), Peter Siering (ps), Axel Vahldiek (axv)

Mitarbeiter dieser Ausgabe: Stephan Bäcker, Markus Richter

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

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

Digitale Produktion: Christine Kreye (Ltg.), Kevin Harte, Thomas Kaltschmidt, Martin Kreft, Pascal Wissner

Fotografie: Andreas Wodrich, Melissa Ramson

Illustration: Rudolf A. Blaha, Frankfurt am Main; Albert Hulm, Berlin; Andreas Martini, Wettin; Moritz Reichartz, Viersen

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, Beate Gerold

Mitglieder der Geschäftsleitung: Jörg Mühle, Falko Ossmann

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: Andre Lux (-299)

Service Sonderdrucke: Julia Conrades (-156)

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

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

Einzelpreis: € 14,90; Schweiz CHF 27.90;
Österreich € 16,40; Luxemburg € 17,10

Erstverkaufstag: 21.03.2023

Hergestellt und produziert mit Xpublisher: www.xpublisher.com

Printed in Germany.

Bild: Andreas Martini

Virensuche mit dem Notfall-Windows

Vom Schnelltest bis zur Intensivtherapie: Mit dem c't-Notfall-Windows besitzen Sie ein universelles Hilfsmittel bei Virenbefall. Wir leiten Sie Schritt für Schritt durch den Heilungsprozess.

Von **Axel Vahldiek**

Die reine Lehre besagt: Wenn bei einem Betriebssystem auch nur der geringste Verdacht auf einen Virenbefall besteht, gehört es gelöscht und neu aufgesetzt. Oder, noch besser, Sie ersetzen es durch ein vor dem Virenbefall erstelltes Backup. Genau für solche Situationen ist es ja da. So jedenfalls die Theorie, denn in der Praxis ist ein Backup dann eben doch nicht da oder veraltet, defekt, unvollständig … Doch selbst wenn Sie über ein rechtzeitig angefertigtes, aktuelles, vollständiges und getestetes (!) Backup verfügen, sieht es bei um Hilfe rufenden Freunden und Verwandten meist anders aus.

Dann schlägt die Stunde des Notfall-Windows. Die aktuelle Version hat vier Virenscanner an Bord. Damit können Sie versuchen, Viren auch ohne Neuinstallation loszuwerden. Weil das Notfallsystem vom Stick startet, hat der gesuchte Schädling auf dem internen Datenträger keine Chance, die Suche zu sabotieren – er läuft ja nicht.

Schnelltest

Eine gründliche Virenprüfung dauert je nach Hardware und zu prüfender Datenmenge gern mal Stunden. Zu ersten Ergebnissen können Sie aber weit schneller gelangen, denn unser Notfallsystem bietet eine Art Virenschnelltest. Der ist zwar bei Weitem nicht so gründlich und wenn dabei keine Schädlinge zu entdecken sind, können trotzdem welche vorhanden sein.

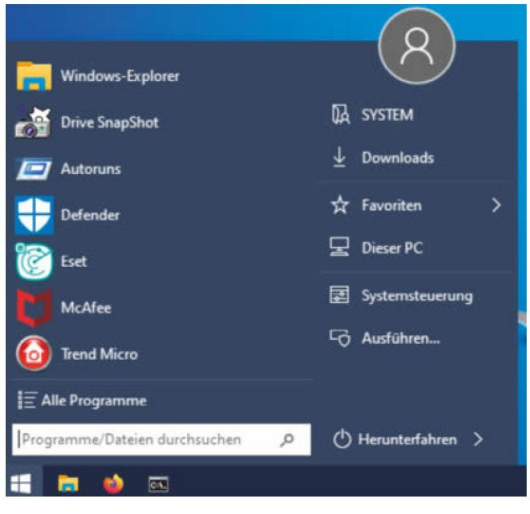
Aber wenn Sie dabei Auffälligkeiten entdecken, dann wissen Sie wenigstens, dass die gründliche Suche mit den Virenscannern lohnt. Der Trick: Das Sysinternals-Programm „Autoruns“ kann alle Autostart-Einträge der Windows-Installation durchforsten und die gefundenen Programme auf einen Schlag von über 70 Scannern prüfen lassen. Das gelingt im Idealfall sogar rasend schnell, denn Autoruns lädt dazu Hashes der ausführbaren Dateien bei VirusTotal.com hoch, die sich viel schneller prüfen lassen als die kompletten Dateien. Das ist ein von Google betriebener Dienst. Nur bei dort unbekannten Hashes ist der Upload der zu prüfenden Datei selbst erforderlich.

Noch ein Schnelltest

Auch beliebige einzelne Dateien können Sie mit dem Notfall-Windows einem Schnelltest unterziehen. Klicken Sie dazu im Kontextmenü einer verdächtigen Datei auf „Senden an/Sigcheck“. Sigcheck ist ebenfalls ein Programm von Sysinternals. Es prüft erstens die Signatur der Datei, bildet zweitens diverse Prüfsummen (MD5, SHA1, SHA256 ...) und lädt drittens ebenfalls einen Hash bei VirusTotal hoch. Das Ergebnis erscheint in einer zwar hässlichen, aber funktionalen Eingabeaufforderung. Was die Interpretation der Ergebnisse betrifft: Es gilt im Wesentlichen dasselbe wie bei Autoruns. Sofern die Datei von einem bekannten Anbieter signiert ist und kein Virenscanner etwas zu meckern hat, ist sie wahrscheinlich harmlos – obwohl es keine Garantie gibt, dass dem wirklich so ist. Wenn hingegen die Signatur fehlt oder Seltsamkeiten aufweist, sollten Sie vorsichtig sein.

Vorbereitungen

1. Falls auch nur der geringste Verdacht auf einen Erpressungstrojaner besteht: Rechner sofort hart ausschalten! Anschließend Notfall-Windows booten und alles an Daten retten, was noch unverschlüsselt ist.
2. Sonst das auf der Platte installierte Windows laufen lassen, aber alle Netzwerkverbindungen kappen.
3. Explorer öffnen, im Kontextmenü der Windows-Partition (üblicherweise C:) „Eigenschaften“ auswählen, auf „Bereinigen“ klicken, um die Datenträgerbereinigung zu starten. Dort „Systemdateien bereinigen“ anklicken, Nachfrage bestätigen, alle Häkchen setzen, Nachfragen bestätigen.
4. Browser-Cache leeren. Firefox: „Einstellungen/Datenschutz und Sicherheit/Chronik löschen“. Edge: im Drei-Punkte-Menü klicken auf „Einstellungen/Datenschutz, Suche und Dienste/Browserdaten jetzt löschen: Zu löschende Elemente auswählen“. Chrome: Strg+Umschalt+Entf drücken, den „Zeitraum“ auf „Gesamte Zeit“ umstellen, „Daten löschen“ anklicken.
5. Im Mail-Client Papierkorb und Spam-Ordner leeren.



Im Startmenü des Notfall-Windows finden Sie „Autoruns“ für einen Virenschnelltest und gleich vier Virenscanner für eine gründliche Schädlingssuche.

Virenschnelltest mit Autoruns

1. Notfall-Windows booten, Netzwerkverbindung herstellen, Windows-Partition auf der Festplatte identifizieren (siehe Artikel „Probleme lösen mit dem Notfall-Windows“ ab S. 64).
2. Aus dem Startmenü „Autoruns“ aufrufen.
3. Laufenden Scan bei Eile durch Drücken der Esc-Taste abbrechen.

4. In der Menüleiste unter „Options“ auf „Scan Options“ klicken. Häkchen vor „Check VirusTotal.com“ setzen. Auf „Rescan“ klicken.
5. In der Menüleiste auf „File“ und „Analyze Offline System“ klicken. Im Dialog hinter „System Root“ den Pfad zum Windows-Ordner eintragen (üblicherweise `C:\Windows`), hinter „User Profile“ den Pfad des Nutzerprofils (`C:\Users\<Kontoname>`).
6. Nach dem Scan in der Spalte „Virus Total“ nachschauen (Anzeige dazu eventuell nach rechts scrollen): Steht hier hinter einem Autostart-Eintrag „0/76“, haben null Scanner etwas gefunden. Die Zahl hinter dem Schrägstrich ist die Anzahl der prüfenden Scanner und variiert, entscheidend ist die Zahl vor dem Schrägstrich. Steht hier eine andere Zahl als 0, kommts drauf an: Ist es nur eine 1, handelt es sich vermutlich um einen Fehlalarm, bei 2 oder 3 womöglich auch. Spätestens bei höheren Zahlen ist aber eine gründliche Virensuche angebracht.
7. Sollten auf dem PC verschiedene Nutzerkonten verwendet werden, Vorgang mit deren Nutzerprofilen wiederholen.
8. Bei Windows-Parallelinstallationen bitte beachten: Jede Windows-Installation muss vom Notfall-Windows mit dem Laufwerksbuchstaben eingebunden sein, den sie selbst zu haben glaubt. Wenn sich also beide Installationen jeweils auf C: wähnen, wird sie das Notfall-Windows trotzdem als C: und D: einbinden, und dann müssen Sie vor der Prüfung von D: mit Autoruns die Buchstaben D: und C: in der Datenträgerverwaltung tauschen. Details dazu haben wir in [1] beschrieben.

Virenschnelltest mit Sigcheck

1. Notfall-Windows booten, Netzwerkverbindung herstellen, Windows-Partition auf der Festplatte identifizieren (siehe Artikel „Probleme lösen mit dem Notfall-Windows“ ab S. 64).
2. Im Explorer verdächtige Datei auswählen, in ihrem Kontextmenü auf „Senden an“ und „Sigcheck“ klicken. Die Ausgabe erscheint in einer Eingabeaufforderung.
3. Zeile „Verified“ prüfen: „Signed“ deutet auf Vertrauenswürdigkeit hin. Alles andere ist ein Alarmsignal, vor allem, wenn die Datei von einer großen Firma wie Microsoft und Google stammen soll. Das gilt für „Unsigned“ ebenso wie für eine vorhandene, aber als nicht vertrauenswürdig eingestufte Signatur (beispielsweise: „Die digitale Signatur des Objekts konnte nicht bestätigt werden“, „Ein Zertifikat wurde explizit durch den Aussteller gesperrt“ oder „Eine Zertifikatskette zu einer vertrauenswürdigen Stammzertifizierungsstelle konnte nicht aufgebaut werden“).
4. Steht ziemlich weit unten in der Zeile „VT detection“ als Ergebnis „0/76“, hat keiner der auf VirusTotal.com versammelten Scanner etwas Verdächtiges gefunden. Die Zahl hinter dem Schrägstrich ist die Anzahl der beteiligten Scanner und variiert, entscheidend ist die Zahl vor dem Schrägstrich. Der Link zur Ergebnisseite der Prüfung steht eine Zeile tiefer. Sie können ihn wie gewohnt mit der Maus markieren, per Strg+C in die Zwischenablage kopieren und im Firefox in die Adresszeile einfügen.

Virensuche …

1. Notfall-Windows booten, Windows-Partition auf der Festplatte identifizieren (siehe Artikel „Probleme lösen mit dem Notfall-Windows“ ab S. 64).
2. Wichtig: Vor dem Start eines Scanners Netzwerkverbindung herstellen.
3. Scanner nacheinander (!) laufen lassen (siehe folgende Anleitungen). Die Reihenfolge ist egal. Vor jedem weiteren Suchlauf das Notfallsystem neu starten und wieder bei der Anleitung „Virensuche …“ beginnen.

… mit Defender Offline

1. Vorab: Der Defender kann nur 64-Bit-Windows-Installationen prüfen. Falls bei Ihnen ein 32-Bit-Windows installiert ist: weiter beim nächsten Scanner.
2. Aus dem Startmenü „Defender“ aufrufen. Das Programm beginnt sofort mit der Virensuche, brechen Sie diese durch einen Klick auf „Cancel scan“ ab.
3. Im Reiter „Update“ auf „Update definitions“ klicken. Warten, bis die frischen Virendefinitionen geladen sind.
4. Im Reiter „Home“ unter „Scan Options“ „Custom“ auswählen, auf „Scan now“ klicken.
5. Laufwerke auswählen, auf „OK“ klicken, die Virensuche beginnt.

… mit Eset Online Scanner

1. Nach dem Booten des Notfall-Windows einige Sekunden warten. Dann aus dem Startmenü

„Eset“ aufrufen, auf „Erste Schritte“ klicken, Nutzungsbedingungen akzeptieren.
2. Es kann passieren, dass die Software als Nächstes eine neue Produktversion von sich herunterlädt und sich dann beendet. Wie sich die künftige Version verhalten wird, lässt sich nicht vorhersagen, aber falls es wie bisher läuft, geht es so weiter: Programm einfach erneut starten und, wichtig: Häkchen vor „Neueste Produktversion herunterladen“ entfernen.
3. Im Dialog „Bevor wir beginnen“ nach Wunsch entscheiden.
4. „Benutzerdefinierter Scan“ anklicken, Laufwerke auswählen und dann auf „Speichern und Fortfahren“ klicken.
5. Über Quarantäne von potenziell unerwünschten Anwendungen entscheiden (Vorsicht, alle Dateien in der Quarantäne werden beim Beenden des Notfall-Windows gelöscht!). Auf den Link „Erweiterte Einstellungen“ klicken, Einstellungen prüfen, auf den Zurück-Knopf oben klicken.
6. Auf „Prüfung starten“ klicken. Programm aktualisiert sich, die Virensuche beginnt.

☑ … mit Trend Micro HouseCall

1. Aus dem Startmenü „Trend Micro“ aufrufen. Mit Klick auf „Next“ die Datenschutz-, im nächsten Dialog die Lizenzbestimmungen bestätigen.
2. Auf den Link „Settings“ klicken. Im Reiter „Smart Feedback“ auf Wunsch das Häkchen vor „Enable Trend Micro Smart Feedback“ entfernen (sonst schickt die Software Informationen zu Ihren Dateien an den Hersteller).
3. In den Settings im Reiter „Scan Type“ „Custom Scan“ auswählen, Häkchen vor die zu prüfenden Laufwerke setzen, mit „OK“ bestätigen.
4. Wahlweise Häkchen vor „Include my home Network“ entfernen oder lassen, auf „Scan now“ klicken. Die Virensuche beginnt.

☑ … mit McAfee Stinger

1. Aus dem Startmenü „McAfee“ aufrufen. Nutzungsbedingungen akzeptieren.
2. Oben rechts auf „Advanced“ und dann auf „Settings“ klicken. Unterhalb von „Scan Targets“ und „Scan Options“ alles anhaken. Unterhalb von „On threat detection“ („was tun bei Virenfund?“) wählen: „Remove“ verschiebt in Quarantäne, „Report“ weist nur auf den Fund hin. Letzteres ist für eine weitere Analyse sinnvoll (siehe Schritt-für-Schritt-Anleitung „Virenfund“). Pull-down-Menü „GTI settings – Sensitivity“ auf „Very High“ ändern (also auf das höchste Heuristik-Level). „Save“ anklicken.
3. Unterhalb der Schaltfläche „Scan“ auf den Link „Customize my scan“ klicken. Laufwerke auswählen, „Scan“ anklicken, Virensuche startet.
4. Falls Sie nach dem Ende des Suchlaufs weitere Programme starten wollen, klicken Sie mit der rechten Maustaste auf das Schildsymbol im Infobereich der Taskleiste (neben der Uhr), wählen Sie „Remove Real Protect“ und bestätigen Sie die Nachfrage. Bei unseren Tests kam es sonst zu Abstürzen von Firefox & Co.

☑ Virenfund

1. Entscheiden, ob die infizierten Dateien in Quarantäne geschoben, gelöscht oder ignoriert werden sollen. Obacht: Die Quarantäne wird beim Beenden des Notfall-Windows gelöscht!
2. Infizierte Datei für genauere Analyse in Firefox bei VirusTotal.com hochladen.
3. Auf Wunsch: Infizierte Datei für weitere Recherche an einen sicheren Ort kopieren, am besten per kennwortgeschütztem ZIP-Archiv, welches Sie mit 7-Zip erstellen (im Startmenü unter „Alle Programme/Utilities“).
4. Infizierte Datei löschen.

☑ Nacharbeiten bei Virenfund

1. Noch unter dem Notfallsystem die Hosts-Datei kontrollieren (C:\Windows\System32\Drivers\etc): per Rechtsklick mit Notepad öffnen, dann unbekannte Zeilen mit # auskommentieren oder löschen.
2. Auf 64-BitSystemen auch prüfen, ob es unter „C:\Windows\SYSwow64\Drivers\etc“ eine weitere Datei namens „hosts“ gibt; die dann genauso behandeln.
3. Installiertes Windows starten.
4. Kontrollieren: Firewall, Virenscanner, Plug-ins von Browser und Mail-Client, Proxy-Einstellungen von Windows, Browser und Mail-Client.
5. Erst danach Netzwerkverbindung wieder herstellen.
6. Aktualisieren: Windows Update, Virenscanner, Browser, MailClient, PDF-Reader. Das gelingt bei modernen Windows übrigens auf einen Schlag mit `winget upgrade --all` [2].
7. Möglichst noch prüfen: Netzwerkfreigaben, Autostarts, laufende Prozesse. (axv) c't

Literatur

[1] Axel Vahldiek, **c't-Notfall-Windows: Autoruns und Parallelinstallation**, c't 4/2021, S. 172, auch kostenlos online lesbar unter ct.de/-5022965

[2] Hajo Schulz, **Power-Updates**, Bequemere Programm-Updates mit WinGet, c't 20/2022, S. 148

Bild: Moritz Reichartz

PowerShell fürs c't-Notfall-Windows

Viele Windows-Anwender und -Administratoren schwören für ihre Arbeit auf die PowerShell. Auch im c't-Notfall-Windows ist sie enthalten. Hier verraten wir die Tipps, die Ihnen dazu gerade noch gefehlt haben.

Von **Hajo Schulz**

Professionelle Administratoren verbringen einen Gutteil ihrer Arbeitszeit in der PowerShell, Microsofts aktueller Interpretation eines Befehls-Interpreters. Aber auch bei ambitionierten Normalanwendern setzt sich die PowerShell mehr und mehr gegen die althergebrachte Eingabeaufforderung durch. Etliche Benutzer unseres c't-Notfall-Windows haben sich deshalb gewünscht, die PowerShell auch dort verwenden zu können. Gerade wenn der Stresspegel ohnehin schon besonders hoch ist, wollen sie nicht auf die gewohnte Umgebung verzichten – zum Beispiel, wenn der Rechner wegen eines Hardwaredefekts oder eines Virenbefalls die Arbeit verweigert: Dann ist das c't-Notfall-Windows häufig der letzte Rettungsanker. Den Wunsch erfüllen wir gern.

In erster Näherung steht die PowerShell nach dem Erstellen des c't-Notfall-Windows „einfach so“

zur Verfügung und lässt sich auch fast genauso benutzen, wie Sie das aus dem normalen Betrieb gewohnt sind. Beim zweiten Hinsehen gibt es aber ein paar Einschränkungen. Außerdem stellen wir ein paar Schräubchen vor, an denen Sie drehen können, um die PowerShell an Ihre Bedürfnisse anzupassen.

Einbauen

Wie im Artikel „Das eigene Notfallsystem bauen“ ab Seite 38 beschrieben, nimmt Ihnen beim Herstellen des Notfall-Sticks das Programm „PEBakery“ die meisten Arbeitsschritte ab. Dessen Oberfläche zeigt auf der linken Seite ähnlich wie der Windows Explorer eine Baumansicht, in der Sie im Zweig „Applications“ alle mitgelieferten Programme finden, die PowerShell steckt im Unterordner „System Tools“. Die Optionen auf der Seite für die PowerShell sollten selbsterklärend sein. Wenn Sie sich gerade das erste Mal mit dem c’t-Notfall-Windows beschäftigen oder es anlässlich dieses Artikels neu bauen, tun Sie gut daran, unter „Program Version“ die aktuelle Versionsnummer der PowerShell einzutragen – bei Redaktionsschluss war die 7.3.2 aktuell.

Benutzen

Nach dem Start des c’t-Notfall-Windows finden Sie die PowerShell im Startmenü unter „Alle Programme/Windows-Bordmittel“. Funktionsweise und Befehlsumfang entsprechen im Großen und Ganzen dem, was Sie von der Benutzung unter einem normalen Windows gewohnt sind. Einige Befehle verweigern aber die Arbeit mit Fehlermeldungen wie „Ungültiger Namespace“ oder „The module could not be loaded“. Bei den meisten betroffenen Kommandos lässt sich das jedoch verschmerzen: Befehle, die sich nur auf das aktuell laufende Windows oder auf das Active Directory beziehen, in dem dieses Mitglied ist, ergeben innerhalb des Notfall-Windows ohnehin wenig Sinn.

Dass es überhaupt zu solchen Fehlermeldungen kommt, liegt an der Art und Weise, wie wir die PowerShell ins c’t-Notfall-Windows eingebaut haben. Das .NET Framework zu integrieren wäre unschön, denn das würde das Notfall-System enorm aufblähen. Damit scheidet auch die normalerweise in das Betriebssystem eingebaute Windows PowerShell aus, denn die fußt auf dem .NET Framework.

Die PowerShell 7 verwendet dagegen nicht die von Microsoft für Windows bereitgestellte .NET-Umgebung, sondern deren Open-Source-Implementierung [1]. Derartige Programme zeichnen sich dadurch aus, dass sie sich nicht auf ein komplettes, bereits im System installiertes .NET verlassen. Stattdessen bringen sie die Komponenten, die sie benötigen, selbst mit und beschränken sich dabei auf das, was sie wirklich verwenden. Deshalb gibt es im c’t-Notfall-Windows also nicht die Windows PowerShell, sondern die PowerShell 7.

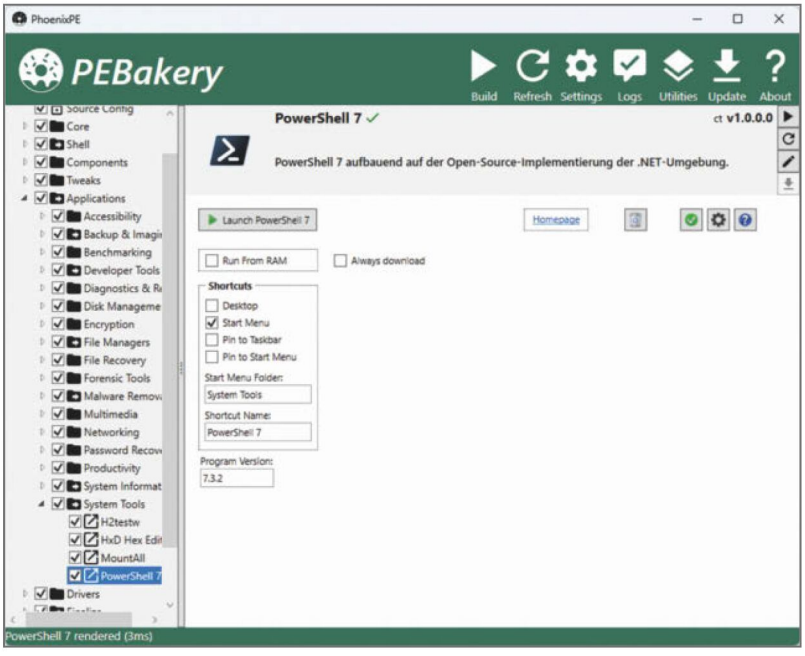
Deren Entwickler haben zwar den Kern und grundlegende Module der PowerShell – ebenfalls als Open Source – neu programmiert, aber bei Weitem nicht alles, was in der Windows PowerShell enthalten ist. Unter einem normalen Windows bedient sich die PowerShell 7 eines Tricks, um Befehle abzuarbeiten, die sie selbst nicht kennt: Sie startet im Hintergrund die Windows PowerShell und verbindet sich in einer Art lokaler Remote-Sitzung mit ihr. Über diesen Kanal schickt sie die ihr unbekannten Befehle und sammelt die Ergebnisse ein.

Die Windows PowerShell besteht ihrerseits aus zahlreichen Modulen. Ein Teil davon funktioniert auch ohne Remoting direkt in der PowerShell 7 – und das ist genau das, was wir uns für das c’t-Notfall-Windows zunutze gemacht haben: Beim Einbauen der PowerShell 7 sorgt die PEBakery einfach dafür, dass auch der komplette Modul-Ordner der Windows PowerShell mit auf dem Stick landet. Ohne vorhandene Windows PowerShell versucht die PowerShell 7, diese Module direkt zu benutzen – und das gelingt ihr bei einigen, aber wegen der anderen .NET-Version leider nicht bei allen. So kommt es, dass die PowerShell im Notfall-Windows ein paar Befehle nicht verarbeiten kann, die Sie aus dem normalen Betrieb kennen. Etwas Schlimmeres als eine Meldung über den Misserfolg ist uns beim Ausprobieren aber noch nie widerfahren. Es spricht also nichts dagegen, dass Sie Ihre gewohnten Befehle einfach zu benutzen versuchen; in den meisten Fällen wird das klappen.

Was auf jeden Fall funktioniert, sind sämtliche Befehle aus dem Kern der PowerShell 7 (eine Liste liefert `Get-Command -Module Microsoft.PowerShell.Core`) sowie die Cmdlets aus ihren eigenen Modulen, die Sie sich mit

```
Get-Module -ListAvailable |
  ? Path -Like "$PSHOME*" |
  % {Get-Command -Module $_}
```

anzeigen lassen können. Das sollten so ziemlich alle Cmdlets sein, die Sie für den täglichen Kleinkram



Wenn Sie das c't-Notfall-Windows neu erstellen, sollten Sie die Versionsnummer der eingebauten PowerShell gelegentlich aktualisieren.

wie das Dateimanagement oder die Ausgabe von Protokollen, aber etwa auch für die Skriptsteuerung brauchen.

Auswärtsspiel

Wie oben bereits angedeutet ergeben allerdings nicht alle Cmdlets, die man aufrufen könnte, innerhalb des c't-Notfall-Windows Sinn: Befehle wie `Get-Process` oder `Get-CIMInstance` liefern ja Informationen über das gerade laufende Windows. An die Zustände, die beim Start des regulär installierten Windows herrschen, kommt man damit also gar nicht heran – und die im Notfall-Windows interessieren nur in Ausnahmefällen.

Anders sieht es schon bei Objekten aus, die sich im Dateisystem wiederfinden: Fehlende Dateien oder solche mit verhunzten Zugriffsrechten kann man aus dem Notfall-Windows heraus aufspüren und eventuell restaurieren. Und weil man dort grundsätzlich mit den Rechten des lokalen Systems unterwegs ist, hat man Zugriff auf alle Dateien und Ordner. Das kommt gelegen, wenn man zum Beispiel Dateien aus Benutzerprofilen herauskopieren will: Manchmal ist das der letzte Rettungsanker, um sie in Sicherheit zu bringen, bevor man das installierte Windows abschreibt und die Platte putzt oder ersetzt. Achtung: Uneingeschränkte Rechte bedeuten auch, dass man beim Löschen oder Verschieben von Dateien besondere Vorsicht walten lassen sollte. Die PowerShell fragt in der Regel nicht nach, und gelöschte Dateien sind wirklich futsch – `Remove-Item` benutzt keinen Papierkorb!

Irgendwo zwischen Informationen zum laufenden System einerseits und dem Dateisystem andererseits sind Features wie die Registry oder die Ereignisanzeige einzuordnen: Deren Inhalte liegen auf dem Systemlaufwerk, ihr internes Format kennt aber nur Windows, und wirklich benutzbar sind sie nur, wenn sie in das gerade laufende System eingebunden sind. An die Objekte des Host-Systems kommt man mit der PowerShell heran, der Weg dorthin ist aber ein bisschen steinig.

Event Log

Zum Auslesen von Systemprotokollen kennt die PowerShell den Befehl `Get-WinEvent`. Normalerweise

gibt man ihm über den Parameter `LogName` den Namen des Protokolls mit, auf das man zugreifen möchte. Gemeint sind damit immer Logs des gerade laufenden Systems – das c't-Notfall-Windows schreibt aber gar keine Protokolle. Alternativ kennt `Get-WinEvent` auch den Parameter `Path`, mit dem man direkt eine Log-Datei aus beliebiger Quelle angeben kann. Windows speichert die Protokolle auf dem Systemlaufwerk im Verzeichnis \Windows\System32\winevt\Logs in Dateien mit mehr oder weniger sprechenden Namen und der Endung .evtx. Auch im Notfall-Windows bekommt das Systemlaufwerk des fest installierten Windows meist den Buchstaben C:. Im Zweifel können Sie es per Explorer identifizieren.

Wie man sich Ereignissen des Windows auf der Festplatte nähert, erklärt am besten ein Beispiel: Angenommen, Sie wollen wissen, ob auf Ihrem Rechner der Windows Defender in letzter Zeit eine Malware gefunden hat. Die zugehörige Log-Datei heißt „Microsoft-Windows-WindowsDefender%4Operational.evtx". Weil `Get-WinEvent` im `Path` auch Platzhalterzeichen akzeptiert, braucht man den Namen aber gar nicht so genau zu wissen. Ein erster Anlauf, um die Ereignisse anzuzeigen, die der Defender protokolliert hat, könnte also folgendermaßen aussehen:

```
$logs = 'C:\Windows\System32\winevt\Logs'
Get-WinEvent -Path "$logs\*Defender*"
```

Das Ergebnis ist eine meist sehr lange Liste größtenteils nutzloser Einträge. Um etwas damit anfangen zu können, muss man sie filtern. Wie bei vielen Protokollen ist auch im Falle des Defender die Ereignis-ID ein sinnvolles Filterkriterium: Der Online-Dokumentation (siehe ct.de/wqxr) kann man entnehmen, dass sie 1006, 1015 oder 1116 lautet, wenn der Defender eine infizierte Datei oder auffälliges Verhalten findet. Sie könnten die Liste also per Pipeline an einen `where`-Ausdruck verfüttern, der die passenden Meldungen herauspickt. Schneller eingetippt, aber vor allem schneller ausgeführt ist ein Filter im Log selbst. In der PowerShell bauen Sie sich dazu eine passende Hashtable mit Filterkriterien zusammen und übergeben die in einem Rutsch an `Get-WinEvent`:

```
$filter = @{
  Path="$logs\*Defender*";
  Id=1006, 1015, 1116;
}
Get-WinEvent -FilterHashtable $filter
```

Sofern das Ergebnis nicht leer ist, der Defender also Virenfunde protokolliert hat, könnten Sie die Liste in einer PowerShell in einem normalen Windows jetzt über die Pipeline per `Format-List` oder `fl *` ausgeben und hätten die gesuchten Informationen. Dem Notfall-Windows fehlen aber die Eventlog-Provider, die nicht nur für das Protokollieren von Ereignissen zuständig sind, sondern auch dafür, das Feld `Message` in abgefragten Ereignissen auszufüllen – im Notfall-Windows bleibt es einfach leer. Dabei stecken in den Objekten, die `Get-WinEvent` zurückliefert, meist noch weitere Informationen, im Fall von Defender-Events etwa der Name der infizierten Datei.

Angenommen, Sie haben einen Eventlog-Eintrag im Rahmen einer `foreach`-Schleife oder durch eine Zuweisung wie `$entry = (Get-WinEvent …)[0]` in der Variable `$entry` gespeichert. Dann liefert `$entry.Properties` eine Liste der erweiterten Eigenschaften dieses Eintrags, allerdings ohne zu verraten, was die einzelnen Felder bedeuten. Um auch die Feldnamen zu sehen, haben wir keine andere Lösung als einen Umweg über die XML-Repräsentation des Event-Objekts gefunden. Er führt um folgende Ecken: `$entry.ToXml()` liefert eine Zeichenkette in XML-Syntax, die Sie gleich wieder interpretieren lassen:

```
$xml = [Xml]$entry.ToXml()
```

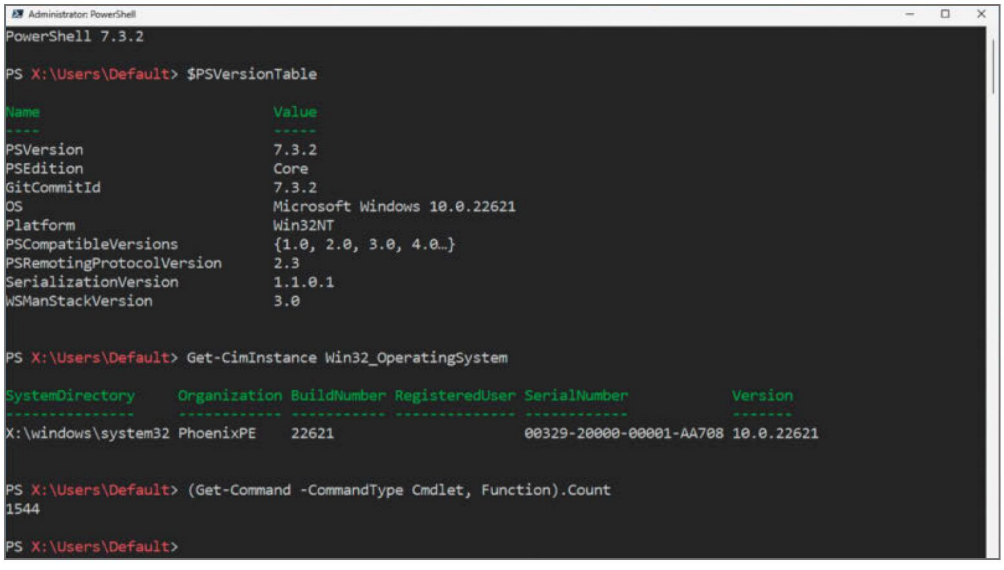
Drei Ebenen tief verschachtelt finden Sie dort schließlich die gesuchten Angaben, nämlich in:

```
$xml.Event.EventData.Data
```

Sollten in der Ausgabe einzelne Felder durch die beschränkte Fensterbreite abgeschnitten sein, können Sie noch `| Format-List` anhängen.

Registry

Über die Art und Weise, wie die PowerShell mit Registry-Einträgen umgeht, gibt es geteilte Meinungen. In aller Kürze: Registry-Schlüssel verhalten sich wie Dateiordner, zur Navigation und zum Bearbeiten verwendet man dieselben Befehle wie im Dateisystem, als Wurzel-Ordner gibt es die beiden virtuellen Laufwerke HKLM: und HKCU:. Die Analogie endet bei Registry-Werten: Sie stellen sich nicht als Dateien dar, sondern als Attribute der Schlüssel. Die Befehle zum Auslesen, Ändern und Löschen von Einträgen sind `Get-ItemProperty` (oder dessen Alias `gp`), `Set-ItemProperty` (kurz `sp`) und `Remove-ItemProperty` (`rp`).



Auch im c't-Notfall-Windows kennt die PowerShell eine erkleckliche Anzahl an Befehlen und die meisten funktionieren wie gewohnt.

Normalerweise greift man mit diesen Befehlen – oder auch mit dem Registry-Editor – auf die Registrierung des gerade laufenden Windows zu, das gilt auch für das c't-Notfall-Windows. Gespeichert sind die Inhalte der Registry aber im Dateisystem, und zwar in den Hive-Dateien – wo genau die liegen, können Sie zum Beispiel in [2] nachlesen. Mit dem Menübefehl „Datei/Struktur laden" des Registry-Editors kann man nun eine solche Hive-Datei zeitweise in die eigene Registry einbinden: benutzerspezifische Registry-Äste unter HKEY_USERS und systemweite unter HKEY_LOCAL_MACHINE. Den Namen, den der Ast in der aktuellen Registry bekommen soll, kann man dabei frei wählen. Mit dem Menübefehl „Datei/Struktur entfernen" kann – und sollte! – man die Datei wieder freigeben, wenn man sie nicht mehr braucht.

Für diesen Mechanismus bringt die PowerShell keine eigenen Kommandos mit. Will man per Skript auf eine fremde Registry zugreifen, ist man zum Laden und Entladen der Hive-Dateien daher auf das Programm `reg` angewiesen, das eigentlich für Batch-Dateien gedacht ist. Damit lädt man nach dem Schema

```
reg load HKLM\Keyname "C:\Pfad\zur\Hivedatei"
```

eine Hive-Datei und entlädt sie mit

```
reg unload HKLM\Keyname
```

nach getaner Arbeit wieder. Zum Auslesen und Bearbeiten der Registry per PowerShell lautet unsere Empfehlung: Bleiben Sie am besten bei `reg` und seinen Unterbefehlen; eine Liste mit Anwendungsbeispielen liefert `reg /?`. Sie müssen deshalb ja nicht gleich zu Batch-Dateien zurückkehren: Die Ausgaben von `reg query`-Aufrufen lassen sich auch bequem etwa mit regulären Ausdrücken zerpflücken. Und statt des aus Batch-Dateien gewohnten

```
if errorlevel 1 ...
```

schreiben Sie in einem PowerShell-Skript einfach:

```
if($LASTEXITCODE -ge 1) { ...
```

Sollten Sie der Registry trotzdem mit den eigentlich dafür vorgesehenen Mitteln zu Leibe rücken wollen, sind Ihnen vielleicht die folgenden zwei Hinweise nützlich: Zum einen gibt es in der PowerShell standardmäßig kein virtuelles Laufwerk, mit dem Sie auf den Registry-Schlüssel HKEY_USERS zugreifen können. Das lässt sich aber recht einfach mit dem Aufruf

```
New-PSDrive HKU -PSProvider Registry ↵
↳-Root HKEY_USERS -EA SilentlyContinue
```

nachrüsten. Den Inhalt einer in diesen Schlüssel eingebundenen Hive-Datei finden Sie anschließend unter HKU:\.

Der zweite Tipp (und der eigentliche Grund für unsere Empfehlung, bei `reg` zu bleiben): Nachdem Sie in einem externen Registry-Ast mit Befehlen wie `Get-Item` unterwegs waren, werden Sie bei dem Versuch, ihn mit `reg unload` wieder freizugeben, gelegentlich einen Fehler der Klasse „Zugriff verweigert“ ernten. Den Grund dafür und die Maßnahmen dagegen zu beschreiben, würde hier den Rahmen sprengen. Eine ziemlich ausführliche Beschreibung haben wir auf der Webseite von Evgenij Smirnov gefunden – den Link gibts unter ct.de/wqxr. Wenn Sie dieser Fehler ereilt, ist das einfachste Mittel dagegen, die PowerShell zu schließen und den Befehl in einem neu geöffneten Fenster erneut einzugeben. Alternativ können Sie den Registry-Ast nach dem Beenden der PowerShell auch per Registry-Editor entladen. Die Fehlermeldung einfach zu ignorieren oder auf das `reg unload` gleich ganz zu verzichten, ist keine gute Idee: Dadurch können die Registry-Dateien der bearbeiteten Windows-Installation Schaden nehmen. Außerdem werden eventuelle Änderungen, die Sie vorgenommen haben, erst beim Entladen sicher auf die Platte geschrieben.

Viel Erfolg!

Zugegeben: Ein bisschen frickelig ist die Art und Weise schon, wie wir die PowerShell in das c’t-Notfall-Windows eingebaut haben. Bei unseren Versuchen hat sie jedoch meist zufriedenstellend funktioniert. Aber die finden ja auch unter Laborbedingungen statt.

Umso mehr interessiert uns, welche Erfahrungen Sie machen: Wobei hat Ihnen die PowerShell geholfen, wo sind Sie an Grenzen gestoßen? Gibt es vielleicht Skripte, die Sie sich speziell für den Einsatz im Notfall-Windows geschrieben haben? Ihre Erfahrungen und Meinungen sind im Forum zu diesem Artikel willkommen, das wir unter ct.de/wqxr verlinkt haben. (hos) ct

Literatur

[1] Hajo Schulz, **FAQ: PowerShell**, c’t 25/2021, S. 178

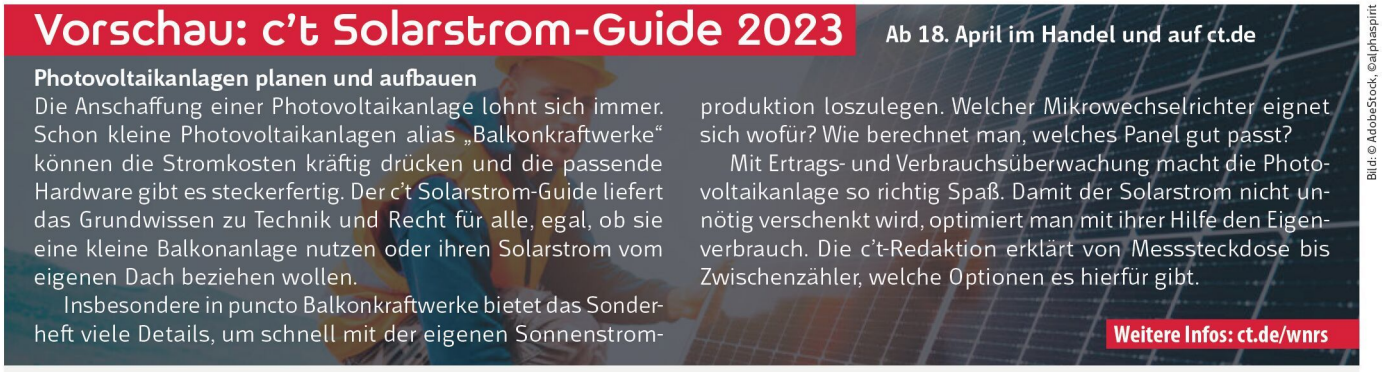
[2] Hajo Schulz, **Registratur**, Was Sie über die Windows-Registry wissen müssen, c’t 17/2021, S. 144

Zusätzliche Dokumentation, Artikelforum

ct.de/wqxr

Vorschau: c't Solarstrom-Guide 2023

Ab 18. April im Handel und auf ct.de



Photovoltaikanlagen planen und aufbauen

Die Anschaffung einer Photovoltaikanlage lohnt sich immer. Schon kleine Photovoltaikanlagen alias „Balkonkraftwerke" können die Stromkosten kräftig drücken und die passende Hardware gibt es steckerfertig. Der c't Solarstrom-Guide liefert das Grundwissen zu Technik und Recht für alle, egal, ob sie eine kleine Balkonanlage nutzen oder ihren Solarstrom vom eigenen Dach beziehen wollen.

Insbesondere in puncto Balkonkraftwerke bietet das Sonderheft viele Details, um schnell mit der eigenen Sonnenstromproduktion loszulegen. Welcher Mikrowechselrichter eignet sich wofür? Wie berechnet man, welches Panel gut passt?

Mit Ertrags- und Verbrauchsüberwachung macht die Photovoltaikanlage so richtig Spaß. Damit der Solarstrom nicht unnötig verschenkt wird, optimiert man mit ihrer Hilfe den Eigenverbrauch. Die c't-Redaktion erklärt von Messsteckdose bis Zwischenzähler, welche Optionen es hierfür gibt.

Weitere Infos: ct.de/wnrs

Bild: © AdobeStock, ©alphaspirit

Themenschwerpunkte

Photovoltaik für alle

- Rahmenbedingungen für die eigene PV-Anlage
- Photovoltaik auf dem Dach mit Eigenleistung
- Was Solardachziegel leisten
- Wie Solarwechselrichter arbeiten

Das eigene Balkonkraftwerk

- Mit Balkonsolaranlagen die Stromrechnung senken
- Mikrowechselrichter: Grundlagenwissen und Marktübersicht
- FAQ: Balkonkraftwerke

Verbrauch und Erzeugung im Blick

- Stromproduktion selbst messen
- Grundwissen Elektrik
- Wann sich ein Smart Meter lohnt
- Zwischenzähler zur Verbrauchsmessung im Sicherungskasten
- Wechselrichter per Web & MQTT überwachen
- Energiekostenmessgeräte im Test

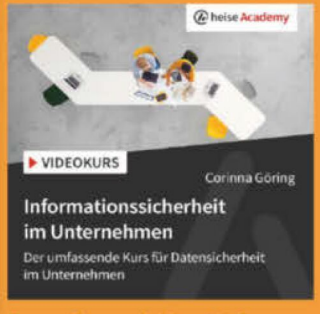
Sind Ihre Daten sicher?

c't DATEN SCHÜTZEN

IT einfach sicher machen

PLUS heise-Academy-Webinar im Wert von 99,- Euro

Der große Security-ONLINEKURS



Der umfassende Kurs für Datensicherheit im Unternehmen, anschaulich erklärt in 80 Lektionen, Laufzeit: 5:33 Stunden

- *Maßnahmenkatalog für Ihr Unternehmen*
- *Stellen Sie den Experten Fragen über das Q&A-Modul*
- *Übungsmaterial zum Mitmachen*

E-Mail sicher nutzen

Tipps für den Alltag
Phishing-Mails erkennen
Verdächtige Mailanhänge untersuchen und entschärfen

Praktischer Datenschutz im Alltag

Office-Dateien in der Cloud verstecken
Onlinedienste datenschutzkonform nutzen
Videoüberwachung legal einsetzen

Sicher speichern und transportieren

Verschlüsselung gegen Datenklau
USB-Sticks & Co.: Sichere Medien für unterwegs

+ GRATIS Videokurs im Wert von 99,- €

Dieses c't-Sonderheft ist Ihr Leitfaden für praktischen Datenschutz im Alltag aber zeigt Ihnen auch wie Sie sich vor Cybergangstern schützen können:

- ► Gefahrloser Umgang mit E-Mails
- ► Office-Dateien in der Cloud verstecken
- ► Sicher speichern und lagern
- ► Verschlüsselung gegen Datenklau
- ► Inkl. GRATIS heise-Academy-Kurs „Informationssicherheit im Unternehmen“
- ► Auch im Paket-Angebot mit Buch „Cloud Computing nach der Datenschutz-Grundverordnung“ zum Sonderpreis

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

shop.heise.de/ct-datenschutz23