



NEU!

196
Seiten!

Alles reparieren!

Mit
Reparatur-DVD
im Heft

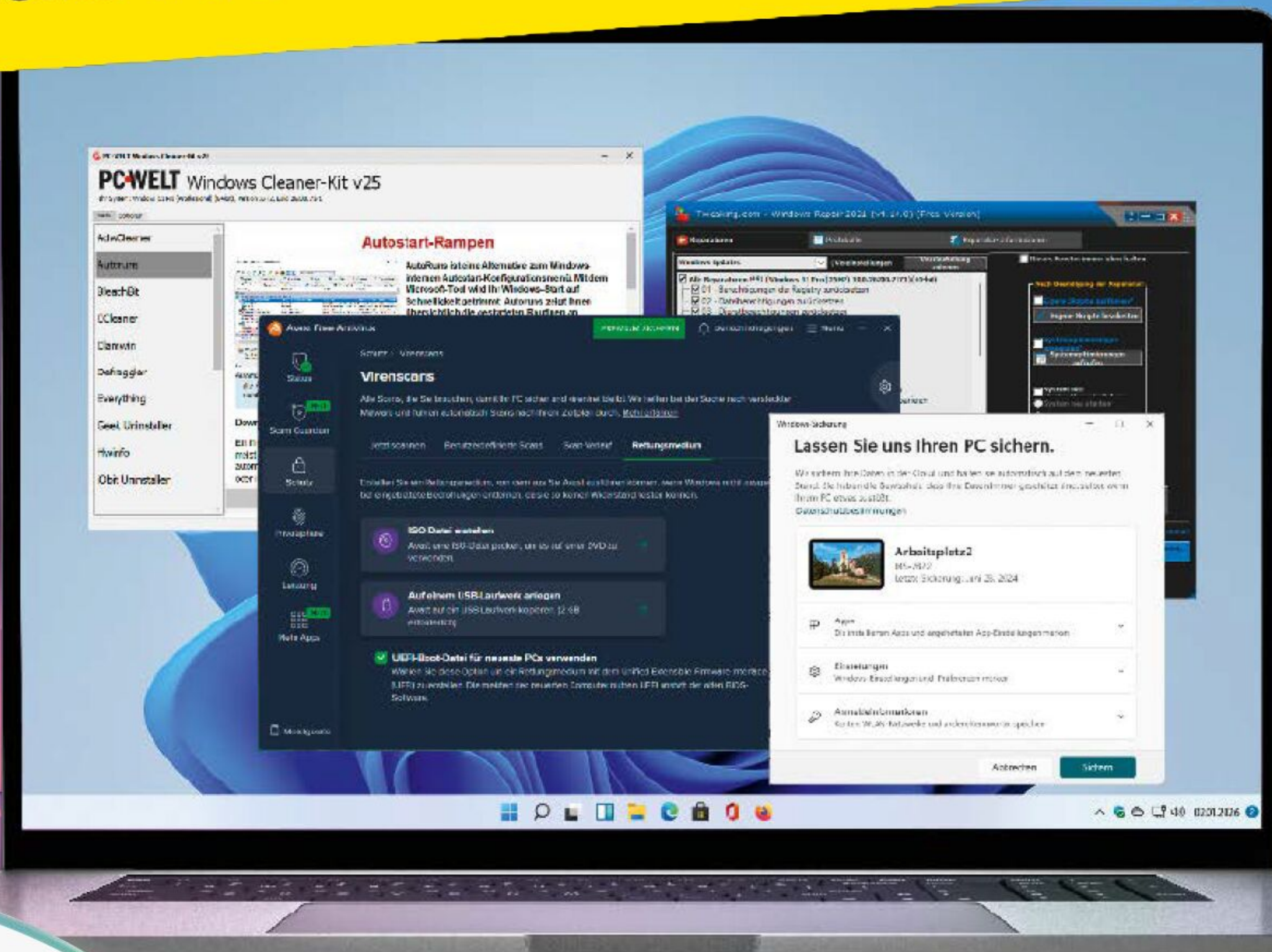
**Windows 11, WLAN & PC:
Das Notfall-Handbuch 2026**

Notfall-Hilfe

Rettungssystem einsetzen
Notfallstick erstellen
Secureboot-Probleme lösen

Windows

Systemstart beschleunigen
Nervereien abstellen
Blockaden entfernen



Netzwerk

WLAN richtig konfigurieren
Fernhilfe für die Fritzbox
Online trotz Stromausfall

Hardware

Oled-Displays pflegen
Druckkosten senken
Geräteakkus tauschen

DVD IM HEFT!
Auch als Download-DVD

PCWELT
Reparatur-DVD
2026

Ein- und Loslegen!

Bootbares
Rettungssystem
für PC-Notfälle

PLUS
150 Tools für
den Notfall

Soforthilfe-Paket
im Wert von über

270€

8 Vollversionen für ein schnelleres Windows · weniger Datenmüll
· aktuelle Treiber und Software · automatisierte Backups u.v.m.



Infotainment
Datenträger
enthält nur Lehr-
oder Infoprogramme



Jetzt
am
Kiosk!

Für nur
5,90€

Mit Software-
Gratis-Paket auf
Download-DVD!

Bestellen unter

www.pcwelt.de/whatsappbooklet oder per Telefon: 0931/4170-177 oder ganz einfach:



1. Formular ausfüllen



2. Foto machen



3. Foto an idg-techmedia@datam-services.de

Ja, ich bestelle das Digital Life Schritt für Schritt Booklet 1/26 WhatsApp für nur 5,90€.

Zzgl. Versandkosten (innerhalb Deutschland 3,- €, außerhalb 4,- €)

BESTELLEN	Vorname / Name			
	Straße / Nr.			
	PLZ / Ort			
	Telefon / Handy		Geburts- tag	TT MM JJJJ
	E-Mail			

BEZAHLEN	<input type="radio"/> Ich bezahle bequem per Bankeinzug. <input type="radio"/> Ich erwarte Ihre Rechnung.
	Geldinstitut
	IBAN
	BIC
	Datum / Unterschrift des neuen Lesers

Schnelle Hilfe im Notfall

Der Umstieg von Windows 10 zu Windows 11 ist für viele Nutzer ein Thema – egal, ob er bereits erledigt ist oder demnächst ansteht. In unserem Sonderheft zeigen wir Ihnen, wie Sie Umstiegsprobleme lösen, Windows-Ärgernisse abstellen und vieles mehr.

Software: Auch installierte Programme können Probleme machen. Beispielsweise nervt es, wenn Updates nicht korrekt aufgespielt oder Dateien vom falschen Programm geöffnet werden. Und ist ein beliebtes Programm plötzlich nicht mehr verfügbar, muss man sich fix umorientieren – alles nicht so einfach.

Netzwerk & Hardware: Wer seine Fritzbox und den Zugriff darauf effektiv absichern möchte, der findet in unserem Sonderheft gleich mehrere Artikel zu diesem Thema. Außerdem beschäftigen wir uns mit Druckern, Monitoren und Akkus.

Internet: Mit unseren Tipps schützen Sie sich vor KI-Angriffen aus dem Internet, Kleinanzeigenbetrug und anderen Online-Gefahren.

Viel Spaß beim Lesen!



Verena Ottmann

Redakteurin

vottmann@it-media.de

Verena Ottmann



NEU! DIGITALE AUSGABEN DER PC-WELT NUN BEI EMAGAZINES

Viele wissen es bereits: Die digitalen Ausgaben der PC-WELT und der LinuxWelt, die Sie im Rahmen Ihres PC-WELT-Plus- oder Ihres Plus-Digital-Abos erhalten, beziehen Sie komfortabel über den Service von eMagazines.

Und so funktioniert es: Jedes Mal, wenn wir eine neue Ausgabe veröffentlichen, teilen wir Ihnen das per E-Mail mit – und schicken auf diesem Weg auch gleich den Link auf das digitale Heft und Ihr persönliches Archiv. Auf diese Weise verpas-

sen Sie keine Benachrichtigung über eine neue Ausgabe.

Tipp: Am besten setzen Sie den Absender der Info delivery@mail.emagazines.com auf die Whitelist Ihres E-Mail-Programms, also auf die Liste der vertrauenswürdigen Absender, damit die Nachricht nicht irrtümlich in Ihrem Spam-Ordner landet.

Übrigens: Im Lesemodus stellt sich das Print-Layout ganz auf Ihren Bildschirm ein.

Ihr Beitrag für mehr Nachhaltigkeit



klimaneutral
gedruckt durch
CO₂-Kompensation

klima druck33 · U-Nr. 24161137

VDM⁺



PEFC-zertifiziert

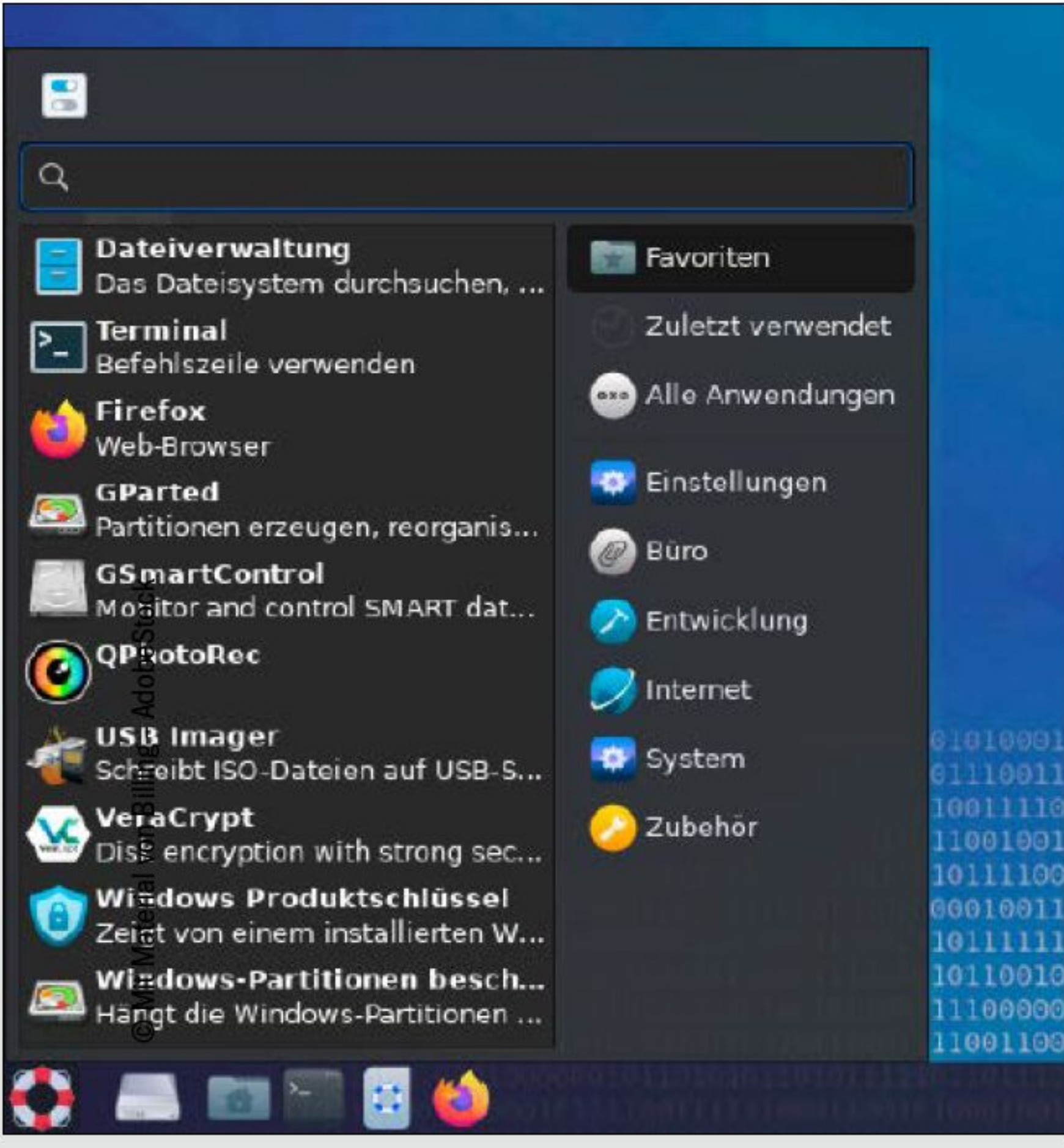
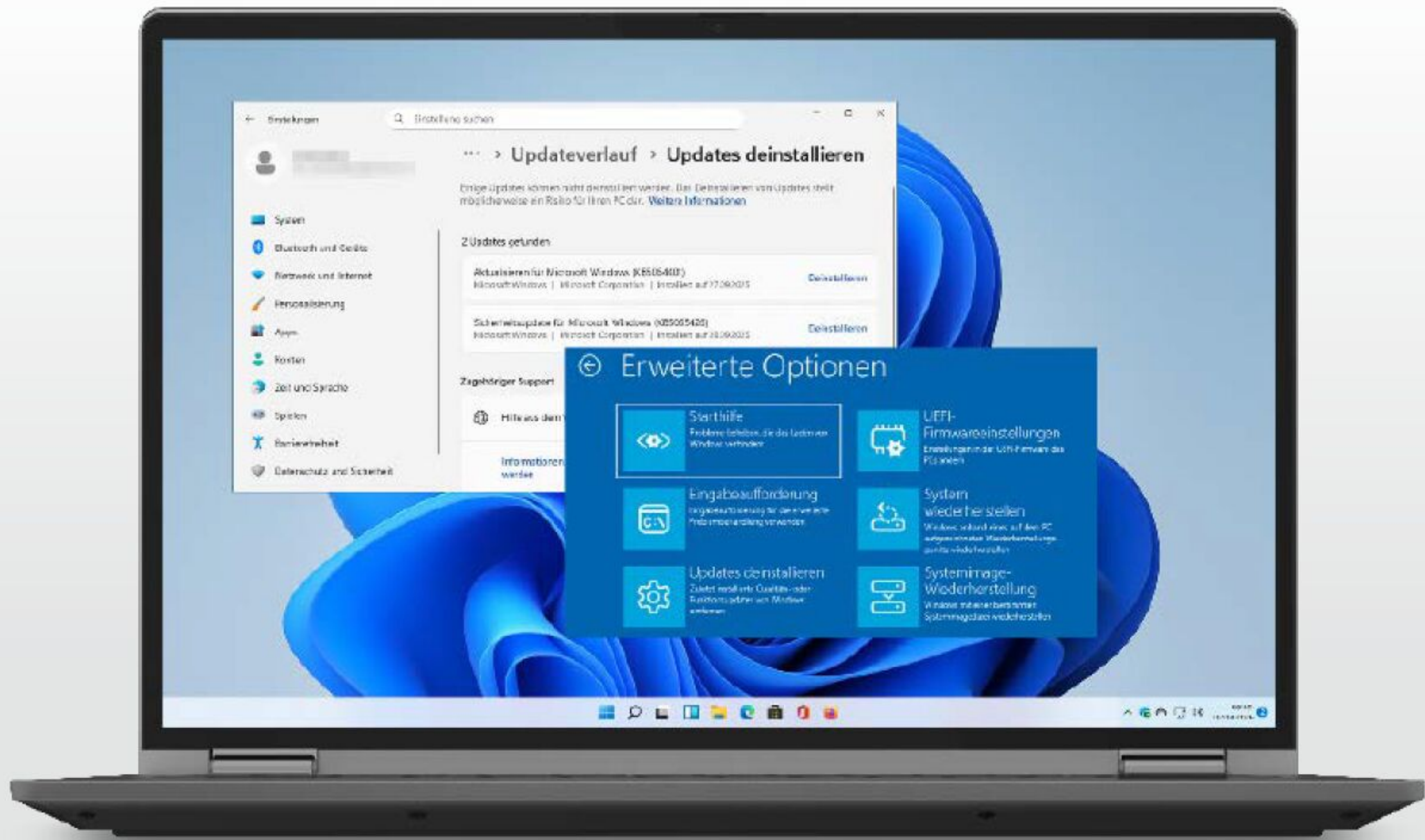
Dieses Produkt stammt
aus nachhaltig
bewirtschafteten Wäldern,
Recycling und
kontrollierten Quellen

PEFC

PEFC/04-31-1036

www.pefc.de

Das PC-WELT-Sonderheft wird auf Recyclingpapier mit mehr als 80 % Altpapieranteil gedruckt.



Die beste Hilfe bei Windows-Problemen

Die Fehlerquellen bei Windows sind vielfältig: Hard- und Software stammen aus unterschiedlichsten Quellen, müssen aber trotzdem reibungslos zusammenarbeiten. Tun sie dies nicht, helfen die in Windows integrierten Hilfe-, Diagnose- und Reparaturfunktionen sowie unsere Tools.

ab S. 10

Neu: PC-WELT Rettungssystem

Die jüngste Version des Rettungssystems der PC-WELT setzt auf verbesserte Tools für PC-Notfälle und auf frische Linux-Komponenten für umfassenden Hardwaresupport. Außerdem lassen sich jetzt auch per Bitlocker verschlüsselte Laufwerke leichter integrieren.

ab S. 66

■ Windows

- 6

DVD-Inhalt
Damit Sie unsere Ratgeber und Tipps gleich ausprobieren können, finden Sie auf der DVD die zugehörige Software
- 10

Die beste Hilfe bei Windows-Problemen
Windows streikt, und die integrierten Hilfe-, Diagnose- und Reparaturfunktionen versagen? Dann helfen unsere Tools
- 16

Windows-Nervereien abstellen
Wenn etwas bei Windows stört, ignoriert man das Problem – oder unternimmt etwas dagegen
- 22

Secure-Boot-Probleme lösen
Damit Secure Boot auch in Zukunft sicher schützt, stehen wichtige Updates an
- 28

Windows-System-Checker
Wenn Windows nicht rund läuft, ist es Zeit für eine Systemprüfung
- 34

Windows-Upgrade: Jede Blockade lösen
Beim Umstieg von Windows 10 auf 11 wie auch beim Aktualisieren hakt es immer wieder
- 38

Windows ungebremst
Lahmt der PC, liegt es meist an zu vielen Startprozessen, die die Ressourcen ausschöpfen
- 44

Power-Tuning für das Startmenü
Mit unseren Tipps können Sie das Windows-Startmenü verschönern, aufräumen und erweitern
- 48

Fernhilfe bei Umstieg auf Windows 11
Wenn Familie oder Freunde Hilfe beim Upgrade benötigen, müssen Sie nicht anreisen: Wir zeigen, wie Sie remote unterstützen
- 52

PC-Upgrade für Windows 11
Bei vielen Rechnern genügt ein gezieltes Upgrade, um sie mit Windows 11 weiter zu nutzen

- 56

Der perfekte Notfallstick
Packen Sie die Tools unserer DVD auf einen USB-Stick, damit bei Bedarf sofort eine nützliche Werkzeugsammlung bereitsteht
- 62

Für jeden Stick das richtige Dateisystem
Wenn ein USB-Sticks nicht richtig funktioniert, liegt es oft am Dateisystem: an FAT32 oder NTFS

■ Software & Daten

- 66

PC-WELT Rettungssystem
Die neue Version setzt auf verbesserte Tools für PC-Notfälle
- 72

Datenrettung leicht gemacht
Die Wiederherstellung gelöschter Dateien ist mit dem Wechsel von HDD zu SSD schwieriger
- 76

Mehr Platz und Leistung
CCleaner verspricht weniger Datenmüll, mehr Speicherplatz, bessere Performance und weniger PC-Probleme
- 80

Sofort-Update für Software
Endlich funktionierten Paketmanager auch unter Windows, und zwar ganz komfortabel
- 84

Daten perfekt sichern und synchronisieren
Ohne zusätzliche Vorkehrung kann das Synchronisieren in der Cloud zu Datenverlust führen
- 88

Immer das richtige Programm starten
Windows öffnet viele Dateien mit dem falschen Programm
- 92

Von Microsoft gelöscht
Welche Tools verschwinden und wo Sie Ersatz dafür finden
- 96

Alles sicher öffnen
Mit speziellen Tools öffnen Sie Programme und Dateien aus unbekannten Quellen ohne Risiko

Die Highlights der DVD

Gratis für Sie: 8 Vollversionen und 150 Tools für Ihr Windows

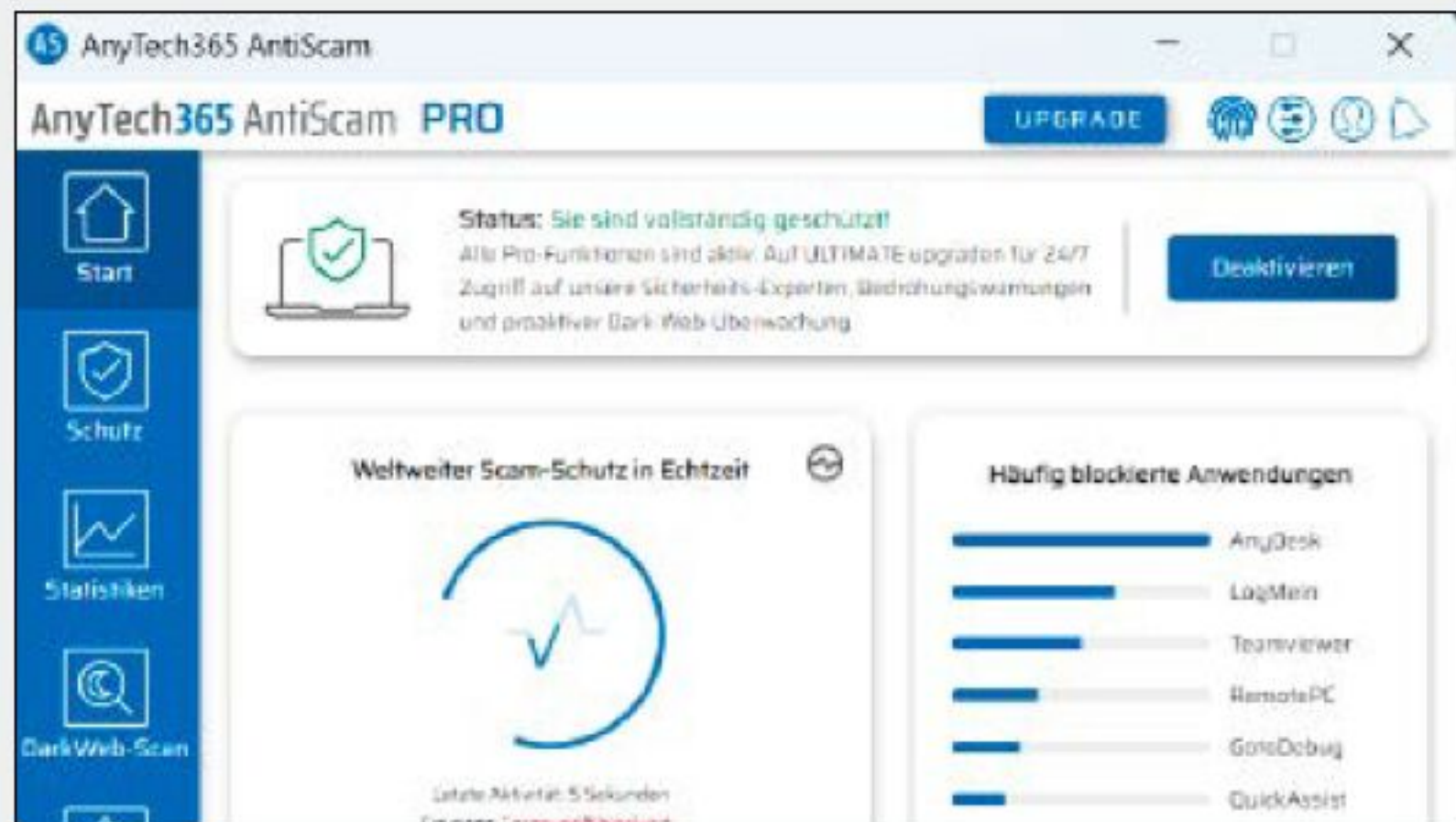
Auf unserer Heft-DVD finden Sie neben acht Vollversionen auch 150 Tools für jeden PC-Notfall.

S. 6



Anytech 365 Antiscam Pro

Warnt vor unbefugten Fernzugriffen, verdächtigen Webseiten und weiteren Internet-Risiken.



Ascomp Cleaning Suite Pro

Deinstalliert Programme, räumt das Startmenü auf, entfernt unnötige Dateien und Registry-Einträge.



Ashampoo Winoptimizer 27

Das Optimierungs-Tool durchforstet Ihren PC nach Tuning-Möglichkeiten und listet die Ergebnisse auf.



Netzwerk & Hardware

100 Sicherer Router-Zugriff

Bei WLAN-Routern lässt sich viel einstellen, um Tempo und Sicherheit im Heimnetz zu verbessern

106 Fernhilfe für Fritzbox & Co

So lösen Sie Probleme mit Fritzbox & Co. in anderen Heimnetzen per Fernzugriff

112 Getrennte WLANs für bessere Sicherheit

Bringen Sie Clients in getrennten Netzen unter, um zu verhindern, dass eine Sicherheitslücke bei einem Gerät alle anderen gefährdet

118 Online bleiben, wenn das Internet ausfällt

Die Fritzbox bietet mit der neuen Firmware einen umfassenden Ausfallschutz

124 Druckerprobleme lösen

Drucker bieten Wartungsseiten an, die Ihnen zeigen, ob und was mit Ihrem Gerät nicht in Ordnung ist

128 So senken Sie Ihre Druckkosten

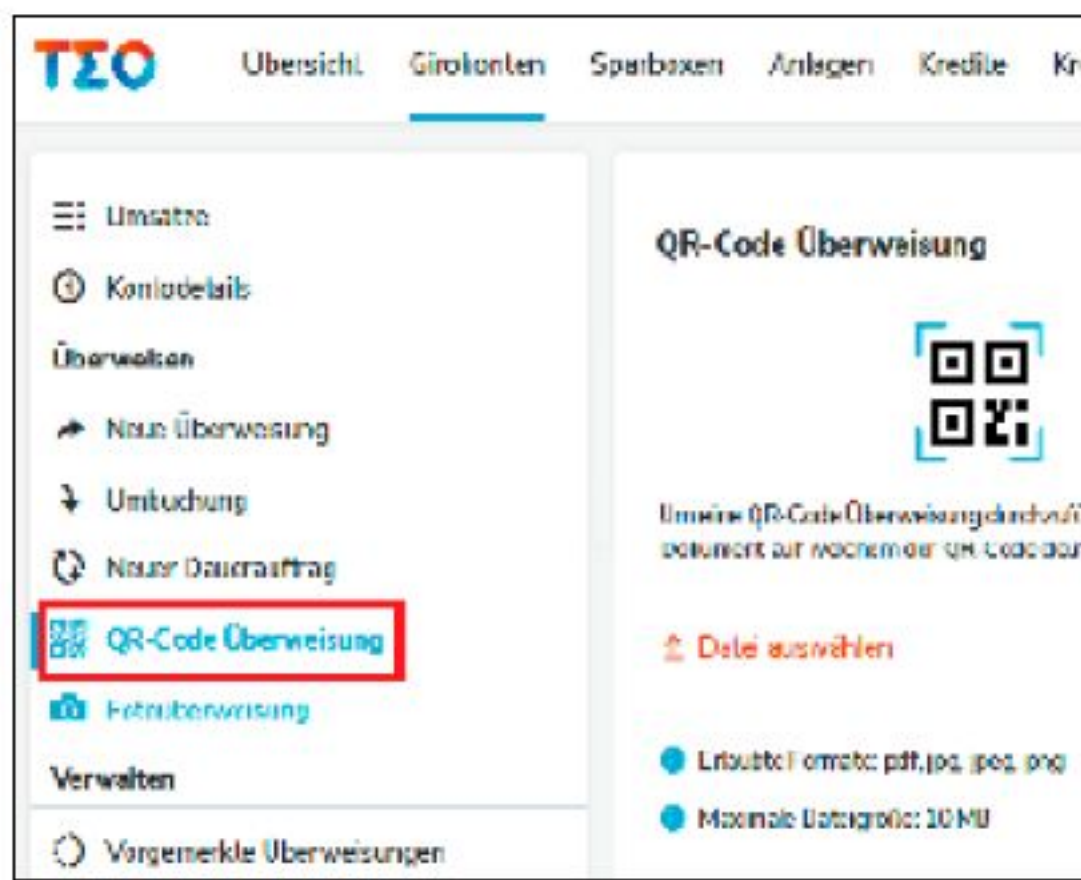
Beim Drucken addiert sich zu den Hardwarekosten der Verbrauch für Tinte oder Toner sowie Papier

132 Oled-Pflege bei Notebook & Monitor

Mit den richtigen Maßnahmen können Sie Einbrennen und anderen Defekten effektiv vorbeugen

136 Akkutauch leicht gemacht

Wir sagen, wie Akkuspezifikationen bei Phone und Notebook zu interpretieren sind, und wie Sie einen Akku am besten tauschen



Virenschutz & Verschlüsselung

140 Neues Jahr 2026, neue Gefahren?

Angrifer und Hacker werden immer raffinierter. So sorgen Sie vor

146 Sicherheitstipps der Experten

Wo die größten Gefahren liegen, und wie man ihnen begegnet

150 Test: Virenschutz für 2026

Aktuelle Sicherheitslösungen

154 Fehlalarm oder Virus?

Wenn das Antivirenprogramm Alarm schlägt, löst das bei jedem Anwender einen Schreckmoment aus. Doch nicht immer ist die Warnung berechtigt

158 Mobil und gut verschlüsselt

Mit Windows und Tools können Sie Notebooks, mobile Festplatten und USB-Sticks per Verschlüsselung sicher schützen

Sicher im Internet

162 10 Sicherheitsfragen

Antworten auf aktuelle Probleme

166 Neue Checklisten des BSI

Was die offiziellen PDF-Anleitungen für Ihre PC-Sicherheit raten

170 Die offiziellen Tipps: Sicher online bezahlen

Jedes Verfahren zum Bezahlen beim Onlineshopping hat seine Vor- und Nachteile

178 Betrug bei Kleinanzeigen

Die populäre Plattform zieht auch Kriminelle an

182 Passwort geklaut?

Prüfen Sie jetzt, ob auch Sie betroffen sind, und schützen Sie sich vor Angriffen

186 Abzocke per Briefpost

Das ist neu: Phishing per Brief und ausgedruckten QR-Codes

190 Eigene Daten vor KI-Nutzung schützen

Im Kampf um die KI-Vorherrschaft zählt das Urheberrecht kaum

Service

6 DVD-Inhalt

194 Impressum

Die Highlights der Heft-DVD

Im PC-Notfall kann das richtige Programm den Unterschied zwischen „läuft wieder“ und „ein Fall für die Tonne“ ausmachen. Daher finden Sie in diesem Sonderheft nicht nur Ratgeber und Tipps für PC-Probleme aller Art, sondern auch, wo möglich, die empfohlenen Tools und Vollversionen auf unserer (Download-)DVD. Damit können Sie gleich loslegen.



VON VERENA OTTMANN

Viele mussten sich in den letzten Wochen mit dem Umstieg von Windows 10 auf Windows 11 beschäftigen. Wer Glück hatte, der konnte das neue Betriebssystem problemlos auf seinem PC installieren und danach auch die angeschlossene Peripherie wieder wie gewohnt nutzen.

Doch leider ist dies nicht bei allen Nutzern der Fall: Von inkompatiblen Rechnern, die erst fit für das Update gemacht werden müssen, über Probleme mit dem Netzwerk oder der angeschlossenen Hardware bis hin zu Ärger mit Windows selbst kann alles vorkommen.

In diesem Heft helfen wir Ihnen beim Lösen Ihrer PC-Probleme mit Ratgebern und Tipps, die alle benötigten Werkzeuge gleich mitbringen – in Form von Tools und anderen Programmen auf unserer (Download-)DVD.

Acht kostenlose Vollversionen

Nicht jede kostenpflichtige Vollversion ist automatisch besser als eine Freeware mit ähnlichem Funktionsumfang. Die acht Vollversionen, die wir für die DVD ausgewählt haben, können wir jedoch vollumfänglich empfehlen: So hilft Ihnen der **Winoptimizer** von Ashampoo dabei, Ihr Betriebssystem über viele kleine Stellschrauben optimal einzustellen, um beispielsweise Ihre



Mit dem bootbaren PC-WELT Rettungssystem in der neuesten Version haben Sie alle Werkzeuge zur Hand, die Sie im PC-Notfall benötigen, aber auch Virenschutz, Browser und mehr.

Privatsphäre besser zu schützen. **Ashampoo Backup Pro 25** lässt Sie automatische Sicherungen Ihrer Dateien, Ordner und Laufwerke einrichten, **Ascomp Cleaning Suite** entfernt nutzlose Programme und Dateien. **Wisecleaner Wise Hotkey** erstellt Tastenkürzel, um etwa Funktionen oder Programme schneller zu starten. **Driver-max Pro 16** und **Iobit Software Updater Pro** kümmern sich automatisch um die Aktualisierung von Treibern respektive installierten Programmen, und mit **Cleverprint**

von Abelssoft sparen Sie Druckkosten. Zu guter Letzt schützt Sie **Anytech 365 Anti-scam Pro** vor Gefahren aus dem Internet.

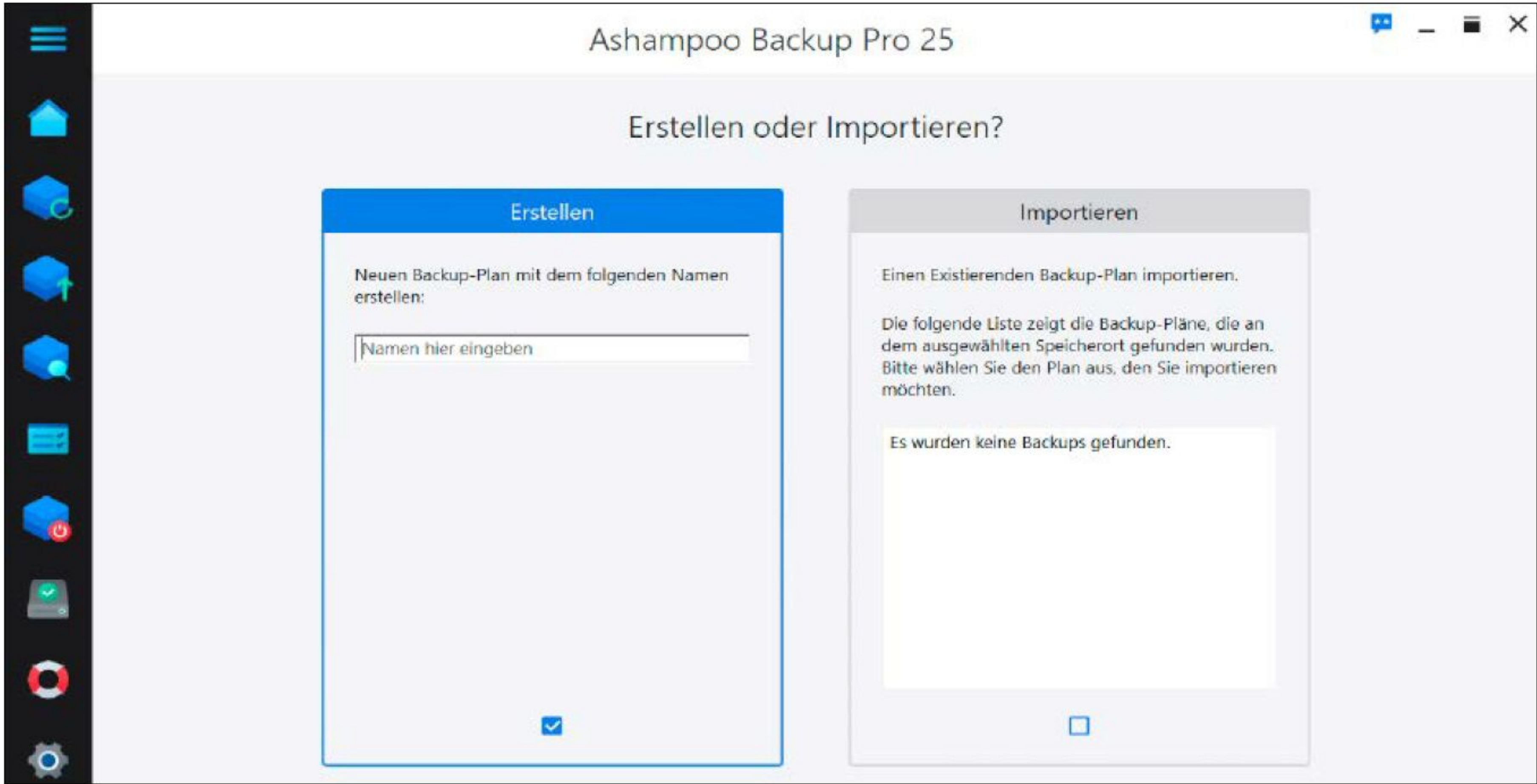
Sicher im Internet

Wer nicht nur seine Daten, sondern auch seine Ausflüge ins Internet schützen will, der muss gleich auf zwei Gebieten tätig werden: Einmal gilt es, den Router optimal abzusichern, damit sich Unbefugte keinen Zugang zum Heimnetz verschaffen können. Hier helfen unsere Anleitungen und Tools,

UNSERE DOWNLOAD-DVD + REGISTRIERUNG

Alle Vollversionen und Gratistools finden Sie auch online auf unserer Download-DVD unter www.pcwelt-dvd.de/dvdsh326. Die Zugangsdaten lauten:
* **Benutzername:** dvdsh326
* **Passwort:** rsk555dv

mit denen Sie etwa Gast-WLANs erstellen und die Fritzbox so konfigurieren, dass mögliche Sicherheitslücken geschlossen werden. Aber auch der richtige Virenschutz ist ausschlaggebend für die Sicherheit im Internet. Hier haben wir für Sie neben Expertentipps auch Tests von aktuellen Sicherheitslösungen – kostenpflichtig und kostenlos, einige



Ashampoo Backup Pro 25 ist eine der acht Vollversionen, die Sie auf unserer DVD finden. Das Programm erstellt automatische Sicherungen von Dateien, Ordnern und Laufwerken, bringt aber noch weitere nützliche Funktionen mit. Mehr dazu erfahren Sie im Ratgeber ab Seite 72.

davon auf unserer DVD. Und als Zuckerl obendrauf sagen wir Ihnen, wie Sie mobile Datenträger wie externe Festplatten, USB-Sticks, aber auch Notebooks effektiv verschlüsseln. Die benötigte Software finden Sie natürlich auch auf unserer DVD. ■

AUF HEFT-DVD: DIE INHALTE IM ÜBERBLICK



Vollversionen

- Abelssoft Cleverprint
- Anytech 365 Antiscam Pro
- Ascomp Cleaning Suite
- Ashampoo Backup Pro 25
- Ashampoo Winoptimizer 27
- Drivermax Pro 16
- Iobit Software Updater 8 Pro
- WiseCleaner Wise Hotkey

Software

- .NET (32 Bit) 9.0.11
- .NET (64 Bit) 9.0.11
- 7-Zip (32 Bit) 25.01
- 7-Zip (64 Bit) 25.01
- Abiword 2.9.4
- All Dup 4.5.72
- Angry IP Scanner 3.9.3
- Anvir Task Manager Free 9.4.0
- Anydesk 9.6.7
- Aomei Backupper Standard 8.1.0
- Aomei Partition Assistant Standard 10.9.2
- APFS für Windows 3.1.1
- AS SSD Benchmark 2.0
- Ashampoo Backup Free 25.6.0
- Autoruns 14.11
- Autoruns Portable 14.11
- Avast Free Antivirus 25.12
- AVG Antivirus Free 25.12
- Avira Antivir Rescue System 2025
- Avira Free Security 1.1.112
- Bitwarden 2025.12.0
- Bootice (32 Bit) 1.3.4.0
- Bootice (64 Bit) 1.3.4.0
- Bootracer 9.40
- CCleaner 7.03
- CCleaner Portable 6.39
- Check UEFI Secure Boot Variables 1.1
- Clamwin Portable 0.103.2.1
- Cleanmgr Plus 1.50
- CPU-Z Portable 2.17
- Cryptomator (64 Bit) 1.18.0
- Cryptsync (32 Bit) 1.4.11
- Cryptsync (64 Bit) 1.4.11

- CrystallDiskInfo 9.7.2
- CrystallDiskInfo Portable 9.7.2
- CrystallDiskmark 9.0.1
- CrystallDiskmark Portable 9.0.1
- Defender Control 2.1
- Defender Exclusion Tool 1.4
- Defender UI 1.46
- Doc Fetcher 1.1.26
- Easeus Partition Master Free 19.23
- Easeus Todo Backup Free 18.0
- Easeus Todo PCTrans Free 14.1.0
- Emsisoft Emergency Kit Portable 2025.7.0
- Eset Internet Security (64 Bit) 19.0.14.0
- Everything (32 Bit) 1.4.1
- Everything (64 Bit) 1.4.1
- Explorer Patcher for Windows 11
- F3 für Windows 8.0
- Flyby11 3.10
- Free File Sync 14.6
- Free Firewall 2.6.2
- Free Hide Folder 3.5
- Free Password Generator 5.43
- G Data Total Security 2025
- Google Chrome (32 Bit) 143.0
- Google Chrome (64 Bit) 143.0
- Gpg4win 4.4.1
- GPU-Z 2.68.0
- GPU-Z Portable 2.68.0
- Hard Configurator 7.0.1.1
- Hardentools 2.6
- Hasleo Backup Suite Free 5.5.2.2
- Hirens Boot CD PE 1.0.8
- Hwinfo 8.34
- Hwinfo Portable 8.34
- Java Runtime Environment (32 Bit) 8u471
- Java Runtime Environment (64 Bit) 8u471
- Kaspersky Rescue Disk 2025
- Keepass 2.60
- Keepass, deutsche Sprachdatei 2.60
- Lazesoft Recovery Suite Home Edition Free 5.0
- Libre Office (32 Bit) 25.8.4
- Libre Office (64 Bit) 25.8.4
- Malwarebytes Adwcleaner 8.7.0

- Malwarebytes Anti-Malware 5.4.6
- Medienerstellungstool für Windows 11 10.0
- Microsoft Safety Scanner (32 Bit)
- Microsoft Safety Scanner (64 Bit)
- Minitool Partition Wizard Free 13.5
- Mitec Taskmanager Deluxe 4.9.0
- Onionshare (64 Bit) 2.6.3
- Open Shell Menu 4.4
- Open With View 1.11
- Open With View, deutsche Sprachdatei 1.11
- Opera (32 Bit) 125.0
- Opera (64 Bit) 125.0
- Paint.Net 5.1.11
- Paragon Backup & Recovery (64 Bit) 18.2.0
- Paragon HFS+ für Windows 14.0.24
- Paragon Linux File Systems for Windows 7.0.29
- PC-Integritätsprüfung
- PCI-Z 2.0
- PCI-Z Portable 2.0
- PC-WELT Beitrag: Profi-Befehle für Windows
- PC-WELT Beitrag: Support-Aus Windows 10
- PC-WELT Beitrag: Windows 11 auf alten PCs
- PC-WELT Beitrag: Windows 11 wie 10
- PC-WELT Performance 1.1
- PC-WELT Rettungssystem 11
- PC-WELT Windows Cleaner-Kit 25.0
- Picocrypt 1.49
- Portableapps.com Platform 30.1.3
- Powershell-Sys-Checker 1.0
- Private Prompts 0.0.5
- Privazer 4.0
- Process Explorer Portable 17.09
- Process Monitor 4.01
- Produkey (32 Bit) 1.97
- Produkey (64 Bit) 1.97
- Produkey, deutsche Sprachdatei 1.97
- Proton VPN (64 Bit) 4.3.11
- Puresync 8.0.5
- Recuva 1.54
- Reset Windows Update Tool 11.1.0
- Revo Uninstaller 2.6.5.0
- Rufus (32 Bit) 4.11
- Rufus (64 Bit) 4.11

- Rufus Portable 4.9
- Sandboxie (64 Bit) 5.71.9
- Sandboxie Plus (64 Bit) 1.16.8
- Sardu 5.5.0
- Speccy 1.33.75
- Speccy Portable 1.33.75
- Spybot-Search & Destroy 2.9.85.5
- SSD-Z 16.09.09
- SSD-Z Portable 16.09.09
- Start 11 2.5.6.3
- Start All Back 3.9.20
- System Informer 3.2
- Teamviewer (32 Bit) 15.73.5
- Teamviewer (64 Bit) 15.73.5
- Teamviewer Quick Support (32 Bit) 15.73.5
- Teamviewer Quick Support (64 Bit) 15.73.5
- Teracopy 3.17
- Tweak Power 2.076
- Unchecky 1.2.0
- UnigetUI 3.3.6.0
- USB Imager 1.0.10
- Ventoy 1.1.10
- Ventoy Portable 1.1.10
- Veracrypt 1.26.24
- Veracrypt Portable 1.26.24
- Virtualbox 7.2.4
- Why Not Win 11 (64 Bit) 2.7.0
- Why Not Win 11 (64 Bit) 2.7.0
- Windows 11 Installationsassistent 1.4
- Windows Assessment and Deployment Kit 10.1
- Windows Manager 2.3.0
- Windows Repair Free Portable 4.14.0
- Windows Repair Toolbox 3.0.4.8
- Windows System Control Center Portable (32 Bit) 10.0.1.4
- Windows System Control Center Portable (64 Bit) 10.0.1.4
- Windows Update Blocker 1.8
- Wise Folder Hider Free 5.0.9

Bootfähig

- PC-WELT Rettungssystem 11

Anytech 365 Antiscam Pro

Sicher im Internet

Vollversion mit Registrierung, Jahreslizenz für Windows 10, 11

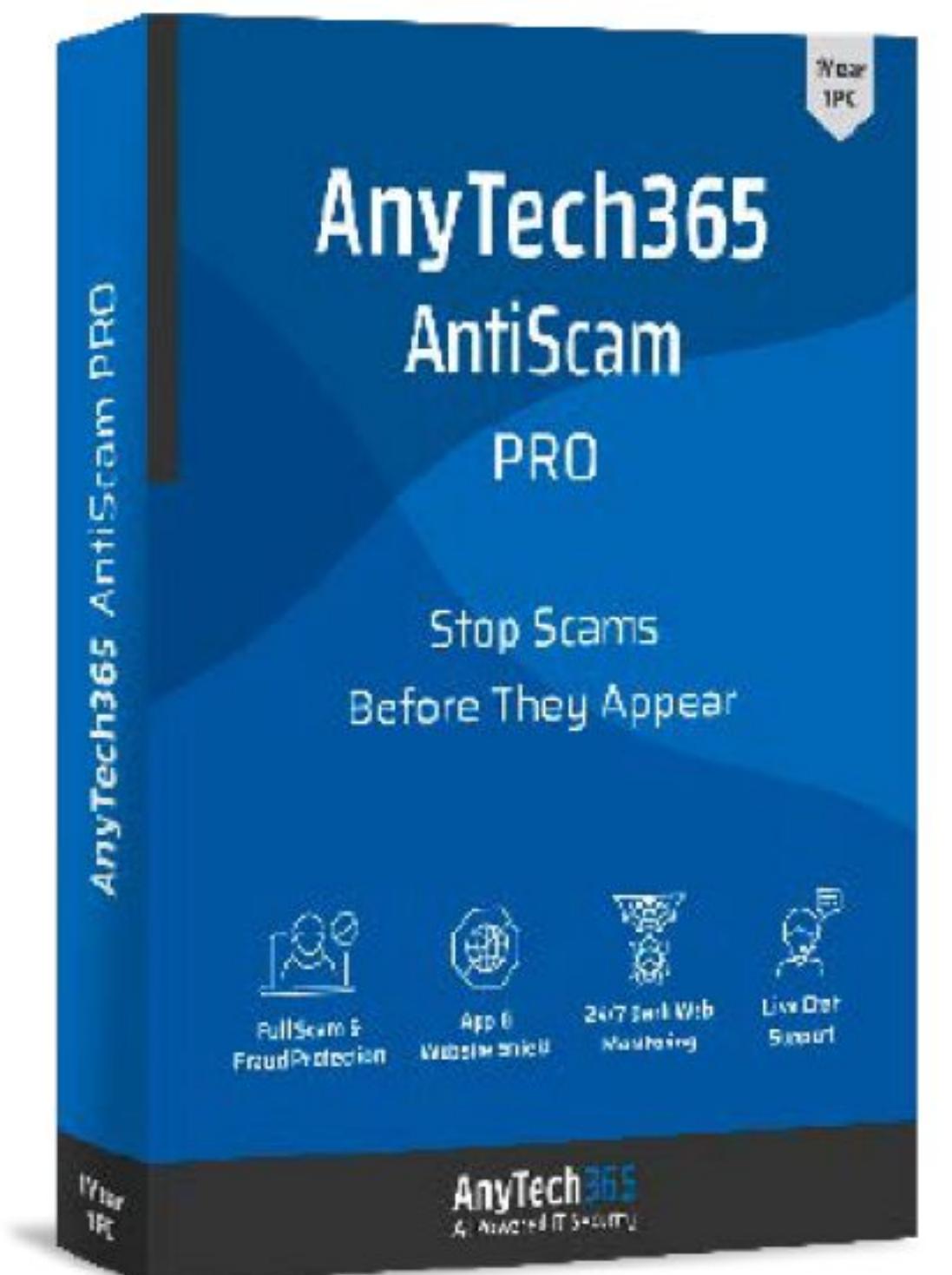
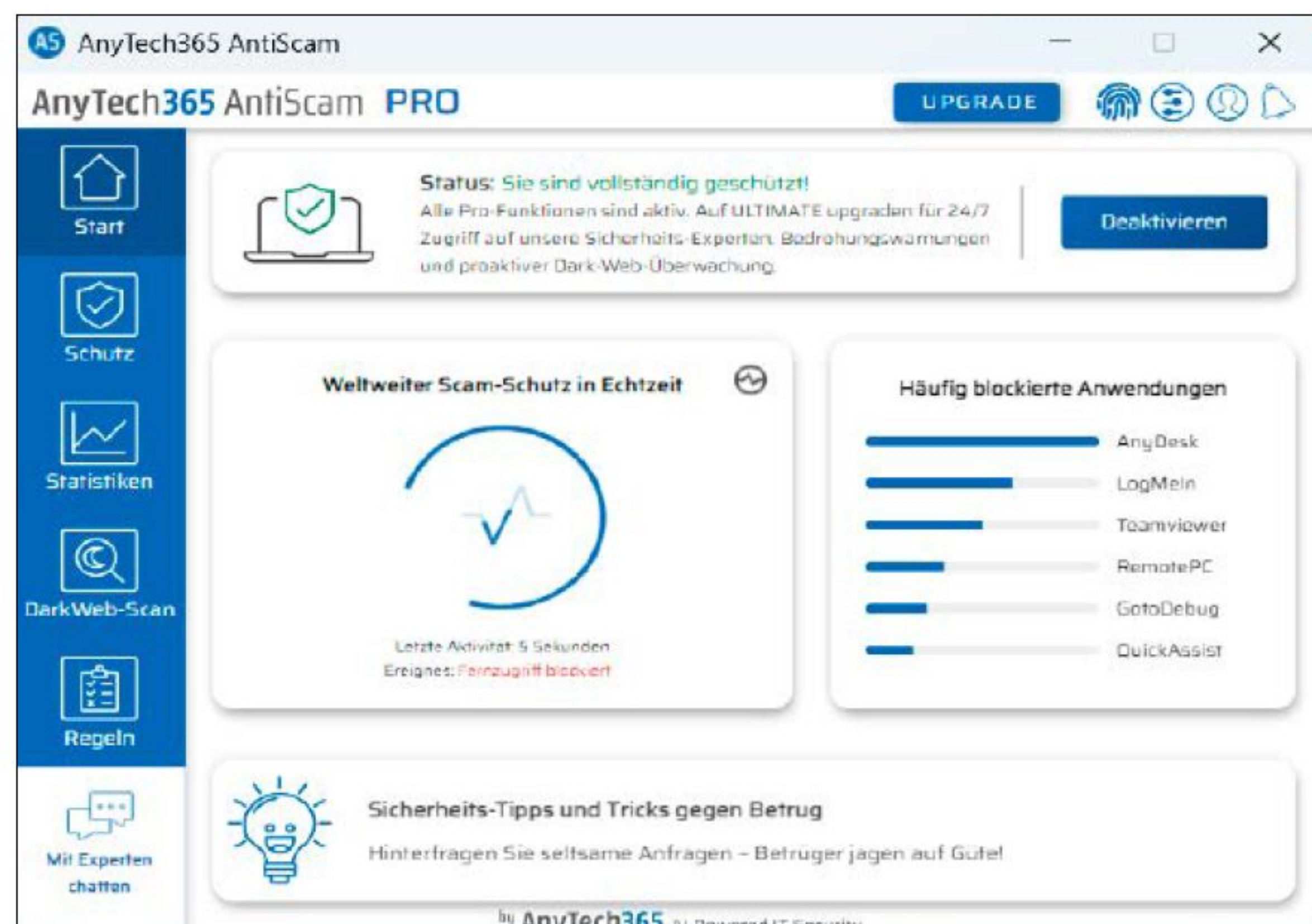
Antiscam Pro warnt Sie vor Fernzugriffen, verdächtigen Webseiten und weiteren Internet-Risiken. Zudem sind ein Dark-Web-Scanner und ein konfigurierbarer Netzwerkschutz an Bord. Statistiken geben ei-

nen Überblick über die Wirksamkeit des Programms, und über „Regeln“ lassen sich Ausnahmen definieren.

Installation: Klicken Sie auf „Hier Registrieren“ und geben Sie Ihre Mailadresse ein.

Stimmen Sie der Speicherung Ihrer Daten sowie dem Erhalt des Newsletters per Haken zu, bestätigen Sie, dass Sie kein Roboter sind, lösen Sie das Captcha und klicken Sie auf „Download starten“. Melden Sie sich mit

Antiscam Pro von Anytech 365 schützt Sie vor Gefahren aus dem Internet, indem das Programm vor Zugriffen warnt, den Schutz Ihres Netzwerks übernimmt u.v.m.



Ihrem Softwarezirkel-Konto an oder erstellen Sie ein neues Konto. Sie bekommen einen Downloadlink angezeigt und zugeschickt. Laden und starten Sie den Installer. Klicken Sie auf „Installieren“ (sic!). Beim ersten Start müssen Sie sich mit Hilfe eines Codes verifizieren und erhalten daraufhin Ihren Lizenzcode per Mail. Wichtig: Dieser ist an den PC gebunden, auf dem Sie Antiscam registriert haben. Das Programm wird damit automatisch zur Pro-Version. ■

Ascomp Cleaning Suite

Ungenutzte Dateien, Programme und mehr entfernen

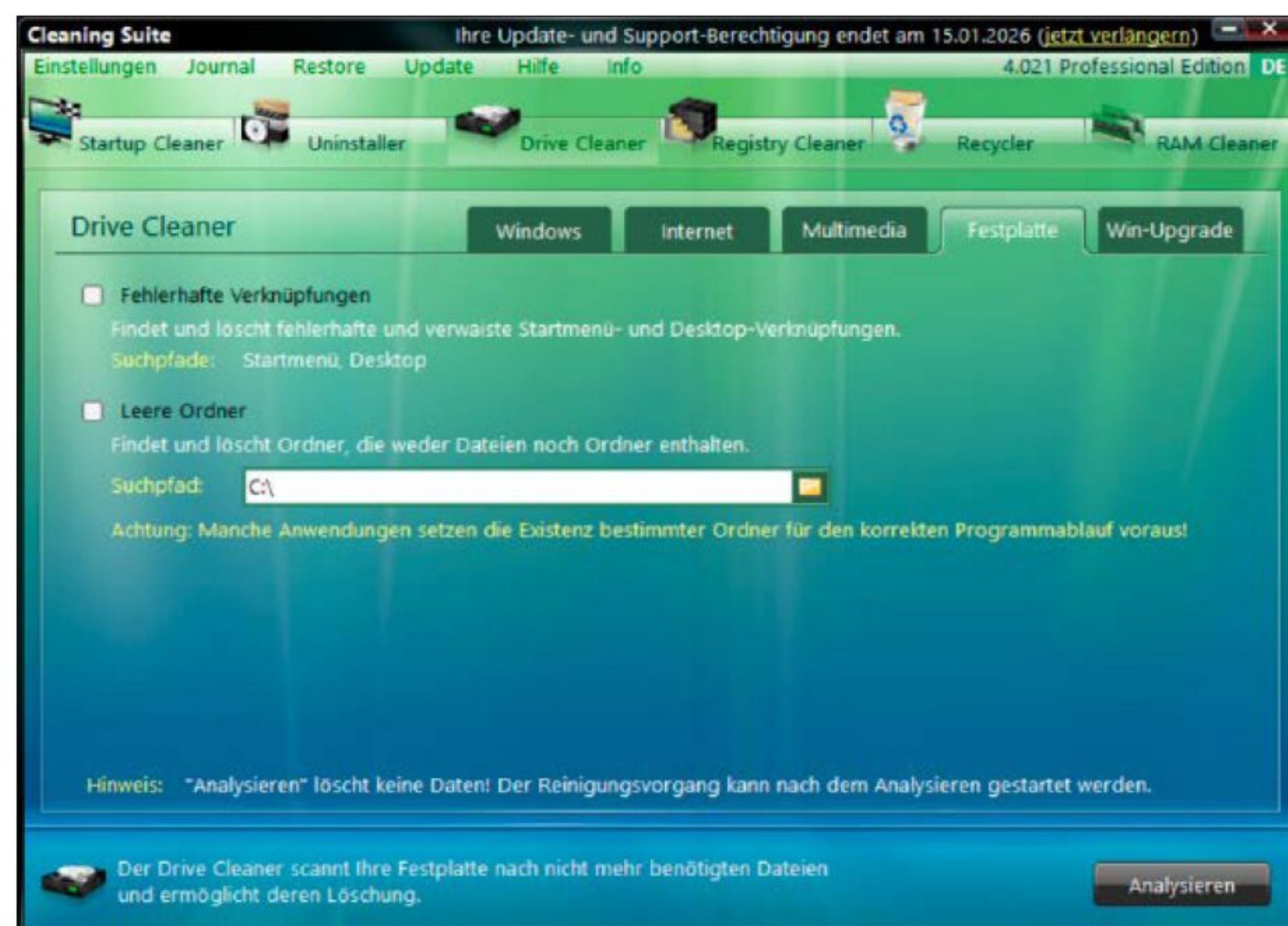
Vollversion mit Registrierung für Windows 10, 11

Ascomp Cleaning Suite Professional deinstalliert Programme, räumt das Startmenü auf, entfernt nicht mehr benötigte Dateien und mistet die Registry aus.

Installation: Klicken Sie auf „Jetzt registrieren“ und geben Sie Ihren Namen, Ihre Mailadresse sowie Ihr Wohnland an. Klicken Sie auf „Abschicken“. Haben Sie noch

kein Ascomp-Konto, erhalten Sie einen Link zu Ihrem (neuen) Kundenmenü per Mail. Haben Sie bereits ein Kundenkonto, melden Sie sich über den Link in der Mail an und speichern das Programm

Ascomp Cleaning Suite Professional befreit Ihre Windows-Installation von überflüssigen Dateien, Programmen, Registry-Einträgen und mehr.



über „Vollversion herunterladen“. Kommt keine Mail (auch nicht im Spam-Ordner), oder erhalten Sie eine Fehlermeldung, dass das Programm bereits auf Ihre Mailadresse registriert wurde, verwenden Sie eine andere Mailadresse. Schließen Sie das Fenster vom Anfang und führen Sie den Installer aus. Wählen Sie die Setup-Sprache, klicken Sie auf „OK“ und „Weiter“ und akzeptieren Sie die Lizenzvereinbarung. Wählen Sie mehrmals „Weiter“, dann „Installieren“ und „Fertigstellen“. Beim ersten Start geben Sie Ihre Kundennummer ein und klicken auf „Freischalten“. ■

Ashampoo Winoptimizer 27

PC optimieren

Vollversion mit Registrierung für Windows 10, 11

Das Optimierungs-Tool durchforstet Ihren PC nach Tuning-Möglichkeiten. Dafür listet es nach der Analyse nicht mehr benötigte Dateien, Browser-Spuren, kaputte Verknüpfungen sowie Registry- und Autostart-Einträge auf und markiert die Funde blau. Alles, was okay ist, wird grün dargestellt.

Benchmarks testen, ob die Maßnahmen erfolgreich waren. Das Programm spürt auch Speicherfresser auf, sogar eine Verschlüsselungsfunktion ist an Bord.

Installation: Stimmen Sie den Nutzungsbedingungen sowie der Datenschutzerklärung über „Akzeptieren & Weiter“ zu. Klicken Sie auf „Lizenzschlüssel anfordern“ und tragen Sie Ihre Mailadresse ein. Bestätigen Sie mit „Hier Vollversionsschlüssel anfordern“. Lösen Sie ggf. das Captcha.

DerAshampoo Winoptimizer 27 bietet einige Funktionen, über die Sie Ihren PC beziehungsweise das Windows-System optimieren können.



Melden Sie sich mit Ihrem Ashampoo-Konto an, beziehungsweise erstellen Sie ein neues Konto mit Hilfe des Assistenten. Sobald Ihre Seriennummer angezeigt wird, übertragen Sie diese per Copy & Paste in das Fenster vom Anfang und klicken auf „Jetzt aktivieren!“. Klicken Sie auf „Weiter“, um die Installation zu starten, beenden Sie mit „Fertigstellen“.

Drivermax Pro 16

Automatische Treiber-Updates

Vollversion mit Registrierung, Jahreslizenz für Windows 10, 11

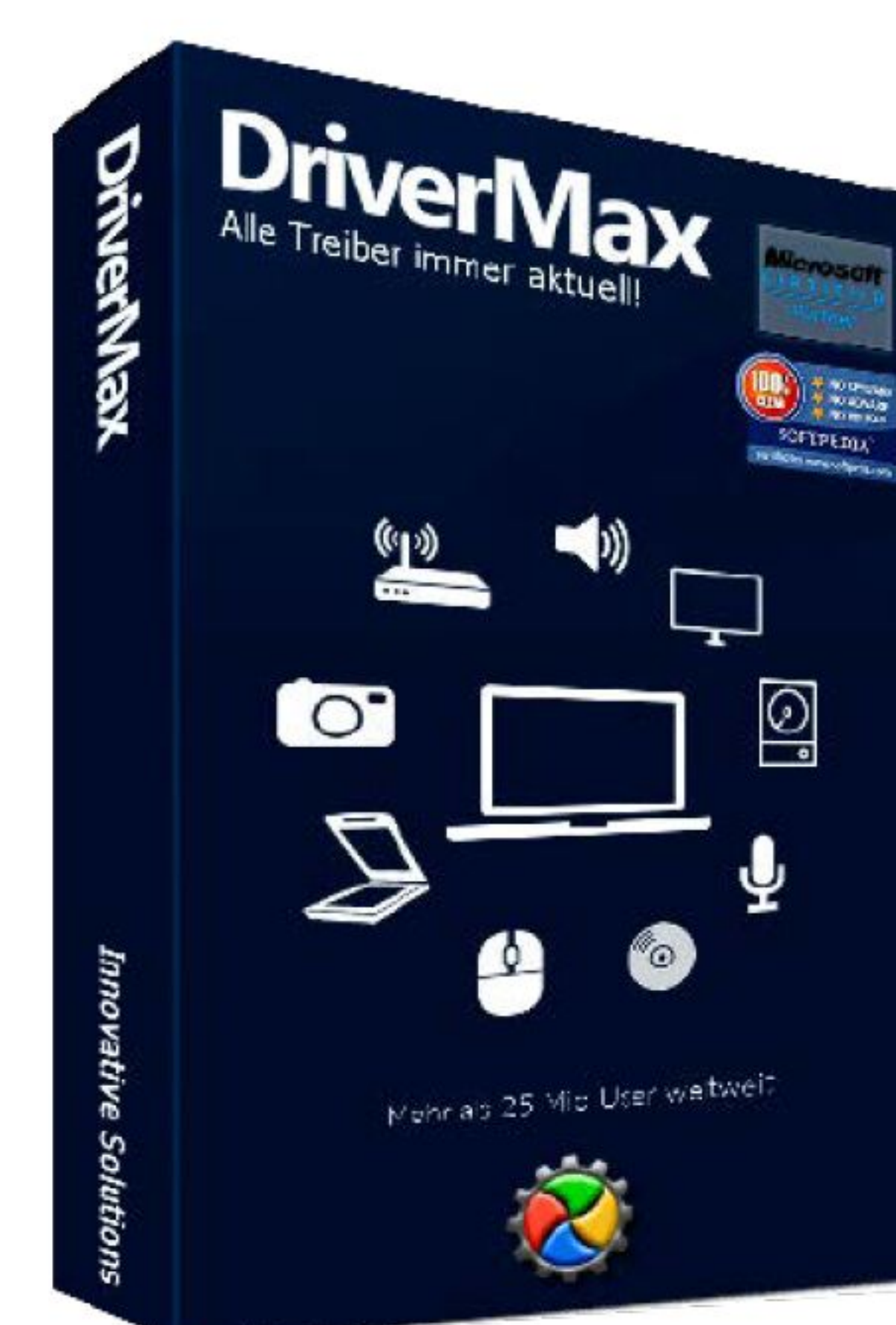
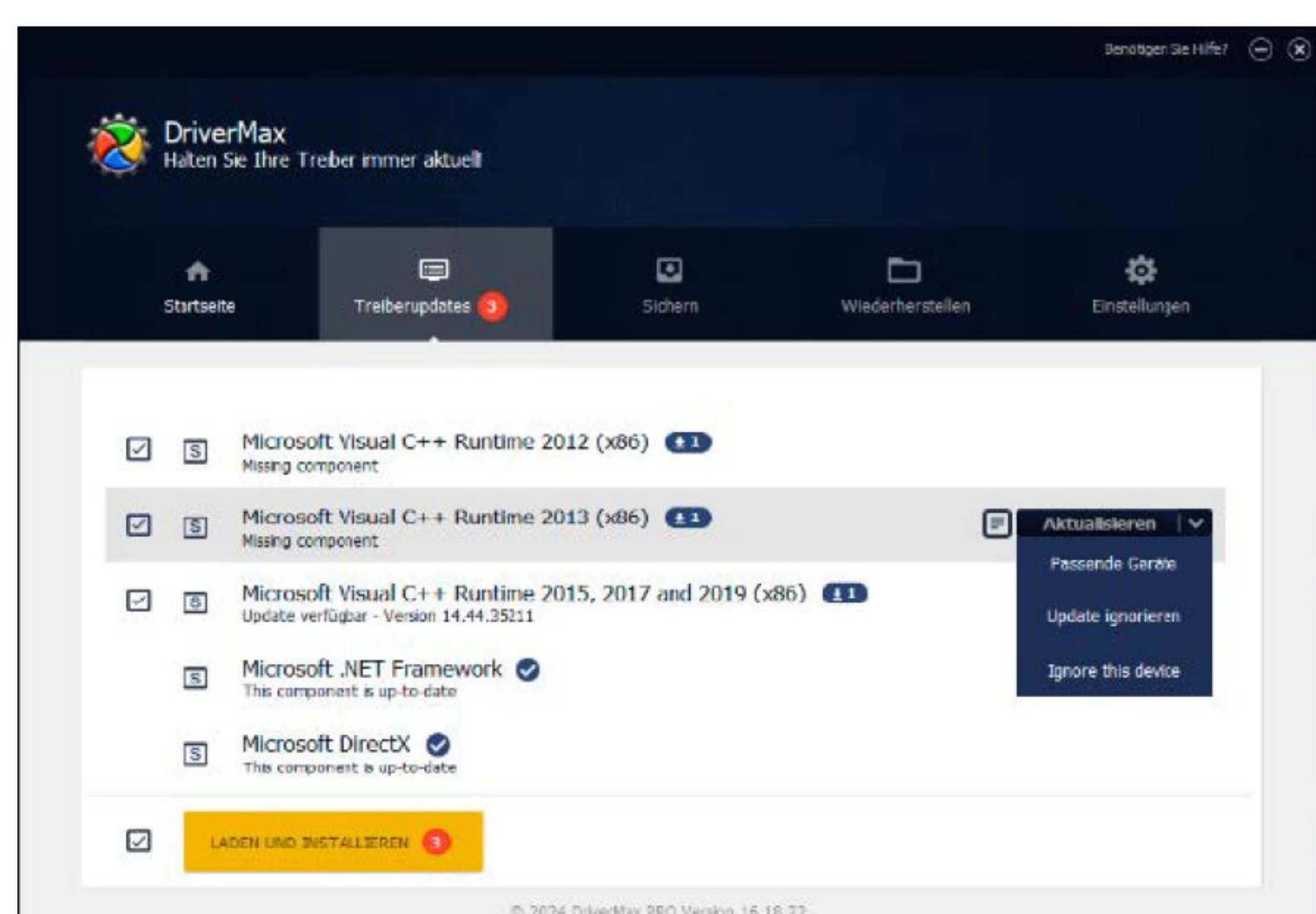
Drivermax Pro 16 hält Ihren PC auf dem neuesten Stand, was Treiber angeht. Dabei arbeitet das Programm selbstständig und listet nach einem Scan alle ausstehenden Updates für CPU, Audiogeräte, Schnittstel-

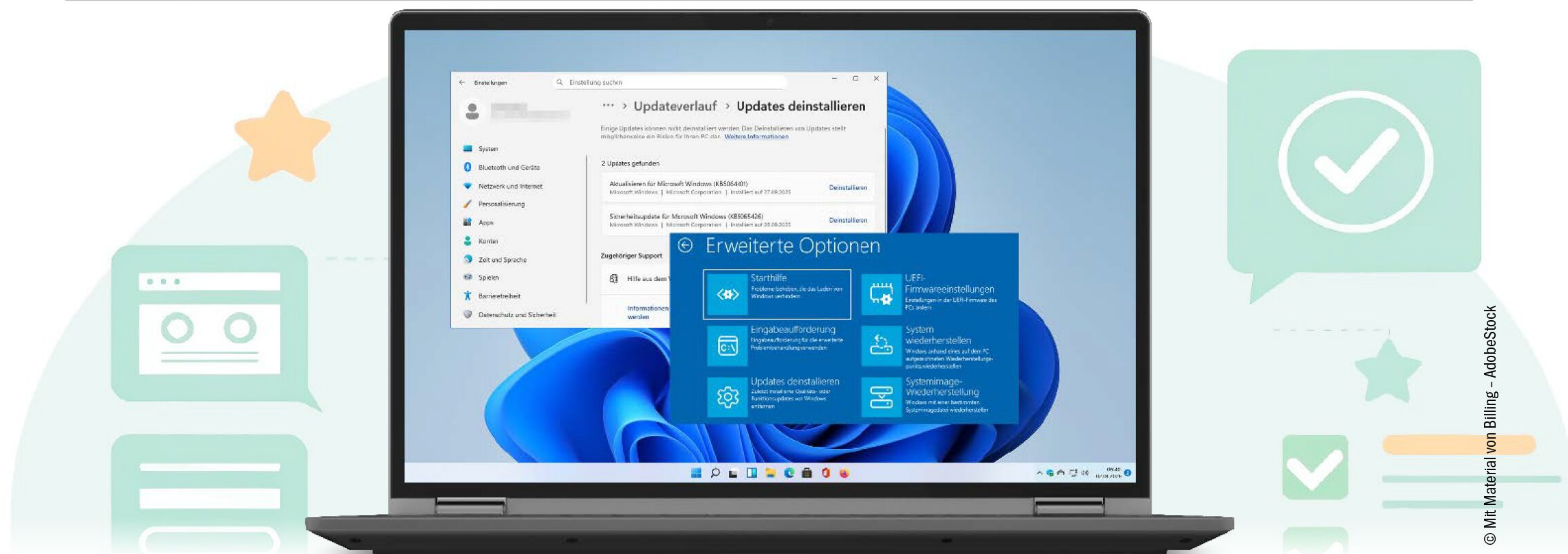
len-Controller etc. auf, sodass Sie diese nur noch ausführen müssen.

Installation: Um den Registrierungscode für die Jahreslizenz von Drivermax Pro 16 zu bekommen, müssen Sie sich unter <https://drivermax.de/notfallhandbuch2026/> registrieren und der Speicherung Ihrer Daten sowie dem Erhalt des Newsletters per Haken zustimmen. Bestätigen Sie, dass Sie

kein Roboter sind, und senden Sie das Formular ab. Sie erhalten Ihre User-ID sowie den Registrierungscode anschließend per Mail. Führen Sie den Installer aus, wählen Sie die Setup-Sprache und bestätigen Sie mit „OK“ und „Weiter“. Akzeptieren Sie die Lizenzvereinbarung und klicken Sie mehrmals auf „Weiter“. Nach der Installation öffnet sich das Programm, und Sie müssen den Registrierungscode eingeben. Nach der Vergabe eines Passwords ist das Programm einsatzbereit.

Drivermax listet alle Treiber und Systemkomponenten auf, die nicht mehr aktuell sind. Diese lassen sich direkt aktualisieren.





© Mit Material von Billing - AdobeStock

Die beste Hilfe bei Windows-Problemen

Nicht immer funktioniert alles, wie es soll. Für Probleme bietet Windows integrierte Hilfe-, Diagnose- und Reparaturfunktionen. Wenn diese nicht weiterhelfen, verwenden Sie die Tools der Heft-DVD.

VON THORSTEN EGGELING

Die Fehlerquellen bei Windows sind vielfältig, weil kein PC dem anderen gleicht. Hardware, Treiber und installierte Software stammen aus unterschiedlichsten Quellen, müssen aber trotzdem reibungslos mit dem Betriebssystem zusammenarbeiten. Updates für Windows, Treiber und Software beseitigen Sicherheitslücken und fügen neue Funktionen hinzu. Bisweilen werden Sie auch weitere Hardware anschließen, etwa einen neuen Drucker oder neue USB-Geräte. Jede dieser Änderungen kann zu

Fehlfunktionen führen. Dann streikt etwa plötzlich der Internetzugang, der Drucker arbeitet nicht, oder Programme können nicht mehr gestartet werden. Im schlimmsten Fall startet Windows nicht mehr, weil die Bootumgebung oder Systemdateien beschädigt sind.

Microsoft hat in Windows einige Assistenten und Hilfsmittel eingebaut, die Sie bei der Untersuchung und Reparatur des Systems unterstützen. Wir zeigen, wie Sie diese ansteuern, und stellen alternative Tools (auf Heft-DVD) vor, die in bestimmten Situationen mehr Erfolg versprechen.

1. Die integrierten Windows-Hilfefunktionen nutzen

In Windows sind bereits seit langer Zeit Assistenten für die Behebung von Problemen enthalten. Sie verwenden die „Problembehandlung“, etwa um Fehler beim Windows Update, der Audio- und Video-Wiedergabe oder bei Netzwerkverbindungen zu beseitigen. Die Funktionen finden Sie in der Einstellungen-App (Win-I) über „System → Pro-

blembehandlung“ (Windows 10: „Update & Sicherheit → Problembehandlung“). Windows bietet die Problembehandlung teilweise automatisch an. Wie sich das System verhält, können Sie unter „Empfohlene Problembehandlung“ festlegen. Der Standard ist „Mich vor dem Ausführen fragen“. Zu den Assistenten gelangen Sie nach einem Klick auf „Andere Problembehandlungen“ (Windows 10: „Zusätzliche Problembehandlungen“). Klicken Sie bei der gewünschten Problembehandlung auf „Ausführen“. Nutzer von Windows 10 klicken die Rubrik an und dann auf „Problembehandlung ausführen“.

Ab Windows 11 Version 23H2 hat Microsoft die Problembehandlung deutlich umgebaut. Bisher war das Microsoft Support Diagnostic Tool (MSDT) für die Funktionen zuständig, jetzt hat Microsoft es durch die Get-Help-App ersetzt. Sie können die App auch direkt aufrufen, etwa über den Ausführen-Dialog (Win-R) durch Eingabe von *Gethelp* oder über eine Suche nach *Hilfe* im Startmenü. Das Fenster „Hilfe anfordern“

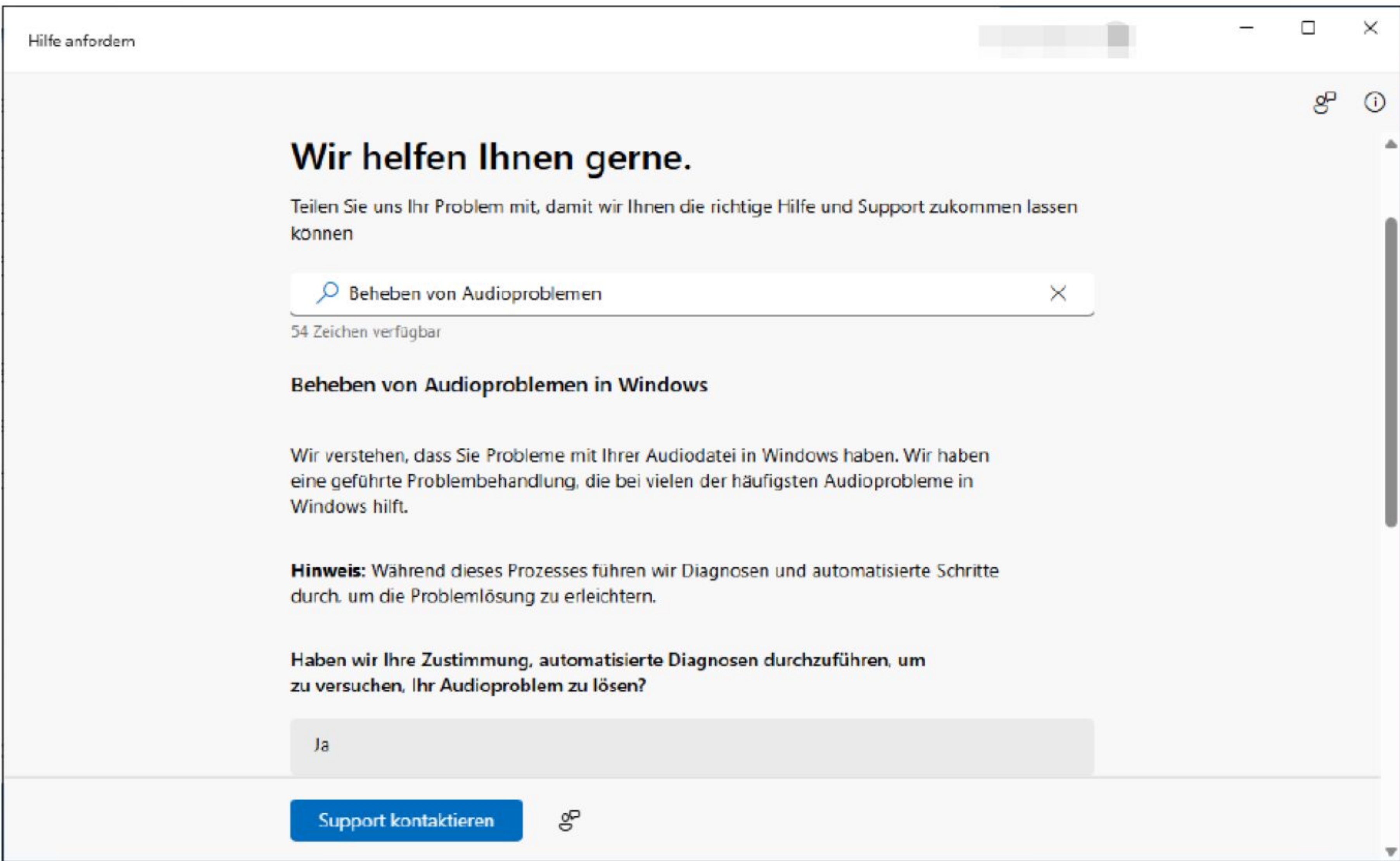
„Die Assistenten der Windows-Problembehandlung bieten Anleitungen und Diagnosefunktionen.“

zeigt eine Eingabezeile, in die Sie ein Stichwort oder die Problembeschreibung eingeben. Bereits während Sie tippen, erhalten Sie Vorschläge zum Thema. Diese liefern dann Anleitungen zur Problembehebung. Links zu weiteren Hilfen im Internet führen zu den Assistenten, die Sie auch gezielt über „Andere Problembehandlungen“ aufrufen können.

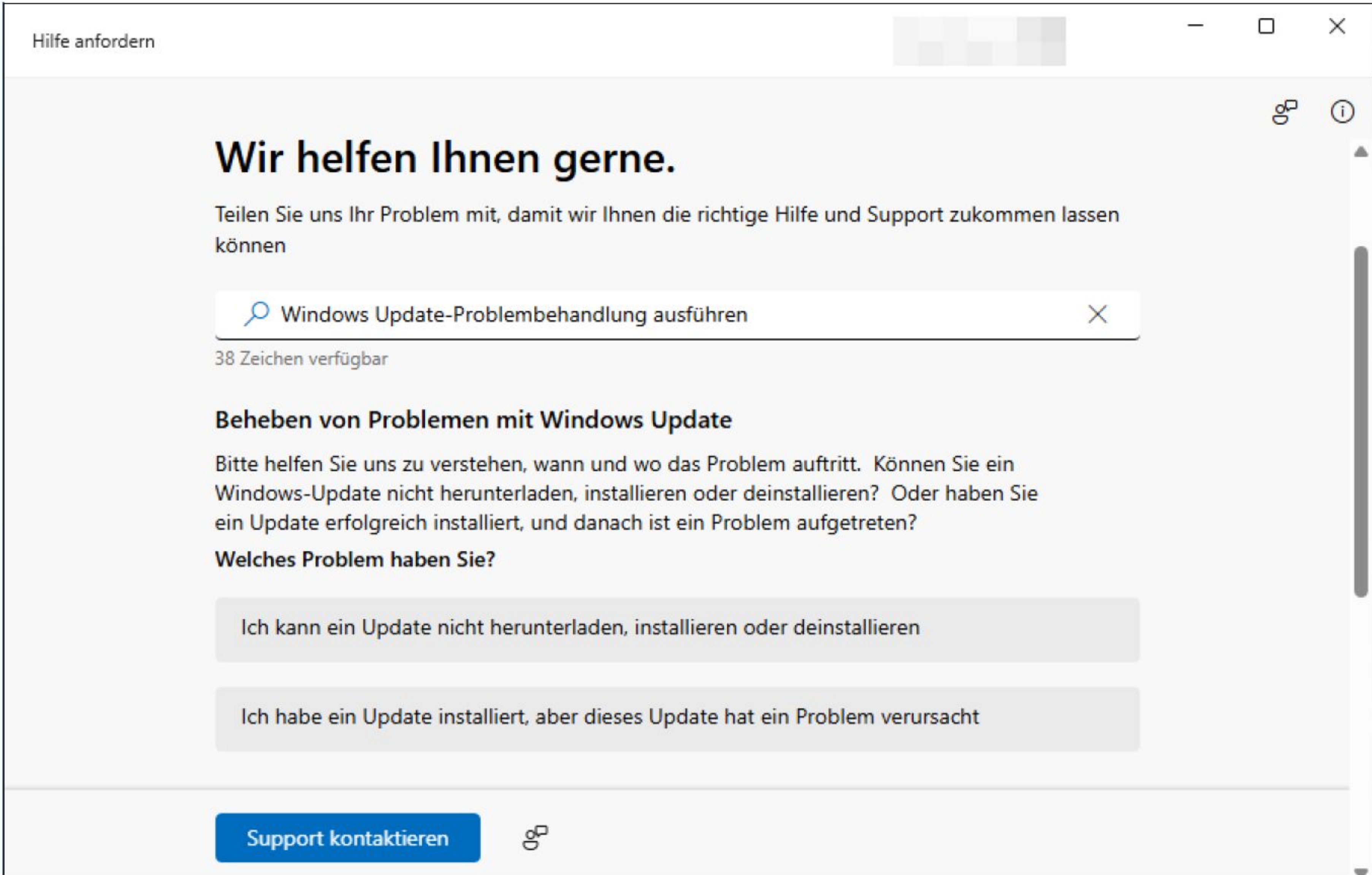
Der Zugang zur Problembehandlung wird teilweise auch an anderen Stellen angeboten. Ist keine Internetverbindung möglich, sehen Sie die Schaltfläche „Hilfe anfordern“ in den Einstellungen bei „Netzwerk und Internet“. Im Kontextmenü des Netzwerk-Icons im Infobereich finden Sie etwa die Funktion „Diagnostizieren von Netzwerkproblemen“ und beim Lautsprecher-Icon „Soundprobleme behandeln“.

2. Fehler beim automatischen Windows Update beheben

An jedem zweiten Dienstag im Monat ist es so weit: Microsoft liefert am sogenannten Patchday Updates für Windows und weitere Programme aus. Download und Installation erfolgen standardmäßig automatisch und ohne Zutun des Benutzers. Für Aufmerksamkeit sorgt ein Update erst, wenn ein Neustart angefordert wird. Das gilt aber nur, solange Updates nicht fehlschlagen. Windows Updates verursachen manchmal Probleme, die einzelne Funktionen blockieren. Man kann dann das letzte Update deinstallieren oder auf ein verbessertes Update warten. Deutlich häufiger sind Fehler bei der Update-Installation. Eine Aktualisierung lässt sich dann nicht durchführen und Sie sehen nur eine Fehlermeldung. Windows wiederholt den Update-Versuch fortwährend, ist aber nicht erfolgreich. Was diese Fehler verursacht, ist nur schwer auszumachen. Manchmal sind Update-Dateien oder Systemdateien beschädigt, oder eine Software blockiert die Aktualisierung.




Hilfe erhalten: Die in Windows 11 neu gestaltete Problembehandlung kann Diagnosen durchführen und Fehler beheben. Sie können Ihr Problem auch manuell beschreiben.



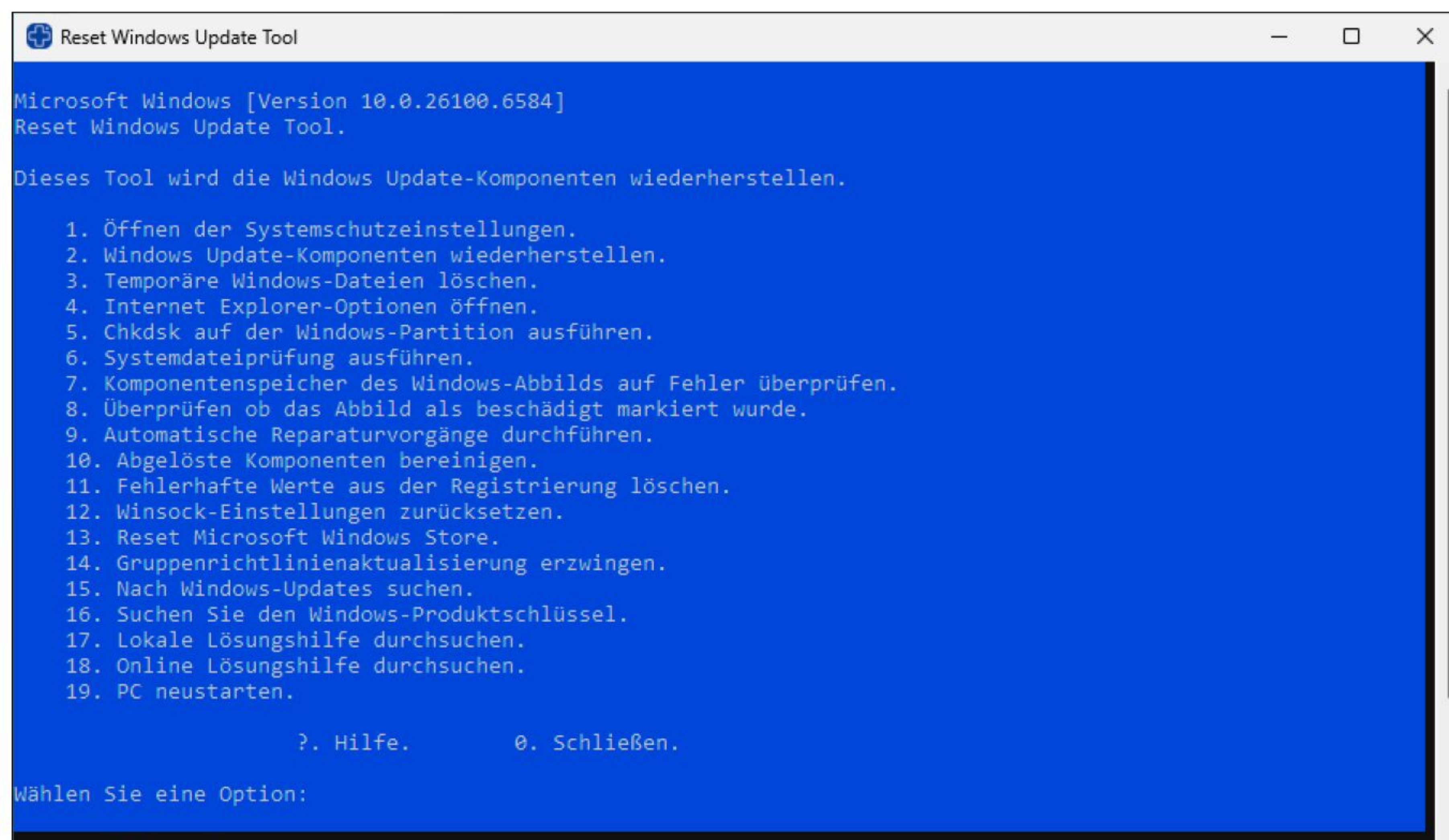
Update-Fehler: Der Assistent der Problembehandlung gibt Problembeschreibungen vor. In der Regel müssen Sie den Fehler ausführlicher beschreiben, um weitere Hilfen zu erhalten.

Problemlösung mit Bordmitteln: Gehen Sie in den Einstellungen (Win-I) auf „System → Problembehandlung → Andere Problembehandlungen“. Sie sehen eine Liste der verfügbaren Assistenten. Klicken Sie hinter „Windows Update“ auf „Ausführen“.

IM ÜBERBLICK: WARTUNGS-TOOLS FÜR WINDOWS

Name	Beschreibung	Auf	Internet	Sprache
Cleanmgr Plus	Aufräum-Tool	-	https://github.com/builtbybel/CleanmgrPlus	Deutsch
Lazesoft Recovery Suite Home Edition Free	Reparatur-Tools und Notfall-System	Heft-DVD	www.lazesoft.com	Englisch
Reset Windows Update Tool	Windows Update reparieren	Heft-DVD	https://wureset.com	Deutsch
Tweak Power	Windows konfigurieren und aufräumen	Heft-DVD	https://kurtzimmermann.com	Deutsch
Windows Manager	Windows reparieren und optimieren	Heft-DVD*	www.yamicsoft.com	Deutsch
Windows Repair Free Portable	Bietet Reparaturfunktionen bei Systemproblemen	Heft-DVD	www.tweaking.com	Deutsch
Windows Repair Toolbox	Tools für die Hardware- und Systemanalyse	Heft-DVD	https://windows-repair-toolbox.com	Englisch

* 20-Tage-Testversion, danach ab 20 Dollar



Reset Windows Update Tool: Eine einfache Menüführung leitet Sie durch die Reparaturschritte. Meist genügt Schritt „2. Windows Update-Komponenten wiederherstellen.“.

Windows 11 fragt Sie zuerst nach dem bestehenden Problem. Klicken Sie auf „Ich kann ein Update nicht herunterladen, installieren oder deinstallieren“, wenn einer dieser Fehler vorliegt. Danach bestätigen Sie „Können wir die automatische Windows Update-Diagnose ausführen?“ mit „Ja“. Windows untersucht das Problem und führt automatisch Reparaturen durch.

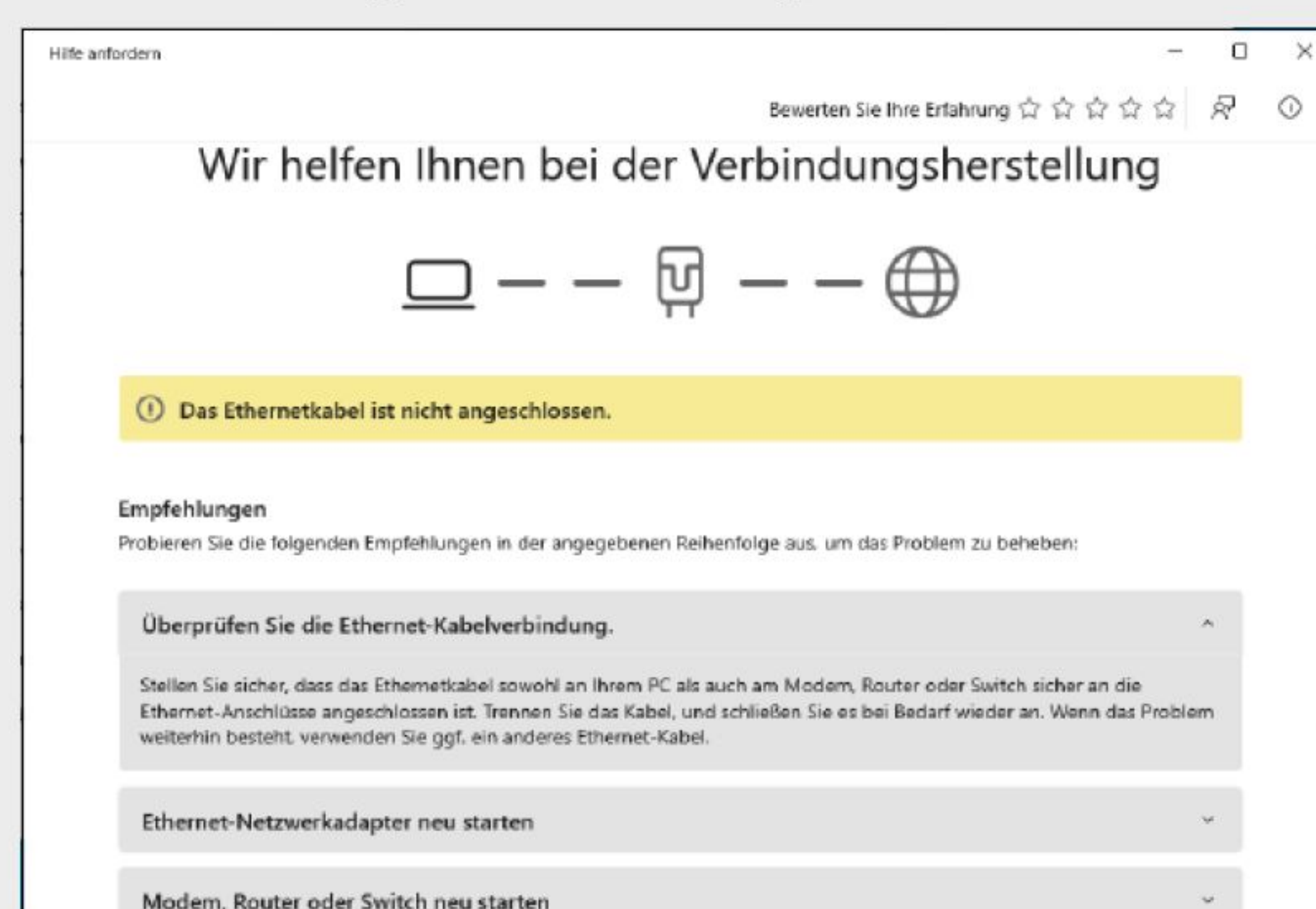
Die zweite Option ist „Ich habe ein Update installiert, aber dieses Update hat ein Problem verursacht“. Der Assistent möchte dann wissen, welche Fehlfunktion genau aufgetreten ist. Geben Sie die Beschreibung in die Eingabezeile ein und nutzen Sie die automatische Ergänzung als Eingabehilfe. Nach unserer Erfahrung zeigt der Assistent dann Hinweise zur Problemlösung

HILFE OHNE INTERNETVERBINDUNG?



Die Get-Help-App von Windows 11 hat einige Vorteile. Die Hilfetexte werden dynamisch aus dem Internet geladen oder per KI generiert und sollten daher stets aktuell sein. Microsoft reduziert damit zugleich den Aufwand, der in der Vergangenheit mit der Pflege von Hilfedateien oder der Problembehandlung verbunden war. Das hat allerdings zur Folge, dass die Assistenten der Problembehandlung ohne Netzwerkverbindung überhaupt nicht arbeiten.

Besteht gerade keine Internetverbindung, bemerkt die Get-Help-App das und zeigt allgemeine Empfehlungen zur Problemlösung. Unter „Benötigen Sie weitere Hilfe?“ ist ein QR-Code eingeblendet, den Sie mit dem Smartphone scannen können. Vorausgesetzt, dort ist der Internetzugriff möglich, öffnet sich im Browser die Seite <https://support.microsoft.com/home/contact>. Diese entspricht funktional der Get-Help-App – beziehungsweise: Die App zeigt eigentlich diese Seite an. Geben Sie eine Problembeschreibung ein, um sich bei der Lösung helfen zu lassen.



Hilfe ohne Internet: Die Problemhandlung setzt eine Internetverbindung voraus. Ist keine vorhanden, erhalten Sie nur allgemeine Anleitungen zur Behebung von Netzwerkproblemen.

ohne Erwähnung eines bestimmten Updates. Das ist jedoch eine Momentaufnahme, da die Inhalte stets aktuell vom Microsoft-Support stammen. Wenn Sie vermuten, dass das letzte Update einen Fehler verursacht hat, sollten Sie es einfach deinstallieren (siehe Punkt 4).

3. Windows Update mit Zusatz-tool reparieren

Wenn die Update-Problembehandlung Fehler beim Windows Update nicht beheben konnte, verwenden Sie das Reset Windows Update Tool. Entpacken Sie es in ein beliebiges Verzeichnis, klicken Sie Wureset.exe mit der rechten Maustaste an und wählen Sie „Als Administrator ausführen“. Das Tool verwendet eine einfache Menüführung, bei der die Auswahl durch Eingabe der angezeigten Ziffern erfolgt, was Sie mit der Enter-Taste bestätigen. Geben Sie zuerst 2 für eine deutschsprachige Oberfläche ein. Das Hauptmenü bietet zahlreiche Reparaturoptionen, die in bestimmten Fällen nützlich sein können, sich aber nicht direkt auf das Windows Update beziehen. Relevant ist „2. Windows Update-Komponenten wiederherstellen.“. Wenn Sie diese Option wählen, stoppt das Tool den Windows-Update-Dienst, bereinigt die zugehörigen Komponenten und stellt den Originalzustand wieder her. Danach starten Sie Windows neu und prüfen, ob das Windows Update jetzt korrekt arbeitet.

Wenn nicht, starten Sie Reset Windows Update Tool erneut und probieren „6. Systemdateiprüfung ausführen.“ sowie „7. Komponentenspeicher des Windows-Abbilds auf Fehler überprüfen.“. Starten Sie Windows nach jedem Reparaturschritt neu. Sollten Probleme mit App-Updates über den Microsoft Store auftreten, bietet das Tool „13. Reset Microsoft Windows Store.“ an. Kommt es weiter zu Fehlern, hilft wohl nur noch ein System-Reset (siehe Punkt 5).

4. Fehlerhafte Windows Updates entfernen

Nach der Installation eines Windows Updates können Probleme auftreten. Gehen Sie zuerst in der Einstellungen-App auf „Windows Update“ (Windows 10: „Update & Sicherheit → Windows Update“). Stellen Sie hinter „Updates aussetzen“ einen längeren Zeitraum ein, beispielsweise „Für 4 Wochen aussetzen“. Dadurch verhindern Sie, dass ein fehlerhaftes Update sogleich

wieder installiert wird. Windows-10-Nutzer klicken auf „Erweiterte Optionen“ und stellen unter „Anhalten bis:“ ein Datum in der Zukunft ein.

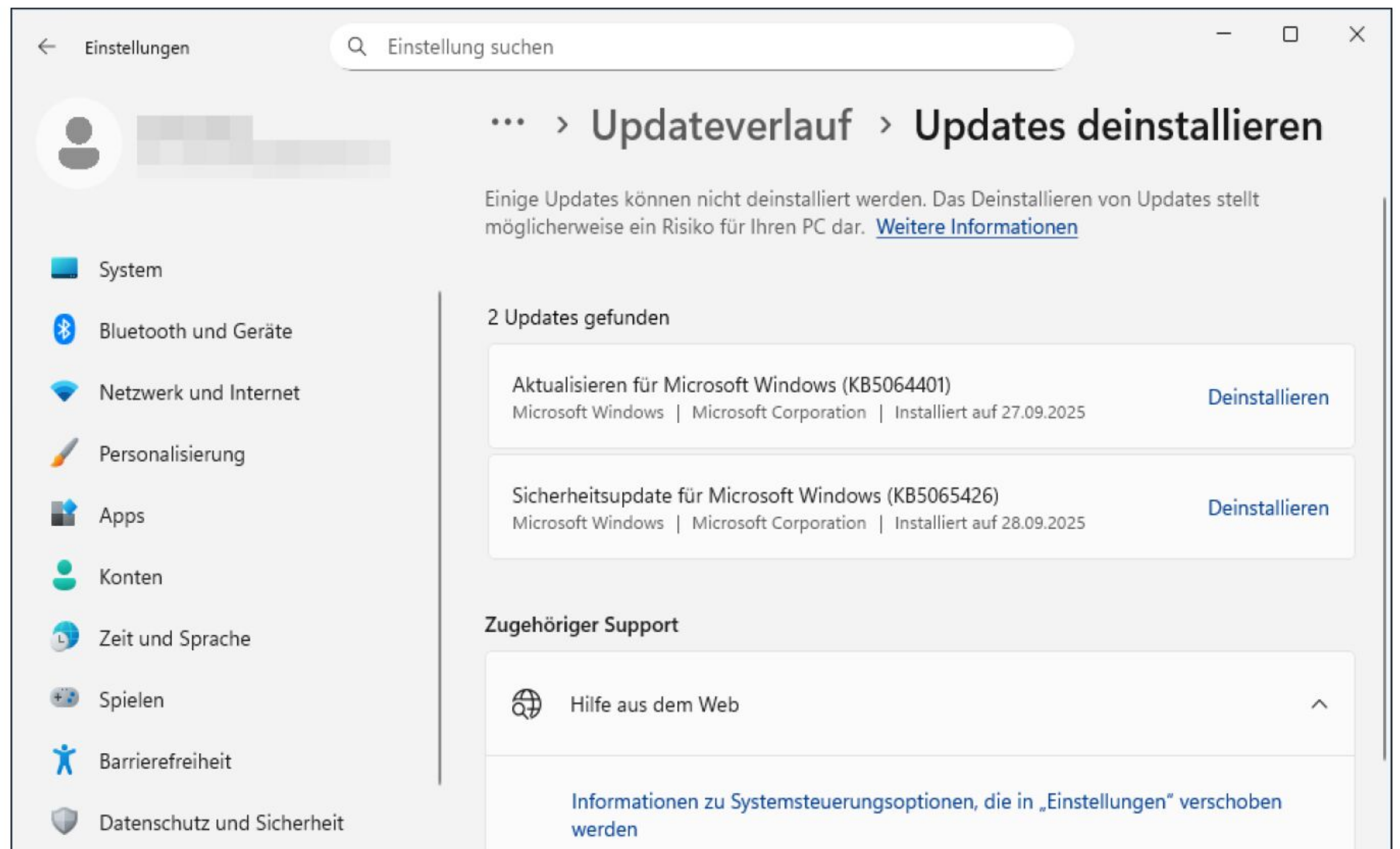
Klicken Sie auf „Updateverlauf“ oder bei Windows 10 auf „Updateverlauf anzeigen“. Unter Rubriken wie „Qualitätsupdates“ und „Treiberupdates“ sehen Sie chronologische Listen der installierten Updates mit den zugehörigen KB-Nummern. Der Klick auf einen Eintrag führt zu einer Microsoft-Seite mit weiteren Informationen zu einem Update. Eine Internetsuche nach der jeweiligen KB-Nummer kann Informationen darüber liefern, ob Fehler oder Abstürze im Zusammenhang mit diesem Update bereits bekannt sind.

Klicken Sie weiter unten unterhalb von „Verwandte Einstellungen“ auf „Updates deinstallieren“ (Windows 10: „Updates deinstallieren“ oben im Fenster) und entfernen Sie das Update, das einen Fehler verursacht. Bei Windows 10 führt der Link in der Systemsteuerung auf „Updates deinstallieren“. Sie können allerdings nicht beliebige Updates entfernen, weil diese aufeinander aufbauen. Windows 11 zeigt daher nur die letzten Updates an, die Sie auch deinstallieren können. Windows 10 zeigt auch ältere Updates, die Schaltfläche „Deinstallieren“ erscheint aber nur, wenn Sie einen der neueren Einträge anklicken. Wenn Microsoft den Fehler im Windows Update behoben hat, dann kann das Update erneut installiert werden. Die eingestellte Update-Verzögerung sollte hierfür genügend Zeit verschaffen.

5. Reparaturen über ein Zweitsystem durchführen

Sollte Windows aufgrund eines fehlerhaften Updates oder aus anderen Gründen nicht mehr starten, benötigen Sie ein Rettungssystem, das Sie von einem USB-Stick booten. Für mehr Komfort verwenden Sie das Lazesoft-Rettungssystem (Kasten „Tools, die bei Windows-Problemen helfen“).

Sie können auch das Windows-11-Installationssystem booten. Nach den Spracheinstellungen wählen Sie „Meinen PC reparieren“ und gehen dann auf „Problembehandlung“. Wählen Sie „Starthilfe“, um Fehler in der Bootumgebung zu beseitigen. Über „Updates deinstallieren“ entfernen Sie das letzte Qualitäts- oder Funktionsupdate, wenn dieses Probleme verursacht. Verwenden Sie „System wiederherstellen“, um



Updates entfernen: Problematische Windows Updates können deinstalliert werden. Da diese aufeinander aufbauen, ist das nur mit den letzten Updates möglich.

TOOLS, DIE BEI WINDOWS-PROBLEMEN HELFEN

Die Windows-Problembehandlungen können wertvolle Hilfe leisten, die Reparaturfunktionen sind jedoch begrenzt. Unsere Tool-Empfehlungen haben mehr zu bieten.

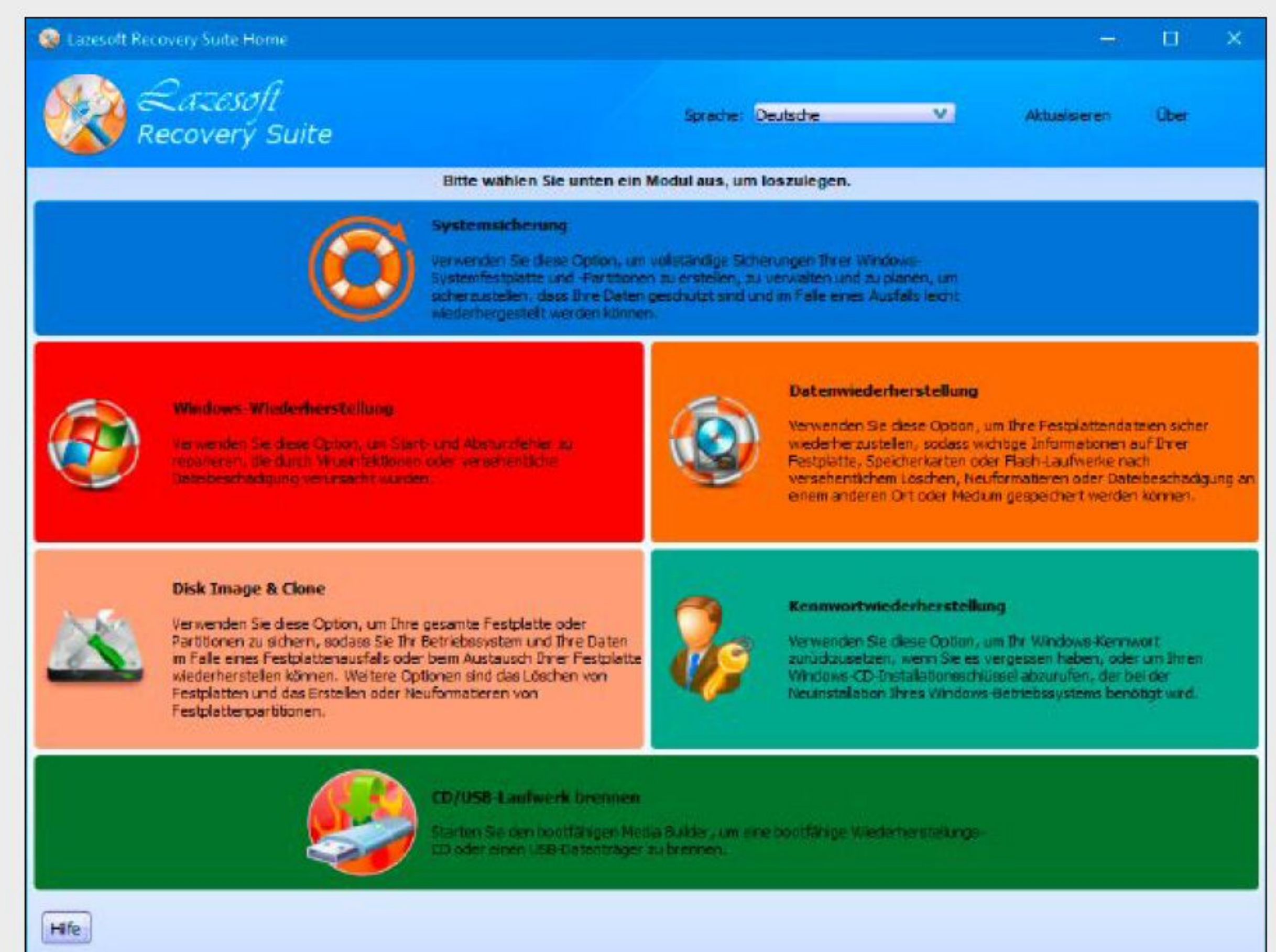
Cleanmgr Plus ersetzt die Windows-Datenträgerbereinigung, aber mit mehr Funktionen. Sie räumen damit Windows auf und löschen unnötige Dateien.

Lazesoft Recovery Suite enthält Funktionen für die Wiederherstellung gelöschter Dateien und kann Image-Backups von Laufwerken erstellen. Besonders nützlich ist das Rettungssystem, das Sie von einem USB-Stick booten können. Damit retten Sie wichtige Dateien von der Festplatte, reparieren die Bootumgebung oder setzen das Windows-Passwort zurück. Sie haben im Rettungssystem außerdem Zugriff auf die Microsoft-Wiederherstellungsumgebung, über die Sie auch Updates deinstallieren können.

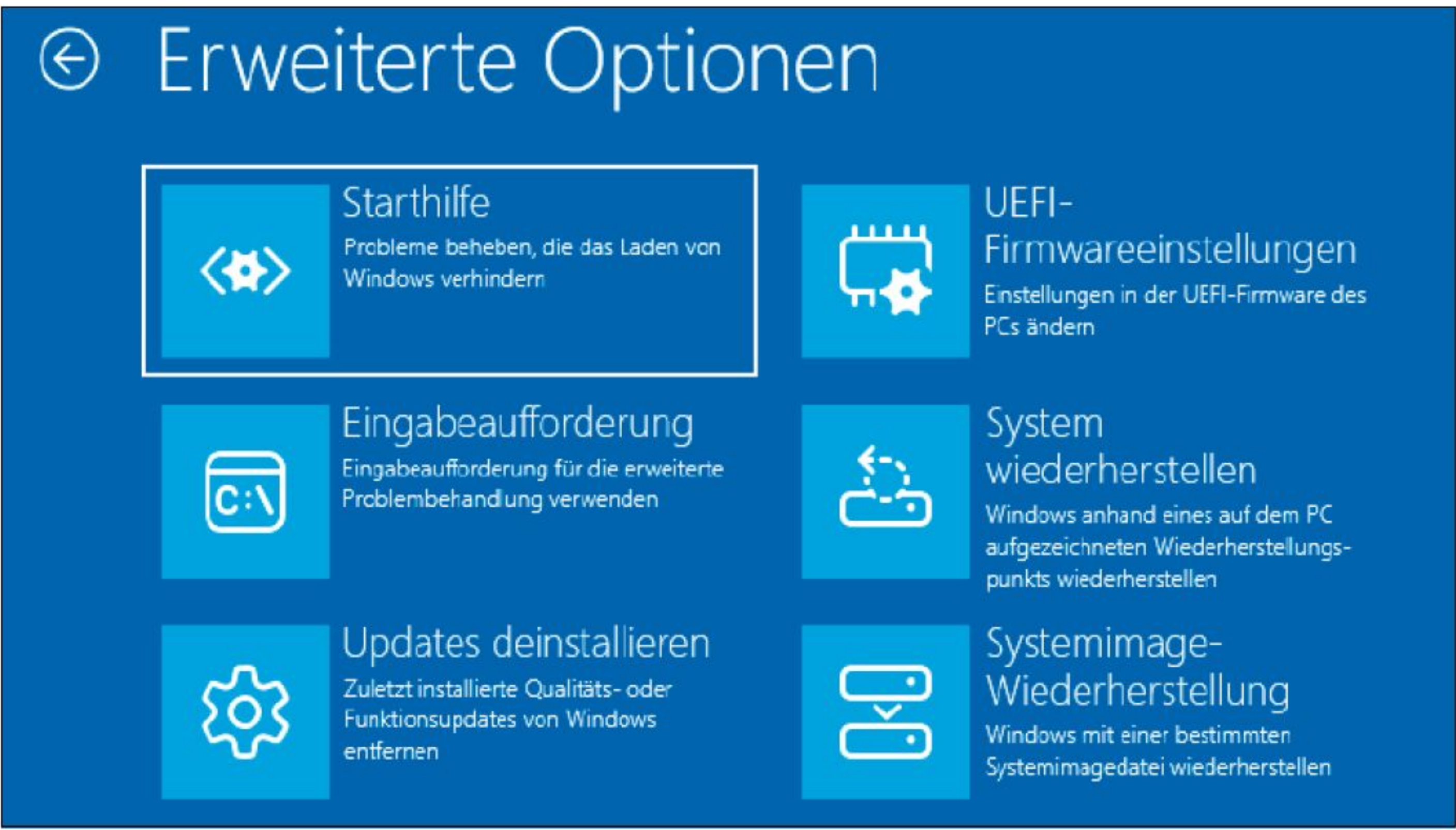
Tweak Power ist eine Oberfläche für die Windows-Optimierung und den schnellen Zugriff auf wichtige Optionen. Unter „System → Windows reparieren“ bietet das Tool Bereiche wie

„Windows“, „Sicherheit“ und „Browser“ und darin jeweils eine Liste mit Fehlerbeschreibungen. Klicken Sie an, was Sie beheben wollen, und dann auf „Reparatur ausführen“.

Windows Manager bietet Wartungs- und Optimierungsfunktionen. Unter „System reparieren“ finden Sie zahlreiche Diagnose- und Reparaturoptionen.



Lazesoft Recovery Suite: Über „CD/USB-Laufwerk brennen“ erstellen Sie ein Rettungssystem, das Sie vom USB-Stick booten können. Es enthält zahlreiche Funktionen für die Windows-Reparatur.

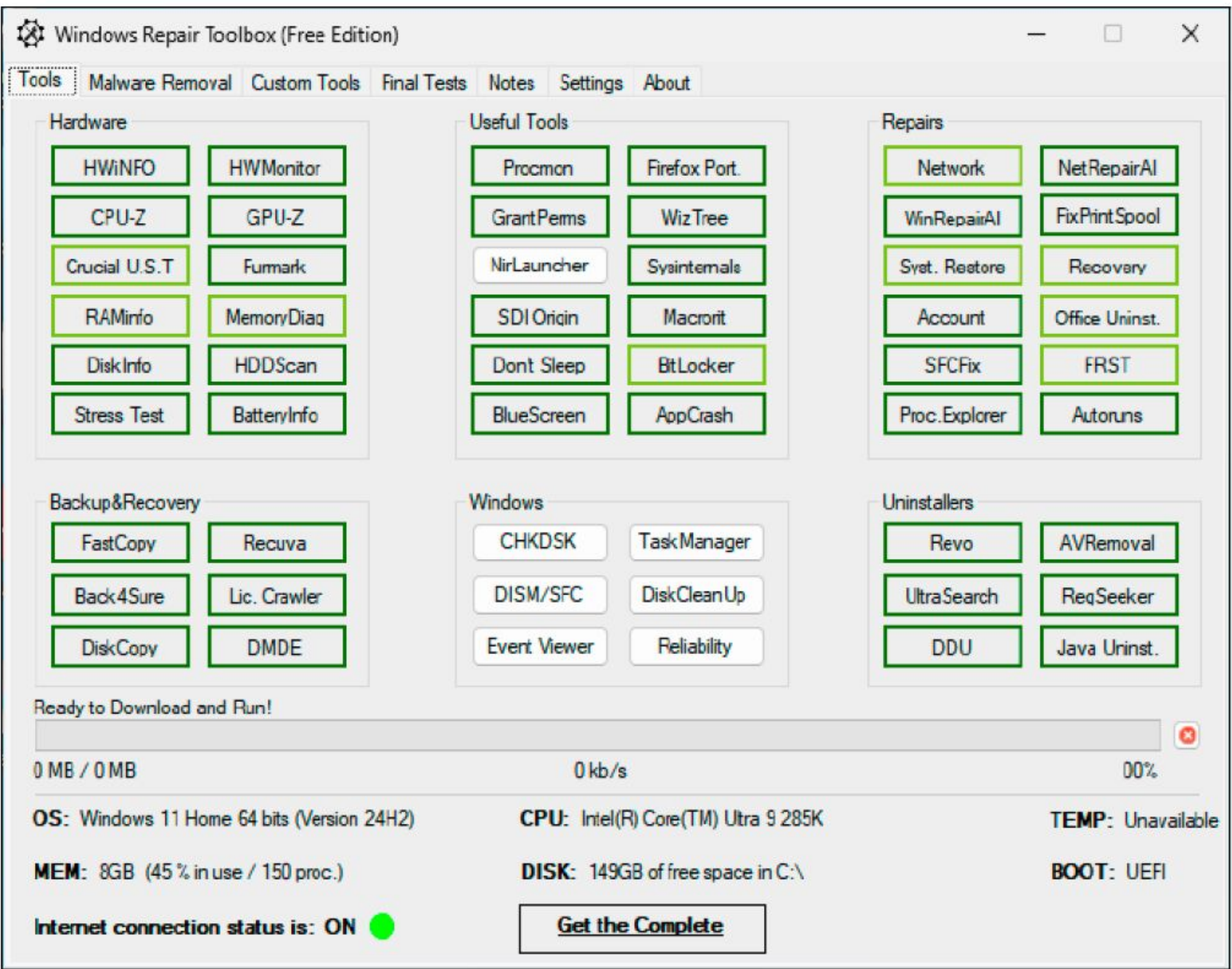


Reparatur bei Startproblemen: Im Rettungs- oder Wiederherstellungssystem können Sie Updates deinstallieren oder das System auf einen Wiederherstellungspunkt zurücksetzen.

wählen Sie nach der automatischen Reparatur „Erweiterte Optionen“ dann „Problembehandlung“ und „Diesen PC zurücksetzen“. Klicken Sie auf „Eigene Dateien beibehalten“ und dann auf „Cloud-Download“ (aktuelle Dateien aus dem Internet) oder „Lokale Neuinstallation“ (schneller). Folgen Sie weiter den Anweisungen des Assistenten. Nach einem Klick auf „Zurücksetzen“ wird Windows neu installiert. Die persönlichen Dateien bleiben erhalten. Apps und Programme werden entfernt und müssen danach neu installiert werden.



Kein Netzwerk: In den Einstellungen sehen Sie unter „Netzwerk und Internet“ den Status der Verbindung. Wenn keine Verbindung möglich ist, erhalten Sie Unterstützung per Klick auf „Hilfe anfordern“.



Windows Repair Toolbox: Das Tool bietet eine Programmsammlung für die Systemdiagnose und Reparatur. Sie können die Toolbox vorab mit den gewünschten Tools bestücken.

6. Fehlfunktionen des Netzwerks untersuchen

Fehler bei Netzwerkverbindungen sind besonders schwierig zu finden, weil zahlreiche Komponenten beteiligt sind. Angefangen beim Ethernet- oder WLAN-Adapter, über Kabel und Funkstrecke, WLAN-Access-Point oder Switch bis zum Router können eine Unterbrechung oder ein Defekt vorliegen. Vielleicht hat auch der Internetanbieter temporär den Dienst eingestellt oder der Browser mag gerade keine Webseiten anzeigen. Um fast alles abzudecken, gibt es bei den Problembehandlungen von Windows 10 die Bereiche „Internetverbindungen“, „Eingehende Verbindungen“, „Freigegebene Ordner“ und „Netzwerkadapter“. Bei Windows 11 hat Microsoft die Optionen auf „Netzwerk und Internet“ reduziert. Eine wirkliche Diagnose findet bei der Problembehandlung jedoch nicht statt. Es wird festgestellt, ob Sie mit dem Internet verbunden sind. Dazu erhalten Sie einige Tipps zur Problemlösung, etwa „Versuchen Sie es mit einer anderen Website“, „Prüfen Sie die Ethernet-Kabelverbindung“ und „Modem, Router oder Switch neu starten“.

Tip: Eine fehlerhafte Konfiguration des Netzwerkadapters oder der Netzwerkkomponenten können den Netzwerk- oder Internetzugang verhindern. Für die Reparatur gehen Sie in den Einstellungen auf „Netzwerk und Internet → Erweiterte Netzwerkeinstellungen → Netzwerk zurücksetzen“ und klicken auf „Jetzt zurücksetzen“. Danach wird der PC neu gestartet.

Windows auf den letzten Wiederherstellungspunkt zurückzusetzen.
Windows komplett zurücksetzen: Sollten sich Windows-Probleme mit den bisher beschriebenen Methoden nicht beheben lassen, hilft nur eine Radikalkur. Nach mehre-

ren vergeblichen Startversuchen führt Windows eine automatische Reparatur durch. Dabei startet das Wiederherstellungssystem von der Festplatte. Nach Abschluss der Reparatur klicken Sie auf „Neu starten“. Wenn Windows weiterhin nicht startet,

7. Netzwerkprobleme analysieren und beheben

Sollten die Anleitungen der Problembehandlung nicht weiterhelfen, probieren Sie das Tool **Windows Repair Toolbox** aus. Es handelt sich dabei um einen Werkzeugkas-

ten mit zahlreichen Tools für die Reparatur und Wartung des Systems. Die Tools stammen größtenteils von anderen Anbietern und müssen erst heruntergeladen werden. Bei Internetproblemen bereiten Sie das Tool rechtzeitig vor, oder Sie erledigen das auf einem funktionstüchtigen Gerät, wofür Sie Windows Repair Toolbox auf einen USB-Stick entpacken.

Nach dem Start von Windows Repair Toolbox gehen Sie auf die Registerkarte „Settings“ und klicken auf „Update All“. Wenn gewünscht, können Sie über die Schaltfläche mit dem Zahnradsymbol die Downloads auf die für Sie wichtigen Programme beschränken. Die Toolbox ermöglicht den Start einiger Werkzeuge für Reparaturen, Hardware-Check, Backups, Virens Scanner und den schnellen Zugriff auf nützliche Windows-Tools.

Auf der Registerkarte „Tools“ klicken Sie unter „Repairs“ auf „NetRepairAll“. Es startet das Tool **Netadapter Repair All in One**, das Ihnen wichtige Daten wie IP-Adressen und DNS-Server anzeigt. Es ist empfehlenswert, einzelne Reparaturen per Klick auf die jeweilige Schaltfläche durchzuführen, etwa „Release and Renew DHCP Address“ (neue IP-Adresse holen) und „Flush DNS Cache“ (DNS-Cache löschen). Hinter „Clear Host File“ klicken Sie auf „View“, um sich die Datei „C:\Windows\System32\drivers\etc\hosts“ anzusehen. Standardmäßig sind alle Zeilen mit dem Zeichen „#“ auskommentiert. Es kann aber sein, dass Schadsoftware die Datei manipuliert hat und IP-Adressen auf fremde Server umleitet. Sollte das der Fall sein, stellen Sie den Standard per Klick auf „Clear Host File“ wieder her.

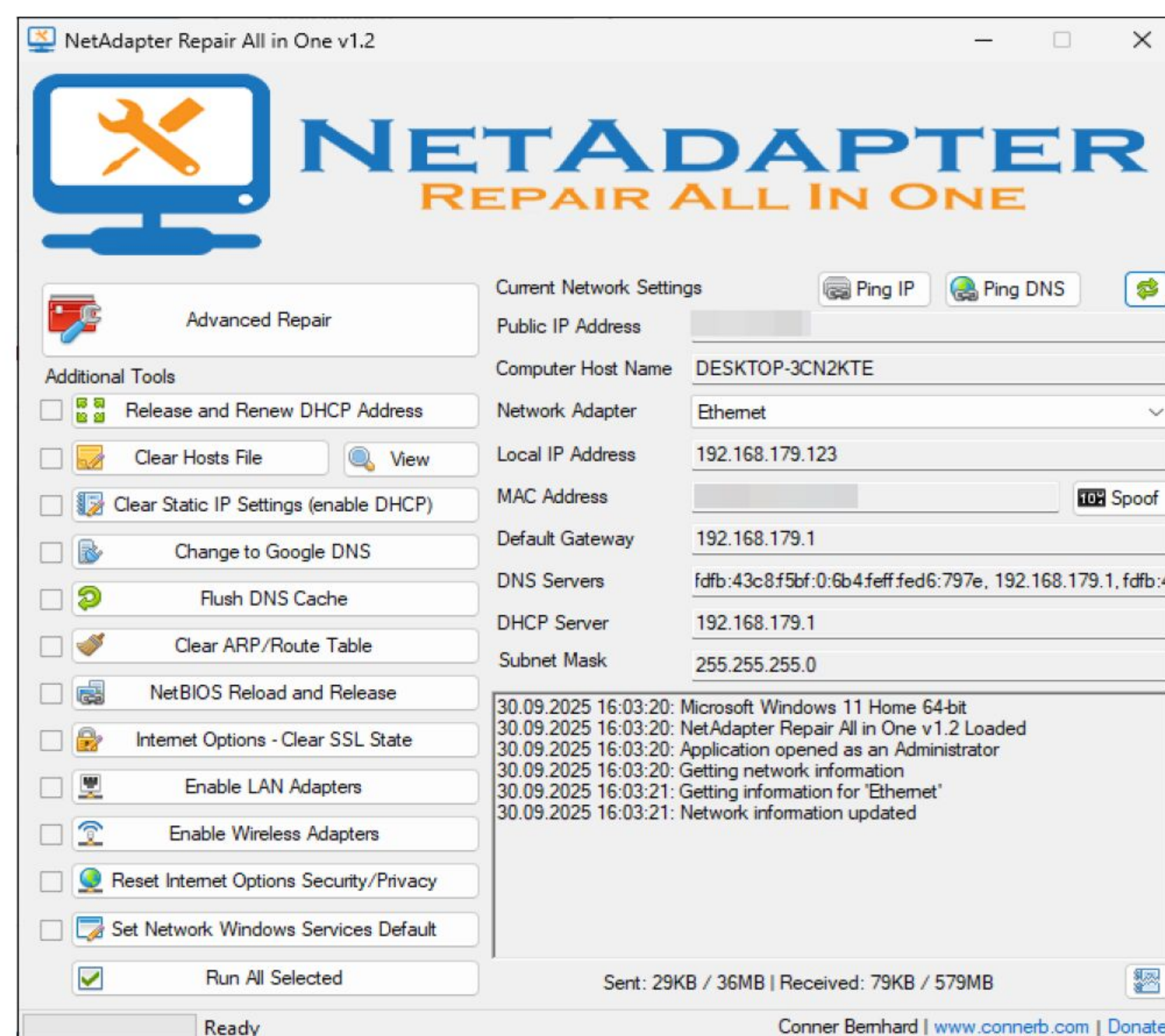
Sie können auch mehrere Reparaturschritte nacheinander durchführen, indem Sie Häkchen vor die für Sie relevanten Schaltflächen setzen und dann auf „Run All Selected“ klicken.

8. Universal-Tool für mehrere Reparaturen nutzen

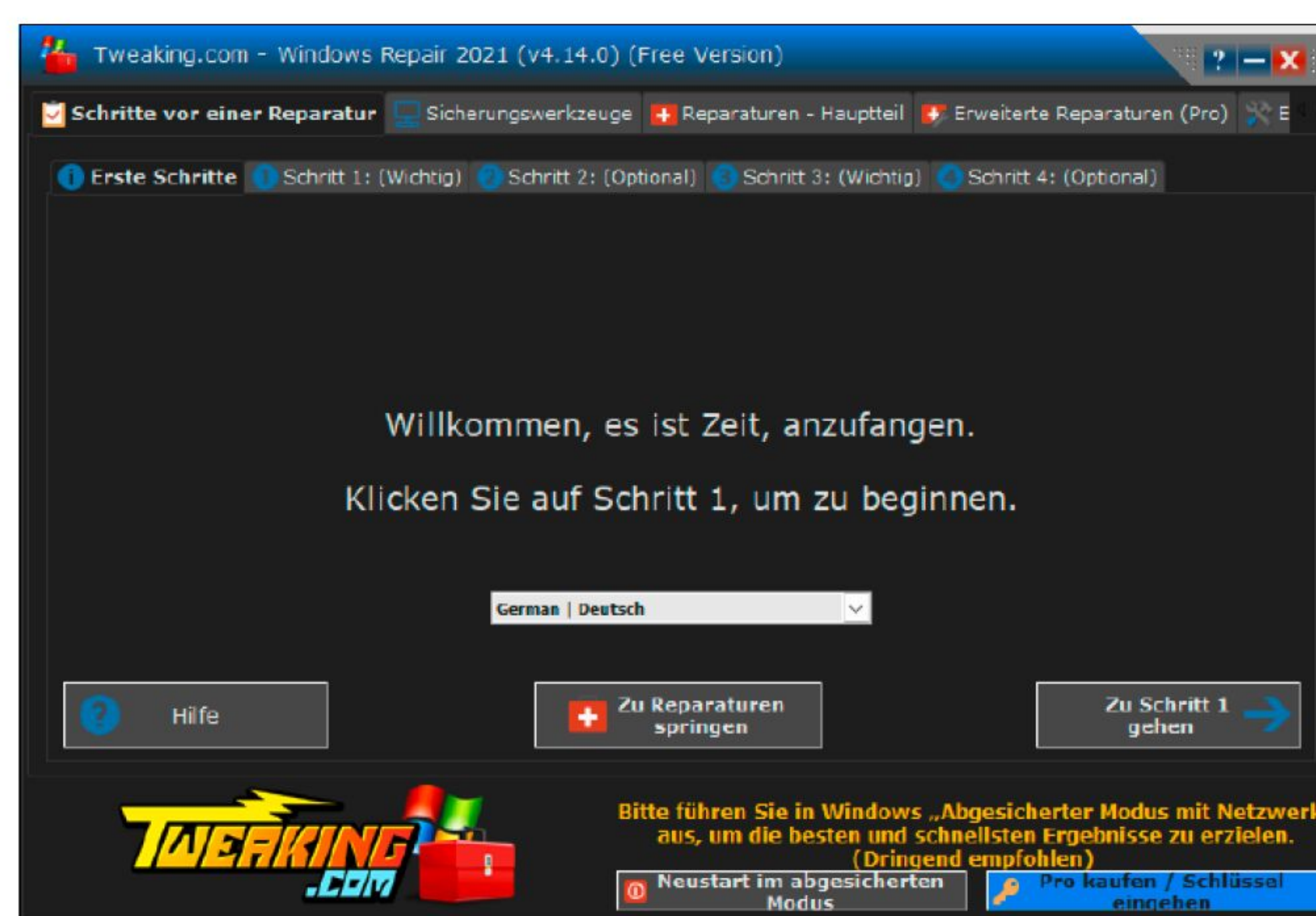
Mit **Windows Repair all-in-one** lassen sich zahlreiche Windows-Probleme beheben, darunter die Reparatur von Windows-Update-Funktionen, Netzwerk, fehlerhaften Berechtigungen im Dateisystem oder in der Registry und vielem mehr.

Sie können Windows Repair all-in-one über Windows Repair Toolbox starten, das portable Programm Windows Free Portable finden Sie ebenfalls auf DVD. Nach dem

Netzwerk reparieren: Starten Sie Netadapter RepairAll in One über Windows Repair Toolbox. Sie können damit häufig auftretende Netzwerkfehler untersuchen und beseitigen.



Windows Repair all-in-one: Das Tool fordert in den Schritten 1 bis 4 einige Vorbereitungen an. Für die reibungslose Reparatur starten Sie das Programm im abgesicherten Modus.

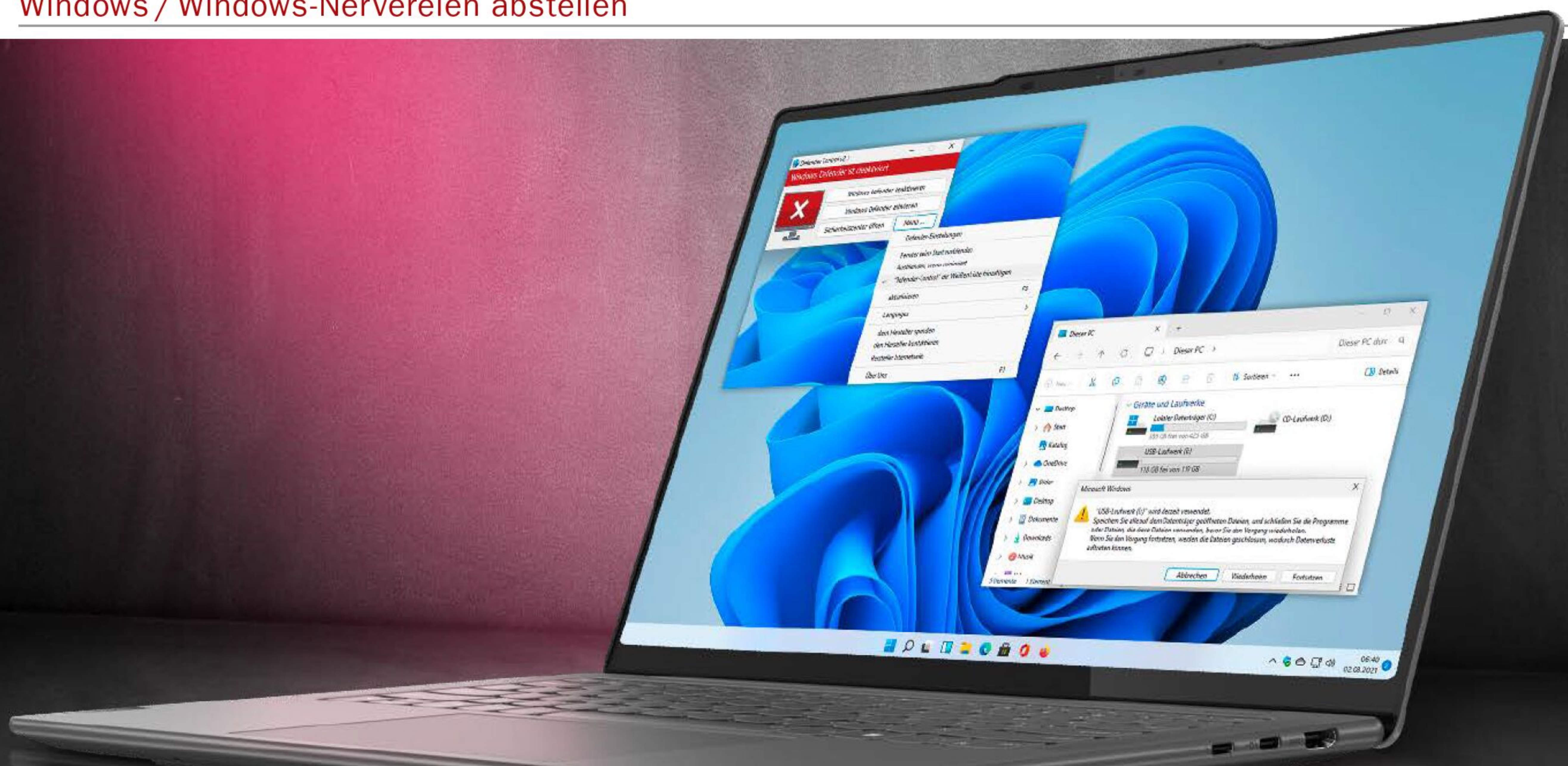


Start des Tools wählen Sie als Sprache „German | Deutsch“. Windows Repair all-in-one empfiehlt, alle Reparaturen im abgesicherten Modus durchzuführen. Dazu klicken Sie auf „Neustart im abgesicherten Modus“ und bestätigen mit „Ja“. Sobald Windows wieder läuft, starten Sie das Tool erneut.

Schritt 1: Windows Repair all-in-one empfiehlt auf der Registerkarte „Schritte vor einer Reparatur“ einige Vorbereitungen. Folgen Sie den Anweisungen des Assistenten von „Schritt 1“ bis „Schritt 4“. Schritt 1 fordert einen „ordnungsgemäßen Neustart“ an. Wenn Sie Windows – wie empfohlen – im abgesicherten Modus neu gestartet haben, ist das bereits erledigt. In den weiteren Schritten führen Sie einen Vorab-Scan, die Prüfung des Dateisystems und der Systemdateien durch. Per Klick auf die Schaltfläche „Hilfe“ können Sie sich über die jeweilige Funktion informieren.

Schritt 2: Gehen Sie auf die Registerkarte „Sicherungswerkzeuge“. Sie sollten zumindest das angebotene Backup der Registry wahrnehmen. Bei Problemen lässt sich die Registry im abgesicherten Modus nach Klicks auf „Wiederherstellen“ und „Restore Registry“ zurücksichern.

Schritt 3: Gehen Sie auf „Reparaturen – Hauptteil“. Klicken Sie auf „Voreinstellung: Windows-Update“, wenn Sie die Update-Funktionen reparieren möchten. Unter „Reparaturen“ ist vor alle Optionen ein Häkchen gesetzt, die Auswirkungen auf das Windows Update haben. Klicken Sie auf „Reparaturen starten“. Nach Abschluss der Reparaturen starten Sie Windows neu. Alternativ können Sie auf „Reparaturen aufrufen“ klicken und Häkchen vor die gewünschten Reparaturschritte setzen, etwa „Windows-Firewall reparieren“ oder „Netzwerk reparieren“.



Windows-Nervereien abstellen

Wenn etwas bei Windows stört, ignoriert man das Problem oder unternimmt etwas dagegen. Mit den Tools auf der Heft-DVD lässt sich einiges verbessern – alles jedoch nicht.

VON THORSTEN EGGELING

Bei Windows läuft nicht immer alles rund. Von Abstürzen und massiven Systemfehlern abgesehen – für die nicht immer Microsoft verantwortlich ist – sind es oft Kleinigkeiten, mit denen Windows unangenehm auffällt. Viele Nutzer klicken unsinnige Meldungen so schnell weg, wie sie erscheinen, und passen einige Einstellungen so an, dass Windows möglichst wenig nervt. Es bleibt dennoch genügend Störendes übrig, was man achselzuckend hinnehmen oder zumindest teilweise reduzieren kann.

„Wer Windows gewohnt ist, hat sich auch an die Probleme gewöhnt. Einige davon lassen sich beseitigen.“

Dabei setzt einem das Betriebssystem allerdings Grenzen. Einige der Windows-Eigenheiten resultieren aus der technischen Konzeption des Systems, was nur Microsoft ändern könnte. Das ist jedoch nicht ohne Weiteres möglich, weil zahlreiche Softwareprodukte auf die gewohnte Windows-Infrastruktur angewiesen sind – und die hat sich seit mehr als 20 Jahren nur unwesentlich verändert. Jeder größere Eingriff hat Konsequenzen und kann zu inkompatibler Hard- und Software führen. Auch wegen der Altlasten sind einige Windows-Funktionen nicht so schnell und einfach, wie sie eigentlich sein könnten.

In diesem Artikel beschreiben wir, was man abstellen oder verbessern kann und aus welchen Gründen das bei einigen Windows-Mängeln zurzeit nicht möglich ist.

1. Fehlende DLL-Dateien und Laufzeitumgebungen

Beim Start eines Programms erhalten Sie eine Meldung, die auf eine fehlende

DLL-Datei hinweist. Nach einem Klick auf „OK“ startet das Programm nicht.

Windows 10 und 11 bieten nur die Basisvoraussetzungen für den Start von Programmen. Das System enthält bereits standardmäßig zahlreiche Programmbibliotheken zur gemeinsamen Nutzung, aus denen Programme unter anderem grafische Elemente für die Oberfläche oder Funktionen für den Netzwerkzugriff beziehen. Abhängig von der Entwicklungsumgebung, mit der ein Programm erstellt wurde, sind weitere Programmbibliotheken erforderlich. In aller Regel übernimmt ein Setup-Programm die Installation von zusätzlichen Komponenten. Bei portablen Tools oder Software, die nur aus einer einzelnen EXE-Datei besteht, muss der Nutzer selbst manchmal für die passende Laufzeitumgebung sorgen, ansonsten startet das Programm nicht.

Es kommt relativ häufig vor, dass die Fehlermeldung das Fehlen von „Vcruntime140.dll“ oder „msvcp140.dll“ bemängelt. Beide

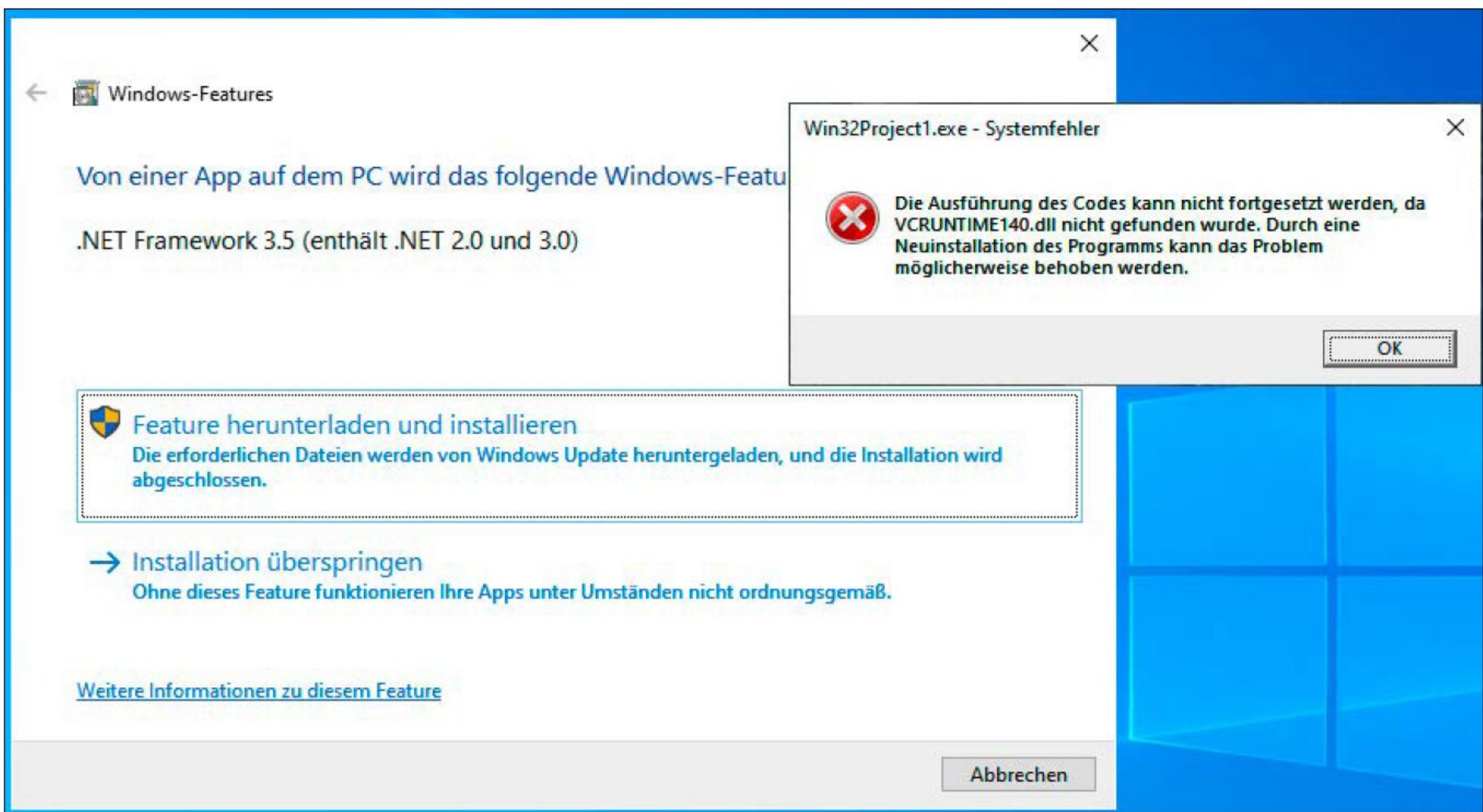
sind Bestandteil des Pakets **Microsoft Visual C++ Redistributable**. Microsoft bietet den Download als Gesamtpaket für die Visual-Studio-Versionen 2015 bis 2022 an (<https://tinyurl.com/MVCRED>). Installieren Sie die 32- und 64-Bit-Version, um auf alle Programme vorbereitet zu sein. Auf der Webseite sind auch Einzelpakete für ältere Visual-Studio-Anwendungen zu finden.

.NET-Laufzeitumgebungen: Bei .NET-Anwendungen ist es für den Nutzer einfacher, die fehlenden Voraussetzungen einzurichten. In der Regel meldet ein Programm beim Start die erforderliche Version und verweist auf den Download. .NET-4.x ist bei Windows 10 und 11 bereits standardmäßig installiert. Ältere oder neuere Versionen muss man nachinstallieren.

2. Das Windows-Update besser kontrollieren

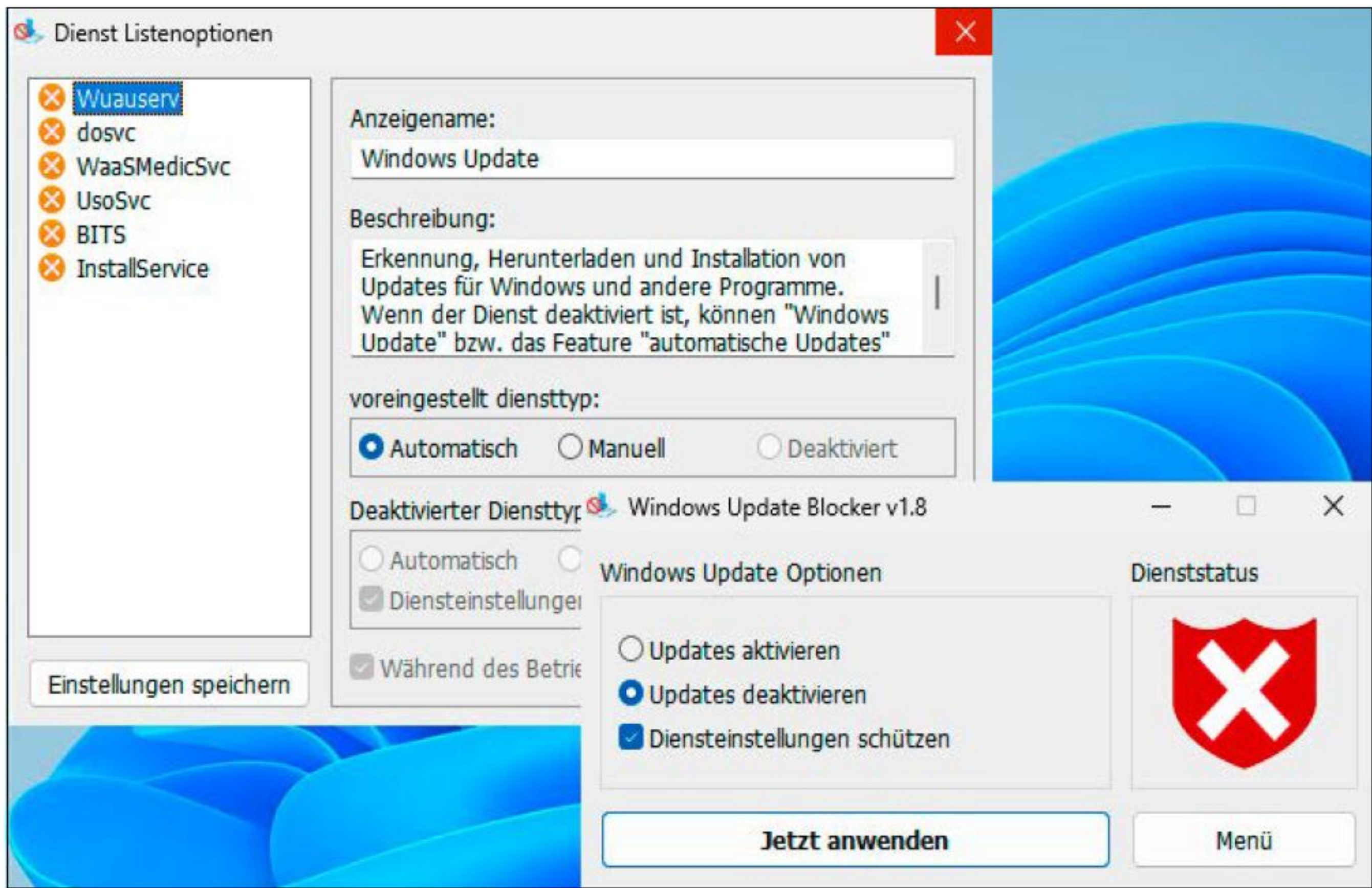
Windows-Updates kommen manchmal zur Unzeit. Etwa wenn Sie gerade mit Ihrem Notebook unterwegs sind und damit arbeiten möchten, statt auf die Update-Installation zu warten. Regelmäßige Updates müssen sein. Denn ein besonders verbreitetes Betriebssystem wie Windows ist ein bevorzugtes Angriffsziel. Microsoft hat die Update-Installation inzwischen etwas beschleunigt, trotzdem kann es ziemlich lange dauern, bis Ihr Windows nach einem Neustart wieder einsatzbereit ist.

Wer Windows-Updates verhindern will, muss rechtzeitig daran denken, also vor der Abreise mit dem Notebook. Bei Windows 11 gehen Sie in den „Einstellungen“ auf „Windows Update“ und stellen hinter „Updates aussetzen“ einen längeren Zeitraum ein, beispielsweise „Für 4 Wochen anhalten“. Windows-10-Nutzer gehen in den



Da fehlt etwas: Ist eine .NET-Laufzeitumgebung nicht vorhanden, erscheint eine klare Meldung mit Downloadangebot. Fehlt eine C++-Runtime, liegt die Lösung eher nicht auf der Hand.

Zeitweise keine Updates: Wenn Updates gerade bei der Arbeit stören, der schaltet das automatische Windows-Update mit dem Tool Windows Update Blocker aus.



„Einstellungen“ auf „Update & Sicherheit → Windows Update“, wo die Option „Updatepause für 7 Tage“ zu sehen ist. Nach einem Klick auf „Erweiterte Optionen“ kann man unter „Updates aussetzen“ ein anderes Datum einstellen.

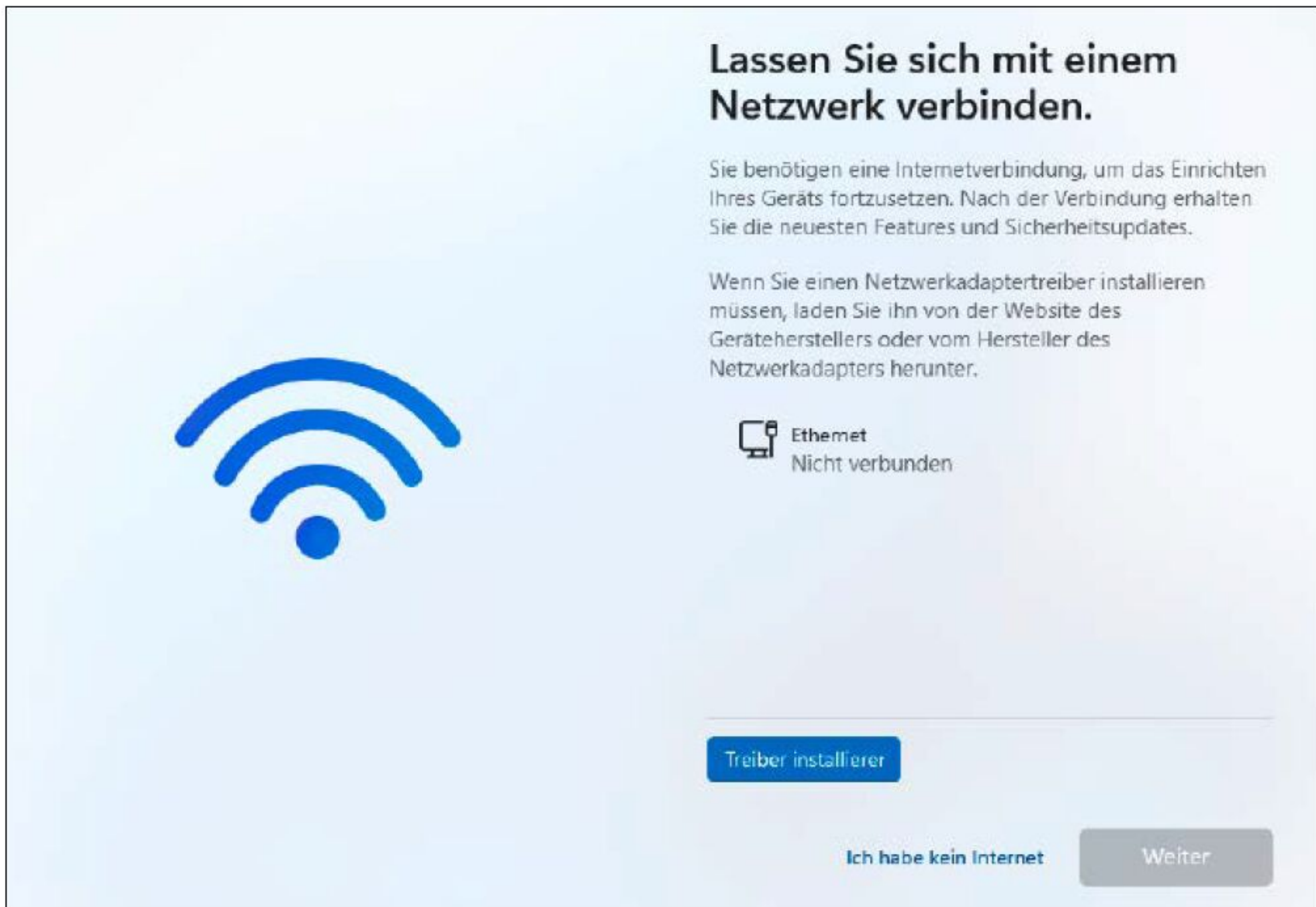
Update-Downloads begrenzen: Sie können Update-Downloads auch auf sicher-

heitsrelevante Aktualisierungen begrenzen und damit das Downloadvolumen reduzieren. Unter Windows 11 gehen Sie in die „Einstellungen“ und auf „Netzwerk und Internet → Ethernet“. Setzen Sie den Schalter hinter „Getaktete Verbindung“ auf „Ein“. Unter Windows 10 gehen Sie ebenfalls auf „Netzwerk und Internet → Ethernet“ und

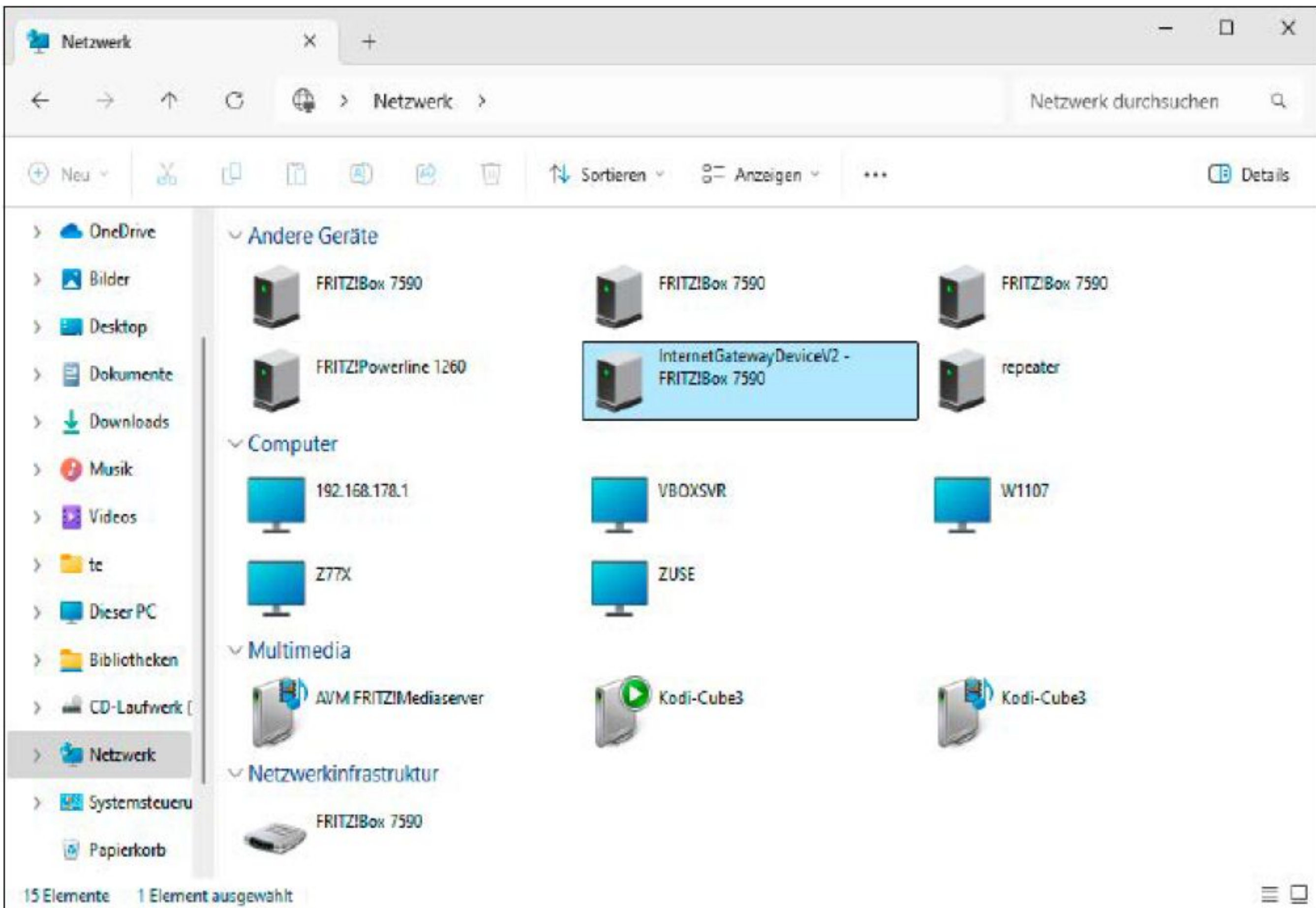
IM ÜBERBLICK: TOOLS FÜR EIN ENTSPANNTES WINDOWS



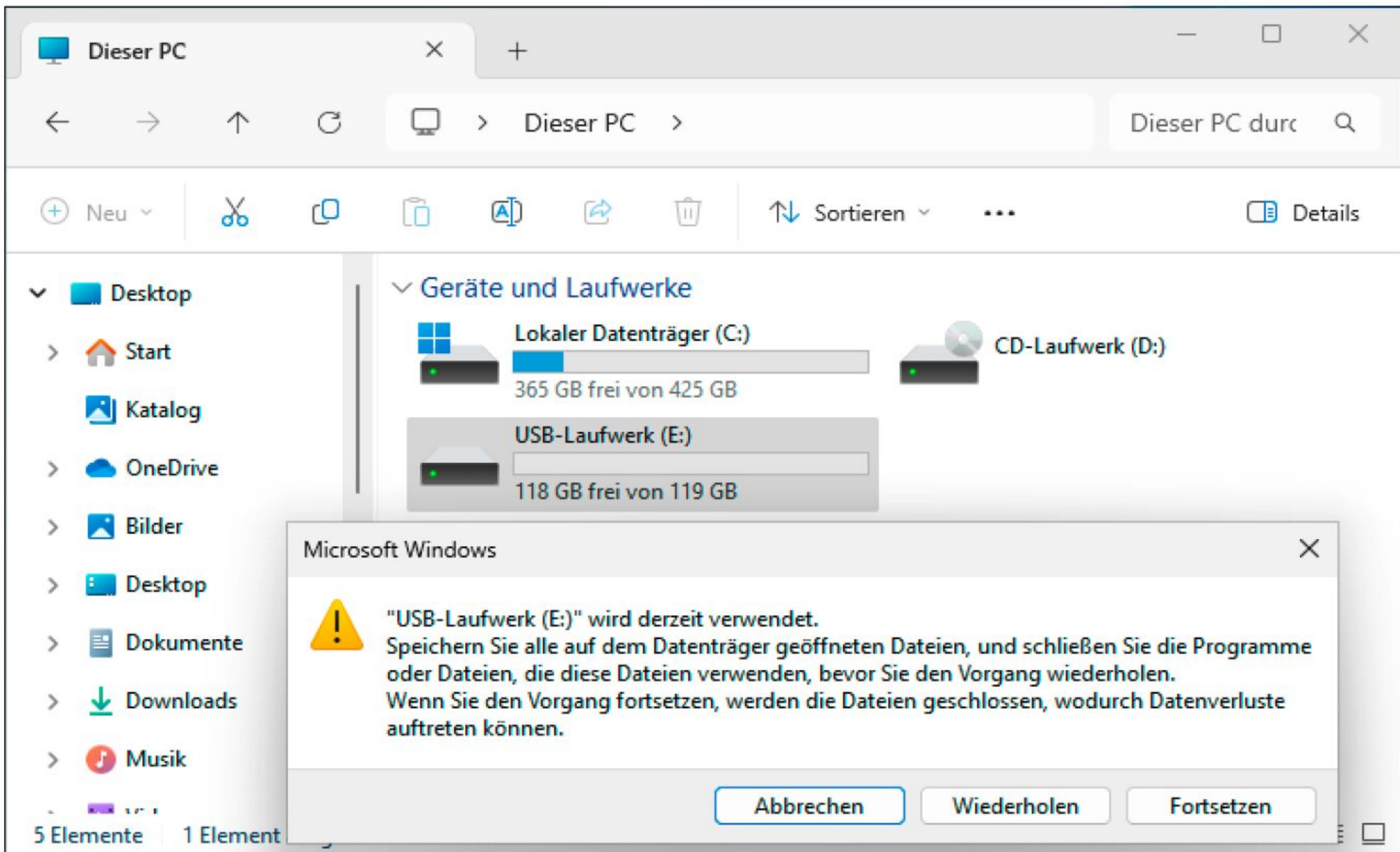
Name	Beschreibung	Auf	Internet	Sprache
Bootice	Windows-Bootmenü bearbeiten	Heft-DVD	https://tinyurl.com/BOOTIC	Englisch
Defender Control	Windows-Sicherheit (Defender) deaktivieren	Heft-DVD	www.sordum.org	Deutsch
Defender Exclusion Tool	Defender-Ausnahmenliste bearbeiten	Heft-DVD	www.sordum.org	Deutsch
Docfetcher	Schnelle Suche in Dokumentinhalten	Heft-DVD	https://docfetcher.sourceforge.io	Deutsch
Everything	Schnelle Suche nach Dateien und Ordnern	Heft-DVD	www.voidtools.com	Deutsch
Java Runtime Environment	Java-Laufzeitumgebung für Docfetcher	Heft-DVD	www.java.com	Deutsch
Microsoft Visual C++ Redistributable	Laufzeitumgebung für Visual-C++-Programme	-	https://tinyurl.com/MVCRED	Deutsch
Open Shell Menu	Alternatives Startmenü	Heft-DVD	https://github.com/Open-Shell/Open-Shell-Menu	Deutsch
Teracopy	Kopiertool für Dateien/Ordner	Heft-DVD	www.codesector.com	Deutsch
Windows Update Blocker	Automatisches Windows-Update ausschalten	Heft-DVD	www.sordum.org	Deutsch



Kontozwang umgehen: Der Klick auf „Ich habe kein Internet“ führt zur Erstellung eines lokalen Benutzerkontos. Dazu muss man Windows aber erst überreden.



Übersichtlich geht anders: Unter „Netzwerk“ tauchen einige Geräte doppelt auf, andere gar nicht. Zudem baut sich die Anzeige manchmal nur sehr zögerlich auf.



Auswerfen wird verweigert: Wenn sich ein USB-Stick nicht aushängen lässt, bleibt der Nutzer über die genauen Ursachen im Unklaren. Meist kann man den Stick aber problemlos abziehen.

klicken dann auf die Netzwerkverbindung unterhalb von „Ethernet“. Setzen Sie den Schalter vor „Als getaktete Verbindung festlegen“ auf „Ein“. Bei WLAN-Verbindungen funktioniert das bei beiden Betriebssystemen über „Netzwerk und Internet → WLAN“ entsprechend.

Updates komplett abschalten: Man kann das automatische Windows-Update auch dauerhaft mit dem Tool **Windows Update Blocker** verhindern. Wählen Sie die Option „Updates deaktivieren“ und klicken Sie auf „Jetzt anwenden“. Das Tool deaktiviert alle Dienste, die für Updates zuständig sind, und sorgt dafür, dass sie nicht wieder aktiviert werden. Deaktivieren Sie das Windows-Update nur, wenn es tatsächlich erforderlich ist. Nachdem Sie

es wieder aktiviert haben, sollten Sie so schnell wie möglich alle fehlenden Updates installieren.

3. Windows 11 mit lokalem Konto installieren

Sie haben nicht vor, Onedrive oder andere Microsoft-Clouddienste zu nutzen. Bei der Neuinstallation von Windows möchten Sie daher kein Microsoft-Konto einrichten.

Die meisten der bisher bekannten Tricks zur Umgehung des Microsoft-Kontozwangs funktionieren seit Version 22H2 nicht mehr. Bis derzeit einschließlich Windows 11 24H2 (Home und Pro) funktioniert aber diese Methode:

Schritt 1: Unterbrechen Sie die Netzwerk-

verbindung des PCs, indem Sie das Ethernet-Kabel abziehen. Sollte das Gerät die Internetverbindung nur über WLAN aufbauen, müssen Sie nichts unternehmen.

Schritt 2: Booten Sie den PC vom Windows-Installationsdatenträger und absolvieren Sie die erste Phase der Installation.

Schritt 3: Die zweite Hauptphase der Installation beginnt mit der Auswahl von Region und Tastaturlayout. Danach stellt Windows fest, dass keine Internetverbindung besteht. Es gibt standardmäßig keine Möglichkeit, die Installation fortzusetzen.

Schritt 4: Drücken Sie die Tastenkombination Shift-F10. Es öffnet sich das Fenster der Eingabeaufforderung, in das Sie

`oobe\bypassnro`

eingeben und mit der Enter-Taste bestätigen. Windows startet neu, und Sie konfigurieren erneut Region und Tastaturlayout. Im Fenster „Lassen Sie sich mit einem Netzwerk verbinden“, erscheint jetzt der Link „Ich habe kein Internet“. Nach einem Klick darauf richten Sie das lokale Konto ein und folgen den weiteren Anweisungen des Installationsassistenten.

4. Probleme beim Zugriff auf Netzwerkressourcen

Der Aufruf von „Netzwerk“ im Windows-Explorer liefert Ergebnisse oft nur zögerlich. Einige Netzwerkfreigaben zeigt er gar nicht an.

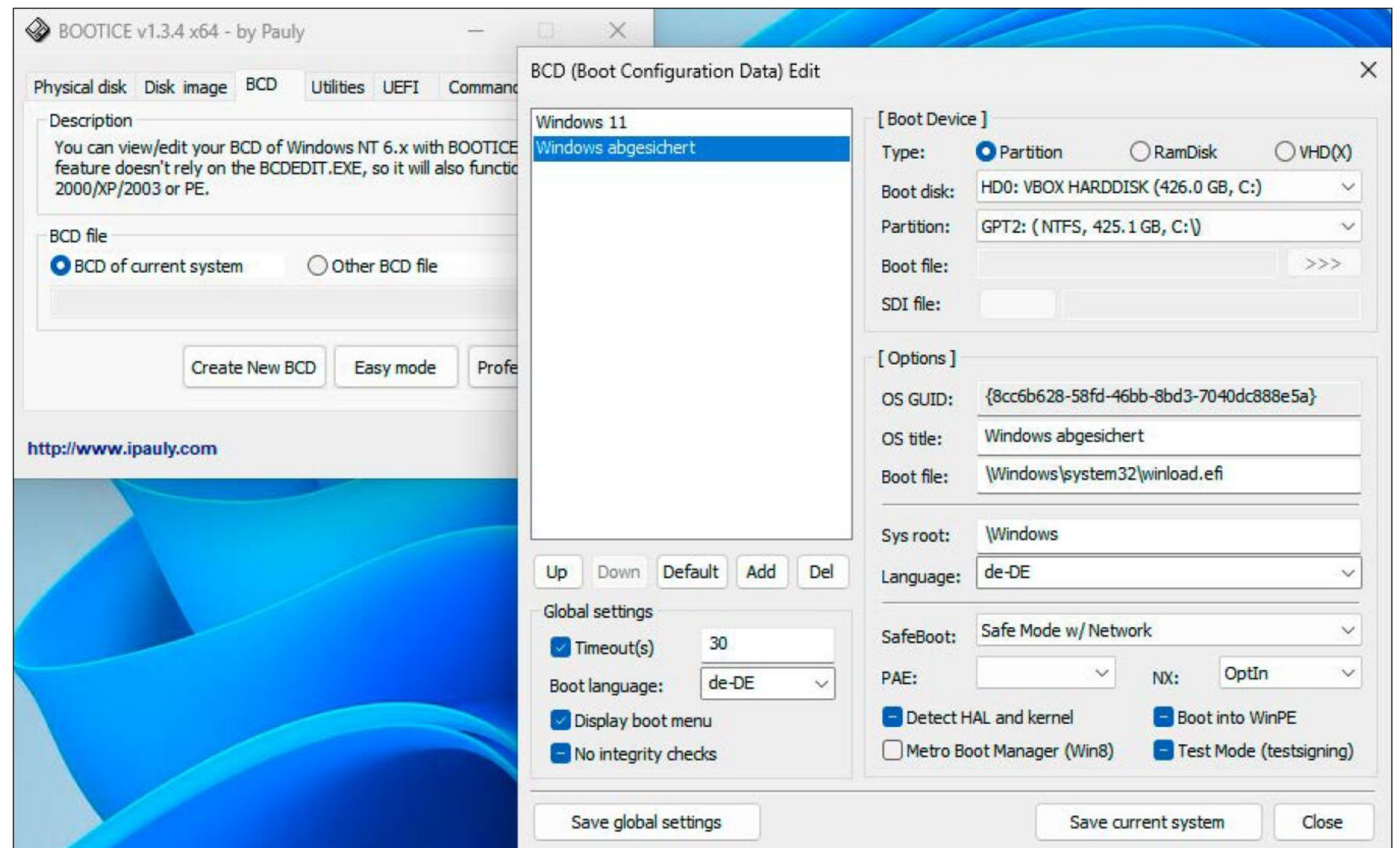
Die Liste unter „Netzwerk“ enthält neben Freigaben im Heimnetz („Computer“) auch Multimediageräte, Geräte mit Weboberfläche für die Konfiguration sowie für die Netzwerkinfrastruktur. Einige sind mehrfach vorhanden, weil sie sich mit unter-

schiedlichen Namen beziehungsweise IDs im Netzwerk bekannt machen. Eine Fritzbox beispielsweise verwendet verschiedene Techniken für ihre Ankündigungen im Netzwerk, unter anderem Web Services on Devices (WSD) und Simple Service Discovery Protocol (SSDP). Da die Fritzbox als Router, NAS und Mediaserver arbeiten kann und über mehrere Adressen erreichbar ist (192.168.178.1 und fritz.box), zeigt Windows das Gerät mehrfach an.

Die Anzahl der von Windows unterstützten Protokolle, mit denen sich Ressourcen entdecken lassen, ist groß. Der Vorteil: Windows bietet eine mehr als vollständige Liste aller Geräte an. Das führt jedoch dazu, dass die Übersicht manchmal nur langsam erscheint oder sich nicht vollständig aufbaut.

Für Freigaben auf anderen Windows-Rechnern ist ebenfalls WSD zuständig. Alle Geräte unterstützen das Protokoll jedoch nicht, weshalb Linux-Server und ältere NAS-Geräte meist nicht unter Windows zu sehen sind. Für Linux finden Sie eine Lösung unter www.pcwelt.de/1518660, beim NAS müssen Sie nach einem Update für das System suchen.

Eine Notlösung besteht darin, das veraltete Protokoll SMB 1.0 zu reaktivieren. Microsoft rät davon jedoch aus Sicherheitsgründen ab. Wenn Sie es trotzdem nutzen



Erweitertes Bootmenü: Auf die Taste F8 reagiert Windows nicht mehr. Die Funktionen lassen sich aber reaktivieren, indem man den klassischen Bootmanager wiederherstellt.

wollen, drücken Sie Win-R, tippen Sie *optionalfeatures* ein und bestätigen Sie mit „OK“. In der Liste der Einstellungen setzen Sie einen Haken vor „Unterstützung für die SMB 1.0/CIFS-Dateifreigabe“ und führen einen Windows-Neustart durch. Jetzt funktioniert der Zugriff wieder.

Direkter Zugriff auf Netzwerkressourcen: Netzwerkfreigaben sind immer auch über ihre IP-Nummer oder den Namen des PCs/Servers erreichbar. Auf die Liste unter

„Netzwerk“ sind Sie daher nicht angewiesen. Sie können eine Freigabe jederzeit über die Eingabe einer URL in der Form `\\PC-Name\Freigabename` in die Adressleiste des Windows-Explorers öffnen.

5. USB-Laufwerk lässt sich nicht sicher entfernen

Aus Sorge vor Datenverlust möchten Sie ein USB-Laufwerk nicht einfach vom PC

WARUM MUSS MAN WINDOWS STÄNDIG NEU STARTEN?

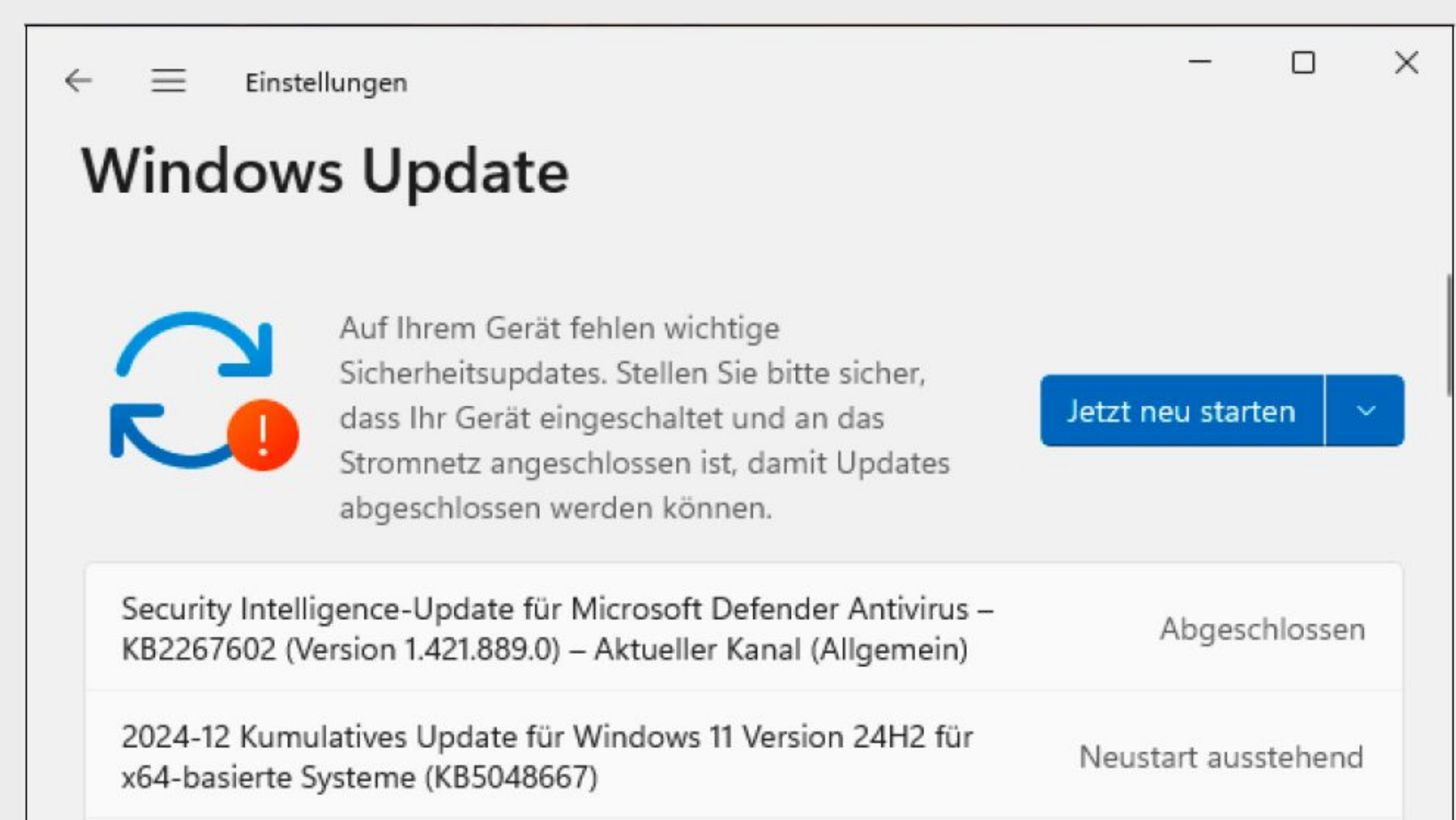


Spätestens nach einem Update ist es wieder so weit. Windows fordert einen Neustart an, um die Updates zu installieren. Zahlreiche Programme wollen nach der Installation ebenfalls, dass man Windows neu startet. Andere Betriebssysteme können das besser. Bei Android oder Linux ist ein Neustart in der Regel nur nach einem Upgrade des Betriebssystems nötig. Windows enthält zahlreiche Komponenten, die von mehreren Programmen gemeinsam verwendet werden. Während eine Anwendung oder ein Dienst läuft, sind einige Programmbibliotheken geöffnet und gesperrt und können nicht durch neuere Versionen ersetzt werden. Erst nach einem Neustart, wenn die meisten Dienste noch nicht laufen und kein Benutzer angemeldet ist, lassen sich die Dateien ersetzen.

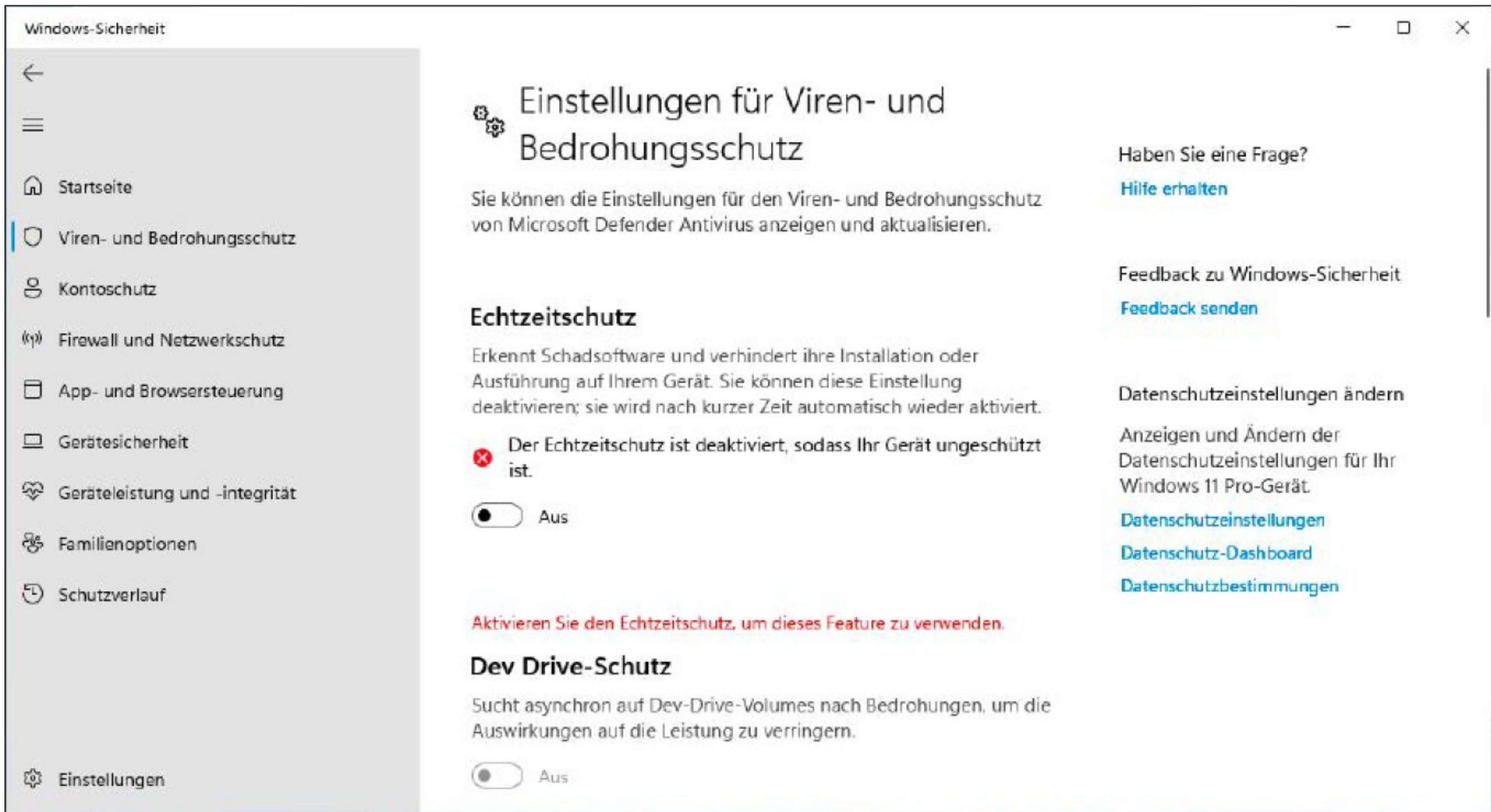
Bei der Installation eines Programms sind die Ursachen meist andere. Es ist zwar möglich, neue Dienste jederzeit zu starten, und auch neue Treiber lassen sich beliebig laden, den Entwicklern der Programme ist das aber offenbar zu unsicher. Nur durch einen Windows-Neustart ist gewährleistet, dass Windows alles in der richtigen Reihenfolge aktiviert und lädt.

Man kann es darauf ankommen lassen und bei Programmen

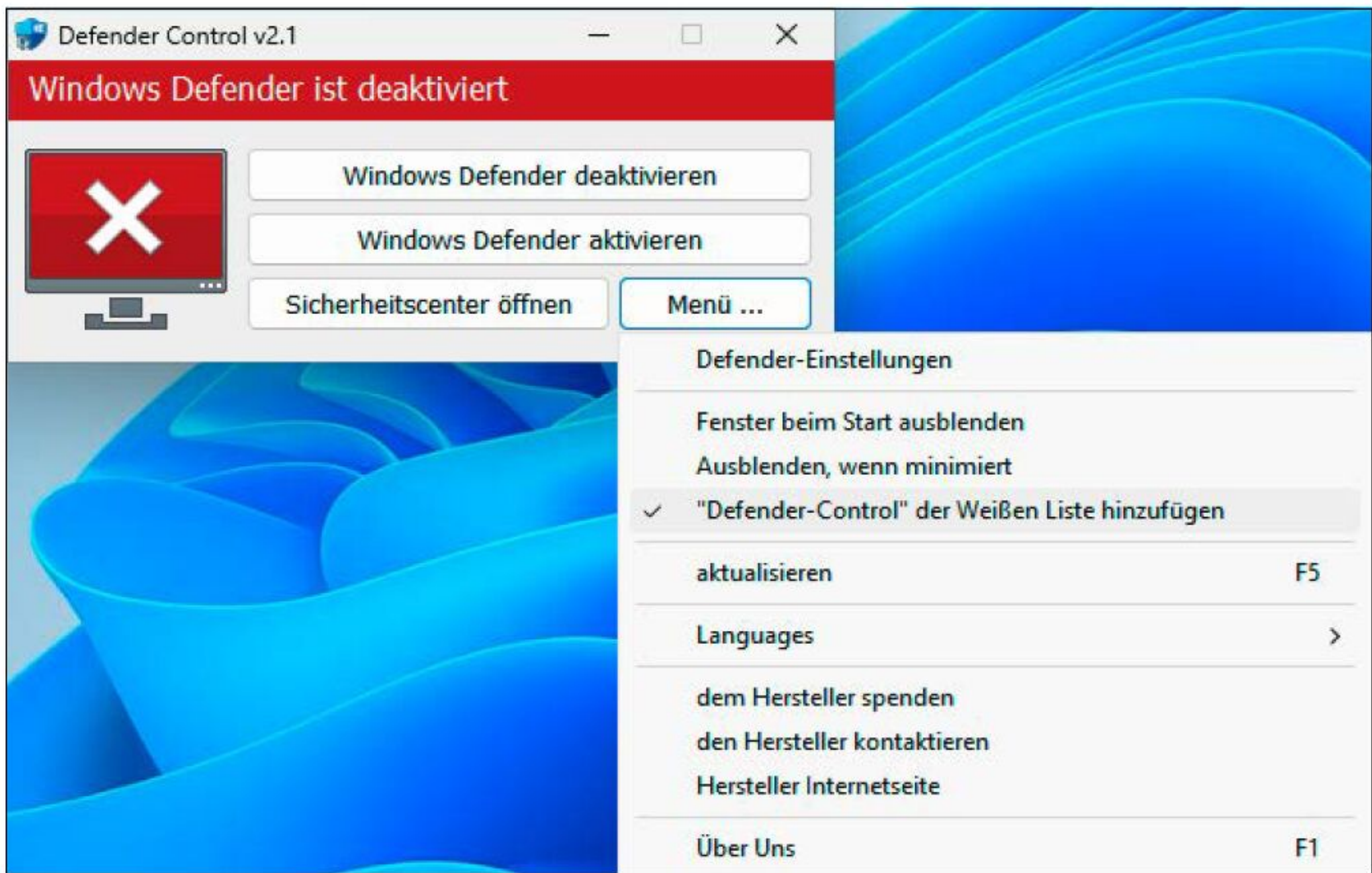
die Aufforderung zum Neustart ignorieren. Häufig funktioniert es trotzdem, manchmal bemerkt das Programm es und gibt eine entsprechende Meldung aus, oder die Anwendung startet erst gar nicht.



Ständige Neustarts. Es gehört zu den Eigenheiten von Windows, dass sich nicht alle Dateien im laufenden System ersetzen lassen. Das ist erst beim nächsten Start möglich.



Pause für den Virenschanner: Für bestimmte Aufgaben sollte oder muss man den Echtzeitschutz deaktivieren. Windows aktiviert die Option jedoch nach kurzer Zeit automatisch erneut.



Zeitweise komplett abschalten: Mit Defender Control deaktivieren Sie Windows-Sicherheit vollständig. Nutzen Sie das Tool jedoch nur in Ausnahmefällen, um die Sicherheit zu gewährleisten.

trennen, sondern über das Icon im Info-bereich oder den Kontextmenüpunkt „Auswerfen“ sicher entfernen. Das funktioniert aber oft nicht.

Solange Dateien auf dem USB-Laufwerk geöffnet sind, lässt es sich nicht sicher entfernen. Windows informiert allerdings nicht darüber, um welche Dateien es sich handelt. Schließen Sie alle Programme – und auch die Fenster des Windows-Explorers – und versuchen Sie es noch einmal. Sollte das nicht klappen, greift ein Programm auf das USB-Laufwerk zu, das nicht sichtbar oder abgestürzt ist. In der Regel können Sie ein USB-Laufwerk bedenkenlos trennen, ohne Datenverlust befürchten zu müssen. Bereits seit Windows 10 Version 1809 verwendet Windows standardmäßig keinen Schreibcache bei USB-Laufwerken. Das sollten Sie jedoch zur Sicherheit kontrollieren. Öffnen Sie die Datenträgerverwaltung über die Tastenkombination Win-X oder einen rechten Maus-

klick auf das Startmenü. Im unteren Bereich des Fensters klicken Sie mit der rechten Maustaste ganz links auf den Eintrag des USB-Sticks und wählen im Kontextmenü „Eigenschaften“. Wechseln Sie auf die Registerkarte „Richtlinien“, auf der die Option „Schnelles Entfernen (Standard)“ aktiviert sein sollte.

6. Reparatursystem oder abgesicherten Modus starten

Über die Taste F8 konnte man in früheren Windows-Versionen beim Start das Reparatursystem oder den abgesicherten Modus aufrufen. Bei Windows 10 und 11 scheint das nicht mehr zu funktionieren. Durch den Schnellstartmodus startet Windows insbesondere von SSDs so schnell, dass man den richtigen Zeitpunkt für die Taste F8 kaum treffen kann. Microsoft hat sich daher entschlossen, die Taste gar nicht mehr abzufragen. Wer für den Notfall ge-

wappnet sein möchte, kann das aber ändern. Der Trick besteht ganz einfach darin, das Menü des klassischen Bootmanagers zu reaktivieren.

Verwenden Sie dafür das Tool **Bootice**, in dem Sie auf die Registerkarte „BCD“ wechseln und auf „Easy mode“ klicken. Erstellen Sie nach einem Klick auf „Add“ einen neuen Booteintrag mit dem Namen „Windows abgesichert“. Passen Sie die Optionen so an, dass sie denen des bereits vorhandenen Eintrags für Windows 10 oder 11 entsprechen. Abweichend davon wählen Sie hinter „SafeBoot:“ den Eintrag „Safe Mode w/ Network“. Klicken Sie auf „Save current system“. Entfernen Sie bei beiden Bootmenüeinträgen die Markierung vor „Metro Boot Manager (Win8)“ und klicken Sie jeweils auf „Save current system“. Unter „Global settings“ setzen Sie ein Häkchen vor „Display boot menu“ und klicken auf „Save global settings“. Wenn Sie Windows neu starten, erscheint das klassische Bootmenü auf schwarzem Hintergrund. Mit der Taste F8 gelangen Sie zum Menü mit den erweiterten Startoptionen („Computer reparieren“, „Abgesicherter Modus“, „Automatischen Neustart bei Systemfehlern deaktivieren“). Oder Sie wählen direkt „Windows abgesichert“ im Bootmenü.

7. Microsofts Virenschutz abschalten

Man sollte Windows nicht ohne Virenschanner betreiben. Es gibt jedoch Situationen, in denen die Microsoft-Sicherheitsfunktionen den Nutzer mehr behindern als schützen. Umfangreiche Datensicherungen beispielsweise werden vom Virenschanner deutlich ausgebremst. Und einige systemnahe Tools können nicht gestartet werden, weil der Virenschanner fälschlicherweise Schadsoftware erkennt.

Der Microsoft-Virenschanner ist seit Windows 10 ein Bestandteil des Betriebssystems. Er ist unter dem Namen Windows Defender bekannt, die offizielle Bezeichnung lautet inzwischen Windows-Sicherheit. Unter diesem Namen ist die Konfiguration auch in den „Einstellungen“ unter „Datenschutz und Sicherheit → Windows-Sicherheit“ (Windows 10: „Update & Sicherheit → Windows-Sicherheit“) zu finden. Unter „Viren- und Bedrohungsschutz → Einstellungen für Viren und Bedrohungs-

schutz“ und Klick auf „Einstellungen verwalten“ lässt sich der Echtzeitschutz deaktivieren. Der Virenschanner prüft dann die einzelnen Dateien nicht mehr, etwa bei einer Kopieraktion. Programme, die Sie herunterladen, entpacken und starten werden allerdings auch nicht mehr berücksichtigt. Der Echtzeitschutz lässt sich nur kurz abschalten, und Windows aktiviert ihn nach einiger Zeit automatisch erneut.

Eine nachhaltigere Methode ist, unter „Ausschlüsse → Ausschlüsse hinzufügen oder entfernen“ einzelne Dateien (bei fehlerhafter Erkennung) oder ganze Ordner vom Virenschanner auszunehmen.

Ausschlüsse schneller aufnehmen: Das **Defender Exclusion Tool** ist ein übersichtliches Programm, über das sich die Ausnahmenliste von Windows-Sicherheit bequemer bearbeiten lässt. Sie können Dateien und Ordner in die Liste einfügen und löschen. Per Klick auf „Datei → Export List“ speichern Sie die Liste in einer Konfigurationsdatei, die man über „Datei → Import List“ auch auf einem anderen Rechner wieder einlesen kann.

Virenschanner per Tool abschalten: Mit **Defender Control** deaktivieren Sie Windows-Sicherheit schnell und einfach. Das lässt sich Windows jedoch ohne vorherige Maßnahmen nicht gefallen, was verständlich ist. Eine Software, die den Virenschutz abschalten möchte, muss als Bedrohung eingestuft werden. Zuvor müssen Sie daher den Echtzeitschutz manuell deaktivieren, wie zuvor beschrieben. Außerdem setzen Sie in den „Einstellungen für Viren und Bedrohungsschutz“ den Schalter unter „Manipulationsschutz“ auf „Aus“.

Die ZIP-Datei auf der Heft-DVD und auch der Download beim Hersteller sind mit dem Passwort *sordum* geschützt, das Sie beim Entpacken eingeben. Ansonsten würde der Virenschanner bei aktiviertem Echtzeitschutz das Tool sofort entfernen.

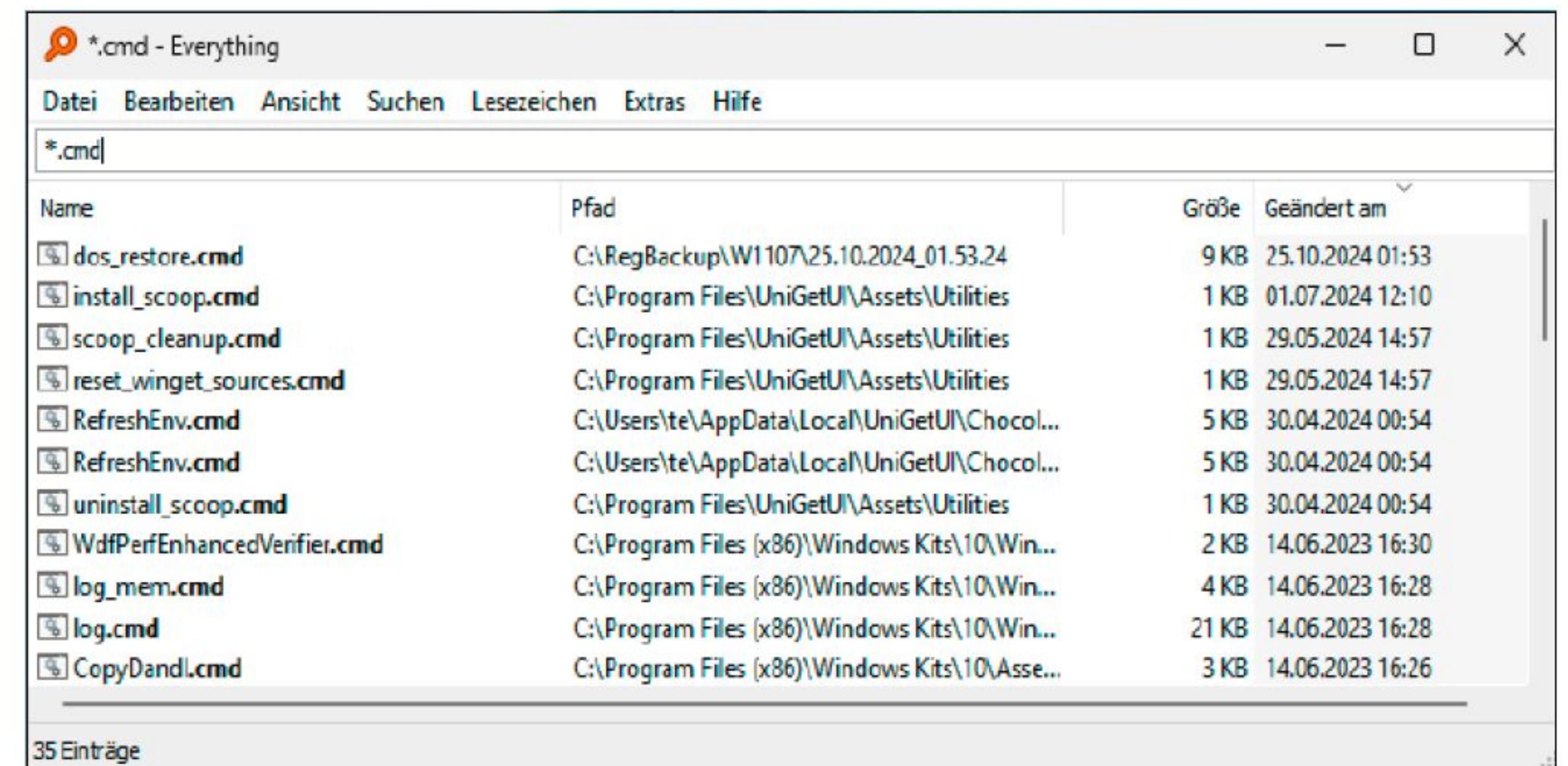
Ist Defender Control erfolgreich gestartet, gehen Sie als Erstes auf „Menü → Defender Control der Weißen Liste hinzufügen“. Danach wird das Tool vom Echtzeitschutz ignoriert. Über die Schaltfläche „Windows Defender deaktivieren“ schalten Sie den „Viren- & Bedrohungsschutz“ komplett ab und per Klick auf „Windows Defender aktivieren“ wieder an.

Tipp: Wer Dateien schneller kopieren möchte, als es der Windows-Standard erlaubt, installiert das Tool **Teracopy**.

Schneller finden:

Everything zeigt das Ergebnis bei der Suche nach Dateien und Ordnern blitzschnell an.

Das Tool erfasst neue Dateien außerdem fast in Echtzeit.



8. Schneller nach Dateien und Inhalten suchen

Die Windows-Suche arbeitet nicht besonders schnell, etwa wenn man auf dem ganzen Laufwerk nach Dateien sucht. Die Suche nach Dokumentinhalten scheint nicht immer zuverlässig zu funktionieren, und die Anzeige der Suchergebnisse ist wenig aussagekräftig.

Die Windows-Suche verwendet einen Suchindex, der standardmäßig nur die Verzeichnisse der Benutzer und das Startmenü erfasst. Die Optionen lassen sich in den „Einstellungen“ unter „Datenschutz und Sicherheit → Windows durchsuchen“ anpassen (Windows 10: „Suche → Windows durchsuchen“). Es ist allerdings nicht empfehlenswert, sehr viele Ordner in den Suchindex aufzunehmen, weil die Suche dadurch deutlich mehr Systemressourcen benötigt und langsamer wird.

Alternative Suchtools bieten eine bessere Leistung. **Everything** ist ein Spezialist für die Suche nach Dateien und Ordnern. Das Tool erstellt einen kleinen Hilfsindex, nutzt aber ansonsten direkt die Datenbank des NTFS-Dateisystems. Daher ist Everything besonders schnell und überwacht auch neue Dateien, die sofort gefunden werden. Bei anderen Dateisystemen als NTFS bietet das Tool diese Vorteile nicht.

Setzen Sie **Docfetcher** ein, wenn Sie nach Dateiinhalten suchen wollen. Im Programm geben Sie die Ordner an, die Sie durchsuchen wollen. Docfetcher erstellt einen Suchindex für die meisten gängigen Dateitypen, was einige Zeit dauert. Dafür ist die Suche schnell, und nach einem Klick auf ein gefundenes Dokument sehen Sie dessen kompletten Inhalt im unteren Bereich des Fensters. Der Suchbegriff ist hervorgehoben, und der Kontext der Fundstelle ist klar erkennbar. ■

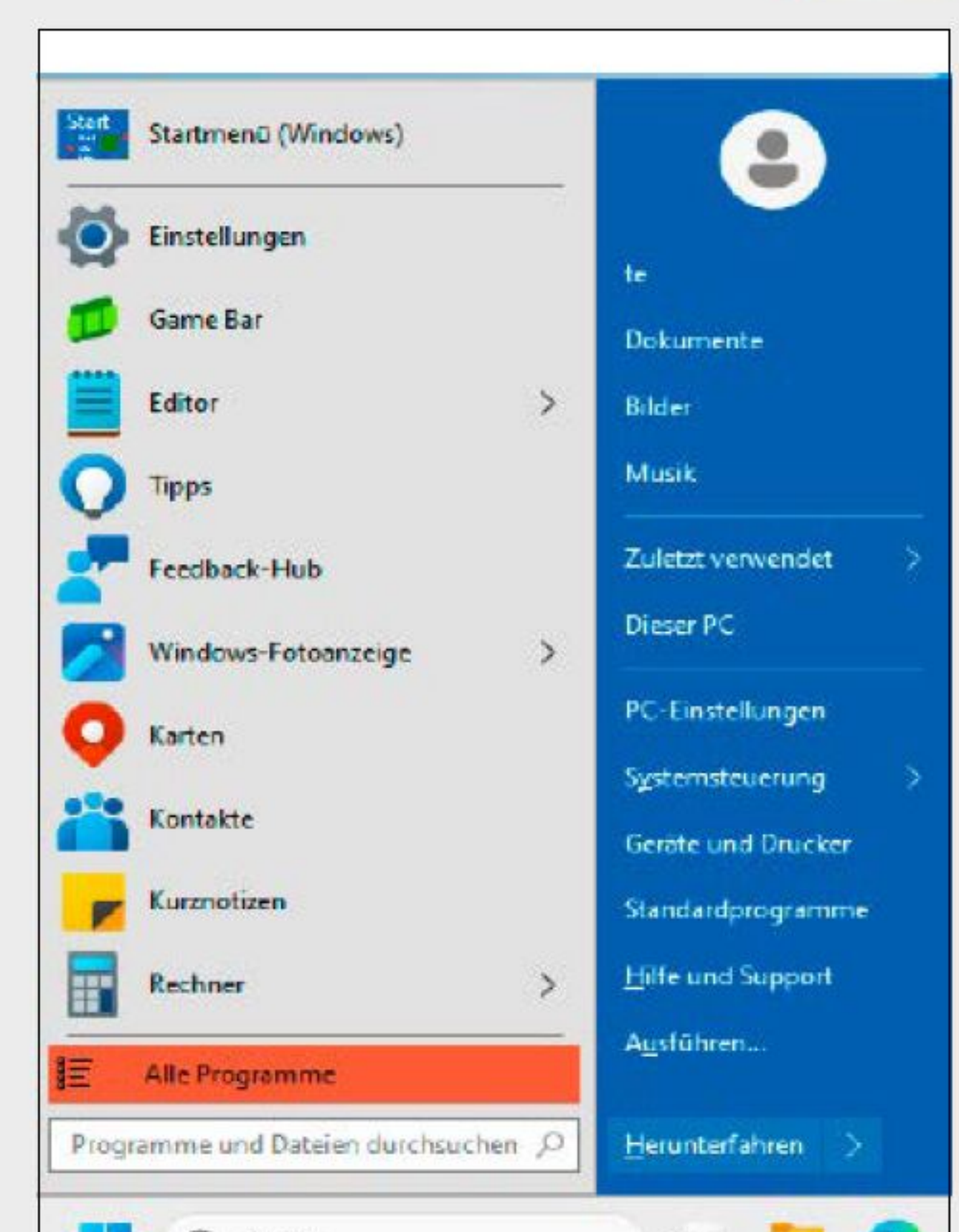
DAS WINDOWS-STARTMENÜ AUSTAUSCHEN



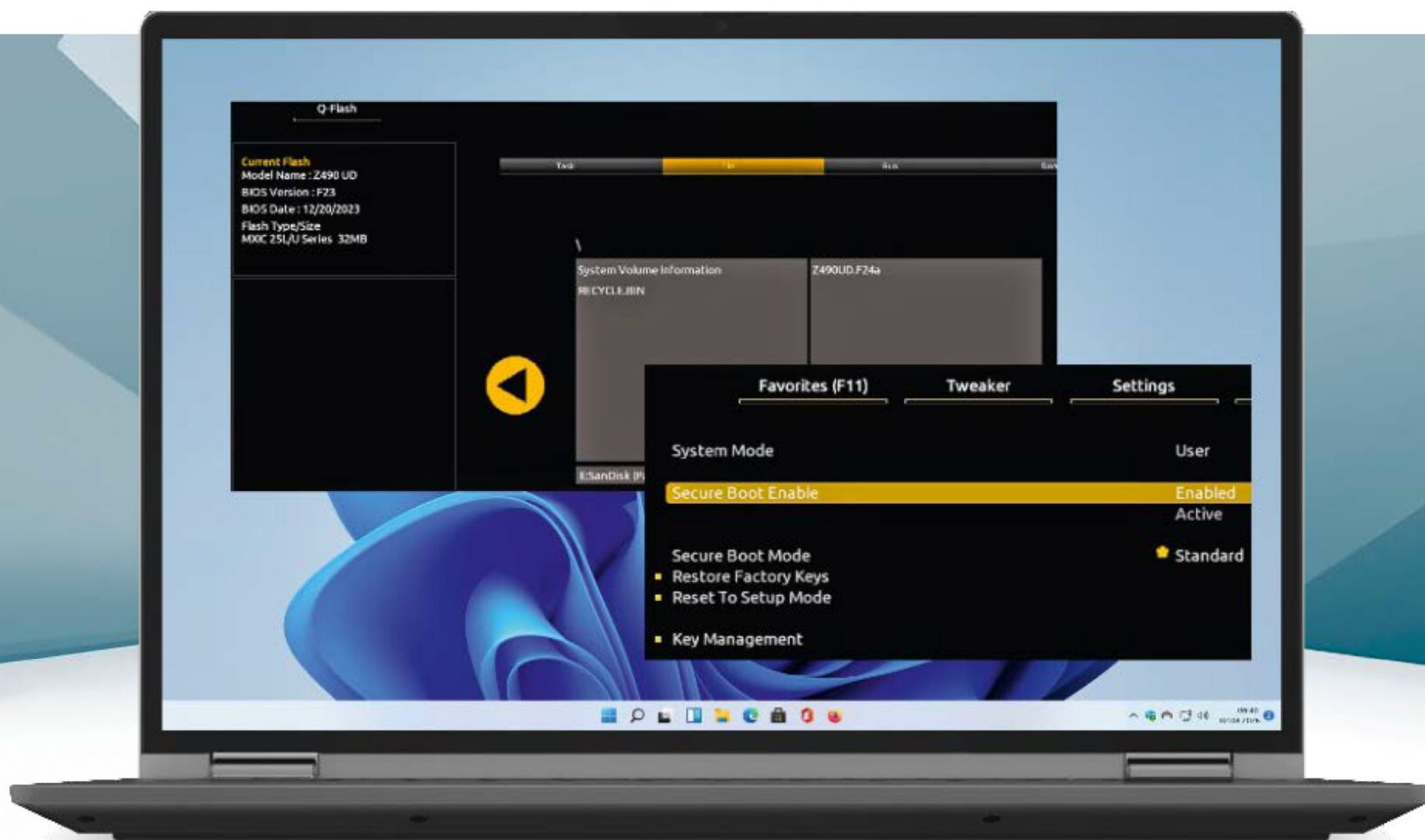
Das Startmenü von Windows 11 sorgt weiterhin nicht bei allen Anwendern für ungeteilte Freude.

Nach den überladenen Experimenten in Windows 8 und der leichten Reduzierung in Windows 10 ist das Startmenü von Windows 11 nach Ansicht vieler Nutzer immerhin brauchbar. Wer auch jetzt noch das Design von Windows 7 vermisst, installiert **Open Shell Menu**. Das Tool ersetzt das Startmenü von Windows 10 oder 11 komplett und zeigt die von Windows 7 gewohnten Menüeinträge und Schaltflächen. Nach der Installation erscheint nach einem Klick auf die Schaltfläche „Start“ ein Konfigurationsdialog. Hier legen Sie fest, wie das neue Startmenü aussehen soll.

Das Original-Windows-Startmenü lässt sich auch weiterhin noch aufrufen. Dazu halten Sie die Shift-Taste gedrückt und klicken auf die Schaltfläche „Start“.



Klassisches Startmenü: Wer nichts von den Neuerungen in Windows 11 hält, installiert Open Shell Menu. Das Tool bietet ein einfaches Startmenü im Stil von Windows 7.



Secure-Boot-Probleme lösen

Damit Secure Boot auch in Zukunft sicher schützt, stehen einige Updates an. Sie sollten die Situation auf Ihrem PC untersuchen und bei Bedarf Maßnahmen einleiten, um den problemfreien Windows-Weiterbetrieb zu gewährleisten.

VON THORSTEN EGGELING

Ein Windows-PC ist permanenten Hacker-Attacken ausgesetzt. Um davor zu schützen, ist Secure Boot ein wichtiger Baustein im Windows-Sicherheitskonzept. Die Funktion steckt in der PC-Firmware und sorgt dafür, dass nur zertifizierte Uefi-Dateien während des Bootvorgangs geladen werden. Das soll verhindern, dass sich Schadsoftware bereits vor dem Start des Betriebssystems und vor der Prüfung durch einen Virens Scanner einnistet.

„Damit Secure Boot sicherer wird, sind neue Zertifikate nötig. Prüfen Sie den Update-Stand Ihres PCs.“

Secure Boot hat jedoch einige konzeptionelle Mängel, die Wartung und Aktualisierung erschweren. Hinzu kommt, dass einige der zurzeit verwendeten Microsoft-Zertifikate im Juni 2026 ablaufen. Der PC wird voraussichtlich noch einige Zeit auch Uefi-Dateien starten, die mit dem dann veralteten Zertifikat signiert sind. Microsoft kann damit aber keine neuen Dateien mit gültigen Signaturen erzeugen, was für zukünftige Updates erforderlich ist. Deswegen müssen auf allen PCs neue Zertifikate in die Firmware integriert werden, damit Windows auch nach dem nächsten Update noch startet. Das gilt für Windows 11 und auch für Windows 10, wenn das System weiter mit Updates versorgt wird. Der Artikel beschreibt, wie Secure Boot genau funktioniert, welche Voraussetzungen für Updates gelten und wie Sie den Update-Status prüfen können.

Wichtig: Lesen Sie als Erstes im Kasten „Bitlocker-Schlüssel und TPM“, wie Sie den

Bitlocker-Wiederherstellungsschlüssel sichern oder die Verschlüsselung abschalten.

Die Bedeutung von digitalen Signaturen

Digitale Signaturen bestätigen die Herkunft und Integrität einer Datei. Das kryptografische Verfahren kommt etwa bei Dokumenten, Programmdateien und Treibern zum Einsatz. Der Aussteller verwendet seinen privaten Schlüssel, um einen einzigartigen digitalen Fingerabdruck (Hashwert) in der Datei zu erzeugen. Der Empfänger nutzt den zugehörigen öffentlichen Schlüssel, um die Signatur zu prüfen. Wenn die Prüfung erfolgreich ist, bestätigt dies die Herkunft und dass die Datei nicht verändert wurde.

Die Ausstellung des privaten und öffentlichen Schlüssels erfolgt über eine anerkannte Zertifizierungsstelle. Dabei wird das Teilnehmer-Zertifikat mit einem Zwischen-Zertifikat (Intermediate) signiert

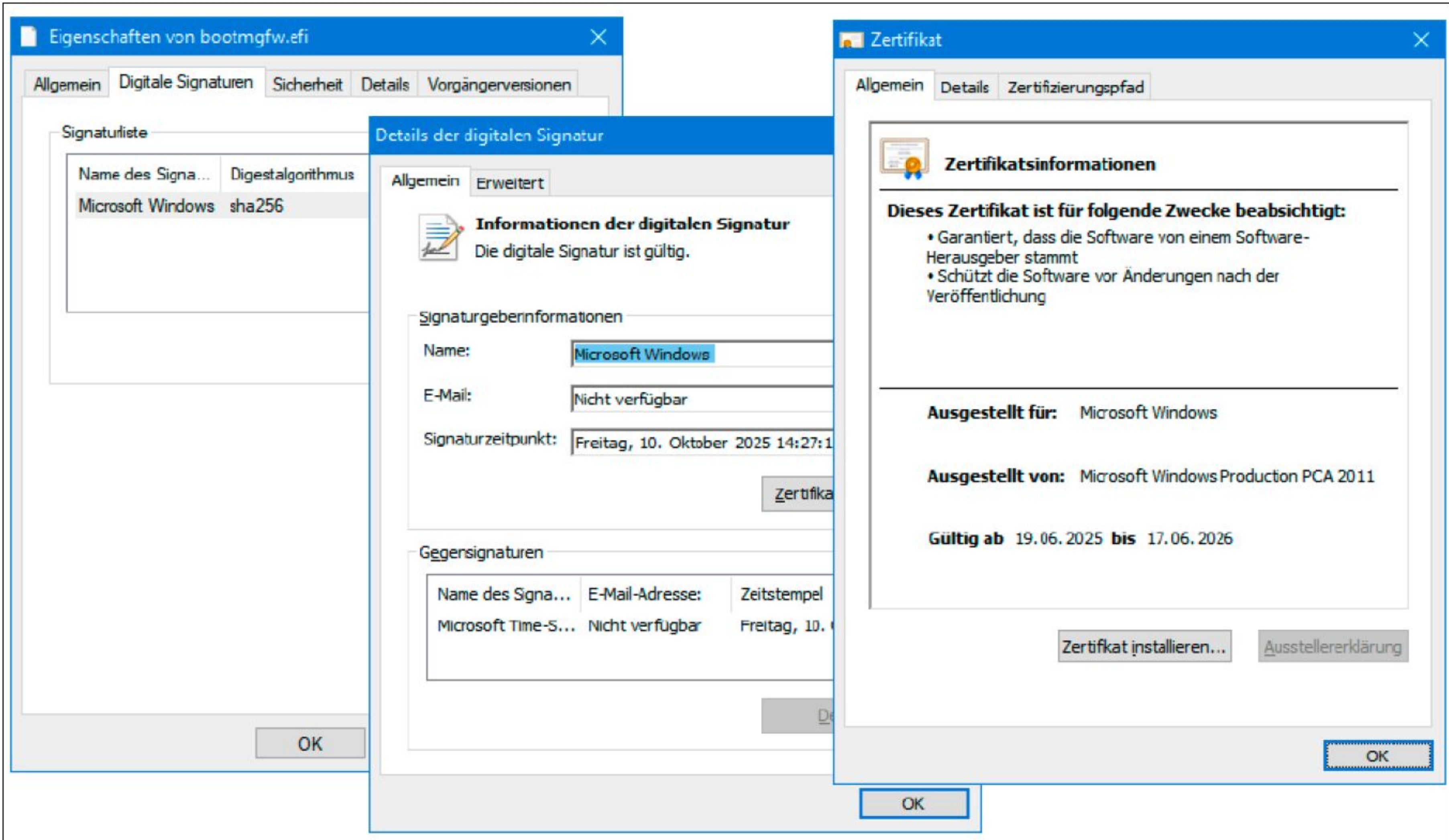
und dieses wiederum mit einem Root-Zertifikat (Stammzertifikat). Die gesamte Vertrauenskette (Chain of Trust) muss bei der Validierung gültig sein, damit die Quelle als vertrauenswürdig eingestuft wird. Wenigstens das Stammzertifikat muss dem Betriebssystem oder einer Software bekannt sein, damit eine Validierung erfolgreich sein kann.

Alle Zertifikate haben ein Ablaufdatum. Danach kann der Besitzer es nicht mehr für neue Signaturen nutzen. Die zuvor signierten Dateien bleiben jedoch gültig, wenn der enthaltene Zeitstempel innerhalb des Zeitraums der Zertifikatsgültigkeit liegt und das Zertifikat nicht zurückgezogen wurde. Andernfalls müsste man jedes Programm aktualisieren, dessen Zertifikat abgelaufen ist. Welche Zertifikate in einer Datei enthalten sind, kann man über die Eigenschaften prüfen.

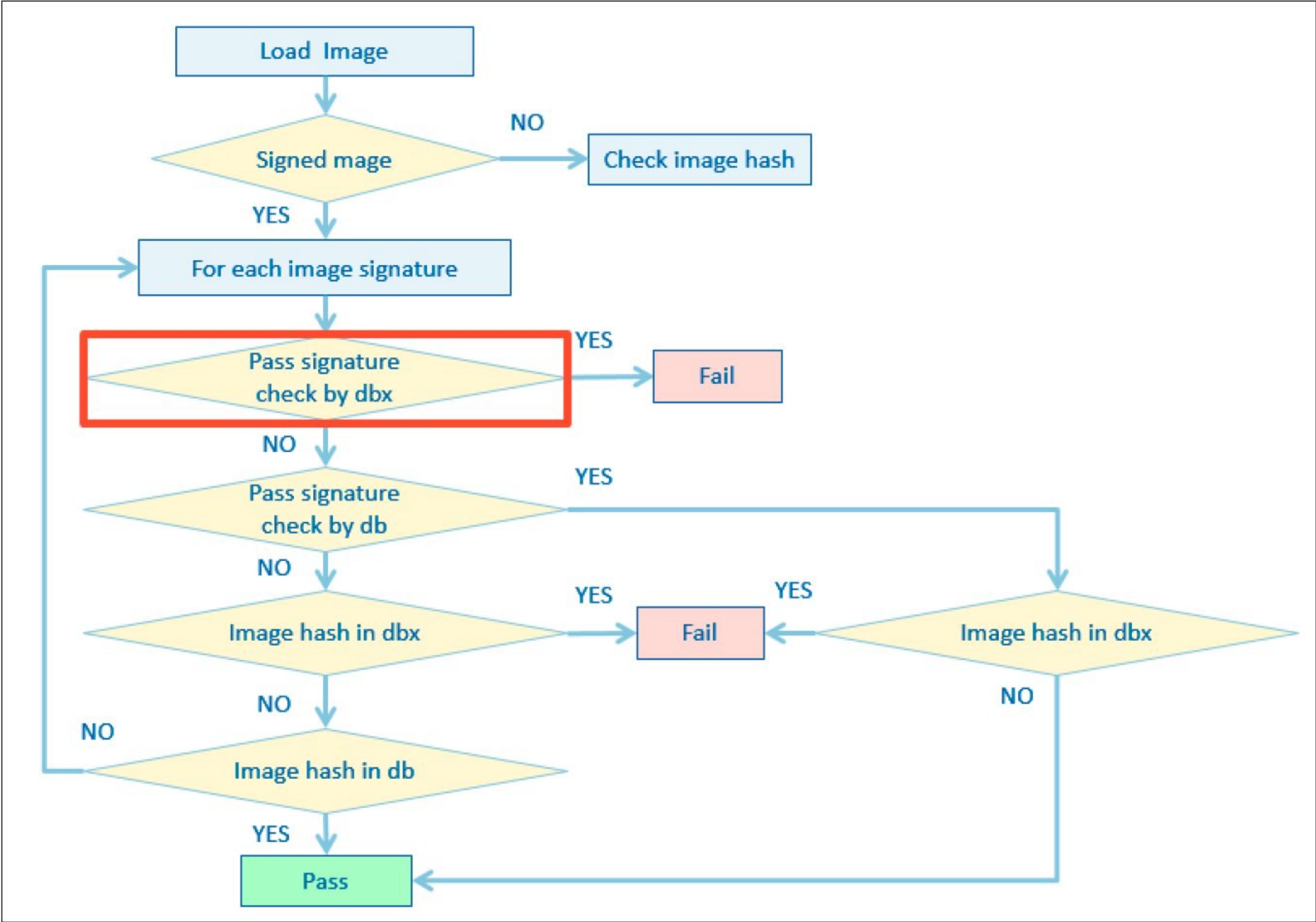
So läuft der Bootvorgang des PCs mit Secure Boot ab

Auch bei Secure Boot kommen digitale Signaturen zum Einsatz. Die nötigen Zertifikate dafür sind im Speicher der Firmware hinterlegt. Beim Start des PCs sucht die Firmware auf der Uefi-Partition nach Bootloadern, die üblicherweise die Dateinamenerweiterung „.efi“ besitzen. Die Dateien werden gestartet, wenn sie digital signiert sind und ein Zertifikat die Signatur als gültig erklärt. Es geht auch ohne Signatur, wenn die Prüfsumme (Hash) einer Datei als vertrauenswürdig hinterlegt ist. Die Firmware verwaltet zwei Datenbanken: Die Signatur-Datenbank (DB) enthält erlaubte Zertifikate und Hash-Werte, eine weitere Datenbank (DBX) enthält eine Liste mit verbotenen Zertifikaten sowie Hash-Werten. Die Firmware startet nur Programme, die über „DB“ verifiziert wurden und nicht in „DBX“ enthalten sind (siehe Abbildung).

Die genannten Datenbanken sind bereits vor der Installation eines Betriebssystems vorhanden und können über ein Firmware-Update aktualisiert werden. Die Daten



Zertifikate prüfen: In den Eigenschaften einer Datei gelangt man über „Digitale Signaturen“ zu den Zertifikaten. Das Beispiel zeigt den Windows-Bootmanager mit dem 2011-Zertifikat.



Uefi-Dateiprüfung: Das vereinfachte Ablaufdiagramm zeigt die Tests, die jede Efi-Datei beim Start des PCs durchlaufen muss. Schlägt die Prüfung fehl, startet das System nicht.

liegen in einem permanenten und beschreibbaren Speicher auf der Hauptplatine. Es ist möglich, die Inhalte auch per Software zu ändern und Zertifikate, Hash-Wert und Sperrlisteneinträge zu aktualisieren. Das darf natürlich nicht jeder, weil sich sonst Schadsoftware einfach verankern könnte. Deshalb gibt es noch zwei weitere Datenbanken: Der Plattform-Schlüssel (PK) stammt vom Hersteller der

IM ÜBERBLICK: ALTE UND NEUE UEFI-ZERTIFIKATE



Altes Zertifikat	Ablaufdatum	Neues Zertifikat	Ablaufdatum	Zweck
Microsoft Corporation KEK CA 2011	24.06.2026	Microsoft Corporation KEK 2K CA 2023	02.03.2038	Key Exchange Key. Signiert DB- und DBX-Updates.
Microsoft Windows Production PCA 2011	19.10.2026	Microsoft UEFI CA 2023	13.06.2038	Signatur-Datenbank (DB). Signiert Windows-Boot-Loader.
Microsoft UEFI CA 2011	27.06.2026	Microsoft UEFI CA 2023	13.06.2038	Signatur-Datenbank (DB). Signiert Bootloader von Fremdanbietern.
Microsoft UEFI CA 2011	27.06.2026	Microsoft Option ROM UEFI CA 2023	26.10.2038	Signiert Treiber von Fremdanbietern.

Vendor Keys	Valid
Provision Factory Defaults	Disabled
■ Restore Factory Keys	
■ Reset To Setup Mode	
■ Export Secure Boot variables	
■ Enroll Efi Image	
Device Guard Ready	
■ Remove 'UEFI CA' from DB	
■ Restore DB defaults	
Secure Boot variable Size Keys Key Source	
■ Platform Key(PK)	808 1 Custom
■ Key Exchange Keys	1560 1 Custom
■ Authorized Signatures	3143 2 Custom
■ Forbidden Signatures	23200 481 Mixed
■ Authorized TimeStamps	0 0 No Keys
■ OsRecovery Signatures	0 0 No Keys

Uefi-Datenbanken in der Firmware: In diesem Beispiel ist DBX (Forbidden Signatures) mit etwas über 23 KB schon gut gefüllt. Verfügbar sind nur 32 KB, bei einigen Geräten auch weniger.

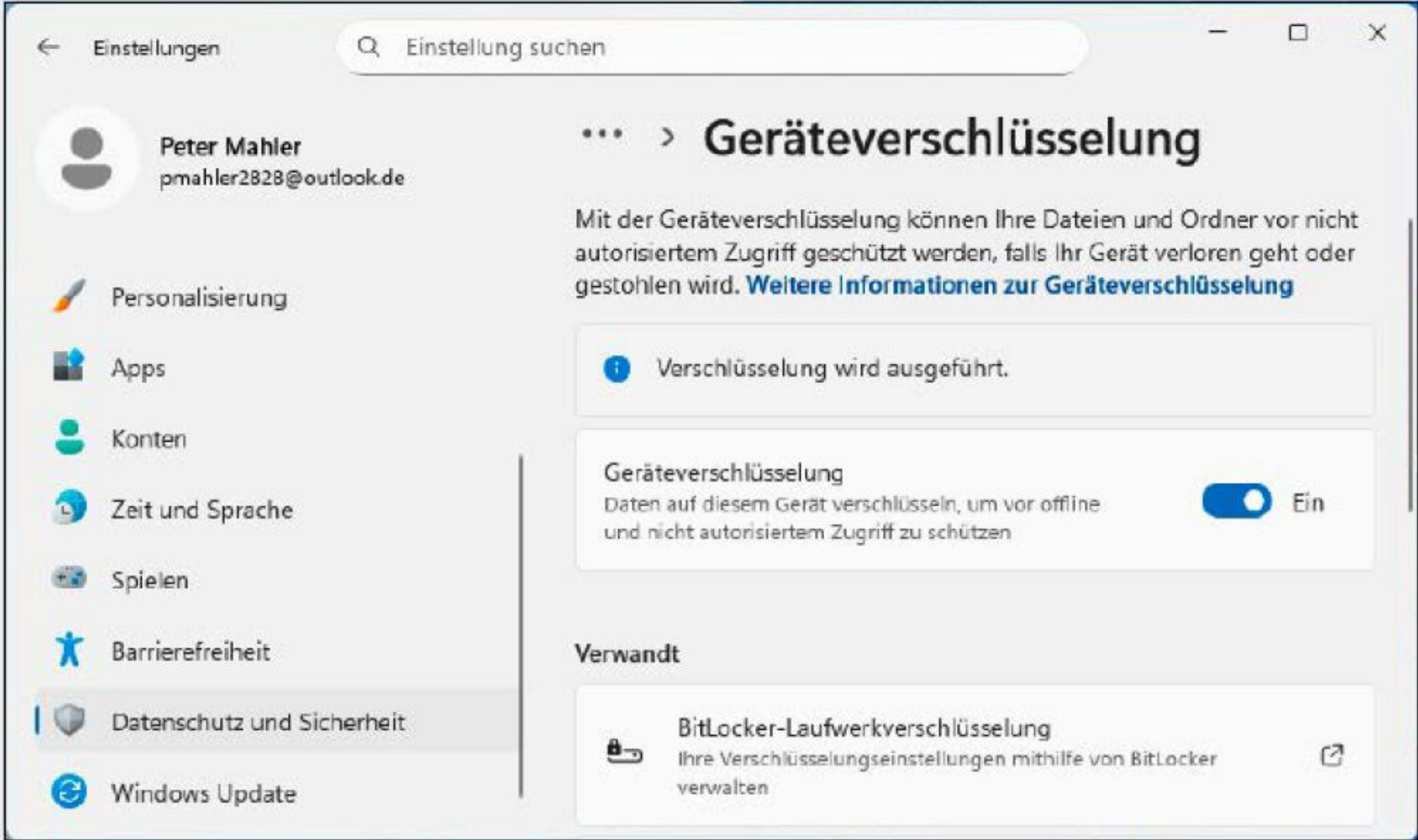
Hardware und die KEK-Schlüssel (Key Exchange Key) legen fest, welche Zertifikate eingetragen werden dürfen. In der Zertifikatskette sind PK und KEK Stammzertifikate, einer der KEKs gehört Microsoft und ist mit dem PK signiert.

BITLOCKER-SCHLÜSSEL UND TPM



Bitlocker und der TPM-Sicherheitschip haben mit Secure Boot eigentlich nichts zu tun. Allerdings bemerkt Bitlocker Änderungen im Secure-Boot-Setup durch die über TPM gespeicherten Prüfsummen. Aus Sicherheitsgründen fordert Bitlocker dann den Wiederherstellungsschlüssel an, um die Integrität des Systems zu gewährleisten. Den Schlüssel benötigen Sie auch, wenn Sie Secure Boot deaktivieren. Besitzer einer Pro-Edition öffnen die Einstellungen-App, suchen nach Bitlocker und klicken auf „Bitlocker verwalten“. Wenn Bitlocker aktiviert ist, klicken Sie auf den Link „Wiederherstellungsschlüssel sichern“ und folgen den Anweisungen des Assistenten. Bei der Home-Edition kann die Festplatte verschlüsselt sein, auch wenn Sie die Funktion selbst nicht aktiviert haben. Gehen Sie in der Einstellungen-App auf „Datenschutz und Sicherheit → Geräteverschlüsselung“. Wenn die Option „Geräteverschlüsselung“ aktiviert ist, öffnen Sie im Browser die Adresse <https://aka.ms/myrecoverykey> und melden Sie sich mit Ihrem Microsoft-Konto an. Notieren Sie die Schlüssel-ID und den Wiederherstellungsschlüssel.

Achtung Verschlüsselung! Die Geräteverschlüsselung der Home-Edition kann auch ohne Ihr Zutun aktiviert sein. Der Wiederherstellungsschlüssel ist im Microsoft-Konto gespeichert.



Der Nutzen und die Schwächen von Secure Boot

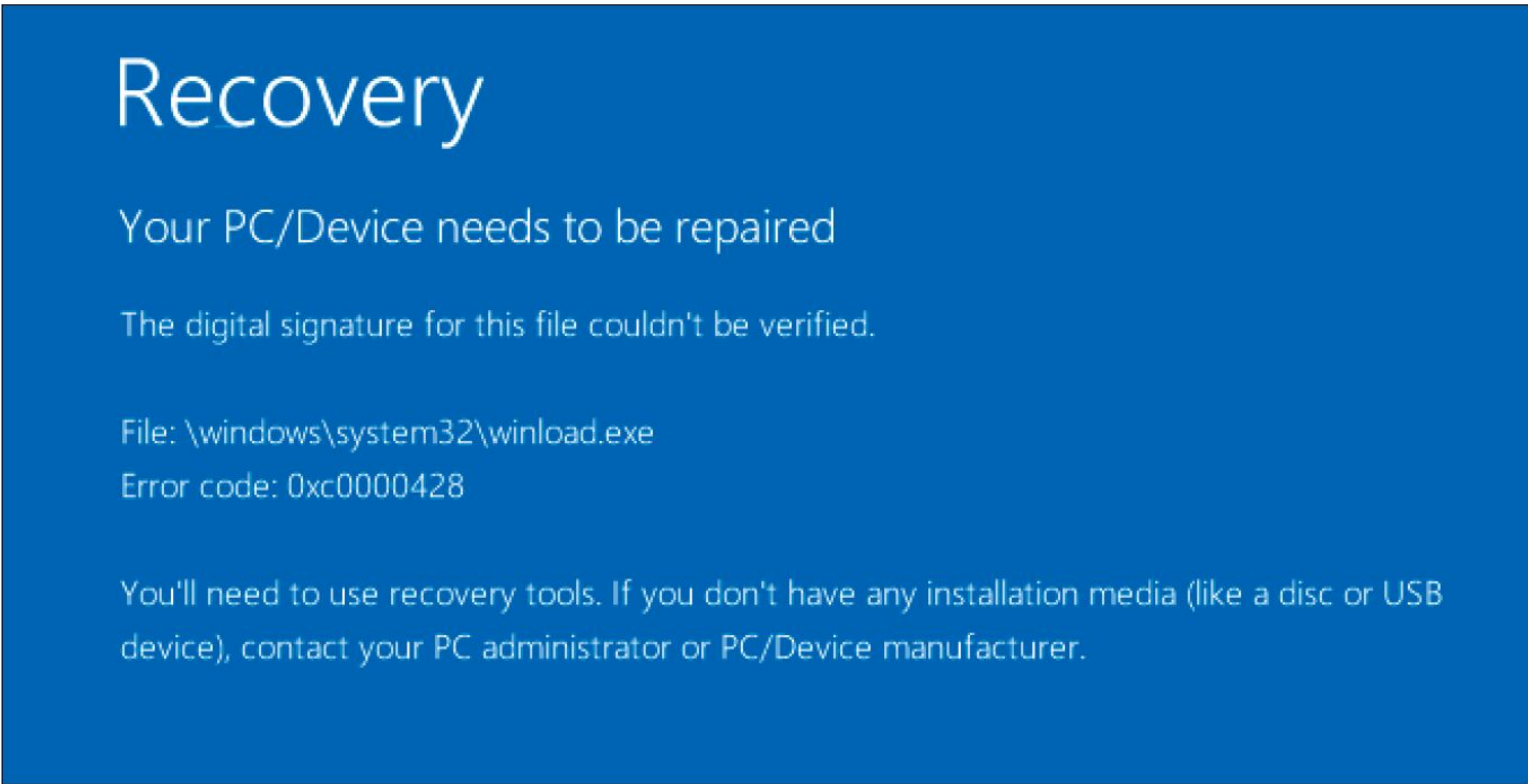
Grundsätzlich ist Secure Boot eine gute Idee, um die Startdateien eines Betriebssystems zu schützen. Findige Hacker haben trotzdem Wege gefunden, Schadsoftware einzuschleusen. Ein Beispiel dafür ist das Bootkit Black Lotus, das Schwachstellen in den Microsoft-Bootloadern ausnutzt und Dateien auf der Efi-Partition unterbringt, die Secure Boot aushebeln. In der Folge lässt sich ein Treiber installieren, der weitere Schadsoftware herunterlädt. Die Bitlocker-Verschlüsselung und die Antivirensoftware werden deaktiviert, weshalb der Befall unbemerkt bleibt. Die Gefahr, sich Black Lotus einzufangen, ist jedoch eher gering. Angreifer benötigen physischen Zugang zum PC und administrative Rechte, um das Bootkit zu installieren. Trotzdem ist das Problem nicht zu unterschätzen, weil es auch andere Wege geben könnte, Abwandlungen von Black Lotus einzurichten. Die Gefahren haben die Secure-Boot-Entwickler jedoch bedacht und deshalb mit der Sperrliste (DBX) eine Funktion eingebaut, die fehlerhafte oder böswillig manipulierte Dateien blockiert. Allerdings ist der Speicher für die Uefi-Datenbanken begrenzt. Meist stehen nur 32 KB zur Verfügung, es kann aber auch weniger sein. In der Uefi-Spezifikation ist die Speichergröße nicht vorgeschrieben. Deshalb kann die Situation eintreten, dass die inzwischen sehr umfangreiche Sperrliste nicht mehr hineinpasst. Eine nachhaltige Lösung wäre, dass Microsoft die bisherigen Zertifikate auf die Sperrliste setzt, und nur noch die neuen Zertifikate zum Einsatz kommen. Der Schritt liegt nahe, insbesondere weil die Zertifikate 2026 ablaufen. Das hätte den Vorteil, dass nur die alten Zertifikate in der DBX-Datenbank stehen müssten, die Hash-Werte anfälliger Bootloader könnten entfallen. Das hätte jedoch zur Folge, dass viele Systeme nicht mehr starten würden. Betroffen wären ältere Installationsmedien und auch zuvor angelegte Rettungsmedien, etwa zur Wiederherstellung von Backups. Auch eine zweite Windows-Installation auf dem PC würde nicht mehr starten, sofern sie über eine eigene Uefi-Partition mit veralteten Startdateien verfügt. Probleme sind auch bei der Wiederherstellung von Windows auf einem anderen PC zu erwarten, etwa nach einem Hardwaredefekt. Wenn der Firmware die neuen Uefi-Zertifikate noch

nicht bekannt sind, startet ein aktualisiertes Windows nicht. Linux-Systeme oder Rettungsmedien auf Linux-Basis würden ebenfalls nicht mehr booten, denn auch deren Bootloader sind in der Regel mit einem Microsoft-Zertifikat signiert. Die Sperrung des alten Zertifikats ist daher erst möglich, wenn die damit signierten Dateien in keinem unterstützten Betriebssystem mehr genutzt werden.

Die Folgen eines unbedachten DBX-Updates

Welche Folgen ein Update der Sperrliste haben kann, zeigte sich im Jahr 2020. Eine Sicherheitslücke im Linux-Bootloader Grub konnte zum Einschleusen von Schadsoftware genutzt werden – trotz aktiviertem Secure Boot. Microsoft hat dann kurzerhand den signierten Teil des Bootloaders per Windows-Update auf die schwarze Liste gesetzt, weshalb einige parallel installierte Linux-Systeme nicht mehr starteten. Rettungsmedien von Backup-Software konnten davon ebenfalls betroffen sein, wenn sie auf Linux-Basis arbeiten. Ein derartiges Problem lässt sich vom Nutzer allerdings leicht beheben, indem man Secure Boot im Firmware-Setup deaktiviert und das System aktualisiert. Soweit schon verfügbar, werden dann die Startdateien durch neuere Versionen ersetzt, man kann Secure Boot erneut aktivieren und das System bootet wieder. Einige Firmware-Setups bieten eine Rücksetzungsfunktion für Secure-Boot-Datenbanken an. Damit werden die Daten des Auslieferungszustands wiederhergestellt und die neuen DBX-Einträge gelöscht. Sie sollten diese Funktion jedoch nur in Ausnahmefällen nutzen, weil Nebenwirkungen zu erwarten sind. Das betrifft vor allem Installationen mit aktiver Bitlocker-Verschlüsselung (→ Kasten „Bitlocker-Schlüssel und TPM“).

Startverhinderung I: Wenn eine Datei die Prüfung durch die Firmware nicht besteht, erzeugt diese eine Fehlermeldung, etwa mit dem Text „Security Violation“.



Startverhinderung II: Auch wenn die Firmware nichts zu beanstanden hat, kann eine Datei nachträglich noch von Windows über die Code Integrity Boot Policy blockiert werden.

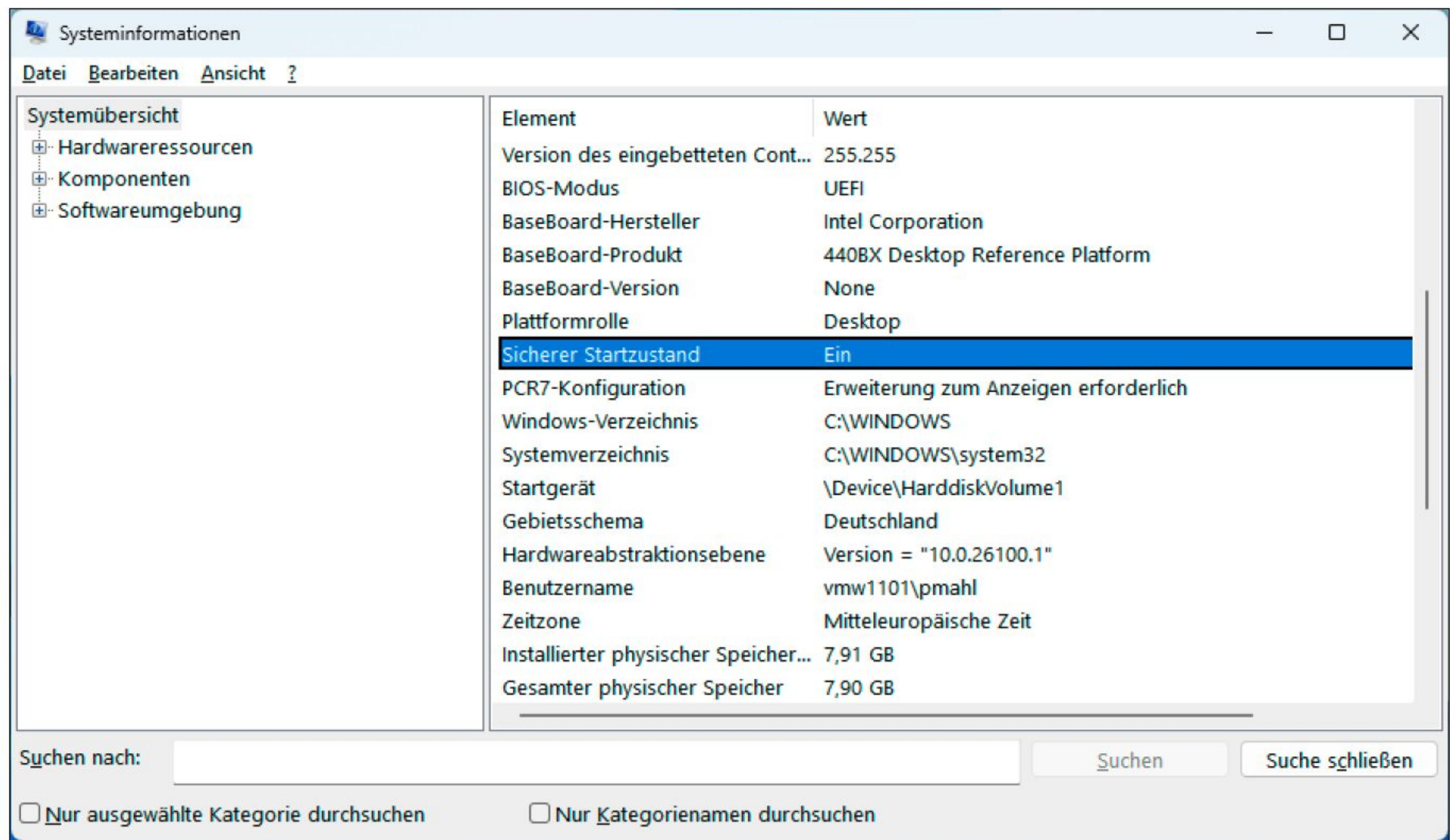
Zusätzliche Sperrlisten umgehen Platzprobleme

Microsoft hat wohl schon 2015 geahnt, dass man sich auf die DBX-Datenbank aufgrund des begrenzten Speichers nicht verlassen kann. Seit Windows 10 Version 1511 gibt es die Code Integrity Boot Policy. Diese wird über die Datei „SkuSiPolicy.p7b“ realisiert, die auf der Efi-Partition im Ordner „EFI\Microsoft\Boot“ liegt. Die gleiche Datei ist noch einmal unter „C:\Windows\System32\SecureBootUpdates“ zu finden, zusammen mit anderen Update-Dateien für die Uefi-Datenbanken. Die Efi-Startdateien absolvieren zuerst die Prüfung durch die Uefi-Firmware. Schlägt

diese fehl, sehen Sie die Meldung „Secure Boot Violation“ (oder ähnlich) der Firmware. Andernfalls startet der Bootloader und führt eine weitere Prüfung mit den Daten aus der Datei „SkuSiPolicy.p7b“ durch. Sollte der Hash-Wert einer Datei in der Sperrliste enthalten sein, erscheint die Meldung „The digital signature for this file couldn't be verified“. Diesmal auf hellblauem Hintergrund, da es sich um eine Nachricht von Windows beziehungsweise vom Bootloader handelt. Dieses Verfahren hat den Vorteil, dass andere Systeme auf dem Rechner von einer möglichen Sperrung nicht betroffen sind. Anders als bei der DBX-Sperrliste werden nur Windows-Bootloader berücksichtigt.

IM ÜBERBLICK: TOOLS FÜR SECURE BOOT UND REPARATUREN

Name	Beschreibung	Verfügbar auf	Internet	Sprache
Bootice	Partitionieren und Bootumgebung bearbeiten	Heft-DVD	https://tinyurl.com/BOOTIC	Englisch
Check-UEFI Secure Boot Variables	Uefi-Zertifikate prüfen	Heft-DVD	https://github.com/cjee21/Check-UEFISecureBootVariables	Englisch
Hasleo Backup Suite Free	Backup und Klonen	Heft-DVD	www.easyuefi.com	Deutsch
Hiren's Boot CD	Zweitsystem auf Windows-Basis	Heft-DVD	www.hirensbootcd.org	Englisch
Hwinfo Portable 8.34	Informationen zur Hardware ermitteln	Heft-DVD	www.hwinfo.com	Deutsch
Rufus Portable	Windows-Installationsstick erstellen	Heft-DVD	https://rufus.ie	Deutsch
Ventoy	Multiboot-Stick erstellen	Heft-DVD	www.ventoy.net	Deutsch
Why Not Win 11	Prüft Hardwarevoraussetzungen für Windows 11	Heft-DVD	https://github.com/rcmaehl/WhyNotWin11	Deutsch



Secure Boot prüfen: Das Tool Msinfo32 gibt Auskunft zur Hardwarekonfiguration. Wenn hinter „Sicherer Startzustand“ der Wert „Ein“ steht ist Secure Boot aktiviert.



Secure-Boot-Einstellungen: Im Firmware/Bios-Setup legen Sie den Secure-Boot-Status fest. Deaktivieren Sie Secure Boot nicht ohne Bitlocker-Wiederherstellungsschlüssel.

Für Open-Source-Systeme gibt es eine ähnliche Lösung mit dem Namen Secure Boot Advanced Targeting (SBAT), die sich nur um Linux-Bootloader kümmert. In der Uefi-Variablen „SbatLevetRT“ sind Werte hinterlegt, die nur Bootloader ab einer festgelegten Generation erlauben. Der Vorteil von SBAT liegt in der Einfachheit. Statt einer umfangreichen Liste mit verbotenen Hash-Werten genügen wenige Generationsnummern. Windows aktualisiert diese Variable bei einem Secure-Boot-Update ebenfalls. Schließlich sind nicht nur Nutzer von Sicherheitslücken im Linux-Bootloader betroffen, die das System neben Windows installiert haben. Einige Wiederherstellungssysteme basieren auf Linux und Angreifer könnten anfällige Linux-Startprogramme unbemerkt auf der Efi-Partition unterbringen.

Den Secure-Boot-Status des Systems untersuchen

Windows 10 und 11 sind standardmäßig mit aktiviertem Secure Boot installiert. Bei

Windows 11 ist das sogar eine Systemvoraussetzung – allerdings nur bei der Installation. Danach kann man Secure Boot bei den meisten Rechnern in der Firmware deaktivieren, wenn man auf den Schutz verzichten möchte. Zertifikate und Signaturen spielen dann keine Rolle mehr. Ob Secure Boot aktiviert ist, erfahren Sie am schnellsten in den Systeminformationen. Drücken Sie die Tastenkombination Win-R, tippen Sie msinfo32 ein und klicken Sie auf „OK“. Hinter „BIOS-Modus“ steht „UEFI“ und hinter „Sicherer Startzustand“ finden Sie den Eintrag „Ein“. Ohne Uefi ist auch Secure Boot nicht verfügbar. Das Tool **Why Not Win** prüft ebenfalls den Secure-Boot-Status und auch andere Systemvoraussetzungen für Windows 11. Um Secure Boot ein- oder auszuschalten, rufen Sie kurz nach dem Einschalten des PCs das Firmware-Setup meist über Tasten wie Esc, „Entf“ („Del“) oder eine der F-Tasten auf. Das gelingt oft nicht, weil Windows zu schnell startet. In diesem Fall klicken Sie im Windows-Anmeldebildschirm rechts unten

auf die „Ein/Aus“-Schaltfläche oder nach der Anmeldung auf die Schaltfläche „Ein/Aus“ im Startmenü. Halten Sie die Shift-Taste gedrückt und klicken Sie im Menü der Schaltfläche auf „Neu starten“. Gehen Sie auf „Problembehandlung → Erweiterte Optionen → UEFI-Firmwareeinstellungen“ und klicken Sie auf „Neu starten“.

Die Einstellungen für Secure Boot finden Sie meist unter einem Menü wie „Bios Features“, „Security“, „Boot“ oder ähnlich. Setzen Sie die Option auf „Enabled“ (Aktiviert) oder „Disabled“. Bei einigen Mainboards ist der Eintrag auch unterhalb von „Advanced → Windows OS Configuration“ zu finden. Voraussetzung ist in der Regel, dass nur Uefi als Bootmodus aktiviert ist. Der CSM/Legacy-Modus (Compatibility Support Module) darf nicht eingeschaltet sein, sonst steht Secure Boot nicht zur Verfügung.

Welche zusätzlichen Optionen es für Secure Boot gibt, hängt vom jeweiligen Gerät ab. Vielfach kann man die Secure-Boot-Datenbanken bearbeiten oder auf den Werkszustand zurücksetzen. Diese Einstellungen sind jedoch nur für Experten und Entwickler gedacht. Unbedachte Änderungen können den Windows-Start verhindern.

Ein Firmware/Bios-Update durchführen

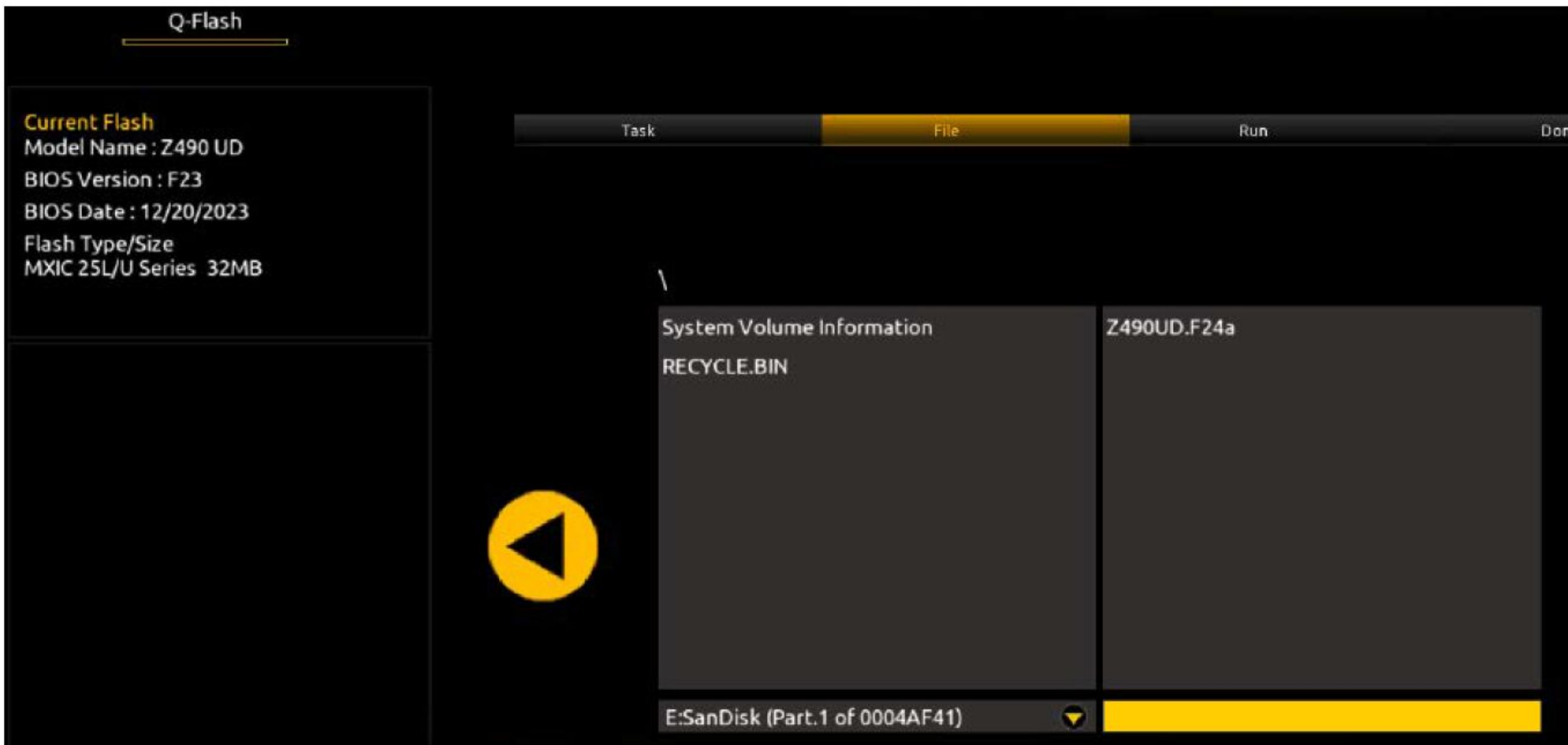
Microsoft empfiehlt, bei allen PCs und Notebooks die Firmware auf den neusten Stand zu bringen. Das erhöht die Wahrscheinlichkeit, dass sich die Aktualisierung der Uefi-Datenbanken problemlos durchführen lässt. Außerdem gelangen die neuen Zertifikate teilweise auch über das Update vom Hersteller der Hauptplatine auf den Rechner. Für ältere Geräte steht jedoch meist kein Update mehr bereit. Informieren Sie sich im Support- oder Downloadbereich, was verfügbar ist.

Das Tool **Hwinfo** hilft beim Herausfinden der genauen Modellbezeichnung. Gehen Sie im Hauptfenster im Baum auf der linken Seite auf „Hauptplatine“. Hinter „Hauptplatinen-Modell“ steht die Bezeichnung. Nach einem Klick auf den Link wählen Sie „Produktinformation“ und/oder „Treiber-Download“. Im Browser öffnet sich die Website des Herstellers, auf der Sie nach der Modellbezeichnung suchen. Wird ein Bios-Update angeboten, vergleichen Sie dessen Versionsnummer mit dem, was Hwinfo unter „Bios“ anzeigt.

Wie das Update durchzuführen ist, hängt vom Hersteller ab. Lesen Sie dazu im Handbuch nach. Teilweise gibt es Windows-Tools für eine bequeme Aktualisierung. Meist müssen Sie die Update-Datei herunterladen und auf einen USB-Stick packen, der mit dem Dateisystem FAT32 formatiert ist. Im Firmware-Setup suchen Sie nach der Update-Funktion, die etwa bei Asus „EZ Flash“ heißt oder bei Gigabyte „Q-Flash“. Wählen Sie die Update-Datei auf dem USB-Stick, starten Sie den Vorgang und befolgen Sie die Anweisungen des Assistenten. Nach einem Neustart ist das Update abgeschlossen.

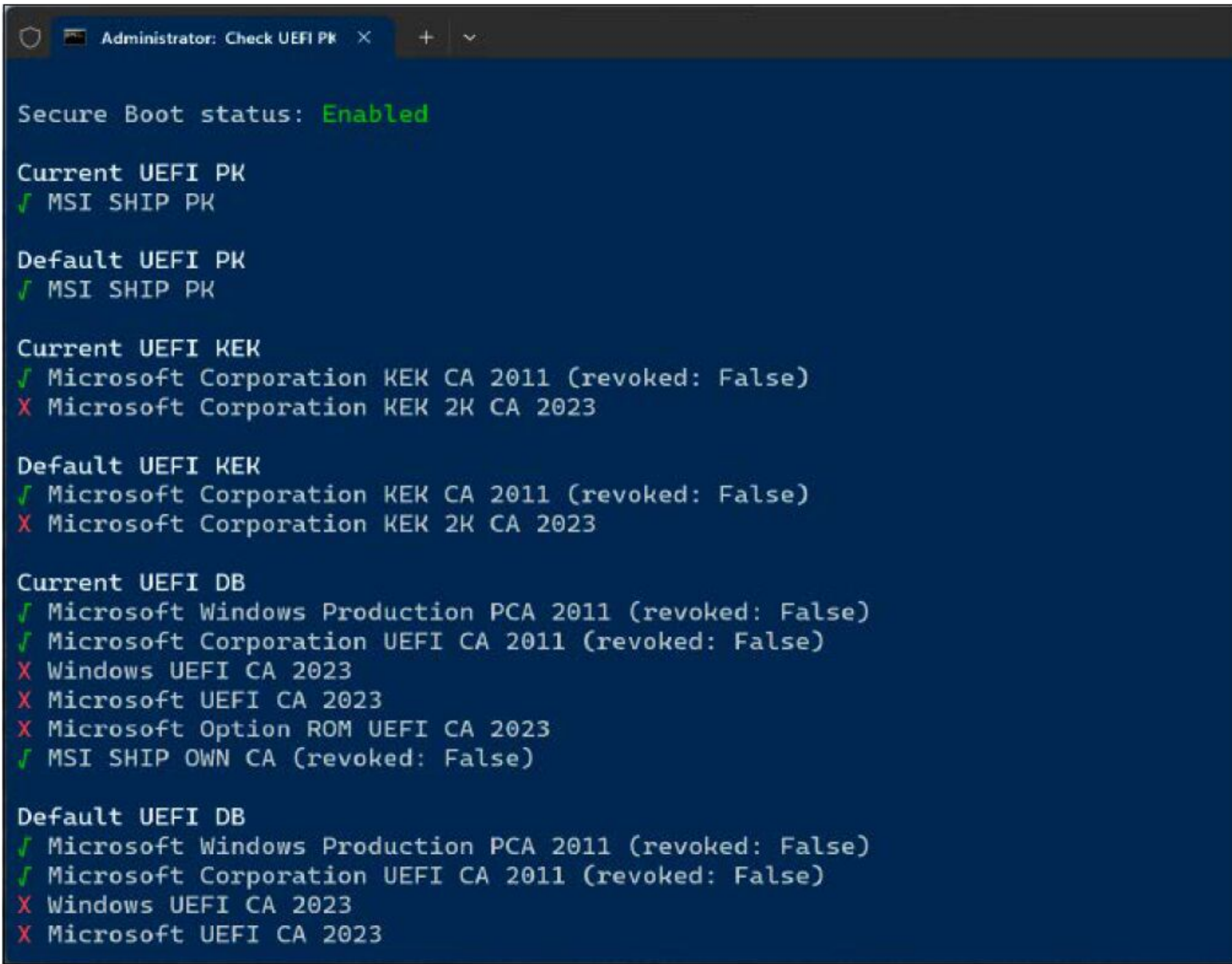
Die auf dem PC installierten Zertifikate prüfen

Ob Ihr PC bereits mit den aktuellen Microsoft-Zertifikaten versorgt ist, ermitteln Sie mit den Batch-Dateien aus dem Paket **Check-UEFI Secure Boot Variables**. Starten Sie „Check UEFI PK, KEK, DB and DBX.cmd“ nach einem rechten Mausklick und Auswahl von „Als Administrator ausführen“. Das ist für alle Batch-Dateien aus dem Paket erforderlich. Das Script zeigt die Inhalte aller Uefi-Datenbanken an, unter „Current UEFI DB“ stehen die relevanten Zertifikate. Bei einem aktualisierten System sollten mindestens „Windows UEFI CA 2023“ und „Windows UEFI CA 2023“ auftauchen. Andernfalls sind nur die Zertifikate mit dem Zusatz „2011“ zu sehen. „revoked: False“ bedeutet, dass ein Zertifikat bisher nicht zurückgezogen wurde. Wenn die neuen Zertifikate noch nicht enthalten sind, haben Sie zwei Möglichkeiten. Sie warten einfach ein paar Monate – Zeit ist bis Juni 2026 –, bis Microsoft die Datenbanken automatisch aktualisiert. Eine Voraussetzung dafür ist, dass Windows Diagnosedaten an Microsoft sendet. In der Einstellungen-App muss dafür unter „Datenschutz und Sicherheit → Diagnose und Feedback“ mindestens „Erforderliche Diagnosedaten senden“ aktiviert sein. Wenn nicht, haben Sie die Diagnosedaten wahrscheinlich über ein Datenschutztool deaktiviert und Sie müssen diese Maßnahme rückgängig machen. Sie können die Aktualisierung auch selbst anstoßen, indem Sie „Apply 2023 KEK, DB and bootmgfw update.cmd“ als Administrator starten. Die Batch-Datei setzt einen Registry-Wert, der Windows für das Update vorbereitet. Ein Eintrag in der Aufgabenplanung führt die Aktualisierung durch. Star-

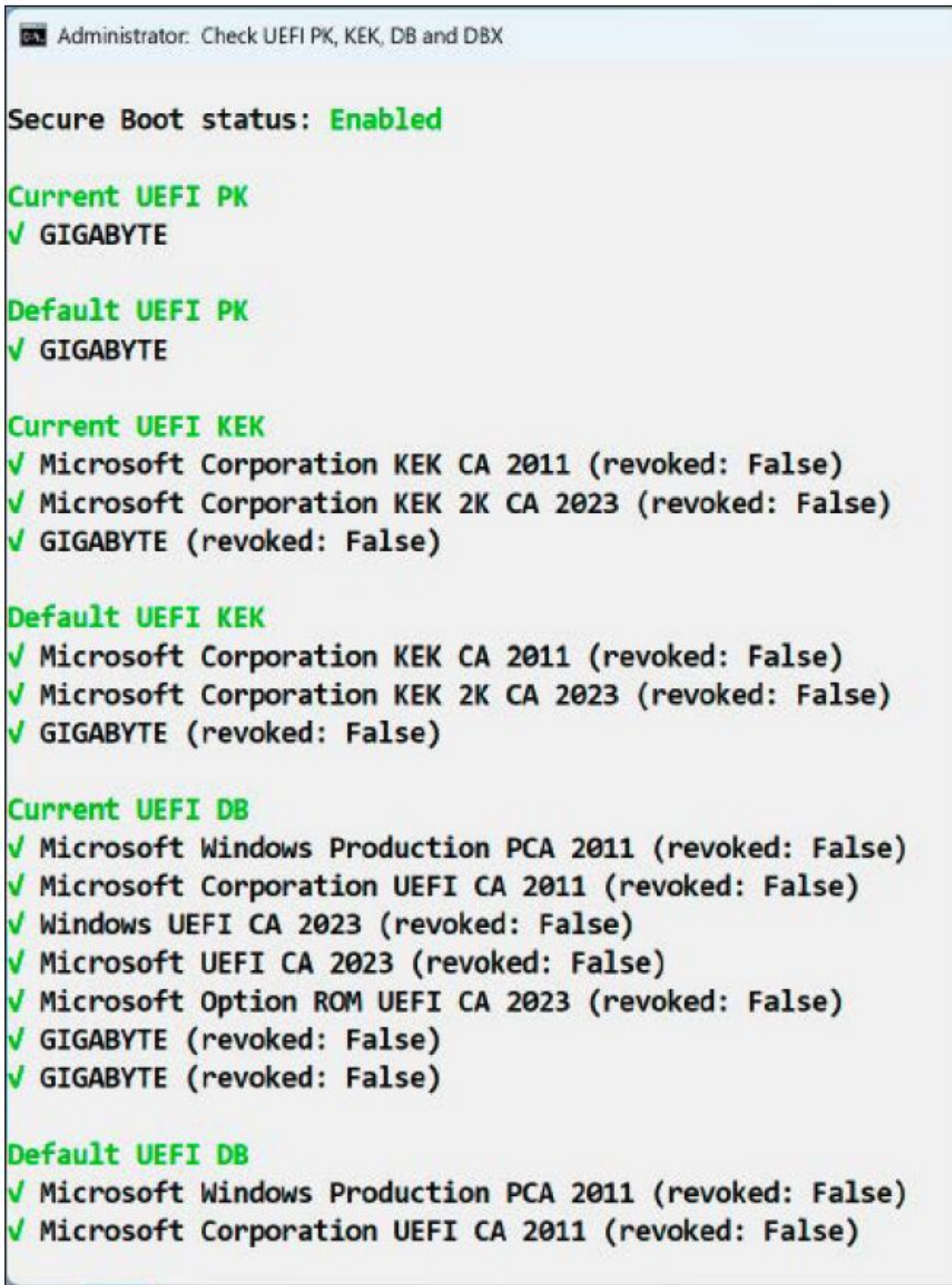


Firmware aktualisieren: Ein Update erfolgt meist über das Bios-Setup. Die Update-Datei wird von einem USB-Stick geladen, geprüft und angewendet.

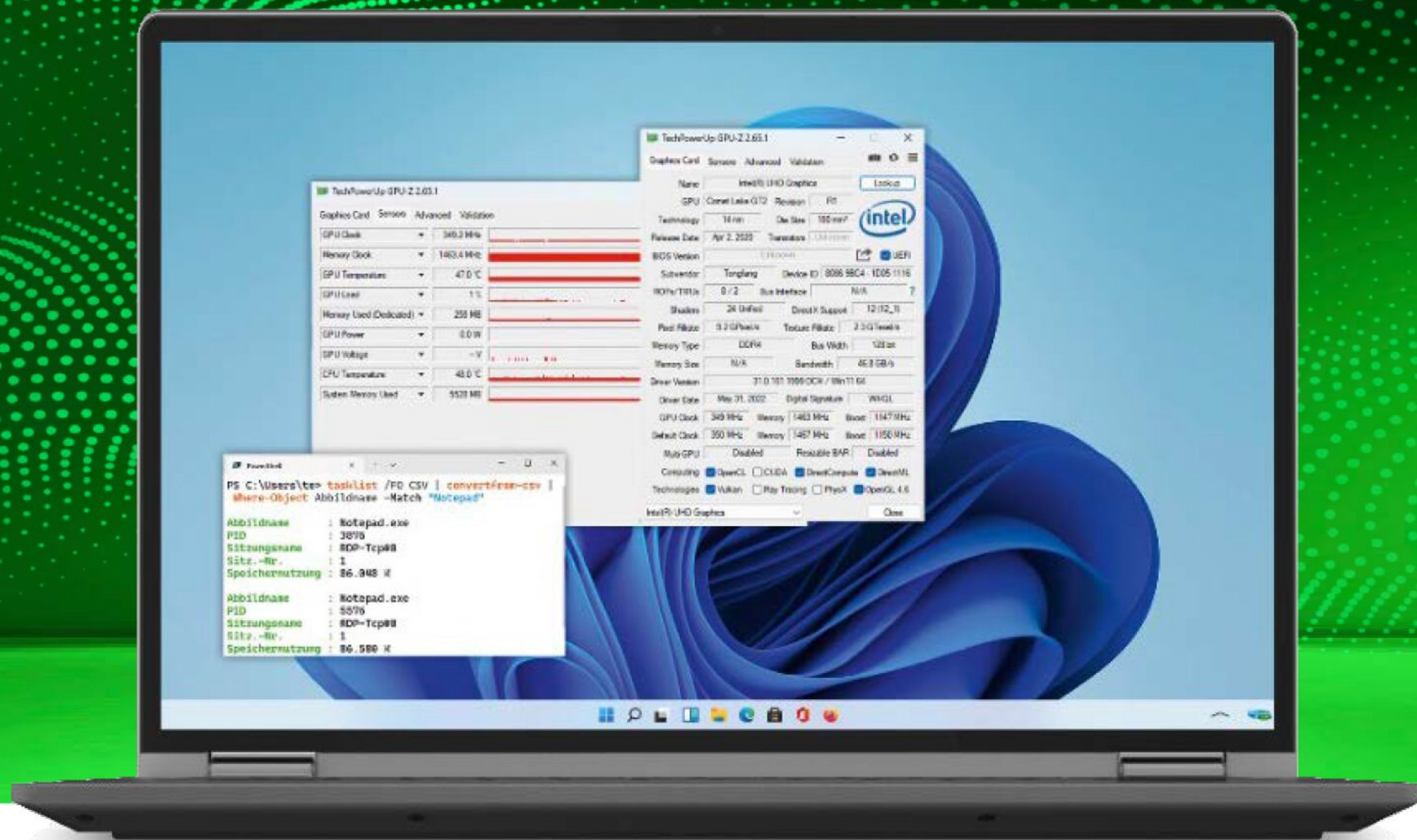
PC ohne Secure-Boot-Updates: In diesem Beispiel sind nur die Microsoft-Zertifikate mit dem Zusatz „2011“ zu sehen. Die aktuellen Zertifikate fehlen noch.



ten Sie Windows mindestens zweimal neu, damit die Einstellungen wirksam werden. Mit „Check Windows state.cmd“ können Sie die Signatur der Startdateien prüfen. Bei unseren Tests im Dezember 2025 war die Datei „bootmgfw“ bereits mit Windows UEFI CA 2023 signiert, die anderen Dateien noch nicht. **Tipp:** Es ist immer sinnvoll, regelmäßig Backups des Betriebssystems zu erstellen. Auf der Heft-DVD finden Sie dafür **Hasleo Backup Suite Free**. Für eventuelle Windows-Probleme sollte man außerdem einen USB-Stick für die Reparatur oder Neuinstallation des Systems bereithalten. Den erstellen Sie mit **Rufus** oder **Ventoy**. Auf dem Ventoy-Stick können Sie auch **Hiren's Boot CD** unterbringen. Das ist ein Rettungssystem auf Windows-Basis, das bei vielen Fehlern helfen kann. Mit **Bootice** können Sie Windows- und Uefi-Booteinträge bearbeiten und etwa die Reihenfolge ändern. ■



Alles aktuell: Bei einem aktualisierten PC findet „Check UEFI PK, KEK, DB and DBX.cmd“ auch die neuen Microsoft-Zertifikate mit dem Zusatz „2013“.



Windows-System-Checker für Profis

Wenn Windows nicht ganz rund läuft, wird es Zeit für eine Systemprüfung. Diese ist mit Bordmitteln möglich – in der Eingabeaufforderung sogar sehr detailliert. Die Tools auf der Heft-DVD ergänzen das Angebot.

VON THORSTEN EGGELING

Windows bietet einige Werkzeuge, mit denen sich das System gründlich prüfen lässt. Den meisten Nutzern dürften Geräte-Manager, Task-Manager und Ressourcenmonitor bekannt sein. Diese Programme für die grafische Oberfläche bieten einen guten Überblick, wenn es um Hardwarefehler, laufende Prozesse oder die Systemauslastung geht. Die Verwendung ist unkompliziert und durch grafische Darstellungen optisch ansprechend.

„Powershell-Befehle helfen bei detaillierten System-Checks und der gezielten Informationsabfrage.“

Allerdings zeigen die genannten Windows-Tools nicht alles an. Das ist auch kaum möglich, weil alle verfügbaren Werte gar nicht in einem Fenster unterzubringen sind. Teilweise muss man sich auch umständlich über den Aufruf von „Eigenschaften“ und die Auswahl einer Registerkarte zu den gewünschten Informationen durchklicken. Es geht aber auch anders: In der Powershell oder der Eingabeaufforderung können Sie Tools starten, über die Sie schnell und gezielt an Informationen gelangen. Anders als bei Desktoptools erschließen sich Bedienung und Nutzen nicht immer unmittelbar. Deshalb liefert dieser Beitrag zu Beginn eine kurze Einführung. Ergänzend dazu können Sie den weiterführenden Artikel **„Profi-Befehle für Windows“** (auf Heft-DVD) lesen. Wir bleiben aber nicht nur auf der Kommandozeile, sondern stellen auch einige Desktoptools vor, die den Windows-Funktionsumfang ergänzen und erweitern. Sie finden alle Tools auf der Heft-DVD.

Powershell und Eingabeaufforderung nutzen

Powershell-Befehle (Cmdlets) und Tools für die Kommandozeile liefern umfassende Informationen zu System und Hardware. Der Aufruf eines Tools allein genügt dafür nicht. Man muss auch die nötigen Optionen kennen und die Ausgabe nach den gewünschten Daten filtern. Für den Einstieg haben wir einige Beispiele in die Datei **„Powershell-Sys-Checker“** auf die Heft-DVD gepackt, an der Sie sich orientieren können. Eine Aktualisierung mit allen Beispielen aus diesem Artikel und weiteren Infos finden Sie online über <https://tinyurl.com/PSSYSCHK>. Für den Einsatz von Powershell und Powershell-Skripts sind allerdings einige Vorbereitungen nötig. Standardmäßig ist bei Windows 10 und 11 Windows-Powershell 5.1 installiert, das über Powershell.exe oder die Terminal-App gestartet wird. Enthalten sind viele für Windows spezifische Befehle, aber auch allgemeine Funktionen zur Auf-

gabenautomatisierung und Konfigurationsverwaltung. Die Software wird nicht mehr weiterentwickelt, und der Nachfolger heißt Powershell 7.x (ohne Windows davor). Der Start erfolgt über Pwsh.exe oder die Terminal-App. Die Beispiele in diesem Artikel funktionieren mit beiden Versionen, bevorzugt sollten Sie jedoch das neuere Powershell 7.x verwenden.

Wer die neue Version verwenden will, startet im Terminal

`winget install Microsoft.`

`PowerShell`

Die Terminal-App sollte inzwischen auf allen Systemen automatisch installiert worden sein. Wenn nicht, kann die Installation mit `winget install Microsoft.`

`WindowsTerminal`

in der Eingabeaufforderung erfolgen. Die Terminal-App ermöglicht die komfortable Verwendung von Windows-Powershell, Powershell und der Eingabeaufforderung in mehreren Tabs. Starten Sie das Tool nach einer Suche im Startmenü nach *Terminal*. Wenn höhere Rechte erforderlich sind, wählen Sie nach einem rechten Mausklick auf das Suchergebnis „Als Administrator ausführen“.

Powershell 7.x ist Open Source und lässt sich auch unter Linux und Mac-OS einsetzen. Aufgrund der Weiterentwicklung haben sich im Vergleich zur Windows-Powershell einige Funktionen geändert beziehungsweise sind weggefallen, neue sind hinzugekommen. Die Powershell-Befehle aus diesem Artikel laufen unter beiden Powershell-Versionen, beim Erstellen von Powershell-Profilen sollte man jedoch die Unterschiede beachten (→ Kasten „Powershell-Profil und eigene Funktionen“).

```
PowerShell 7.5.1
PS C:\Users\te> help Set-ExecutionPolicy

NAME
    Set-ExecutionPolicy

SYNTAX
    Set-ExecutionPolicy [-ExecutionPolicy] {Unrestricted | RemoteSigned | AllSigned | Restricted | Default | Bypass | Undefined} [[-Scope] {Process | CurrentUser | LocalMachine | UserPolicy | MachinePolicy}] [-Force] [-WhatIf] [-Confirm] [<CommonParameters>]

PARAMETERS
    -Confirm

        Required?                false
        Position?                Named
        Accept pipeline input?    false
        Parameter set name        (All)
        Aliases                   cf
        Dynamic?                 false
        Accept wildcard characters? false
```

Powershell mit eingebauter Hilfe: Stellen Sie einem Befehl „help“ voran, um einen kurzen Hilfetext zu erhalten. „Update-Help“ lädt die umfangreichere Hilfe herunter.

Hilfe zu Befehlen anfordern: In der Powershell führt ein vorangestelltes „help“ bei einem Befehl zu einer knappen Übersicht der Optionen. Starten Sie

`Update-Help`

für den Download der ausführlicheren Hilfedateien. Oder Sie hängen „-Online“ an, dann öffnet sich die Hilfe im Webbrowser, zum Beispiel:

`help Set-ExecutionPolicy -Online`

Bei Tools für die Kommandozeile zeigt meist ein angehängtes „/?“ die Hilfe an.

Allgemeine Informationen zum System ermitteln

Im Terminal gibt das Tool Systeminfo Auskunft über die Eckdaten des Systems. Enthalten sind unter anderem Hostname, Betriebssystemname, Betriebssystemversion und Systemstartzeit. Das ist ein Teil der Daten, die auch Msinfo32 in einem Fenster anzeigt.

Sie benötigen nur einen bestimmten Wert aus der Systeminfo-Datenmenge. In der Powershell können Sie die Ausgabe filtern: `systeminfo /FO CSV | convertfrom-csv | Select-Object`

`"Systemstartzeit"`

Der Schalter „/FO CSV“ legt das Format der Ausgabe auf CSV (Comma-Separated Values) fest. Die CSV-Daten werden mit dem Pipe-Zeichen („|“) an das Powershell-Cmdlet „convertfrom-csv“ weitergeleitet, das Powershell-Objekte für jede Zeile der Daten erzeugt. Mit „Select-Object“ wird schließlich nur der gewünschte Wert ausgegeben. Dieser muss nur zwingend in Anführungszeichen stehen, wenn er Leerzeichen enthält. Eine Variante erzeugen Sie mit

`systeminfo /FO CSV | convertfrom-csv | % "Systemstartzeit"`

Dieser Befehl gibt den Wert alleine aus, ohne den Wertnamen. Das Format eignet

IM ÜBERBLICK: TOOLS FÜR DEN SYSTEM-CHECK



Name	Beschreibung	Auf	Internet	Sprache
CPU-Z Portable	Prozessor-Analyse und CPU-Test	Heft-DVD	www.cpubid.com	Englisch
Crystaldiskinfo	Laufwerksinformationen ermitteln	Heft-DVD	https://crystalmark.info	Deutsch
Crystaldiskmark	Benchmark für Laufwerke	Heft-DVD	https://crystalmark.info	Deutsch
F3 für Windows	USB-Sticks prüfen	Heft-DVD	https://tinyurl.com/F3Win	Englisch
GPU-Z	Infos zum Grafikchip abrufen	Heft-DVD	www.techpowerup.com	Englisch
Hwinfo Portable	Informationen zur Hardware ermitteln	Heft-DVD	www.hwinfo.com	Deutsch
PC-WELT-Beitrag: „Profi-Befehle für Windows“	Einführung in Powershell	Heft-DVD	www.pcwelt.de/1153898	Deutsch
PCI-Z	Infos zu Hardware am PCI-Bus	Heft-DVD	www.pci-z.com	Englisch
Powershell-Sys-Checker	Powershell-Befehle für Systeminfos	Heft-DVD	https://tinyurl.com/PSSYSCHK	Deutsch
Speccy Portable	Zeigt Infos zur Hardware an	Heft-DVD	www.ccleaner.com/de-de/speccy	Englisch
SSD-Z	Zeigt Informationen zu SSDs	Heft-DVD	http://aezay.dk	Englisch
System Informer	Task-Manager-Ersatz	Heft-DVD	https://systeminformer.sourceforge.io/	Englisch


```
PS C:\Users\te> $data=systeminfo /FO CSV | convertfrom-csv | % "Systemstartzeit"
PS C:\Users\te> $Start_Date=Get-Date $data
PS C:\Users\te> $End_Date=Get-Date
PS C:\Users\te> New-TimeSpan -Start $Start_Date -end $End_Date

Days           : 0
Hours          : 0
Minutes        : 28
Seconds        : 52
Milliseconds   : 816
Ticks          : 17328167798
TotalDays      : 0,0200557497662037
TotalHours     : 0,481337994388889
TotalMinutes   : 28,8802796633333
TotalSeconds   : 1732,8167798
TotalMilliseconds : 1732816,7798

PS C:\Users\te>
```

Wie lange läuft der PC? Systeminfo gibt nur die Startzeit aus. Mit einigen Powershell-Befehlen lässt sich die Zeitdifferenz zur aktuellen Uhrzeit berechnen.

sich für die Weiterverarbeitung zu anderen Zwecken. Speichern Sie es in einer Variablen, indem Sie der Befehlszeile „\$data=“ voransetzen. Die folgenden vier Powershell-Zeilen berechnen die Zeit, seit der Computer läuft:

```
$data=systeminfo /FO CSV |
    convertfrom-csv | %
    "Systemstartzeit"
```

```
$Start_Date=Get-Date $data
$End_Date=Get-Date
New-TimeSpan -Start $Start_Date
    -End $End_Date
```

Powershell-Cmdlet verwenden: Der Powershell-Befehl Get-ComputerInfo lässt sich ähnlich wie Systeminfo verwenden und liefert teilweise ausführlichere Daten. Führen Sie ihn ohne weitere Optionen aus, wenn Sie

```
PS C:\Users\te> tasklist /FO CSV | convertfrom-csv |
    Where-Object Abbildname -Match "Notepad"

Abbildname      : Notepad.exe
PID             : 3876
Sitzungsname     : RDP-Tcp#0
Sitz.-Nr.        : 1
Speichernutzung : 86.048 K

Abbildname      : Notepad.exe
PID             : 5576
Sitzungsname     : RDP-Tcp#0
Sitz.-Nr.        : 1
Speichernutzung : 86.580 K
```

Prozess-ID herausfinden: Das Tool Tasklist zeigt alle laufenden Prozesse. Per Powershell-Filter kann man nach dem Namen eines Prozesses suchen und seine ID ermitteln.

alle Werte sehen wollen. Oder Sie lassen sich nur ausgewählte Informationen anzeigen:

```
Get-ComputerInfo | Select-Object
    OsName, OsVersion, OsArchitecture,
    OsSystemDrive
```

Alternative für die grafische Oberfläche: Das Tool **Speccy Portable** liefert zahlreiche Daten zu Betriebssystem und Hardware.

Laufende Prozesse kontrollieren oder beenden

Tasklist zeigt alle laufenden Prozesse an, wenn Sie das Tool ohne Parameter aufrufen. Ein Aufruf mit

```
tasklist /FI "imagename eq notepad.exe"
```

zeigt nur Prozesse mit dem Abbildnamen „Notepad.exe“ an. Wildcards am Ende des Ausdrucks werden verarbeitet, beispielsweise „notepad*“. Da Tasklist wie Systeminfo die Option „/FO CSV“ versteht, ist auch hier ein Filter mit Powershell möglich:

```
tasklist /FO CSV | convertfrom-csv |
    Where-Object Abbildname -Match
    "Notepad"
```

Die Ausgabe enthält bei beiden Verfahren die Prozess-ID (PID) des gesuchten Prozesses. Mit

```
taskkill /PID 12345
```

können Sie einen Prozess beenden. Verwenden Sie zusätzlich die Option „/F“, wenn sich ein Prozess nicht beenden lässt, und „/T“, um auch die untergeordneten Prozesse zu beenden. Im jeweiligen Programm nicht gespeicherte Daten gehen dabei verloren.

Powershell-Cmdlet verwenden: Get-Process können Sie für die gleichen Zwecke wie Tasklist einsetzen. Ohne Optionen erhalten Sie eine Liste aller Prozesse. Der Befehl `Get-Process notepad | Format-List *` zeigt nur die Prozesse mit dem Namen

POWERSHELL-PROFIL UND EIGENE FUNKTIONEN



Über das Powershell-Profil kann man eigene Funktionen definieren. Windows-Powershell verwendet den Ordner „C:\Users\[User]\Documents\WindowsPowerShell“, Powershell den Ordner „C:\Users\[User]\Documents\PowerShell“. Erstellen Sie beide Ordner oder nur den für die bevorzugte Version sowie darin (jeweils) eine Textdatei mit der Bezeichnung „Microsoft.PowerShell_profile.ps1“.

Die Profildatei lädt Powershell beim Start automatisch, wenn Sie mit *Set-Execution-Policy* die Script-Ausführung erlaubt haben (siehe auch Kasten „Den Start von Powershell-Scripts erlauben“).

Wenn Sie die Zeile

```
Function no {notepad $args[0]}
```

in der Profildatei unterbringen, können Sie eine neue Textdatei mit

`no` `NeueDatei.txt`

erstellen und im Windows-Editor öffnen. Ist die Datei bereits vorhanden, wird sie geöffnet. Ohne Parameter öffnet sich ein Notepad-Fenster.

Nach dem gleichen Muster erstellen Sie Funktionen für die in diesem Artikel genannten Cmdlets.

Eigene Powershell-Funktionen erstellen: Die Profildatei „Microsoft.PowerShell_profile.ps1“ ist ein Script, das Powershell beim Start automatisch einliest.

```
# Diese Profil-Dateien lädt Powershell automatisch beim Start.
# Sie können die enthaltenen Funktionen dann direkt nutzen.
# Kommentieren Sie die Zeilen aus, die Sie nicht benötigen.

# Datei in Notepad öffnen
Function no {notepad $args[0]}

# Datei in Notepad++ öffnen
Function npp {
    $myApp="C:\Program Files (x86)\Notepad++\notepad++.exe"
    Start-Process -FilePath $myApp `"$($args[0])`"
}
```


„notepad“ an und liefert erweiterte Informationen, etwa zu Programmpfad, RAM-Belegung und zur besseren Identifizierung auch den Fenstertitel.

Stop-Process -Name "notepad"

beendet alle Notepad-Instanzen ohne Rückfrage. Verwenden Sie die Option „-Confirm“, um eine Bestätigung anzufordern, „-Force“ erzwingt das Beenden eines Prozesses.

Zielsicherer ist der Einsatz von

Stop-Process -Id [PID] -Confirm

Setzen Sie für den Platzhalter „[PID]“ die zuvor mit Get-Process ermittelte Prozess-ID ein.

Alternativen für die grafische Oberfläche:

Der Windows-Taskmanager (schneller Aufruf mit Strg-Shift-Esc) sollte für die meisten Benutzer ausreichen, wenn es um die Anzeige und das Beenden von Prozessen geht. **System Informer** sollten Sie sich ansehen, wenn Sie mehr wissen wollen. Das Tool kann Prozesse anzeigen (und beenden), aber auch Datenraten der Festplatten und eine Geräteübersicht.

Die Hardware im PC gründlich untersuchen

Das Tool Systeminfo zeigt auch einige Informationen zum Systemhersteller, Systemmodell (Mainboard), Prozessor und verfügbarem Speicher an. Für eine strukturiertere Ausgabe eignet sich jedoch das Powershell-Cmdlet Get-ComputerInfo besser. Der Befehl

Get-ComputerInfo | Select-Object

BiosSMBIOSBIOSVersion

liest die Versionsnummer der Firmware aus – nützlich, wenn man nach einem Bios-Update suchen will. Den verfügbaren physischen Speicher bekommt man mit

Get-ComputerInfo | Select

CsCaption,@{Name="GB";

Expression={ [math]::round(\$_.OsFreePhysicalMemory/1MB, 2) }}

heraus. Die Angabe hinter „Expression=“ wandelt den ausgegebenen Wert in gerundete Gigabyte um.

Detaillierte Informationen zur Hardware:

Verwenden Sie Get-CimInstance, gefolgt von einer CIM-Klasse (Common Information Model). In der Windows-Powershell funktioniert auch noch der inzwischen veraltete Befehl Get-WmiObject (WMI, Windows Management Instrumentation), der die gleichen Aufgaben erfüllt. Der Befehl **Get-CIMClass**

Name	PID	CPU	I/O total rate	Private bytes	User name	Description
System Idle Process	0	0,00	0,00	0 B	NT-AUTORITÄT\SYSTEM	
System	4	0,05	847,96 kB/s	56 kB	NT-AUTORITÄT\SYSTEM	NT Kernel & System
Registry	224			95,04 MB		
smss.exe	780			1,11 MB		Windows Session Manager
Memory Compression	3264			40 kB		
Interrupts		0,05		0		Interrupts and DPCs
csrss.exe	880			2,16 MB		Client Server Runtime Process
wininit.exe	1140			1,47 MB		Windows Start-Up Application
services.exe	1212	0,03		5,72 MB		Services and Controller app
svchost.exe	1364			10,95 MB		Host Process for Windows Ser...
WmiPrvSE.exe	6700			7,36 MB		WMI Provider Host
SearchHost.exe	7976			158,11 MB	ZIPPO\te	
StartMenuExperienceHost.exe	8208			54,97 MB	ZIPPO\te	Windows Start Experience Host
RuntimeBroker.exe	8264			6,46 MB	ZIPPO\te	Runtime Broker
RuntimeBroker.exe	6112			9,7 MB	ZIPPO\te	Runtime Broker
Widgets.exe	8400			9,99 MB	ZIPPO\te	
msedgewebview2.exe	9776			34,14 MB	ZIPPO\te	Microsoft Edge WebView2
msedgewebview2.exe	8224			2,08 MB	ZIPPO\te	Microsoft Edge WebView2
msedgewebview2.exe	9332			53,44 MB	ZIPPO\te	Microsoft Edge WebView2
msedgewebview2.exe	13688			12,12 MB	ZIPPO\te	Microsoft Edge WebView2
msedgewebview2.exe	13188			8,56 MB	ZIPPO\te	Microsoft Edge WebView2
msedgewebview2.exe	5648			116,23 MB	ZIPPO\te	Microsoft Edge WebView2

Ersatz für den Task-Manager: System Informer zeigt eine gut strukturierte Prozessliste. Das Tool liefert auch Infos zum Netzwerkverkehr und zu Festplattenzugriffen.

Wie viel Platz ist auf den Laufwerken? Get-Volumeliefert Daten zur Festplattenbelegung. Man kann sich den verfügbaren Speicherplatz und den Zustand anzeigen lassen.

DriveLetter	FileSystem	SizeRemaining	Size	HealthStatus
C	NTFS	33309630464	63509098496	Healthy
F	NTFS	120606720	808448000	Healthy
E	FAT32	51552256	98566144	Healthy
	NTFS	88207360	591392768	Healthy
D	NTFS	1272939069440	1999787737088	Healthy
G	NTFS	678292881408	5000810983424	Warning

GPU-Z: Das Tool stellt fast alle Werte dar, die sich über den Grafikchip herausfinden lassen. Eine Grafik zeigt den Verlauf, etwa von Auslastung und Temperatur.

Graphics Card	Sensors	Advanced	Validation
GPU Clock	349.2 MHz		
Memory Clock	1463.4 MHz		
GPU Temperature	47.0 °C		
GPU Load	1 %		
Memory Used (Dedicated)	258 MB		
GPU Power	0.0 W		
GPU Voltage	- V		
CPU Temperature	48.0 °C		
System Memory Used	5528 MB		

ohne weitere Optionen gibt eine sehr lange Liste der CIM-Klassen aus. Mit einem Filter wie beispielsweise

Get-CimClass -ClassName *disk*

schränken Sie die Liste auf einen relevanten Bereich ein. Viele Klassen gibt es doppelt, einmal mit dem Präfix „CIM_“ und auch mit „Win32_“. Letztere bezieht sich auf die älteren WMI-Bezeichnungen, funktional sind aber beide Klassen identisch. Nachfolgend finden Sie einige Beispiele.

Infos zur CPU:

Get-CimInstance Win32_Processor |
Select-Object Name,

NumberOfCores,
NumberOfLogicalProcessors,
MaxClockSpeed | Format-List

Unter anderem Name und Modell sowie RAM des Computers:

Get-CimInstance win32_

ComputerSystem

Laufwerke und Laufwerksgrößen:

Get-CimInstance Win32_DiskDrive

Die installierten Treiber inklusive Versionsnummern:

Get-CimInstance win32_

PnpSignedDriver | Select-Object
DeviceName, DriverVersion,


```
PowerShell
PS C:\Users\te> C:\Tools\F3-8.0-Windows-x64\F3read.exe H:\
F3 read 8.0
Copyright (C) 2010 Digirati Internet LTDA.
This is free software; see the source for copying conditions.

          SECTORS      ok/corrupted/changed/overwritten
Validating file 1.h2w ... 2097152/      0/      0/      0
Validating file 2.h2w ... 2097152/      0/      0/      0
Validating file 3.h2w ... 2097152/      0/      0/      0
Validating file 4.h2w ... 2097152/      0/      0/      0
Validating file 5.h2w ... 2097152/      0/      0/      0
Validating file 6.h2w ... 2097152/      0/      0/      0
Validating file 7.h2w ... 2097152/      0/      0/      0
Validating file 8.h2w ... 2097152/      0/      0/      0
Validating file 9.h2w ... 2097152/      0/      0/      0
Validating file 10.h2w ... 33.46% -- 33.15 MB/s -- 7:20
```

Was taugt der USB-Stick? F3 beschreibt den Speicherstick nahezu vollständig mit Dateien, die zufällige Daten enthalten. Wenn F3Read danach alles fehlerfrei wieder einlesen kann, ist das Gerät in Ordnung.

DriverDate | Format-Table
-AutoSize

Spezialisierte Befehle für einzelne Bereiche: Mit Get-CimInstance ist fast alles möglich, zusätzliche Befehle ermöglichen einen gezielteren Zugriff. Laufwerksbuchstaben, freien Speicherplatz, Größe und Status von Festplatten anzeigen:

Get-Volume | Select-Object
DriveLetter, FileSystem,
SizeRemaining, Size, HealthStatus
| Format-Table -AutoSize

Alle Partitionen auflisten:
Get-Partition

Laufwerk prüfen (entspricht „chkdsk Y:“, als Administrator aufrufen):
Repair-Volume -DriveLetter Y -Scan

Laufwerk prüfen und reparieren (entspricht „chkdsk /F“, als Administrator aufrufen):
Repair-Volume -DriveLetter Y
-OfflineScanAndFix

Status von Secure Boot anzeigen (als Administrator aufrufen):
Get-SecureBootPolicy

DEN START VON POWERSHELL-SCRIPTS
ERLAUBEN



Einzelne Befehle können Sie in der Powershell immer ausführen, Scripts lassen sich jedoch nicht starten. Das gilt auch für das Powershell-Profil. Welche Einstellungen gelten, finden Sie mit

Get-ExecutionPolicy -List

heraus. Wenn bei „CurrentUser“ der Wert „Undefined“ steht, starten Sie in der Windows-Powershell und/oder Powershell

Set-ExecutionPolicy
-Scope CurrentUser
-ExecutionPolicy
RemoteSigned

Damit erlauben Sie dem aktuellen Benutzer die Script-Ausführung in der Powershell. Soll die Einstellung für den PC gelten, verwenden Sie hinter „-Scope“ den Wert „LocalMachine“, wofür Sie die Powershell mit administrativen Rechten starten müssen.

```
PowerShell
PS C:\Users\te> Get-ExecutionPolicy -List

Scope ExecutionPolicy
-----
MachinePolicy Undefined
UserPolicy Undefined
Process Undefined
CurrentUser Undefined
LocalMachine Undefined

PS C:\Users\te> Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy RemoteSigned
```

Script-Ausführung erlauben: Ohne gelockerte „ExecutionPolicy“ führt Powershell kein Script aus und kann auch die Profildatei nicht laden.

Geräte mit einem spezifischen Status anzeigen, etwa „fehlerhaft“:

```
Get-PnpDevice -PresentOnly -Status  
ERROR,DEGRADED,UNKNOWN
```

Konfigurierte Drucker auflisten:

```
Get-Printer
```

Alternativen für die grafische Oberfläche: Auf die Heft-DVD haben wir mehrere Tools mit Hardwarebezug gepackt. **Hwinfo** bietet umfangreiche Funktionen und zeigt unter anderem detaillierte Sensorwerte von CPU, GPU, Festplatten und Mainboard an. Die Tools **CPU-Z**, **GPU-Z**, **PCI-Z** und **SSD-Z** liefern Daten zu Ihren jeweiligen Spezialgebieten. Mit **CrystallDiskmark** messen Sie die Transferraten von Laufwerken, und mit **Crystal-diskinfo** ermitteln Sie Laufwerksinformationen, etwa zum Zustand der Hardware.

Kapazität und Geschwindigkeit
eines USB-Sticks testen

Daten zu externen Laufwerken am USB-Port lassen sich mit den gleichen Methoden auslesen wie bei internen Festplatten und SSDs. Es sind allerdings zahlreiche gefälschte USB-Sticks unterwegs, die eine höhere Kapazität melden, als sie tatsächlich haben. Das fällt erst auf, wenn sich weniger Dateien darauf speichern lassen als angenommen.

Das kleine Tool **F3 (Fight Flash Fraud)** testet die Kapazität und Leistung von Laufwerken. Es füllt einen USB-Stick maximal mit Dateien, die Zufallswerte enthalten. Dann prüft es, ob sich die Dateien wieder korrekt einlesen lassen. Bei gefälschten oder defekten Sticks ist das nicht möglich. F3 ist nur für Linux oder im Quellcode verfügbar. Wir haben daraus eine Version für Windows erstellt.

Wichtig: Bevor Sie F3 verwenden, sichern Sie alle Dateien auf dem USB-Stick an einem anderen Ort.

Kopieren Sie F3 beispielsweise in den Ordner „C:\Tools\F3“ und starten Sie das Programm in der Powershell oder Eingabeaufforderung mit

```
C:\Tools\F3\F3write.exe X:\
```

„X:“ ersetzen Sie durch den Laufwerksbuchstaben des USB-Sticks. Warten Sie, bis F3 alle Dateien erstellt hat. Dabei können Sie die Transferrate beobachten. Anschließend starten Sie

```
C:\Tools\F3\F3read.exe X:\
```

F3 liest die Dateien der Reihe nach ein. In der Fortschrittsanzeige ist zu sehen, ob dabei Fehler aufgetreten sind. Nach Abschluss der Prüfung löschen Sie die auf dem Laufwerk erstellten h2w-Dateien.

Informationen zur Netzwerkkonfiguration einholen

Der Klassiker auf der Kommandozeile ist Ipconfig. Das Tool zeigt die Netzwerkadapter und die dafür konfigurierten IP-Adressen an. Ergänzen Sie den Parameter „/all“, um auch die physische Adresse (eindeutige MAC-Adresse der Hardware, Media Access Control) und die DNS-Server zu sehen. Die Parameter „/flushdns“ (DNS-Cache leeren) und „/renew“ (IP per DHCP erneut abfragen) verwenden Sie bei Netzwerkproblemen.

Powershell bietet für Netzwerkfunktionen mehrere Cmdlets. Get-NetIPAddress zeigt die Namen der Netzwerkadapter, IP-Adressen und DNS-Server an. Verwenden Sie

```
Get-NetIPConfiguration
-InterfaceAlias "[Name]"
```

wenn Sie nur die Konfiguration eines einzelnen Netzwerkadapters sehen wollen. Den Platzhalter „[Name]“ ersetzen Sie durch die Bezeichnung des gewünschten Adapters. Weitere Cmdlets dienen zur Abfrage einzelner Werte oder liefern Zusatzinformationen. Get-NetIPInterface zeigt „InterfaceAlias“ und den Status der Verbindungen („Connected“, „Disconnected“). Get-NetTCPConnection gibt eine Liste der aktiven IP-Verbindungen aus.

Alternativen für die grafische Oberfläche:

Der Windows-Task-Manager zeigt auf der Registerkarte „Leistung“ den Netzwerkdurchsatz und die IP-Adressen an. System Informer gibt auf der Registerkarte „Network“ eine Liste der Netzwerkverbindungen aus, die sich über das Suchfeld filtern lässt.

Funktionen für Netzwerkfreigaben: Der Net-Befehl stellt Funktionen bereit, die man für die Verwaltung von Windows-Freigaben im Netzwerk benötigt.

net share zeigt die auf dem PC freigegebenen Ressourcen an, und was auf anderen Geräten freigegeben ist, erfährt man mit

```
net view \[Computername]
```

Wer eine Freigabe ins Dateisystem einbinden möchte, verwendet

```
net use X: \[Server\Freigabe]
```

Mit

```
net share
```

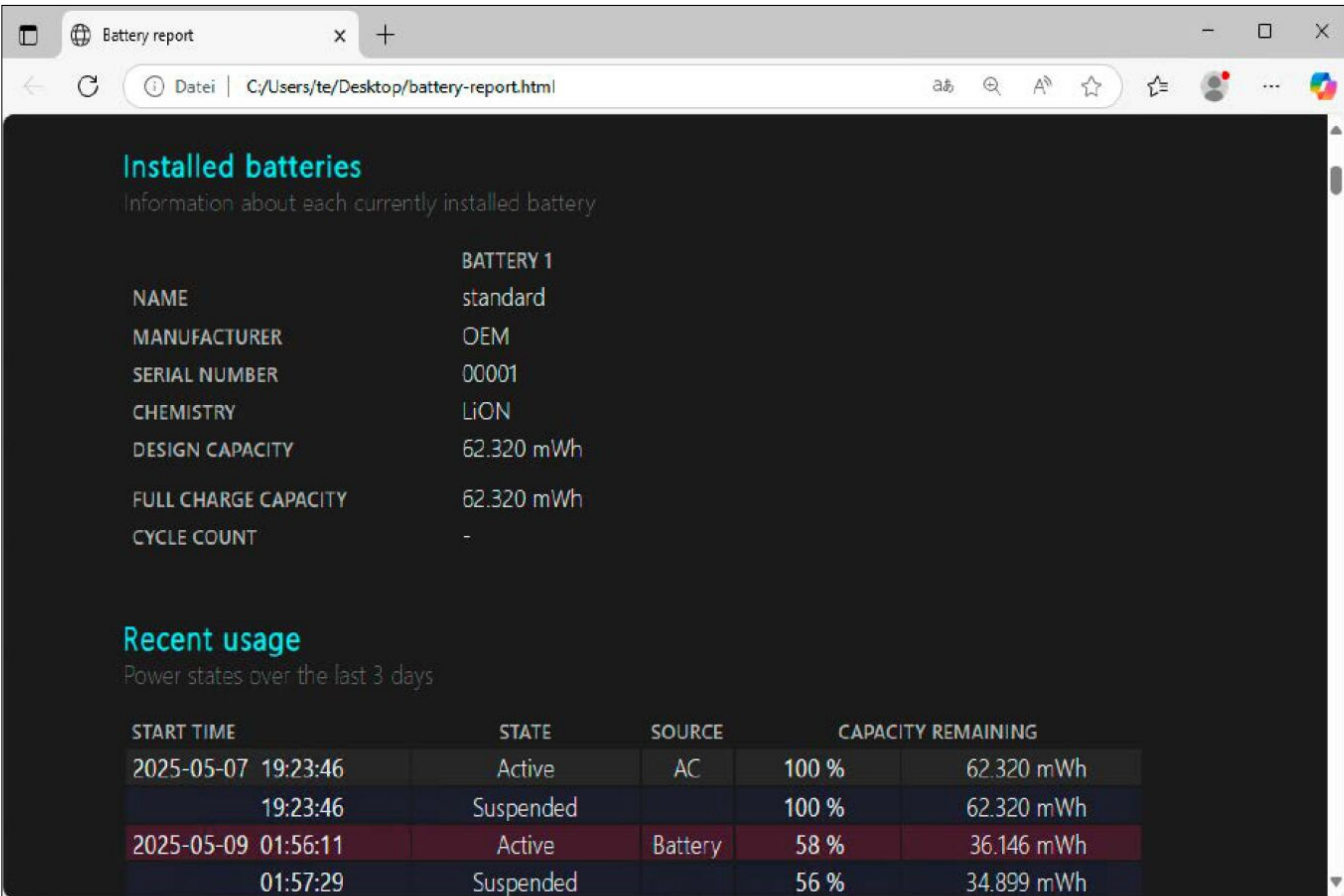
[Freigabename] = [Ordnerpfad] erstellt man eine neue Freigabe. Dafür sind administrative Rechte erforderlich.

Für die Powershell gibt es vergleichbare Cmdlets. Get-SmbShare zeigt die Freigaben auf dem Rechner an, und mit

Netzwerkkonfiguration:

Get-NetIPConfiguration

zeigt die wichtigsten Daten zum Netzwerkadapter an. Man kann unter anderem die IP-Adressen und DNS-Server ermitteln.



Dieser Notebook-Akku ist in Ordnung: Der „Batteryreport“ von Powercfg erzeugt in der Powershell einen HTML-Bericht, der über den Zustand des Akkus und die Entwicklung der Kapazität informiert.

```
New-SmbShare -Name [Freigabename]
-Path [Ordnerpfad]
erstellen Sie eine neue Freigabe.
```

Berichte zur Energieeffizienz und Akkuleistung

Windows versetzt einzelne Komponenten in den Stromsparmmodus, wenn sie gerade nicht benötigt werden. Wichtig ist diese Funktion vor allem für Notebooks – schließlich ist die Akkukapazität begrenzt. Mit dem Standby-Modus lässt sich bei einer Arbeitspause die Akkulaufzeit ebenfalls verlängern. Allerdings macht nicht jede Hardwarekomponente beim Stromsparen mit, woran meist der Treiber schuld ist.

Mit der Befehlszeile

```
powercfg /energy /output
"$env:USERPROFILE\Desktop\
energy-report.html"
```

in einer administrativen Powershell können Sie einen Energiereport erstellen. Unter

Windows 11 24H2 funktionierte das bei unseren Versuchen erst, nachdem wir den Echtzeitschutz von Defender-Antivirus abgeschaltet hatten. Die erzeugte HTML-Datei öffnen Sie zur weiteren Analyse im Browser. Sollten rot hinterlegte Fehler enthalten sein, sehen Sie beim Hersteller nach, ob Treiberupdates verfügbar sind.

Die Befehlszeile

```
powercfg /batteryreport /output
"$env:USERPROFILE\Desktop\
battery-report.html"
```

erstellt einen Bericht mit umfassenden Informationen zum Akku. Sie sehen Statistiken und Diagramme zur Akkuladung und Entladung. Wenn die Werte hinter „Design Capacity“ und „Full Charge Capacity“ sich stark unterscheiden, wird es wahrscheinlich Zeit für einen neuen Akku. Unter „Battery life estimates“ finden Sie eine Tabelle mit der Entwicklung über einen längeren Zeitraum. ■



© Mit Material von Andrii Symonenko – AdobeStock

Windows-Upgrade: Jede Blockade lösen

Beim Umstieg von Windows 10 auf 11 wie auch beim Aktualisieren über die jährlichen Funktionsupdates hakt es immer wieder. Wir erklären, wie Sie die Blockaden beseitigen und weshalb bereits laufende PC-Hardware den Systemanforderungen plötzlich nicht genügen soll.

VON PETER STELZEL-MORAWIETZ

Im vergangenen Jahr ist der automatische Gratis-Support mit Sicherheitsupdates für Windows 10 nach zehn Jahren ausgelaufen.

„Auch PCs, auf denen sich Windows 11 problemlos installieren ließ und läuft, können am Update auf die nächste Version scheitern.“

fen. Nur wer sich beim Programm für erweiterte Sicherheitsupdates (www.microsoft.com/de-de/windows/extended-security-updates) registriert, erhält kostenlos weitere Updates für Windows 10 – allerdings nur bis Oktober 2026. Nach Angaben von Verbraucherzentrale.de lief diese Version des Betriebssystems Ende 2025 noch auf mehr als 30 Millionen Rechnern. Wer sich nicht gleich neue Hardware zulegen will, muss also auf Windows 11 upgraden. Das ist oft leichter gesagt als getan, denn der Umstieg funktioniert nicht immer ganz einfach und scheitert in vielen Fällen. Die Gründe sind vielfältig und vertrackt und lassen sich nicht in wenigen Sätzen zusammenfassen. Dazu braucht es einen ganzen

Ratgeber, den wir Ihnen hier liefern. Die nötigen Tools, die Ihnen beim Wechsel zu Windows 11 helfen, finden Sie auf der DVD.

Die Systemvoraussetzungen und der Hardware-Check

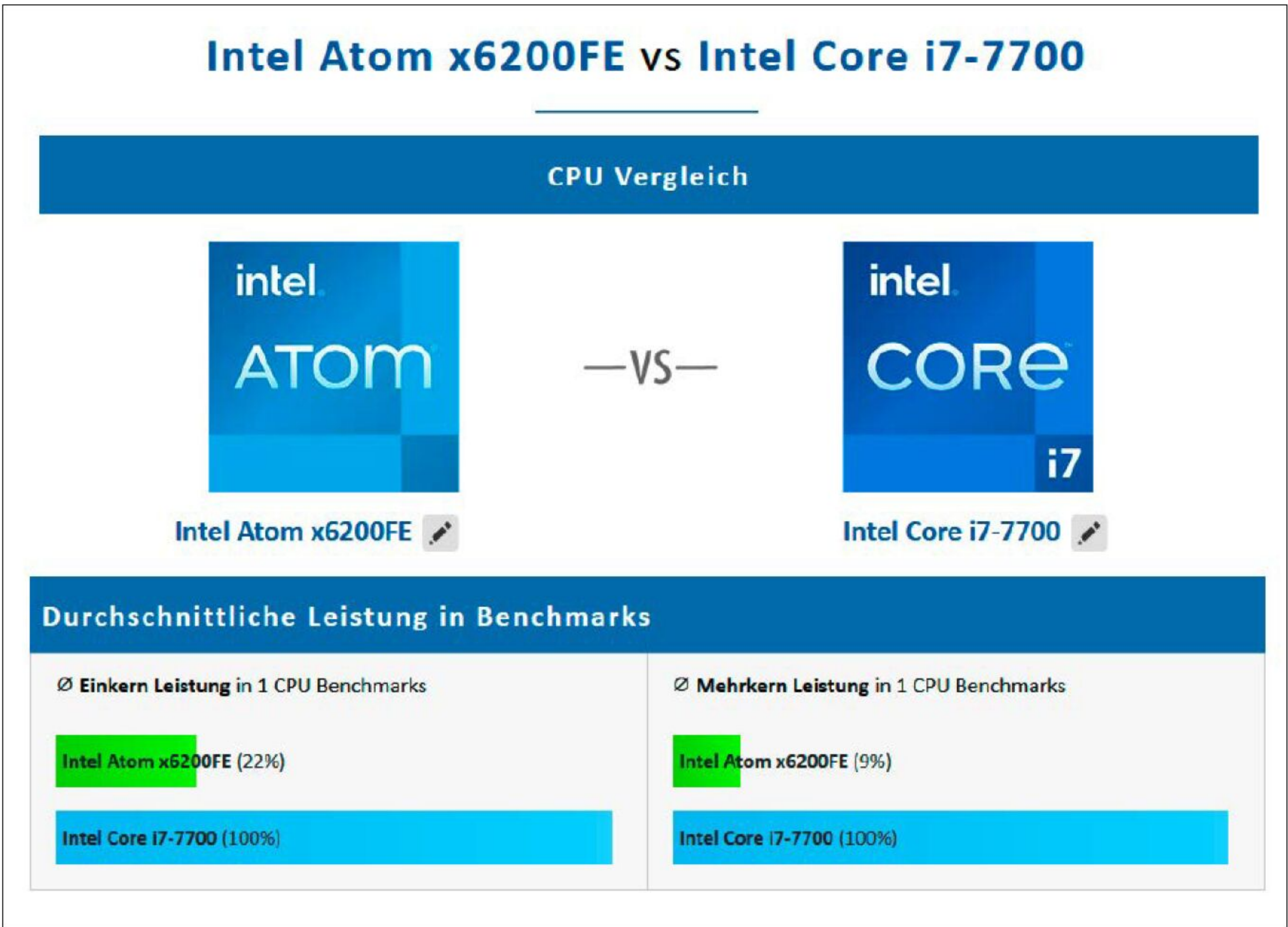
Dass Microsoft die Systemanforderungen für Windows 11 gegenüber der Vorgängerversion erheblich verschärft hat, ist hinlänglich bekannt. So müssen die Rechner im echten Uefi-Modus booten, Secure Boot muss aktiviert sein, das TPM-Sicherheitsmodul auf dem Mainboard in Version 2.0 vorliegen, die Grafikkarte muss DirectX 12 und WDDM-2.0-Treiber unterstützen – und schließlich muss der Prozessor „kompatibel“ sein. Welche CPUs darunterfallen, lis-

tet Microsoft für AMD- und Intel-Modelle separat auf (<https://tinyurl.com/bdfj2bsa>). Man kann nun trefflich darüber streiten, ob die deutlich höheren Hardwareanforderungen von Windows 11 Sinn machen oder nicht – bei den Prozessoren muss man es sogar. Denn die strikte Ausgrenzung beispielsweise von Intels Core-i-Modellen der siebten Generation ist nicht nur willkürlich, sondern geradezu grotesk. So unterstützt Windows 11 neuere, aber ziemlich lahme CPUs wie den Atom x6200FE, während der viel stärkere Core i7-7700 von 2017 außen vor bleibt: Zwischen beiden liegen leistungstechnisch Welten.

Nun gut, so hat es Microsoft eben festgelegt. Doch die Praxis zeigt, dass die offiziellen Anforderungen ohnehin nur bedingt gelten. So bietet Windows 10 das Upgrade auf die aktuelle Version oft genug gar nicht an, obwohl die Hardware alle Systemvoraussetzungen erfüllt und das offizielle Prüftool **PC-Integritätsprüfung** dies ausdrücklich bestätigt: „Dieser PC erfüllt die Anforderungen von Windows 11.“ Will man den Umstieg auf Windows 11 dann per Windows-Update anstoßen, gibt es zwar kein Inkompatibilitätsveto. Der gezeigte Hinweis „Bereiten Sie sich auf Windows 11 vor“ bietet jedoch keinerlei Möglichkeit, den Systemwechsel tatsächlich anzustoßen. Versagt das automatische Upgrade, hängt man erst einmal in einer Falle fest.

So erzwingen Sie den Umstieg auf Windows 11 manuell

Nun bietet Microsoft mit dem **Windows-11-Installationsassistenten** und dem **Media Creation Tool** zwei Optionen, um den Wechsel auf das aktuelle Betriebssystem auch manuell anzustoßen. Beide Tools stellt der Hersteller zum Download zur Ver-



Absurde Systemvoraussetzungen für Windows 11: Der neue, aber lahme Atom-Prozessor (grüner Benchmark-Balken) genügt formal, beim viel stärkeren Core i7-7700 (blauer Balken) verweigert Microsoft das Setup.

fügung (www.microsoft.com/de-de/software-download/windows11). Während sich der Installationsassistent auf das Inplace-Upgrade beschränkt, also auf laufende Windows-10-Systeme, können Sie PCs über das Media Creation Tool auch vom USB-Stick oder der DVD booten und Windows 11 damit frisch aufspielen.

Hier wird es nun ziemlich unübersichtlich. Denn bei der Neuinstallation sind die Systemanforderungen teilweise geringer als beim Inplace-Upgrade: In Szenario eins genügt nämlich ein TPM-Sicherheitschip mit Version 1.2 statt offiziell 2.0. Und beim Prozessor reichen zwei Kerne, während die CPU beim Upgraden laut Microsoft-Liste „kompatibel“ sein muss.

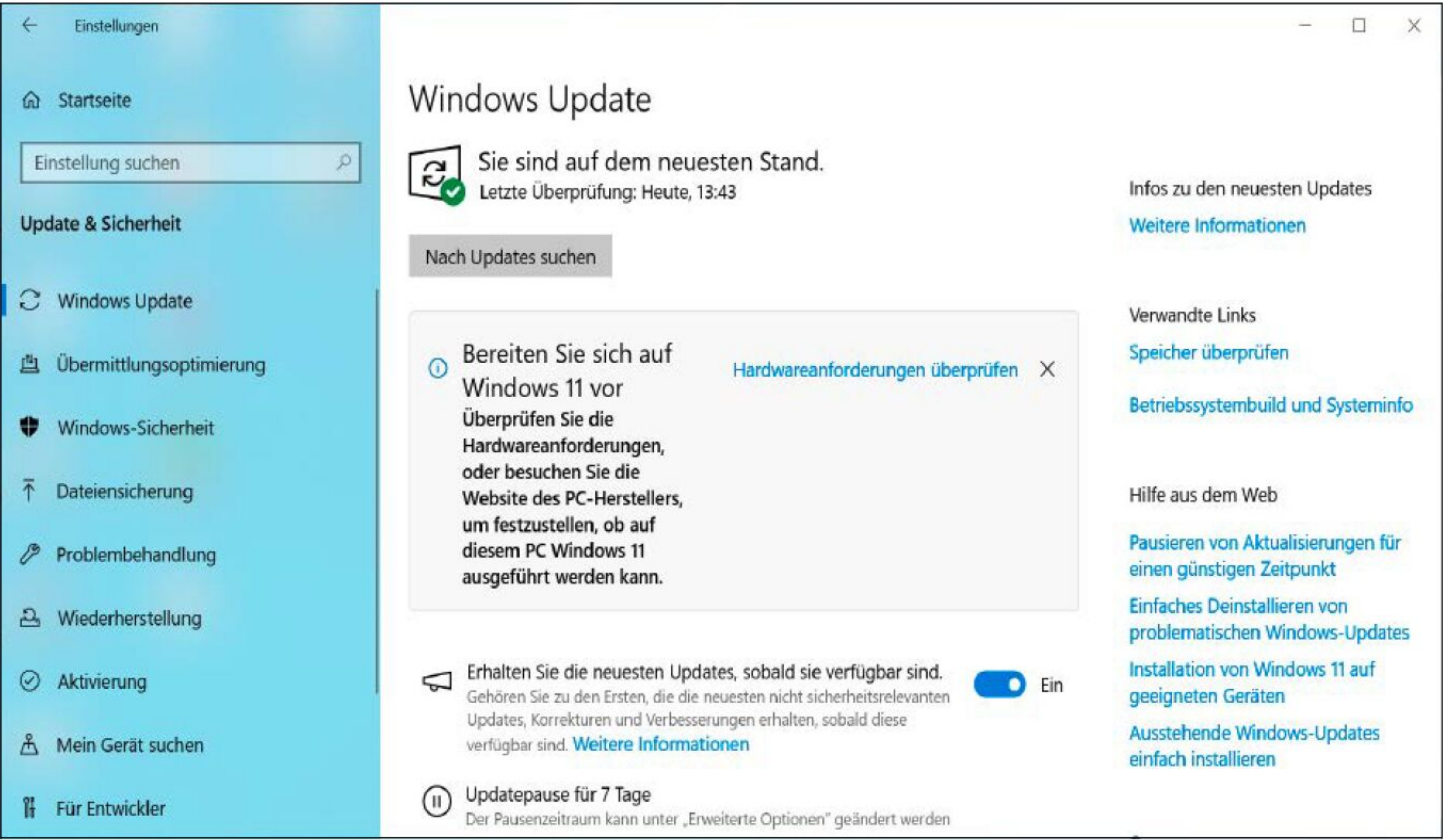
Diese Unterschiede haben zur Folge, dass sich Windows 11 unter Umständen erst

einmal installieren lässt, die anschließenden jährlichen Funktionsupdates später dann aber an den strengeren Hardwarevoraussetzungen scheitern. Da jede einzelne Windows-Version nur zwei Jahre lang Sicherheitsupdates erhält, laufen Sie also nach einiger Zeit gegebenenfalls in eine Updatefalle (siehe Kasten „Die Windows-11-Updatefalle“). So endete der Support für Windows 11 Version 23H2 am 11. November, also nur vier Wochen, nachdem bei Windows 10 endgültig Schluss war.

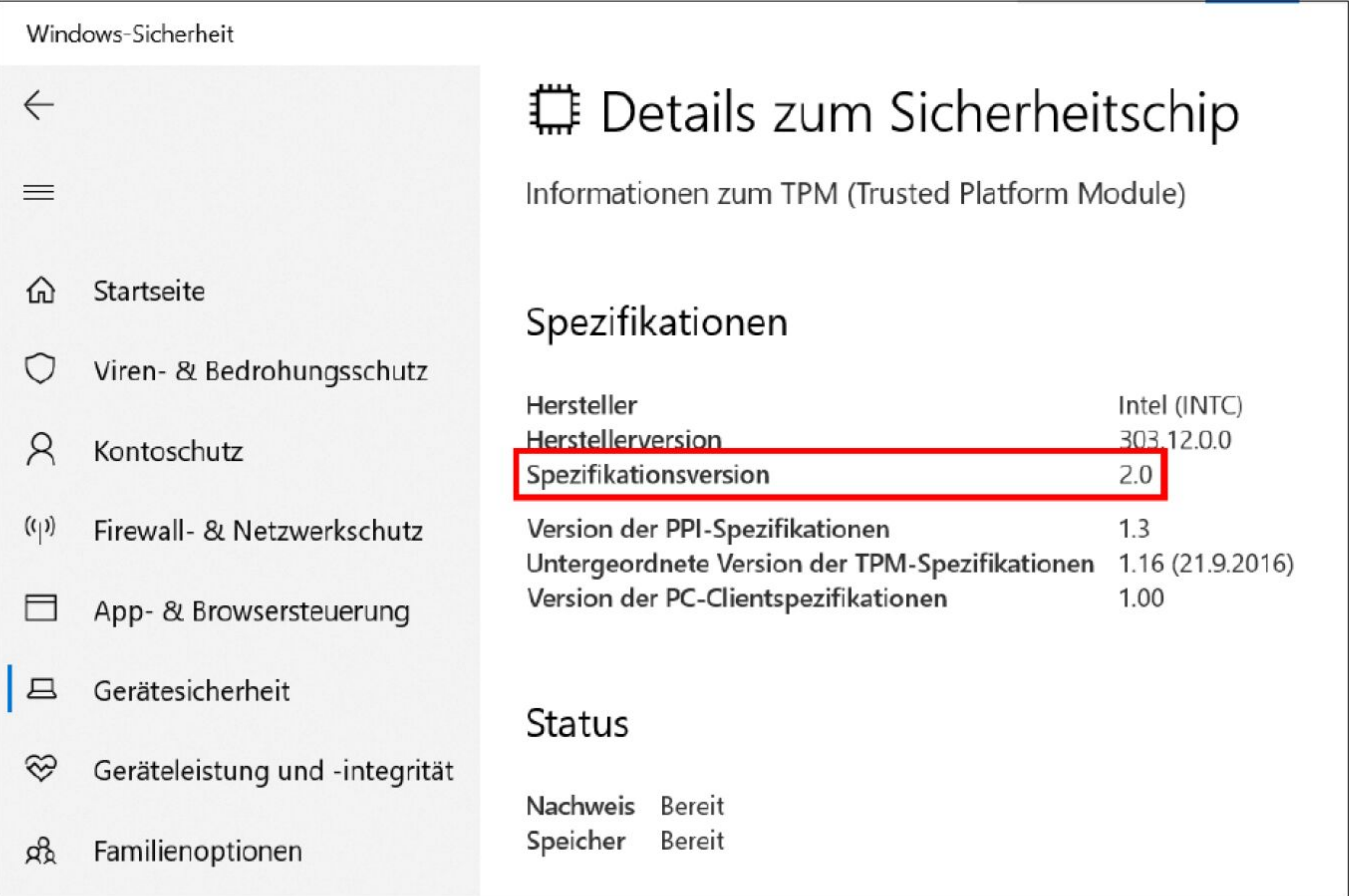
Unser Tipp: Bietet Windows 10 trotz offiziell Windows-11-kompatibler Hardware kein Upgrade an, erzwingen Sie den Umstieg über den Windows-11-Installationsassistenten oder das Media Creation Tool. Die langjährige Erfahrung zeigt, dass das praktisch immer funktioniert.

TOOLS FÜR DAS WINDOWS-UPDATE UND -UPGRADE

Programm	Beschreibung	Auf	Internet	Sprache
Aomei Backupper	Sichert Daten und Festplattenpartitionen	Heft-DVD	www.aomei.de/backup-software	Deutsch
Flyby 11	Umgeht die Systemvoraussetzungen von Windows 11	Heft-DVD	https://github.com/builtbybel	Deutsch
Media Creation Tool für Windows 11	Erstellt Windows-11-Installationsdatenträger	-	https://go.microsoft.com/fwlink/?linkid=2156295	Deutsch
Microsoft Installationsassistent für Windows 11	Startet die Installation und Upgrades von Windows 11	-	https://go.microsoft.com/fwlink/?linkid=2171764	Deutsch
PC-Integritätsprüfung	Prüft die Systemvoraussetzungen von Windows 11	Heft-DVD	https://aka.ms/GetPCHealthCheckApp	Deutsch
PC-WELT-Beitrag: Windows11 auf alten PCs im Dauereinsatz	Ratgeber zur Installation von Windows 11 auf (fast) allen PCs (PDF-Datei)	Heft-DVD	www.pcwelt.de/1199049	Deutsch
Rufus	Umgeht die Systemvoraussetzungen von Windows 11	Heft-DVD	www.rufus.ie	Deutsch
Why Not Win 11	Prüft die Systemvoraussetzungen von Windows 11	Heft-DVD	https://github.com/rcmaehl/WhyNotWin11	Deutsch



Und nun? Dieser Rechner ist zwar uneingeschränkt Windows-11-kompatibel, trotzdem bietet Windows Update keine Möglichkeit zum direkten Upgraden auf das aktuelle Betriebssystem.



Wenn die Installation von Windows 11 nur fehlschlägt, weil der TPM-Sicherheitschip deaktiviert ist, schalten Sie ihn im Uefi ein. Version 2.0 genügt den Hardwarevoraussetzungen.

Windows-Upgrade auch auf nicht kompatibler Hardware ausführen

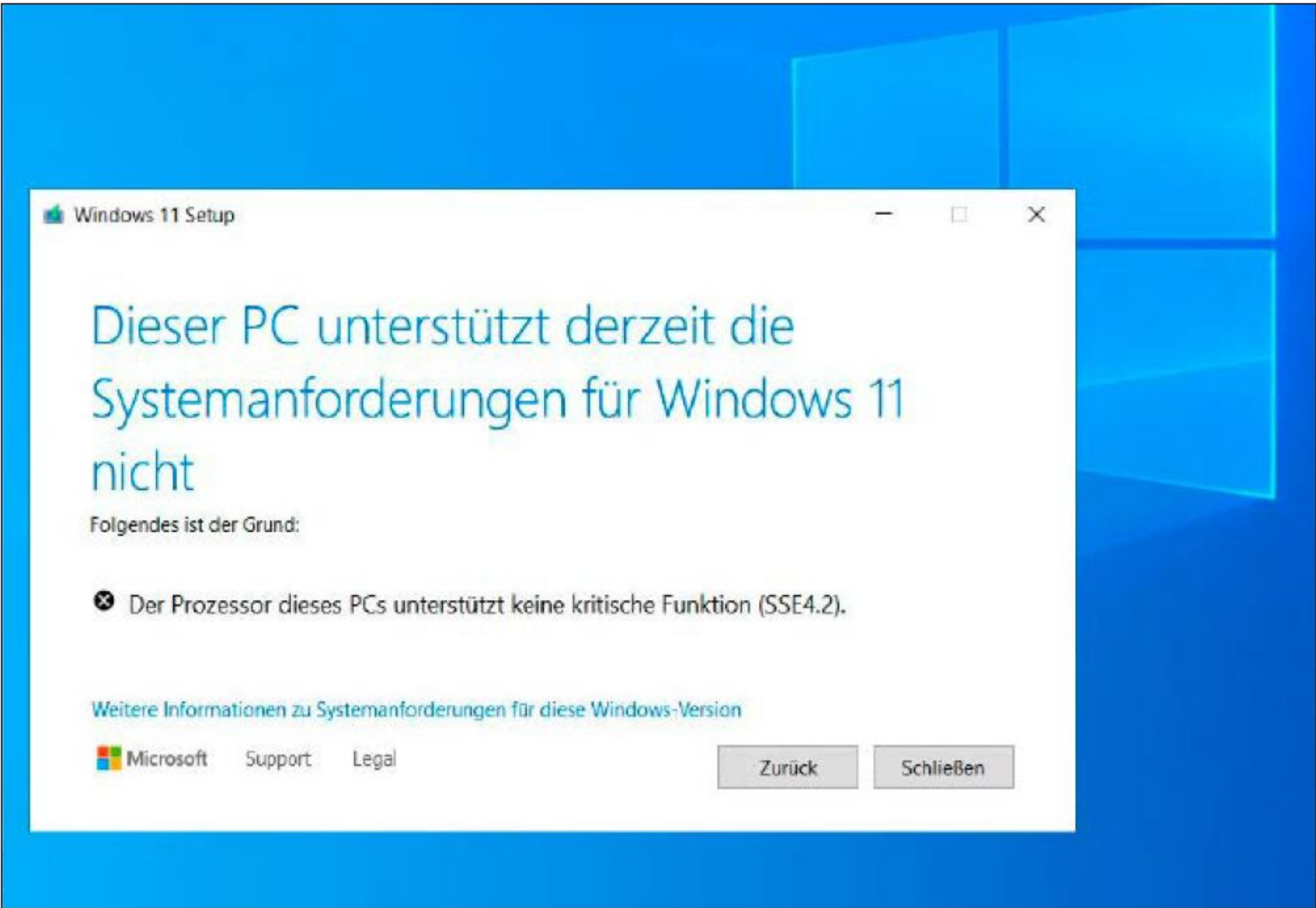
Was aber, wenn der Rechner schon ein paar Jahre alt ist und der Installationsversuch von Windows 11 mit Verweis auf nicht kompatible Hardware abbricht? Wo konkret es im Einzelfall hakt, erfahren Sie über die genannte PC-Integritätsprüfung oder **Why Not Win 11**: Beide Tools zeigen im Detail, woran die Installation gegebenenfalls scheitert. Das ist wichtig für das weitere Vorgehen. Ist nämlich nur der TPM-Sicherheitschip deaktiviert, schalten Sie ihn im Uefi ein. Ob das Modul auf dem Mainboard generell Microsofts Anforderungen entspricht, se-

hen Sie in Windows 10 unter „Einstellungen → Gerätesicherheit → Details zum Sicherheitschip“: Hier muss bei „Spezifikationsversion“ 2.0 stehen. Genauso lässt sich Secure Boot im Uefi einschalten. Versagt das Windows-11-Setup, weil der Rechner statt im echten Uefi- im sogenannten Legacy- oder CSM-Kompatibilitätsmodus läuft, können Sie dies im Uefi ebenfalls umstellen – allerdings nicht ganz so einfach. Denn dazu müssen Sie zuvor den Partitionsstil des Systemdatenträgers von MBR in GPT ändern. Wie das mit dem Windows-Tool MBR2GPT funktioniert, lesen Sie online unter www.pcwelt.de/1191432. Unser

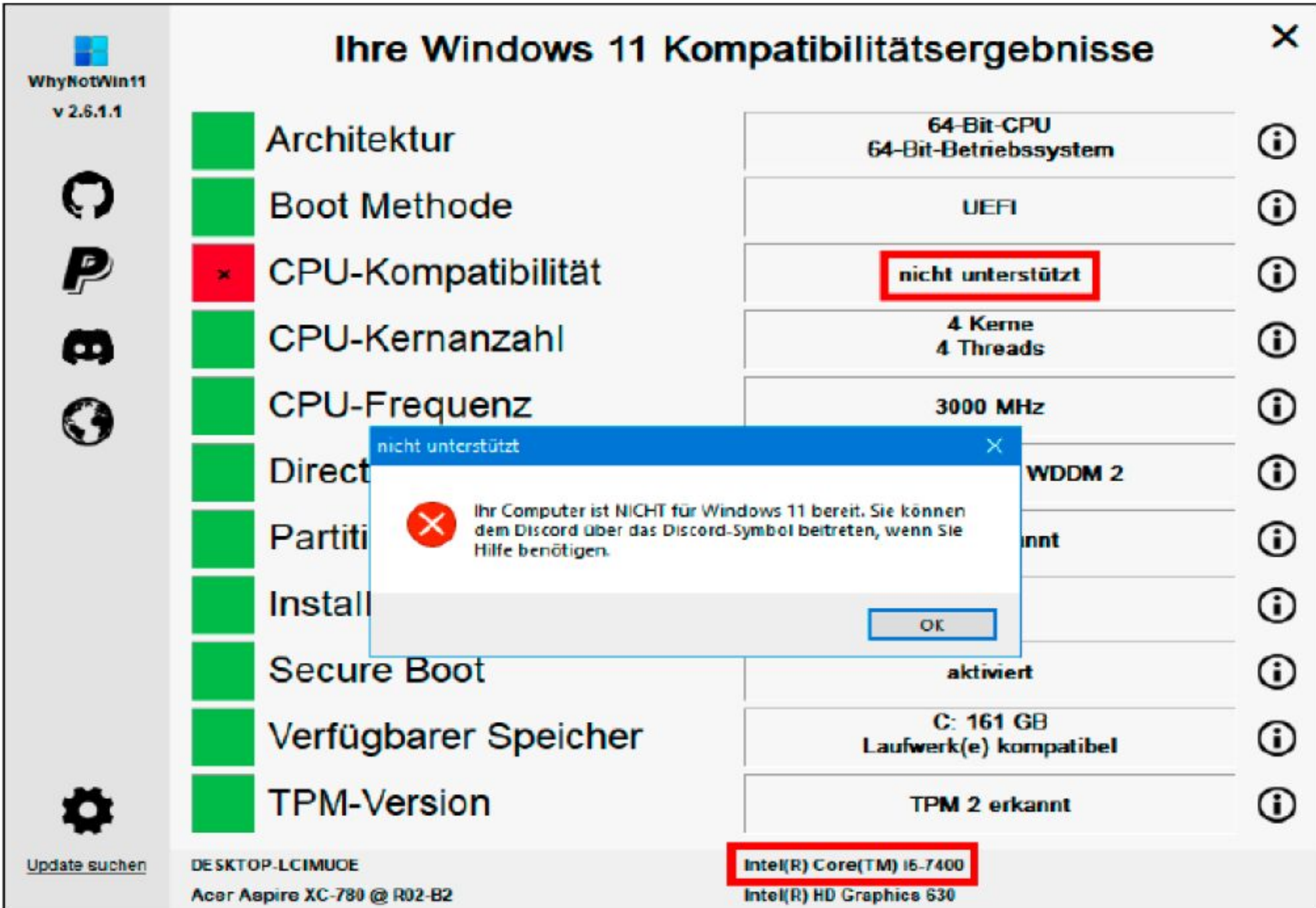
Rat: Weil solche Änderungen an der Festplatte immer ein gewisses Risiko mit sich bringen, erstellen Sie vorher auf einem externen Datenträger ein Backup der Systempartition sowie aller wichtigen Daten, beispielsweise mit **Aomei Backupper**. Bricht die Installation von Windows 11 wegen einer ungeeigneten CPU ab, können Sie den Prozessor mit Ausnahme weniger AMD-Modelle nicht einfach gegen einen kompatiblen austauschen. In diesem Fall nutzen Sie eines der Tools **Flyby 11** oder **Rufus** zum Umgehen des Hardware-Checks. Auch hier zeigt die langjährige Erfahrung, dass dieser inoffizielle Betrieb kaum Probleme bereitet. Während sich Flyby 11 wie der Installationsassistent von Microsoft nur für das In-place-Upgrade eignet, erstellt Rufus einen bootfähigen USB-Installationsstick, von dem das Betriebssystem auch neu installiert werden kann. Und zwar auf fast allen offiziell nicht kompatiblen Computern mit 64-Bit-Prozessor aus den vergangenen zehn Jahren. Ausgenommen sind etwa bei der Windows-11-Version 24H2 nur solche CPUs, die die Befehlssatzerweiterung SSE4.2 nicht unterstützen. Eine ausführliche Anleitung für die Installation mit Rufus lesen Sie im Ratgeber „**Windows 11 auf alten PCs im Dauereinsatz**“ auf DVD.

Wenn die Funktionsupdates an den Systemvoraussetzungen scheitern

Hat man Windows 11 einmal aufgespielt, bedeutet das jedoch nicht, dass dies auch für die folgenden Funktionsupdates jeweils im Herbst gilt. Wird die neue Betriebssystemversion nicht über das Windows-Update angeboten, kann dies unter anderem an inkompatiblen Treibern oder Programmen liegen. Unter Umständen schlägt das Versionsupgrade jedoch auch fehl, weil die identische Hardware an den genannten höheren Systemanforderungen beim späteren Upgraden scheitert. Auch hier ist es im Detail vertrackt: Microsoft bezeichnet die jährlich neuen Windows-11-Versionen (23H2, 24H2, 25H2 und so weiter) stets als Funktionsupdates. Doch längst nicht alle dieser „Updates“ sind einfache Updates, bei denen das System über sogenannte Enablement Packages nur einige Dateien austauscht und dabei die Versionsbezeichnung ändert. Die übrigen dieser „Updates“ – so auch der Wechsel von Version 23H2 auf 24H2 im



Flyby11 oder Rufus modifizieren das Installationsmedium so, dass Windows 11 auch auf den meisten älteren PCs läuft. Ausgenommen sind Systeme mit CPUs ohne die Befehlssatzunterstützung SSE 4.2.



Intel-Core-i-CPU's 7xxx erfüllen die offiziellen Systemanforderungen nicht. Trotzdem lässt sich Windows 11 darauf problemlos neu installieren, spätere Funktionsupdates dagegen nicht mehr.

Herbst 2024 – sind dagegen echte Upgrades. Dabei wird die neue Windows-Version komplett neu installiert und ein „Windows.old“-Ordner zum Wiederherstellen der Vorgängerversion erstellt. Weil das System bei diesem Installationsprozess die Hardwarevoraussetzungen von Windows 11

erneut prüft, kann der Check negativ ausfallen – schließlich gelten beim Upgrade ja strengere Hürden. Ziemlich verrückt! So ärgerlich das ist, immerhin können Sie Ihr bereits laufendes Windows 11 wieder mit Flyby 11 oder Rufus ohne großen Aufwand auch auf nicht kompatiblen PCs auf

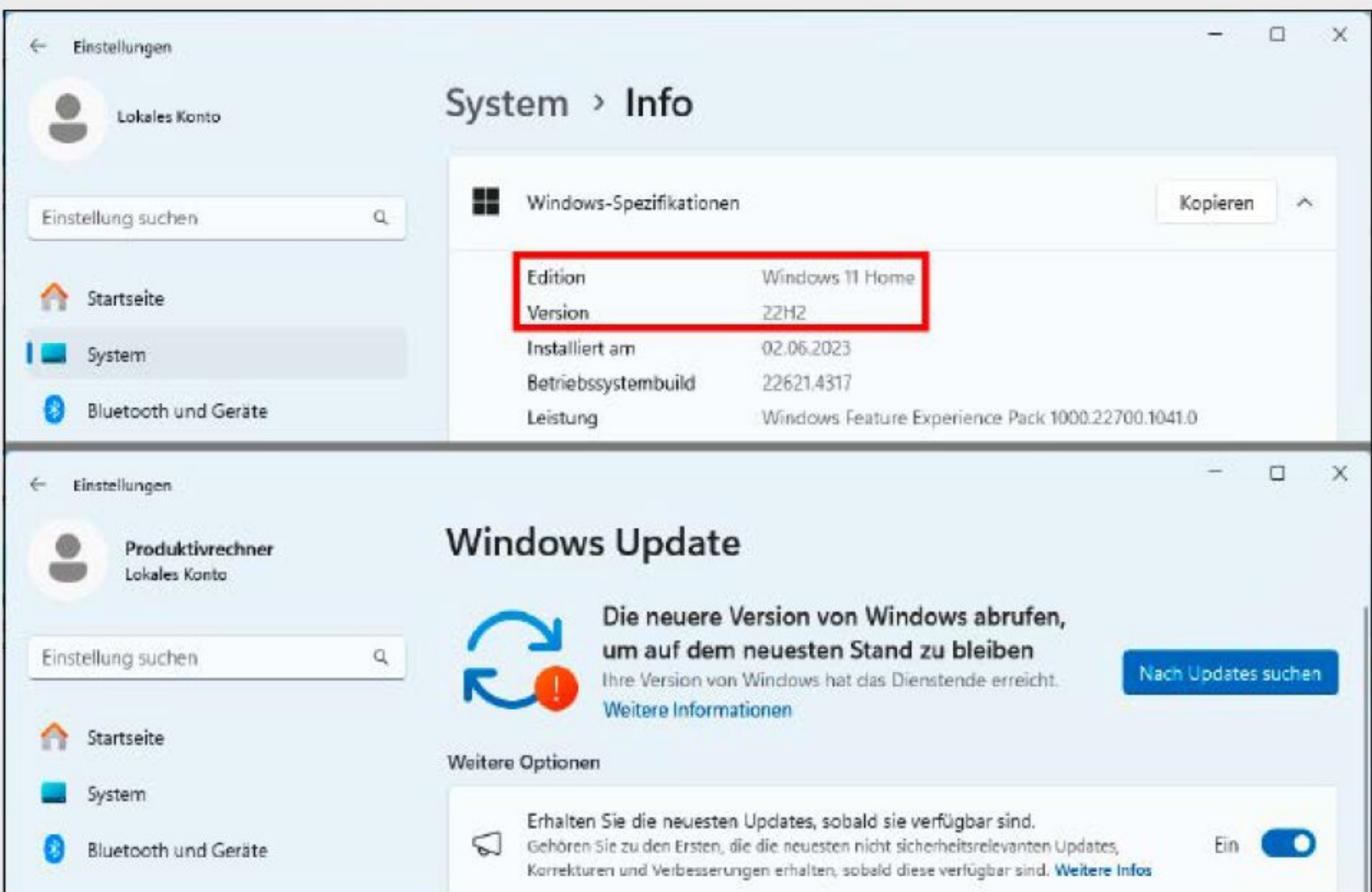
neue Versionen updaten – Entschuldigung, korrekt natürlich: upgraden. Eine gute Nachricht zum Schluss: Beim Umstieg auf 25H2 können Sie sich den zusätzlichen Aufwand sparen, denn bei dieser Version handelt es sich um ein schnelles Enablement Package ohne erneuten Hardware-Check. ■

DIE WINDOWS-11-UPDATEFALLE



Ähnlich wie beim Wechsel von Windows 10 auf 11 kann es auch bei den jährlichen Funktionsupdates von Windows 11 jeweils im Herbst haken. Das ist nicht nur ärgerlich, weil dann die neuen Funktionen fehlen, es birgt auch versteckte Sicherheitsrisiken. Und zwar deshalb, weil das Windows-Update die Anwender mit der Statusmeldung „Sie sind auf dem neuesten Stand“ lange in vermeintlicher Sicherheit wiegt. Jedes große Funktionsupdate klassifiziert Microsoft als neue Windows-Version, die stets nur zwei Jahre Sicherheitsupdates erhält (Home- und Pro-Editionen). Weil Windows die genaue Versionsbezeichnung erst über „Einstellungen → System → Info“ unter den „Windows-Spezifikationen“ preisgibt, bekommen betroffene Nutzer das unter Umständen so lange gar nicht mit, bis das Windows-Update mit einem roten Ausrufezeichen ausdrücklich auf das „Dienstende“ der installierten Version hinweist. Läuft Ihr Rechner derzeit noch mit Windows 11 Version 23H2, endete der System-Support schon im vergangenen Jahr: Seit dem 11. November 2025 gibt es für die Version keine Updates mehr. Die Support-Zeiträume sämtlicher Windows-11-Releases veröffentlicht Microsoft auf seiner Lifecycle-Seite (<https://tinyurl.com/333rje5t>). Sehen Sie also bitte in der Einstellungen-App von Windows 11 nach, ob bei Ihnen bereits die aktuelle Version läuft. Ein Funktionsupdate wie das von Version 23H2 auf 24H2 stoßen Sie genauso an wie den Umstieg von Windows 10 auf 11, nämlich mithilfe des Windows-11-Installationsassistenten

oder des Media Creation Tools von Microsoft (siehe Tools). Mancher PC-Besitzer dürfte bei der Versionsaktualisierung unangenehm überrascht werden, wenn das Update wegen fehlender Systemvoraussetzungen plötzlich fehlschlägt. Wohlgemerkt auf der identischen Hardware, auf der sich Windows 11 zuvor problemlos installieren ließ und läuft. Wie Sie blockierte Funktionsupdates trotzdem aufspielen, lesen Sie ebenfalls in diesem Ratgeber.



Windows Update warnt erst, wenn der Support der installierten Windows-11-Version (hier 22H2) bereits abgelaufen ist. Neue Funktionen fehlen aber schon lange vorher.



© Mit Material von Microsoft

Windows ungebremst

Wenn der PC lahmt, kann das viele Ursachen haben. Meist sind es einfach zu viele Startprozesse, die die Ressourcen mehr als ausschöpfen. Es gibt jedoch einige Mittel, mit denen Sie den Windows-Start wieder beschleunigen.

VON THORSTEN EGGELING

Auf einem neuen PC startet Windows schnell und läuft flüssig. Das ändert sich meist nach einiger Zeit, und Windows scheint immer langsamer zu werden. Dieser Eindruck ist teilweise subjektiv. Im Vergleich zum vorherigen Gerät, das mit weniger leistungsfähiger Hardware ausgestattet war, kann der Performance-Schub immens sein. Nach einiger Zeit gewöhnt man sich an die Geschwindigkeit, und alles scheint langsamer zu laufen.

Windows kann jedoch auch objektiv langsamer werden. Um das zu prüfen, sollte

man gelegentlich die Windows-Startzeiten messen. Wenn sich dabei Auffälligkeiten zeigen, sind genauere Untersuchungen erforderlich. Die Tools auf der Heft-DVD können dabei helfen.

Am schnellsten ist Windows einsatzbereit, wenn Sie das System gar nicht erst herunterfahren. Das System ist bereits standardmäßig für einen schnellen Start konfiguriert, bei dem der vorherige Zustand teilweise wiederhergestellt wird. Die Nebenwirkungen und Alternativen erläutert der Artikel.

1. Windows-Startzeiten mit Bordmitteln kontrollieren

Bevor Sie Windows optimieren, sollten Sie den aktuellen Zustand ermitteln. Sie können dann später feststellen, ob eine Maßnahme tatsächlich erfolgreich war.

Windows protokolliert selbst, wie lange der Systemstart und das Herunterfahren dauern. Diese Informationen finden Sie, indem Sie über einen rechten Mausklick auf das Icon des Startmenüs „Ereignisanzeige“ aufrufen. Gehen Sie im linken Be-

reich des Fensters auf „Anwendungs- und Dienstprotokolle → Microsoft → Windows → Diagnostics-Performance → Betriebsbereit“. Sortieren Sie die Liste per Klick auf den Spaltenkopf „Datum und Uhrzeit“. Die Ereignis-ID 100 bezieht sich auf Startvorgänge, 200 auf das Herunterfahren. Klicken Sie eine der Meldungen mit der ID 100 an und gehen Sie im unteren Bereich auf die Registerkarte „Details“. Hinter „Main Path Boot Time“ steht die Zeit, die Windows für den Start benötigt hat. Zusammen mit der Zeit, die Dienste und Autostart-Anwendungen benötigt haben („Boot Post Boot Time“), ergibt sich der Gesamtwert hinter „BootTime“. Für die Ereignis-ID 200 notieren Sie sich den Wert hinter „ShutdownTime“. Alle Zeitangaben sind in Millisekunden.

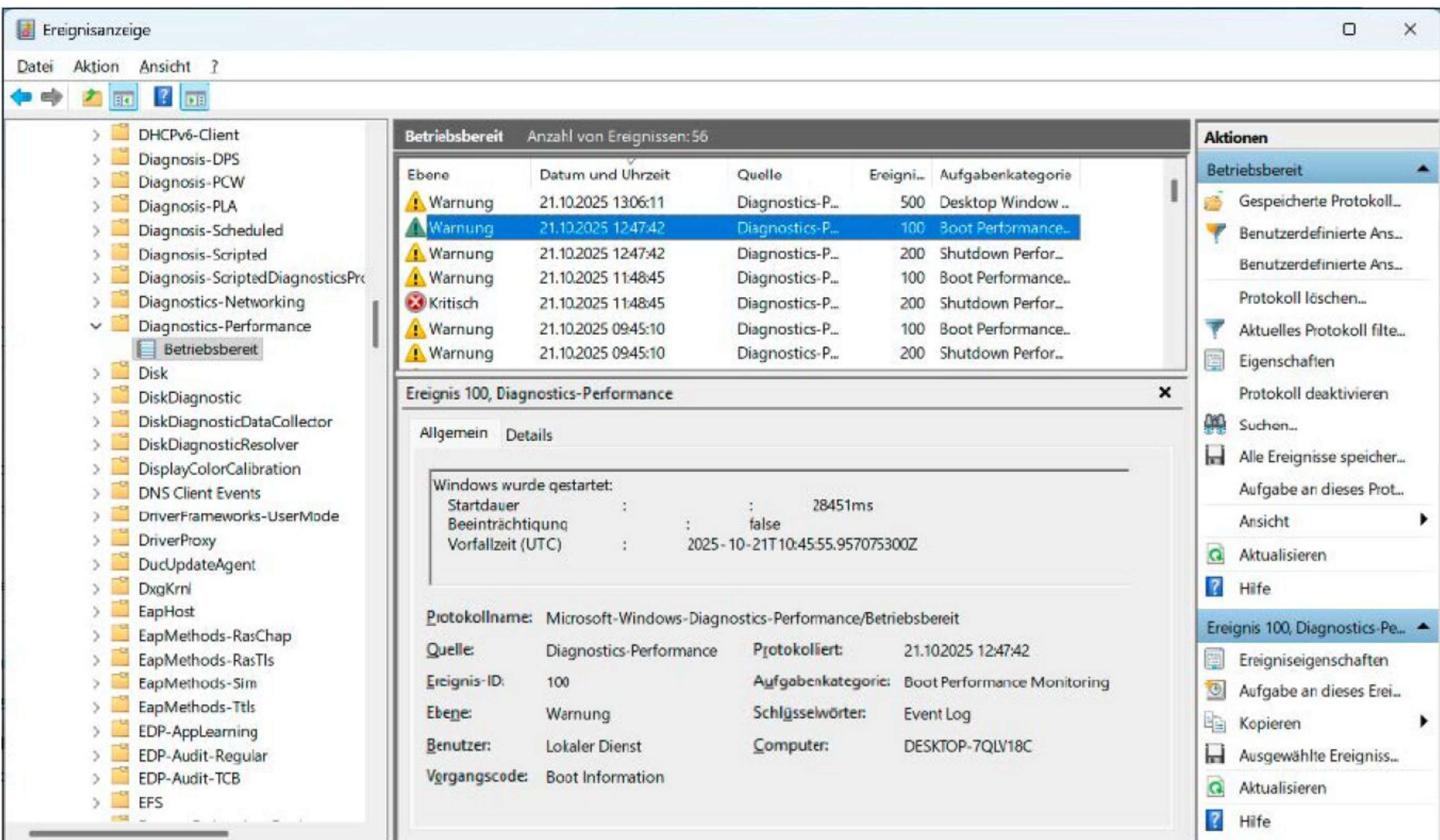
Die IDs von 101 bis 199 geben Hinweise zu Diensten oder Programmen, die eine Verlangsamung verursacht haben. Der Klick auf eine Meldung zeigt unter „Allgemein“ eine kurze Beschreibung des Problems sowie den Namen der betroffenen Software.

„Finden Sie heraus, welche Programme den Windows-Start bremsen, und verhindern Sie deren Autostart.“

Probleme beim Herunterfahren vermerkt Windows mit IDs von 201 bis 299. Im Ereignisprotokoll zeichnet Windows nur Ereignisse auf, die außerhalb der Norm liegen, also länger als gewöhnlich dauern. Alle Einträge sind als „Warnung“ oder „Fehler“ gekennzeichnet, die hohe Anzahl ist erwartbar und unbedenklich. Denn Windows startet nicht immer mit den gleichen Abläufen. Manchmal muss zuerst ein Update verarbeitet werden, oder der Virenschanner benötigt für Prüfungen etwas mehr Zeit. Handlungsbedarf kann bestehen, wenn ein Programm, das nicht von Microsoft stammt, häufiger den Windows-Start bremst. Sie sollten der Sache dann nachgehen und im Internet nach Benutzern mit ähnlichen Erfahrungen suchen. Auch das Support-Forum des Softwareherstellers ist eine gute Anlaufstelle. Vielleicht ist ein Update verfügbar, welches das Problem behebt.

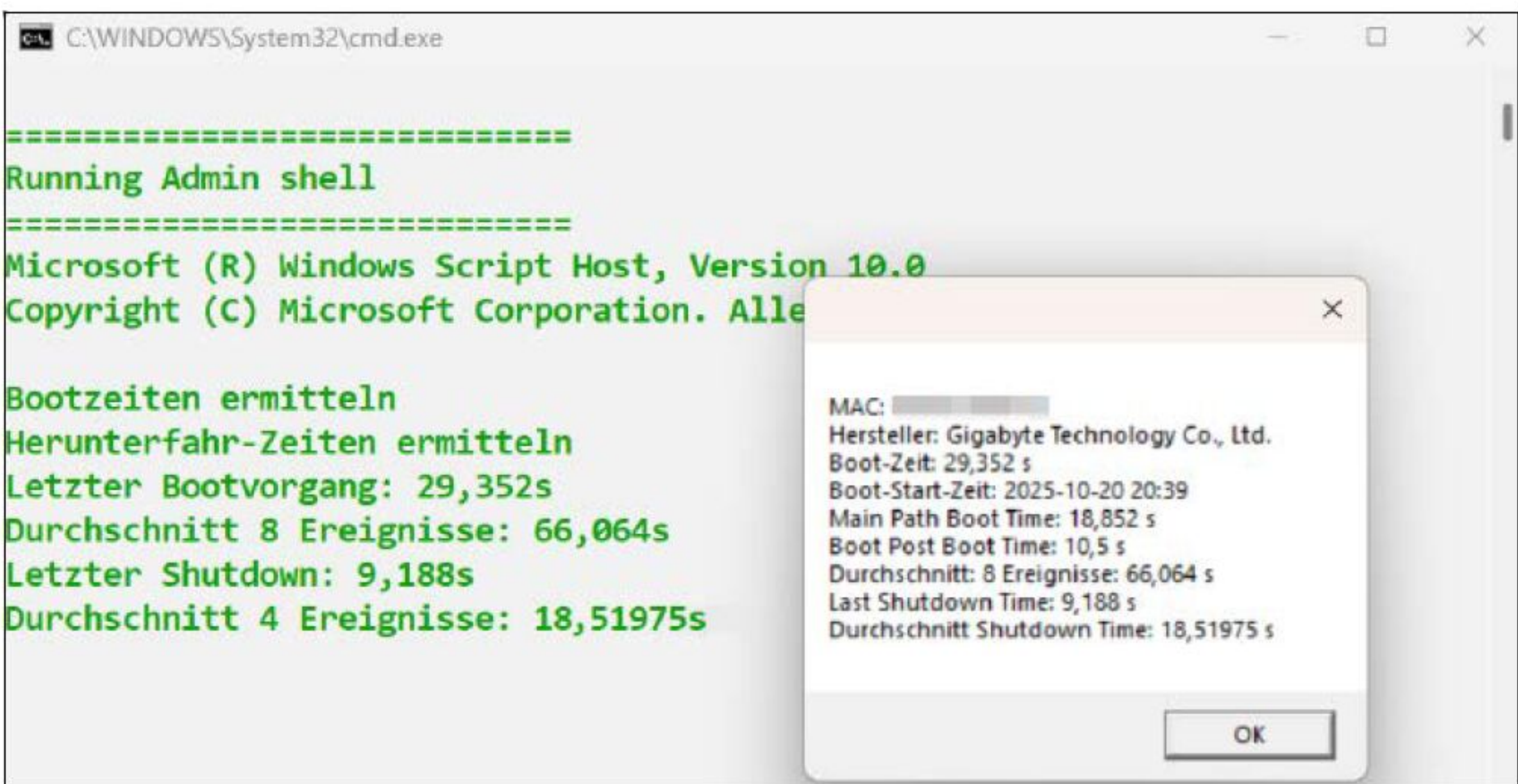
2. Durchschnittswerte aus dem Ereignisprotokoll ermitteln

Die Anzeige der Diagnosedaten in der Ereignisanzeige ist nicht besonders übersichtlich. Neben Stichproben hat eine Zusammenfassung über einen längeren Zeitraum mehr Aussagekraft. Unser Script **PC-WELT Performance** zeigt die letzten Werte für Start und Herunterfahren an und Durchschnittswerte der letzten 20 Ereignisse. Entpacken Sie das ZIP-Archiv in ein beliebiges Verzeichnis und starten Sie *RunAsAdmin.cmd*. Die Anfrage der Benutzerkontensteuerung beantworten Sie mit „Ja“. Sollte der Wert von „Main Path Boot Time“ regelmäßig ungewöhnlich hoch sein (mehr als 20 bis 30 Sekunden), liegt die Ursache möglicherweise bei einem Treiber oder Defekten auf der Festplatte. Wird für „Boot Post Boot Time“ eine Zeit von mehr als 30 bis 40 Sekunden angezeigt, ist das Problem eher bei Programmen zu suchen, die Windows automatisch startet (siehe Punkt 5).



Protokolle für Starten und Herunterfahren: Das Ereignisprotokoll vermerkt nur Zeiten, die Windows als ungewöhnlich ansieht. Sie können ermitteln, was die Verzögerung verursacht hat.

Statistiken des Zeitbedarfs: Das Script **PC-WELT Performance** zeigt, wie lange der letzte Start und das Herunterfahren gedauert haben. Die Werte werden für eine spätere Auswertung gespeichert.



PC-WELT Performance erstellt die Datei *BootLog.csv*, mit den Zeiten maximal der letzten 20 Starts. In *Lastlog.csv* werden bei jedem Scriptlauf jeweils die letzte Startzeit sowie das Datum hinzugefügt. Die CSV-Dateien lassen sich in einer Tabellenkalkulation öffnen. Sie können dann eine Statistik der Windows-Starts erstellen und Änderungen über einen längeren Zeitraum nachvollziehen. Ergibt sich eine Verlangsamung ab einem bestimmten Zeitpunkt, sehen Sie in der Einstellungen-App unter „Apps → Installierte Apps“ nach, was Sie

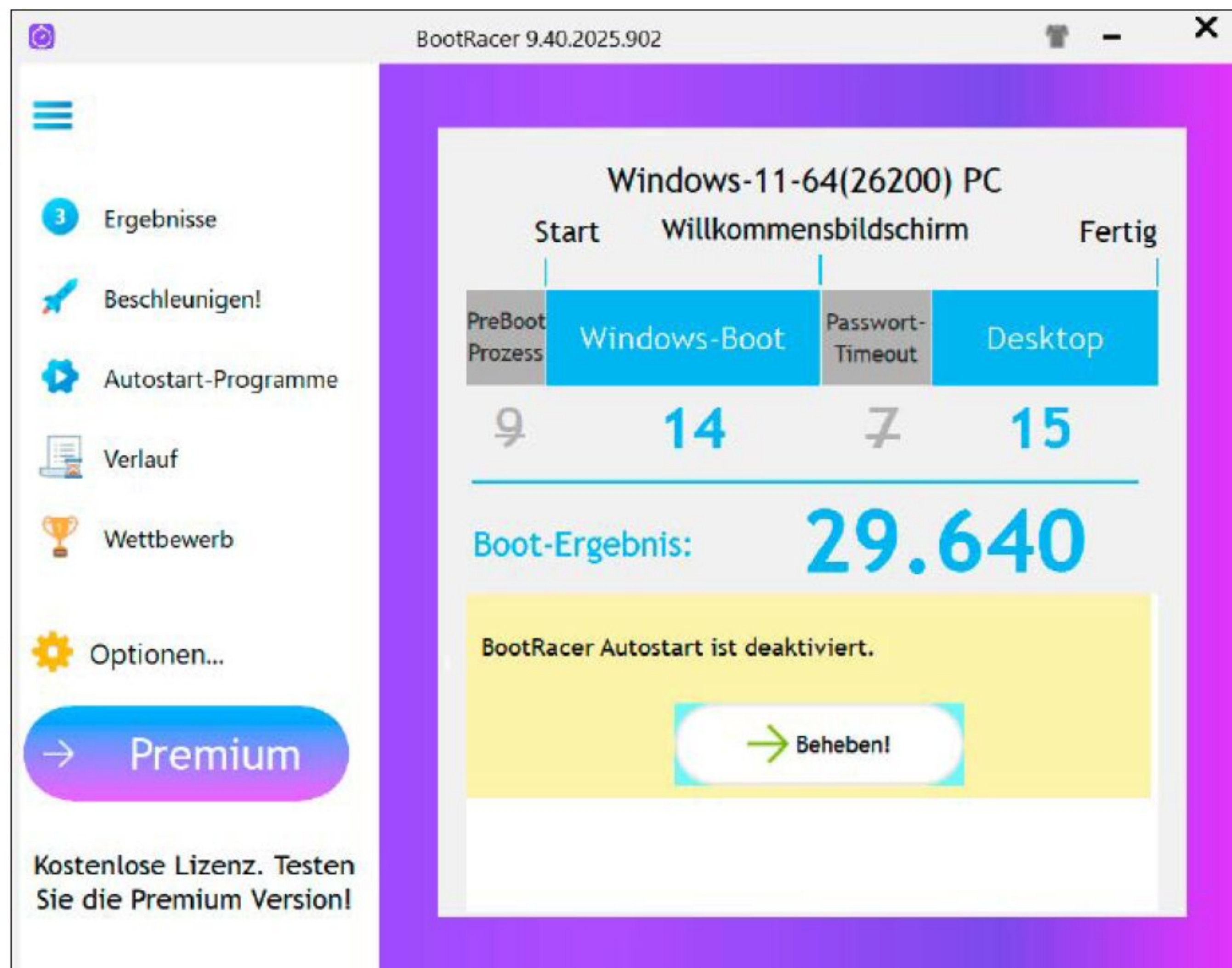
kurz zuvor installiert haben. Für die Verzögerungen können Autostart-Einträge, aber auch Dienste verantwortlich sein, die im Hintergrund starten (siehe Punkt 5).

3. Startzeiten mit Bootracer messen und optimieren

Das Tool **Bootracer** zeigt die Windows-Startzeiten übersichtlich an und ermittelt Verzögerungen durch Autostart-Programme. Bevor Sie Bootracer verwenden, speichern Sie geöffnete Dateien und beenden alle Programme. Wenn Sie das Tool das

IM ÜBERBLICK: TOOLS FÜR EIN SCHNELLERES WINDOWS

Name	Beschreibung	Auf	Internet	Sprache
AS SSD Benchmark	Benchmark-Tool	Heft-DVD	https://m6u.de/ASBEN	Deutsch
Autoruns	Autostart-Programme deaktivieren	Heft-DVD	https://tinyurl.com/SIAUTOR	Englisch
Bootracer	Startzeit messen und Autostarts verwalten	Heft-DVD	https://gratis.com/bootracer	Englisch
Hasleo Backup Suite Free	Backup und Klonen	Heft-DVD	www.easyuefi.com	Deutsch
PC-WELT Performance	Windows-Startzeiten ermitteln	Heft-DVD	www.pcwelt.de/1158391	Deutsch
Process Monitor	Dateizugriffe beim Booten protokollieren	Heft-DVD	https://tinyurl.com/32ju6amu	Englisch
Windows Assessment and Deployment Kit	Windows-Startzeit messen	Heft-DVD	https://tinyurl.com/WADKD	Englisch



Bootracer: Das Tool zeigt den Zeitbedarf der einzelnen Phasen des Windows-Starts an. Ein hoher Wert bei „Desktop“ deutet auf Autostart-Programme hin, die den Start verlangsamen.

Starten Sie Windows über das Startmenü und „Ein/Aus → Neu starten“ mehrfach neu, um aussagekräftige Messwerte zu erhalten. Verwenden Sie danach „Ein/Aus → Herunterfahren“ und schalten Sie den Computer wieder ein. Bei aktiviertem Schnellstart (siehe Punkt 7) sollte sich gegenüber „Neu starten“ eine deutliche Differenz ergeben. Einen weiteren Test führen Sie per Klicks auf „Test ohne Autostart-Programm (Clear Boot Test) → Test starten → Ja“ im Bootracer-Hauptfenster durch. Der Windows-Start bis zum Desktop erfolgt jetzt ohne Autostart-Programme. Diese werden – eins nach dem anderen – erst danach von Bootracer gestartet. Das alleine kann die Startzeit schon um ein paar Sekunden reduzieren. Klicken Sie im Hauptfenster auf „Ergebnisse“. Bootracer zeigt Ihnen die Werte für „Gesamte Startdauer“ und „Startdauer (ohne Autostart, clean)“ sowie die von Autostart-Programmen benötigte Zeit. Klicken Sie für detaillierte Informationen auf „Ausführungsbremsen finden“. Die Liste enthält die Startzeiten für jedes Programm. Wiederholen Sie auch diesen Test mehrfach. Wenn ein Programm beispielsweise nach

erste Mal ausführen, klicken Sie einfach auf „Start“ und dann auf die Schaltfläche „Test starten“. Bestätigen Sie den Windows-Neustart mit „Ja“.

Nach der Windows-Anmeldung meldet sich Bootracer automatisch mit einem Countdown, der die Sekunden bis zum vollständigen Start herunterzählt. Nach kurzer Zeit sehen Sie ein Fenster mit der Gesamtstart-

zeit, in das Sie klicken. Im Hauptfenster gibt Bootracer aus, wie lange der Windows-Start gedauert hat („Windows-Boot“) und nach welcher Zeit die Oberfläche einsatzbereit war („Desktop“). Die Angabe unter „Pre-Boot Prozess“ steht für die Zeit, die vor dem Windows-Start vergangen ist, also während der Initialisierungsphase von Bios beziehungsweise Firmware (siehe Punkt 6).

HARDWARE FÜR MEHR LEISTUNG AUFRÜSTEN



Wenn ein Desktop-PC oder Notebook zu langsam ist, kann das nur mit wenigen Maßnahmen geändert werden. Der Umstieg auf einen schnelleren Prozessor lohnt sich kaum – wenn überhaupt möglich. Mehr RAM kann sinnvoll sein, wenn das Gerät nur mit 4 oder 8 GB ausgestattet ist und es häufiger zu Speicherengpässen kommt. Die Investition in mehr als 16 GB Hauptspeicher ist nur empfehlenswert, wenn das Gerät für anspruchsvolle Aufgaben wie Videoschnitt oder Virtualisierungssoftware genutzt wird. Bei einem typischen Heim-PC mit Büroanwendungen bewirkt noch mehr RAM kaum eine Steigerung der Leistung.

Sollte der PC noch mit einer Festplatte ausgestattet sein, ist in jedem Fall der Umstieg auf eine SSD sinnvoll. Eine schnelle SSD, etwa mit 2 TB, kostet zurzeit um die 150 Euro, 4 TB gibt es für ungefähr 250 Euro. Am SATA-Anschluss liefern SSDs um die 500 MB pro Sekunde, Festplatten nur um die 100 MB/s (sequenzieller Zugriff). Entscheidend sind jedoch die kurzen Zugriffszeiten, weil eine SSD die Speicherzellen direkt adressiert, während bei einer Festplatte der Lese- und Schreibkopf zuerst an die gewünschte Position fahren muss. Das wirkt sich vor allem positiv auf die Windows-Bootzeiten aus.

Mit meist mehr als 3000 MB/s sind NVMe-SSDs noch schneller, weil die Anbindung über den PCIe-Bus erfolgt. Für ein Systemlaufwerk ist das die erste Wahl, wenn das Gerät mit einem NVMe-Steckplatz ausgestattet ist.

Beim Umzug auf eine SSD müssen Sie Windows nicht neu installieren. Verwenden Sie ein Programm wie **Hasleo Backup Suite Free**, mit dem Sie die Festplatte auf eine SSD klonen. Mit **AS SSD Benchmark** können Sie die Geschwindigkeit von SSDs und Festplatten prüfen.



SSD statt Festplatte: Spendieren Sie dem PC eine SSD. Damit verkürzen Sie die Windows-Startzeiten im Vergleich zu einer Festplatte deutlich.

Updates sucht, führt dies zu einer deutlichen Verlangsamung des Windows-Starts. Das sollte jedoch nicht bei jedem Start passieren. Wenn doch, liegt vielleicht eine Fehlfunktion der betroffenen Software vor, die sich durch Neuinstallation oder Update beheben lässt. Wie Sie Autostart-Programme deaktivieren, lesen Sie in Punkt 5.

4. Boot- und Startvorgang noch genauer analysieren

Wenn Sie zuvor Bootracer verwendet haben, deaktivieren Sie das Tool. Dazu klicken Sie auf „Optionen“ und dann unter „BootRacer ausführen“ auf „Autostart deaktivieren“. Nach einem Klick auf „Speichern“ beenden Sie Bootracer.

Sysinternals' **Process Monitor** untersucht den Bootvorgang genauer – inklusive der geladenen Treiber. Klicken Sie nach dem Start des Tools in der Symbolleiste auf die „Play“-Schaltfläche, um die Aufzeichnung der Prozessaktivitäten zu stoppen.

Gehen Sie auf „Options → Enable Boot Logging“, bestätigen Sie mit „OK“ und starten Sie Windows neu. Nachdem Windows vollständig hochgefahren ist, starten Sie Process Monitor erneut, bestätigen die Meldung mit „Ja“, wählen einen Ordner und klicken auf „Speichern“.

Die angezeigte Liste ist umfangreich. Process Monitor zeigt alle Datei- und Registry-Zugriffe während des Starts an. Über „Filter → Filter“ reduzieren Sie die Datenmenge. Filtern Sie beispielsweise nach „Path ends with .sys“, um sich nur die Treiber anzeigen zu lassen.

5. Unnötige Autostarts von Programmen abschalten

Grundsätzlich ist kein Autostart-Programm wirklich erforderlich. Viele der Programme zeigen sich als Icon im Infobereich rechts unten neben der Uhr und können dann über Updates informieren oder Benachrichtigungen anzeigen. Ob das nötig ist, hängt von den Funktionen und den persönlichen Vorlieben ab. Wenn sich ein Programm als zu starke Systembremse erweist, sollten Sie den Autostart besser deaktivieren. Über anstehende Updates informieren Programme meist auch beim Start. Unter Windows 10 und 11 verwalten Sie die Autostart-Programme standardmäßig über den Task-Manager, den Sie am schnellsten mit der Tastenkombination Strg-Shift-Esc aufrufen. Um alle Funktionen zu sehen, kli-

Autostart-Kontrolle			
Datum/Zeit der Session: 21.10.2025 01:14:11			
Gesamte Startzeit: 3.078 s			
	SecurityHealth %windir%\system32\SecurityHealthSystray.exe	2.719 s	21.10.2025 01:14:15
	RtkAudioService "C:\WINDOWS\System32\DriverStore\FileRepository\realtek.service.inf_amd64_7b66b6662cf6d72b\RtkAudioService64.exe" -background	0.031 s	21.10.2025 01:14:17
	Everything "C:\Program Files\Everything\Everything.exe" -startup	0.141 s	21.10.2025 01:14:18
	MicrosoftEdgeAutoLaunch_7D3EC61F384E93E2BD7CB77AA1BD38F2 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start	0.187 s	21.10.2025 01:14:19

Autostarts messen: Bootracer informiert darüber, wie lange ein Programm für den automatischen Start benötigt hat. Starke Systembremsen sollten Sie deaktivieren.

Process Monitor - C:\Users\te\Documents\Bootlog.pml

File Edit Event Filter Tools Options Help

Time o...

Process Name

PID

Operation

Path

Result

Detail

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System32\drivers\lmbkmlcr.sys

SUCCESS

Desired Access: R...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System32\drivers\lmbkmlcr.sys

SUCCESS

CreationTime: 01.1...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System32\drivers\lmbkmlcr.sys

SUCCESS

08:03:3...

MpDefenderCoreService.exe

5456

CreateFileMap...

C:\Windows\System32\drivers\lmbkmlcr.sys

SUCCESS

Desired Access: G...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System32\drivers\lmbkmlcr.sys

SUCCESS

Desired Access: G...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

CreateFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

QueryBasicInfo...

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5456

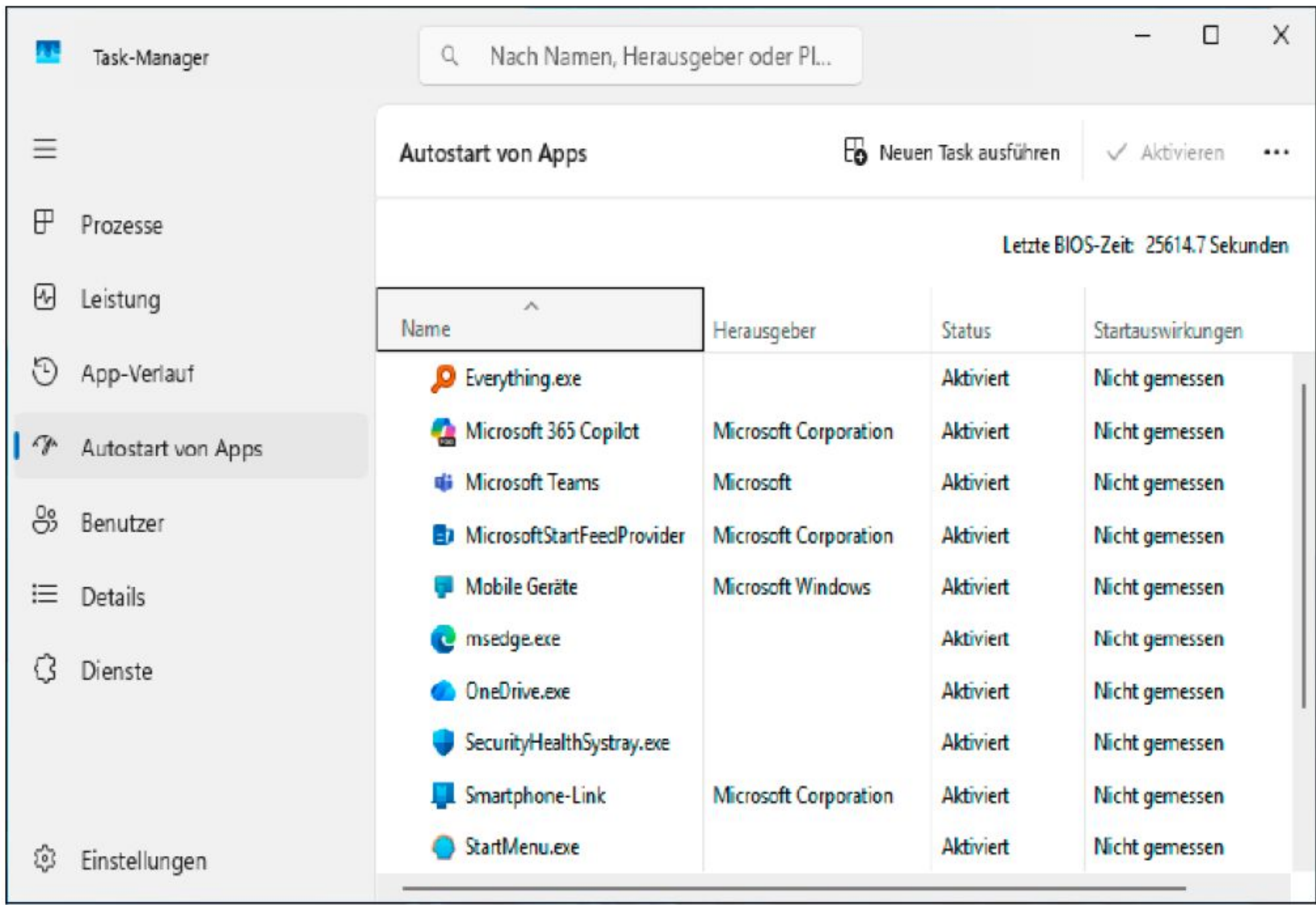
CloseFile

C:\Windows\System...

08:03:3...

MpDefenderCoreService.exe

5



Autostart im Task-Manager: Für die schnelle Kontrolle reicht das Tool aus. Infos zu den „Startauswirkungen“ sind hilfreich, werden aber oft erst nach langer Betriebsdauer angezeigt.

Entry“ gleich entfernen, auch wenn es kaum Zeit kostet, wenn ein Starteintrag ins Leere geht. Bei allen anderen Einträgen, vor allem in den Bereichen „Task Scheduler“ (Aufgabenplanung) und „HKLM\System\CurrentControlSet\Services“, sollten Sie vorsichtig sein und sich erst über die Funktion informieren. Dabei helfen ein rechter Mausklick und der Menüpunkt „Search Online“.

6. Firmware-Einstellungen für den schnelleren Start
Wenn Sie den PC einschalten, initialisiert das Bios beziehungsweise die Firmware die Hardware. Dabei wird auch untersucht, welche USB-Geräte angeschlossen und welche Laufwerke verfügbar sind. Das kann einige Zeit dauern, insbesondere wenn Festplatten erst hochfahren müssen. Sie sollten daher USB-Festplatten vom PC

trennen, wenn diese nicht ständig zur Verfügung stehen müssen. Im Firmware-Setup ist bei PCs meist eine Konfiguration für „Fast Boot“ oder „Quick Boot“ mit mehreren Optionen zu finden. Bei Notebooks kann man „Fast Boot“ oft nur ein- oder ausschalten. Ist die Option aktiviert, erfolgt nur eine minimale Initialisierung der Hardware. Der Rest wird dem Betriebssystem überlassen. Eine Option wie „SATA Support“ (oder ähnlich) mit der Einstellung „Last Boot SATA Devices Only“ reduziert die Zeit für die Suche nach Bootlaufwerken. „USB Support“ steuert die Erkennung von USB-Geräten. Wenn Sie hier „Disable Link“ wählen, wird die USB-Unterstützung vor dem Windows-Start komplett abgeschaltet. „Partial Initial“ deaktiviert nur USB-Speichergeräte, und „Full Initial“ berücksichtigt alle USB-Geräte. Mit „Disable Link“ bootet der PC zwar etwas schneller, eine USB-Tastatur lässt sich vor dem Windows-Start jedoch nicht nutzen. Über die üblichen Tastenkombinationen (Esc, Entf., F2) gelangen Sie dann nicht mehr ins Firmware-Setup. Sie können außerdem kein Rettungssystem von einem USB-Stick booten.

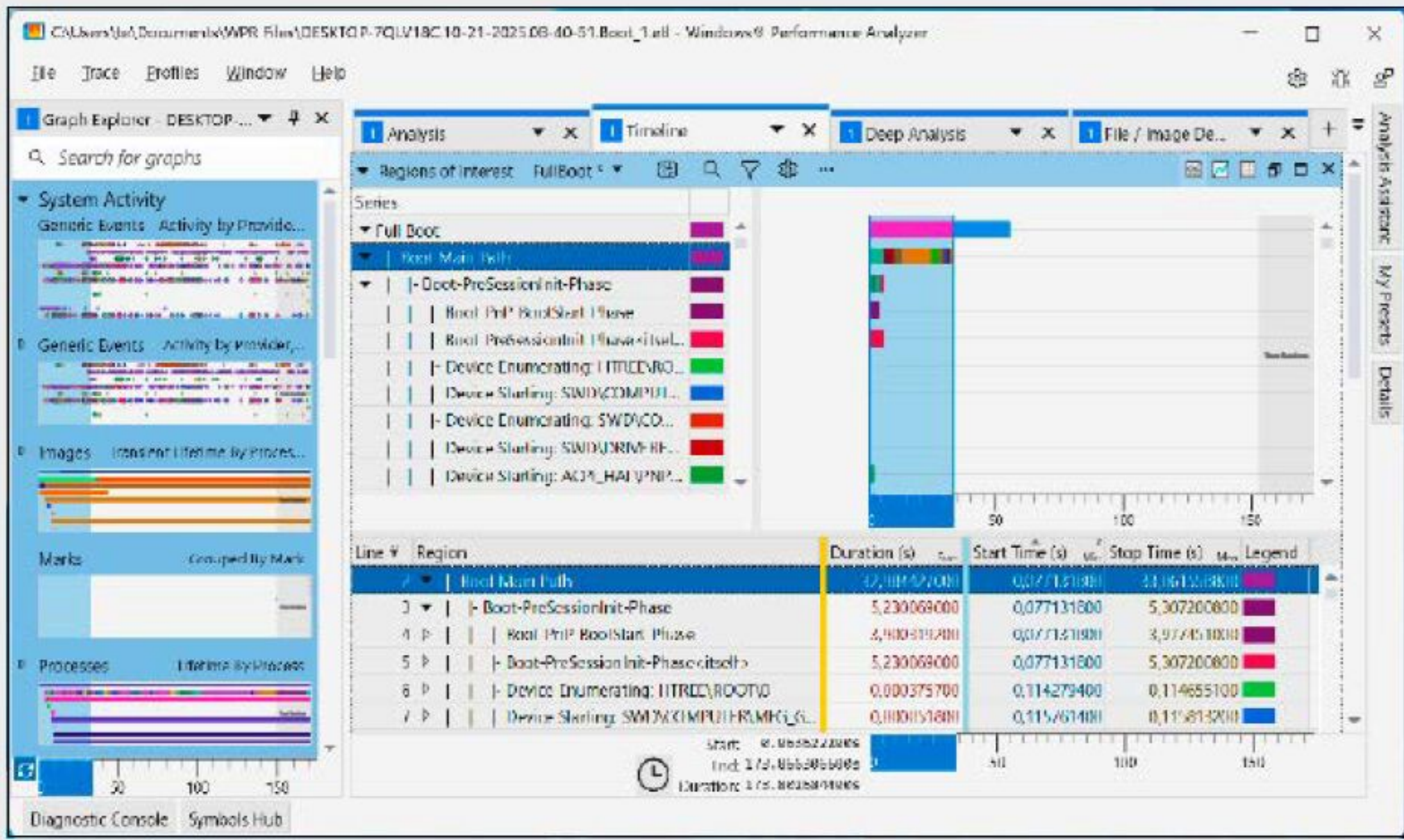
So gelangen Sie trotzdem ins Firmware-Setup: Gehen Sie im Windows-Startmenü auf die Schaltfläche „Ein/Aus“, halten Sie die Shift-Taste gedrückt und wählen Sie „Neu starten“. Weiter geht's mit „Problembehandlung → Erweiterte Optionen → UEFI-Firmwareeinstellungen“ und einem Klick auf „Neu starten“. Deaktivieren Sie dann „Fast Boot“ oder stellen Sie bei „USB Support“ wieder „Full Initial“ ein. **Tipp:** Der Windows-Task-Manager zeigt bei den Autostarts hinter „Letzte BIOS-Zeit“ an, wie lange die Initialisierung durch die Firmware gedauert hat. Sie können damit prüfen, wie wirksam „Fast Boot“ auf Ihrem PC arbeitet.

LEISTUNGSMESSUNGEN FÜR PROFIS



Das Windows Performance Toolkit ist im Windows Assessment and Deployment Kit von Microsoft enthalten. Es ist für Profis gedacht und liefert ausführliche Informationen zum Startvorgang. Bei der Installation wählen Sie nur „Windows Performance Toolkit“, die anderen Programme benötigen Sie für unsere Zwecke nicht. Starten Sie den Windows Performance Recorder aus dem Toolkit, klicken Sie auf „More options“ und wählen Sie unter „Performance scenario“ den Eintrag „Boot“. Hinter „Number of iterations“ tippen Sie eine 1 ein. Klicken Sie auf „Start“ und folgen Sie den weiteren Anweisungen des Tools. Nach der Anmeldung startet der Windows Performance Recorder automatisch. Das Tool liest die Protokolle ein, und nach Abschluss klicken Sie auf „Open in WPA“ (Windows Performance Analyzer). Gehen Sie auf „Profiles → Apply“, klicken Sie auf „Browse Catalog“, öffnen Sie „FullBoot.Boot.wpprofile“ und gehen Sie auf die Registerkarte „Timeline“. Klicken Sie beispielsweise auf „Boot Main Path“. Im Bereich darunter sehen Sie die Dauer des Vorgangs, und noch weiter unten im Fenster werden die Prozesse hervorgehoben, die Windows in dieser Phase gestartet hat.

Ausführliche Untersuchung: Der Windows Performance Analyzer gibt die Zeiten beim Windows-Start detailliert an. Damit lässt sich jede Systembremse finden.



7. Windows schneller starten und herunterfahren
Der „Schnellstart“ ist bei Windows 10 und 11 standardmäßig aktiviert. Wenn Sie im Startmenü „Ein/Aus → Herunterfahren“ wählen, beendet Windows alle Anwendungen, schließt die Benutzersitzung und schreibt Teile des Arbeitsspeichers mit dem Abbild des Kernels in die Datei „C:\hiberfil.sys“. Beim nächsten Start liest Windows die Daten aus der Datei wieder ein. Teilweise müssen zwar Treiber neu initialisiert wer-

den, insgesamt läuft das aber sehr zügig ab. Anders sieht es bei „Neu starten“ aus, womit Windows komplett beendet und neu gestartet wird.

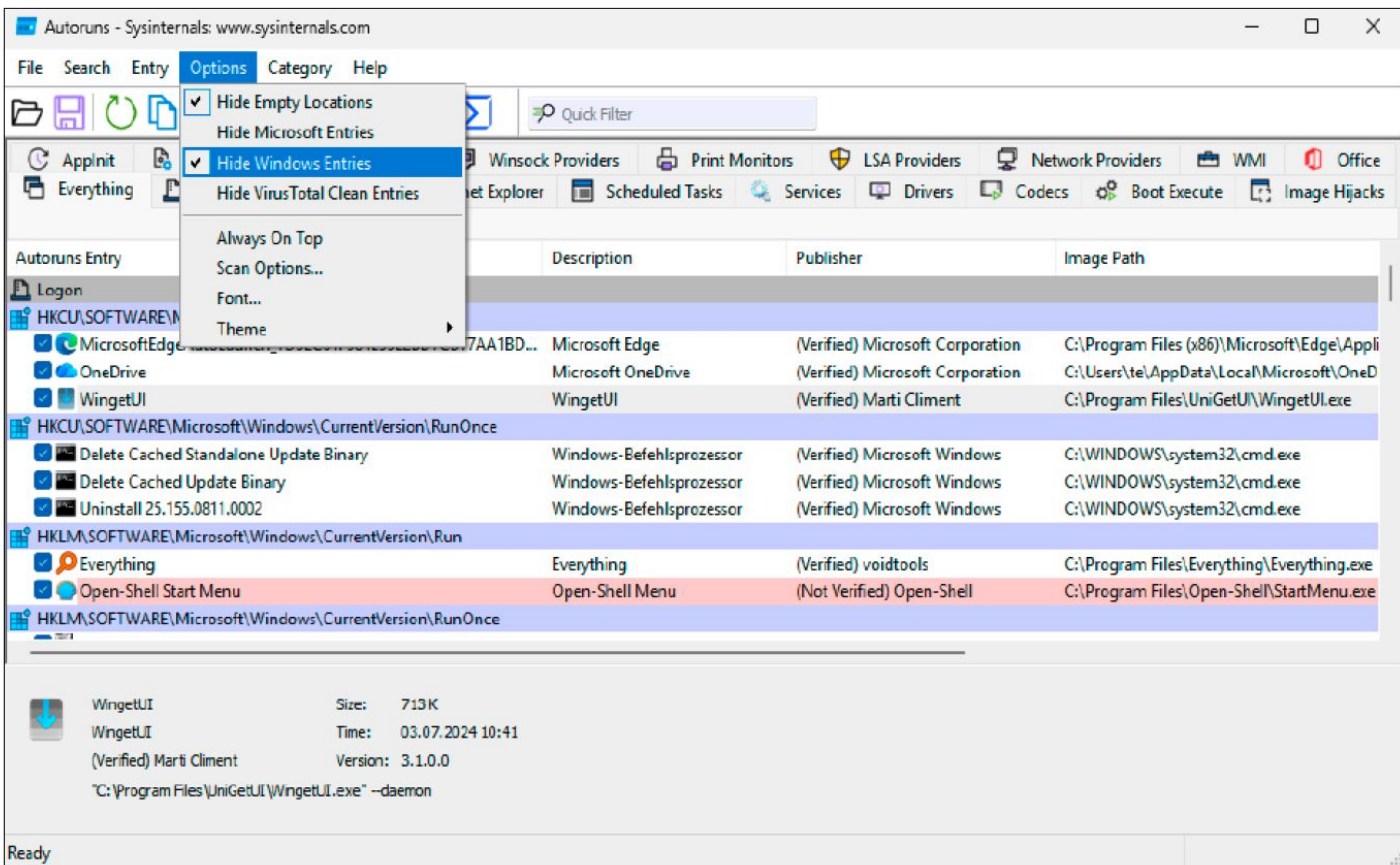
Probleme mit dem Schnellstart sind selten, können aber auftreten, wenn ein Treiber diesen Modus nicht vollständig unterstützt. Es kann dann sein, dass beispielsweise der WLAN-Adapter nicht mehr reagiert. In diesem Fall sollten Sie den Schnellstart deaktivieren. Das ist auch empfehlenswert, wenn Sie Linux auf dem PC nutzen. Denn bei aktiviertem Schnellstart befindet sich das NTFS-Dateisystem nach dem Herunterfahren in einem inkonsistenten Zustand, weshalb Zugriffe von einem anderen System aus zu Datenverlust führen können.

Die Konfiguration des Schnellstarts ist auch bei Windows 11 bisher nicht in die Einstellungen-App gewandert. Rufen Sie den „Ausführen“-Dialog mit Win-R auf, tippen Sie *Control* ein und klicken Sie auf „OK“. In der Systemsteuerung suchen Sie nach „Energie“ und klicken auf „Netzschalterverhalten ändern“. Entfernen Sie das Häkchen vor „Schnellstart aktivieren (empfohlen)“. Wenn es ausgegraut ist, klicken Sie auf „Einige Einstellungen sind momentan nicht verfügbar“.

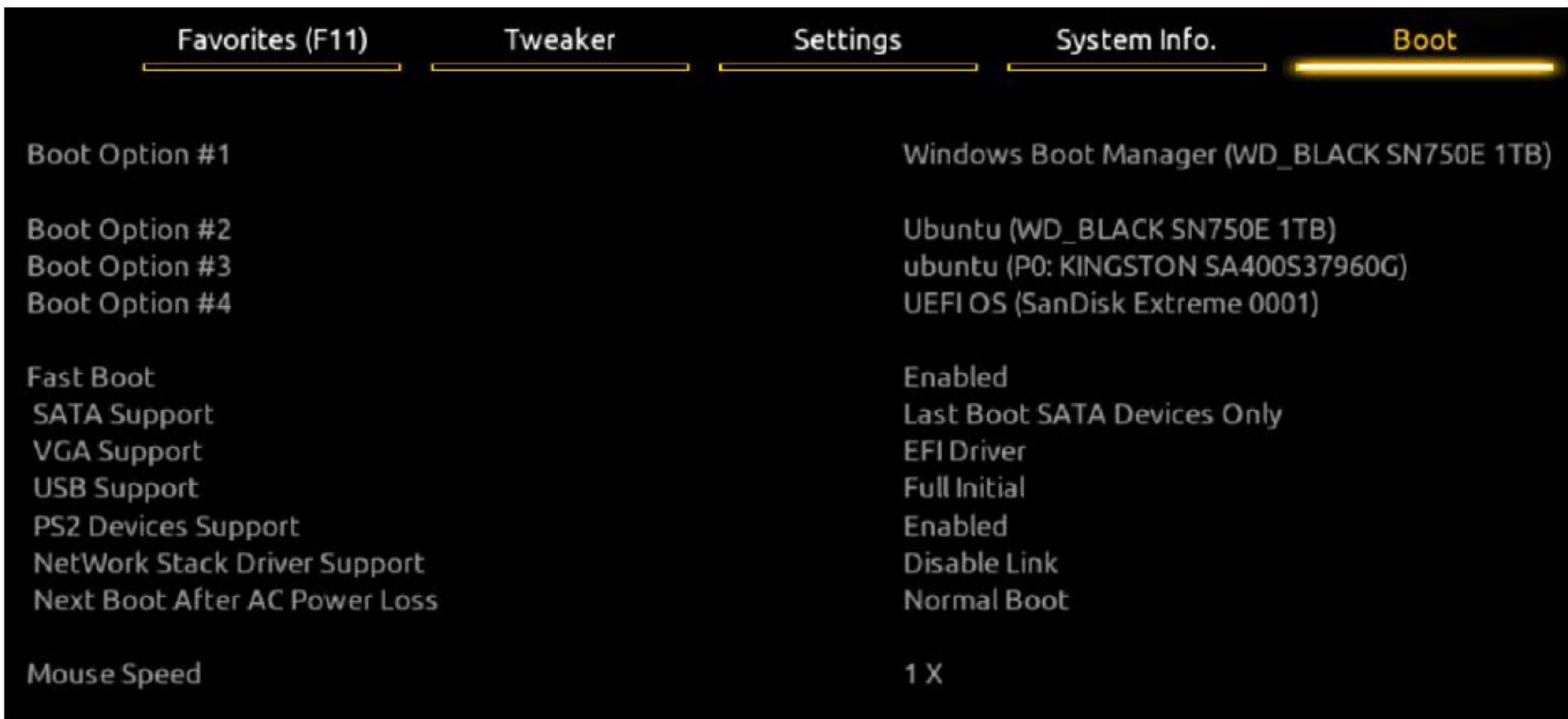
Auf der gleichen Seite können Sie auch das Verhalten von Netzschalter (Standard: „Ruhezustand“) und Energiespartaste (Standard: „Energie sparen“) konfigurieren. „Energie sparen“ versetzt Windows in den Standby-Modus, wobei der Inhalt des Hauptspeichers erhalten bleibt. Wenn Sie Windows über die Tastatur oder Maus wieder aufwecken, können Sie weitermachen, wo Sie aufgehört haben. Alle gestarteten Programme sind weiterhin geöffnet. In diesem Modus liegt die Leistungsaufnahme des Rechners bei einigen wenigen Watt für die Versorgung der nötigen Komponenten. Verwenden Sie „Energie sparen“, wenn Sie die Arbeit an Ihrem PC für kurze Zeit unterbrechen.

Eine Alternative ist „Ruhezustand“, bei dem weniger Energie benötigt wird. Auch hier bleiben die laufenden Anwendungen erhalten. Der Windows-Start erfolgt langsamer als bei „Energie sparen“, jedoch schneller als bei „Herunterfahren“. Dieser Modus ist geeignet, wenn Sie Ihre Arbeit für einen längeren Zeitraum unterbrechen.

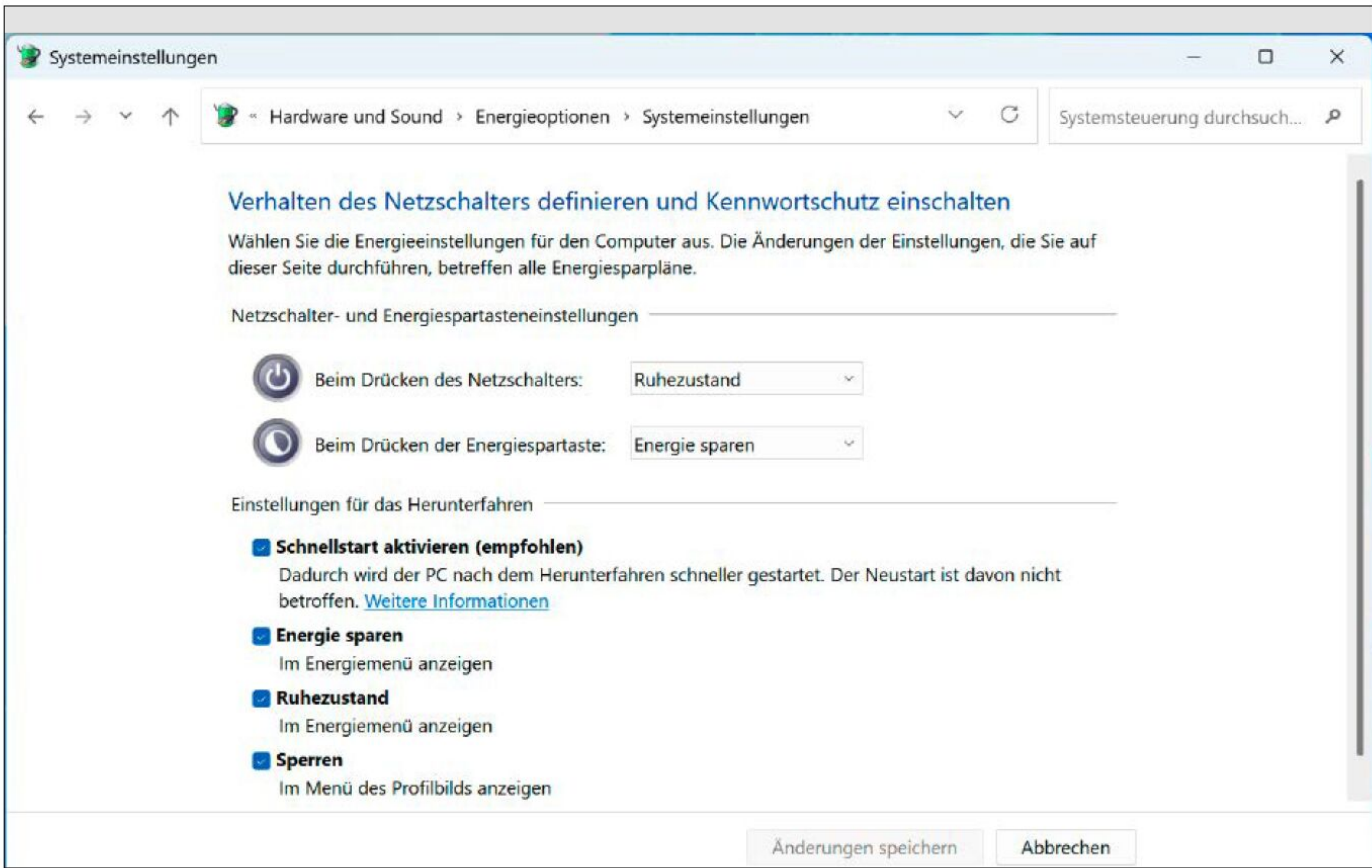
Hinweis: Alle genannten Modi erreichen Sie – soweit vorhanden – auch über „Ein/Aus“ im Startmenü. ■



Umfassende Autostart-Zentrale: Autoruns zeigt alles an, was Windows automatisch startet. Blenden Sie die Windows-Einträge aus, damit die Liste übersichtlicher wird.



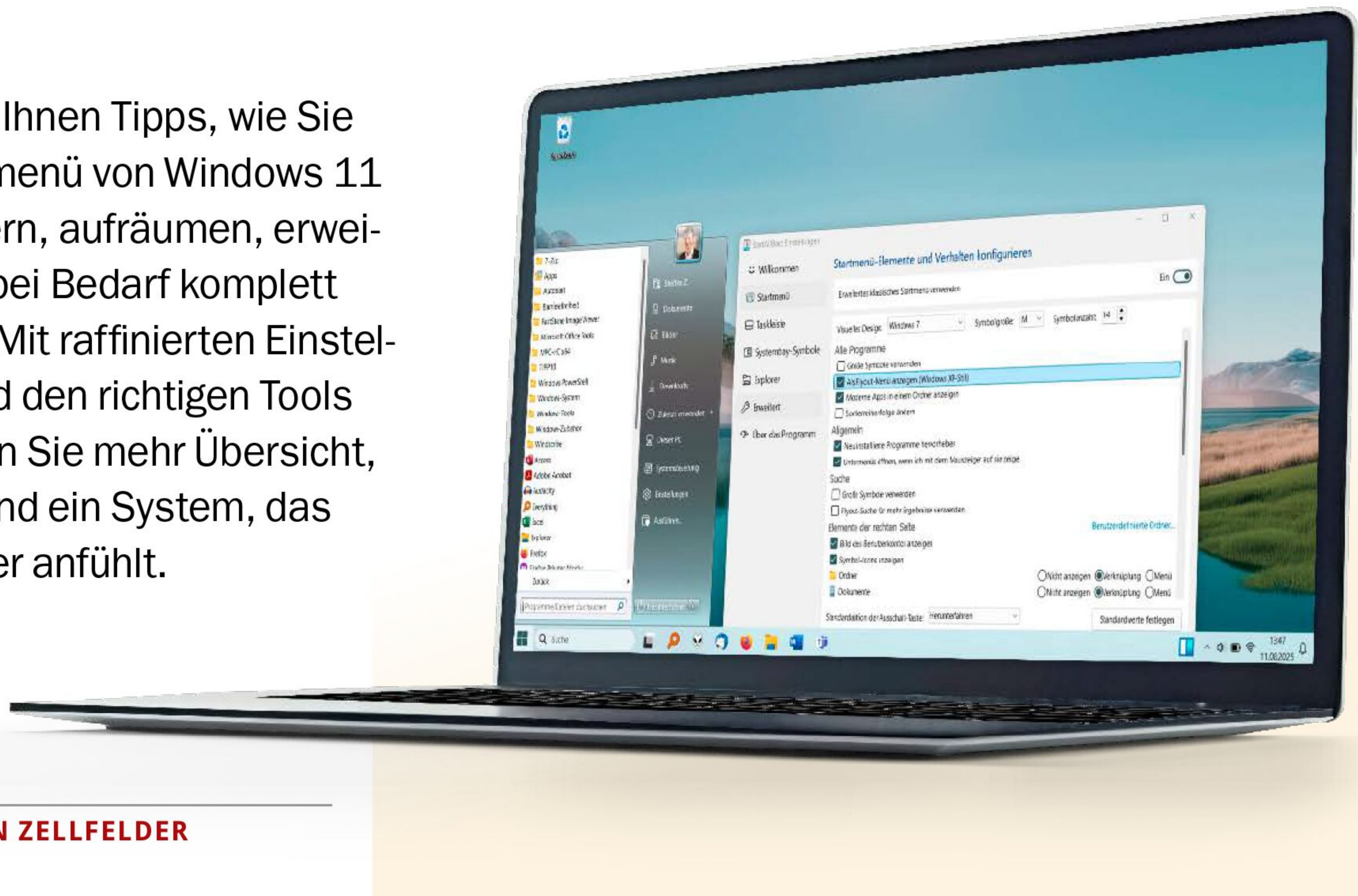
Firmware-Einstellungen: „Fast Boot“ kann den Startvorgang des PCs beschleunigen. „USB Support“ sollten Sie nur deaktivieren, wenn Sie keine USB-Geräte vor dem Windows-Start benötigen.



Windows-Startverhalten: Der Schnellstart sorgt für eine deutliche Beschleunigung des Windows-Starts. Deaktivieren Sie die Option nur, wenn Sie Probleme bemerken oder auch Linux nutzen.

Power-Tuning für das Startmenü

Wir geben Ihnen Tipps, wie Sie das Startmenü von Windows 11 verschönern, aufräumen, erweitern oder bei Bedarf komplett ersetzen. Mit raffinierten Einstellungen und den richtigen Tools bekommen Sie mehr Übersicht, Effizienz und ein System, das sich besser anfühlt.



© Mit Material von Leo - AdobeStock

VON STEFFEN ZELLFELDER

In aktuellen Insider-Builds von Windows 11 experimentiert Microsoft mit einem neuen Startmenü-Design: etwas flexibler, aber noch längst nicht perfekt und funktional überschaubar. Wer darauf nicht warten will, kann schon jetzt nachhelfen – mit Bordmitteln, Registry-Hacks und spezialisierten Tools, die das Menü praktischer und schöner machen oder es sogar komplett ersetzen.

„Das Startmenü ist das Herzstück von Windows 11 – und zum Glück kein starres Korsett. Mit Bordmitteln, Tools oder Registry-Hacks schaffen Sie mehr Ordnung und Komfort.“

Störende Empfehlungen mit Bordmitteln ausblenden

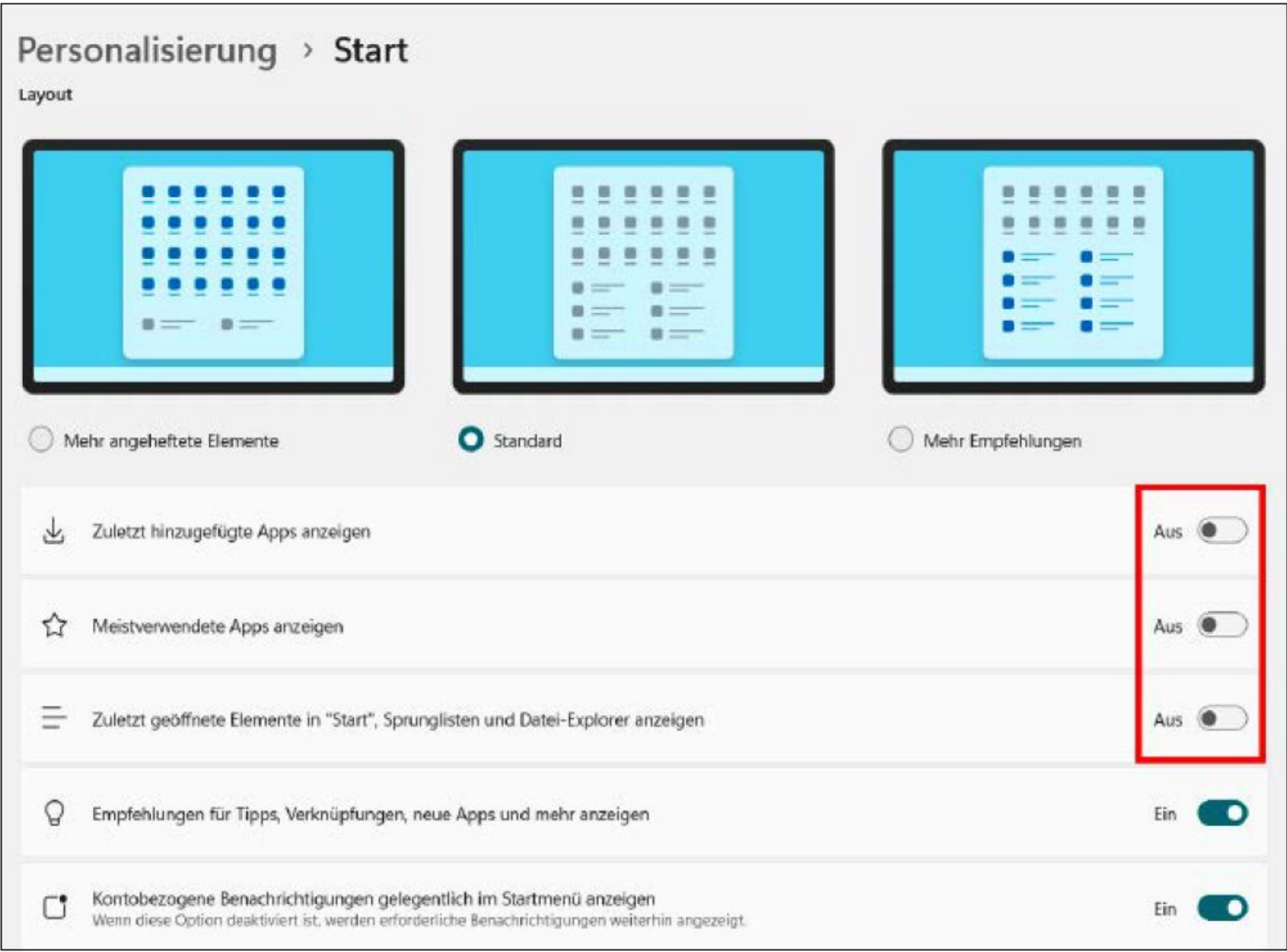
Auch ohne Zusatztools lässt sich das Startmenü von Windows 11 bereits flexibel anpassen und ansprechend individualisieren. Beispielsweise ist einer der größten Kritikpunkte am Windows-11-Startmenü der Bereich „Empfohlen“. Dort tauchen zuletzt verwendete Dateien, neue Programme und teils kryptische Systemvorschläge auf. Wer lieber selbst bestimmt, was im Startmenü erscheint, kann diesen Bereich in wenigen Schritten entschärfen: Öffnen Sie dazu die Einstellungen mit der Tastenkombination Windows-I, navigieren Sie zu „Personalisierung → Start“ und deaktivieren Sie die Schalter bei „Zuletzt hinzugefügte Apps anzeigen“, „Meistverwendete Apps anzeigen“ und „Zuletzt geöffnete Elemente in Start, Sprunglisten und Datei-Explorer anzeigen“. Der Empfehlungsbereich verschwindet damit zwar

nicht ganz. Er bleibt aber leer oder zeigt nur noch einen neutralen Hinweistext.

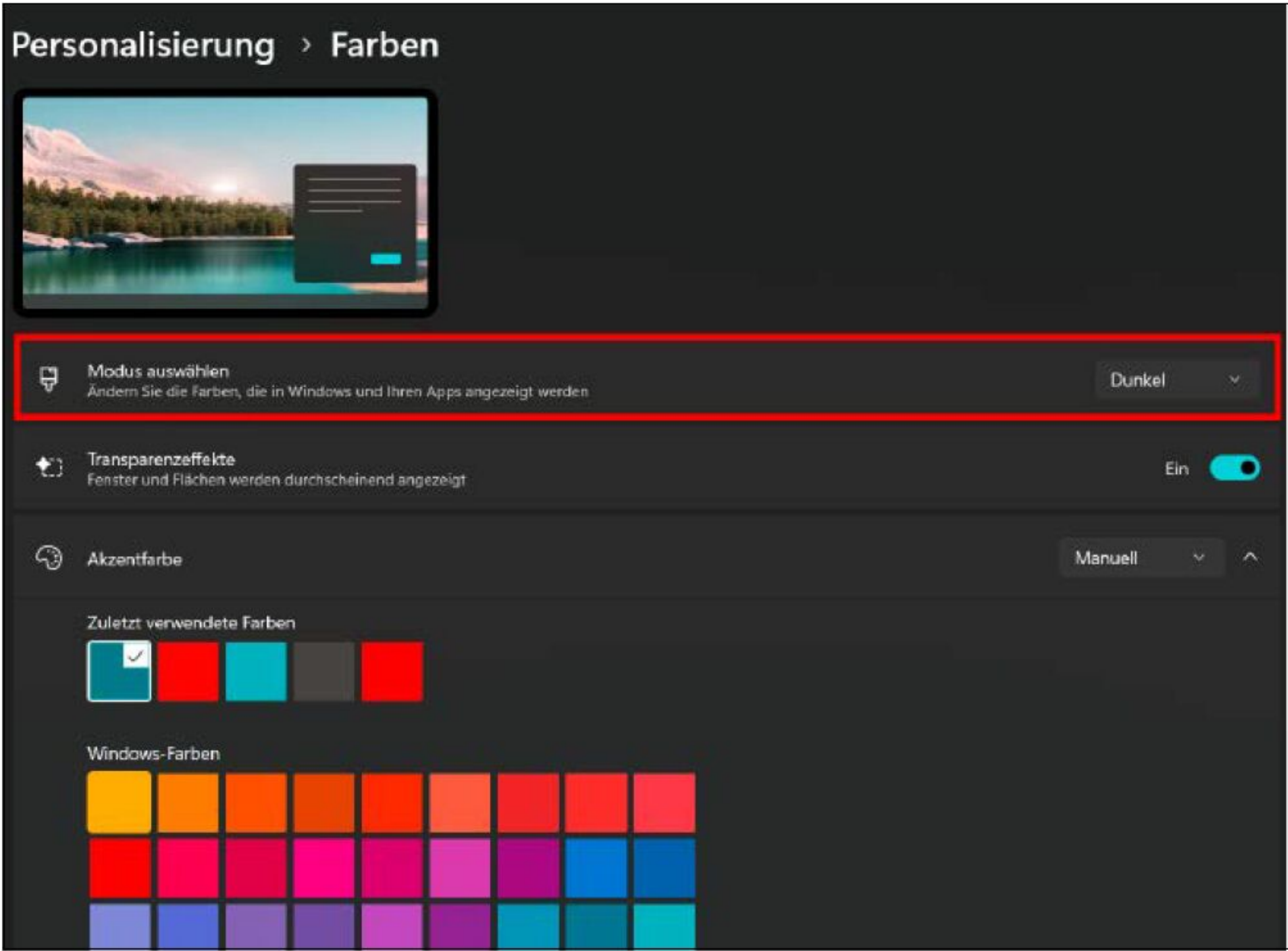
Apps anheften und sortieren für mehr Ordnung im Startmenü

Die oberen zwei Drittel des Startmenüs gehören den angehefteten Apps. Hier lässt sich ganz einfach Ordnung schaffen: Um Apps hinzuzufügen, genügt ein Rechtsklick auf eine App und die Option „An Start anheften“. Möchten Sie eine App entfernen, wählen Sie im gleichen Menü „Von Start lösen“. Zum Verschieben von Apps ziehen Sie sie per Drag & Drop an die gewünschte Stelle, und um einen Ordner anzulegen, ziehen Sie eine App auf eine andere. Dabei entsteht ein Ordner, ähnlich wie beim Smartphone.

Ordner im Startmenü lassen sich auch individuell benennen. Dazu müssen Sie den Ordner nur anklicken und im Kontextmenü „Namen bearbeiten“ wählen. Auch prakti-



Kleine Änderung mit großer Wirkung: Mit diesen Einstellungen wird der Empfehlungsbereich im Handumdrehen weniger aufdringlich.



Das dunkle Design verspricht Abwechslung und schont die Augen. Es lässt sich auch getrennt vom Startmenü in den Systemeinstellungen aktivieren.

sche Verknüpfungen zu Systemtools lassen sich über einen Rechtsklick auf den Desktop und dann „Neu → Verknüpfung“ in das Startmenü einbauen. Für den Geräte-Manager geben Sie anschließend beispielsweise `devmgmt.msc` ein und benennen die Verknüpfung im Folgefenster (etwa „Geräte-Manager“). Per Rechtsklick lässt sich die Verknüpfung dann „An Start anheften“.

Weitere praktische Systemverknüpfungen sind:

- **taskmgr**: Task-Manager
- **services.msc**: Dienste-Verwaltung
- **msconfig**: Systemkonfiguration
- **appwiz.cpl**: Programme und Features (Deinstallation)
- **ncpa.cpl**: Netzwerkverbindungen
- **compmgmt.msc**: Computerverwaltung
- **eventvwr.msc**: Ereignisanzeige
- **resmon**: Ressourcenmonitor
- **lusrmgr.msc**: Lokale Benutzer und Gruppen (in Pro-Versionen)

Startmenü-Optik mit Dark Mode und Effekten anpassen

Das Startmenü folgt standardmäßig dem Systemdesign. Möchten Sie lieber einen dunklen Desktop mit hellem Startmenü (oder umgekehrt) verwenden, lässt sich das

unter „Einstellungen → Personalisierung → Farben“ getrennt einstellen. Entscheiden Sie sich dazu bei „Modus auswählen“ für „Benutzerdefiniert“ und danach wahlweise für „Standardmäßigen Windows-Modus (Startmenü & Taskleiste)“ oder „Standard App-Modus (Fenster & Programme)“. Für einen moderneren Look sorgen Sie mit einer transparenten Darstellung des Startmenüs. Das ist ein geschickter Weg zu schönerer Optik – ohne umständliche Eingriffe ins System. Die Einstellung finden Sie unter „Personalisierung → Farben“. Aktivieren Sie dort „Transparenzeffekte“, präsentiert sich das Startmenü anschließend leicht durchscheinend und sichtbar eleganter. Optional lassen sich hier auch Akzentfarben aufgreifen, die ins Startmenü übernommen werden. Dazu wählen Sie im Drop-down-Menü unter „Personalisierung → Farben → Akzentfarbe“ die Option „Manuell“ und aktivieren etwas weiter unten „Akzentfarbe auf Start und Taskleiste anzeigen“.

Startmenü nach den eigenen Bedürfnissen anpassen

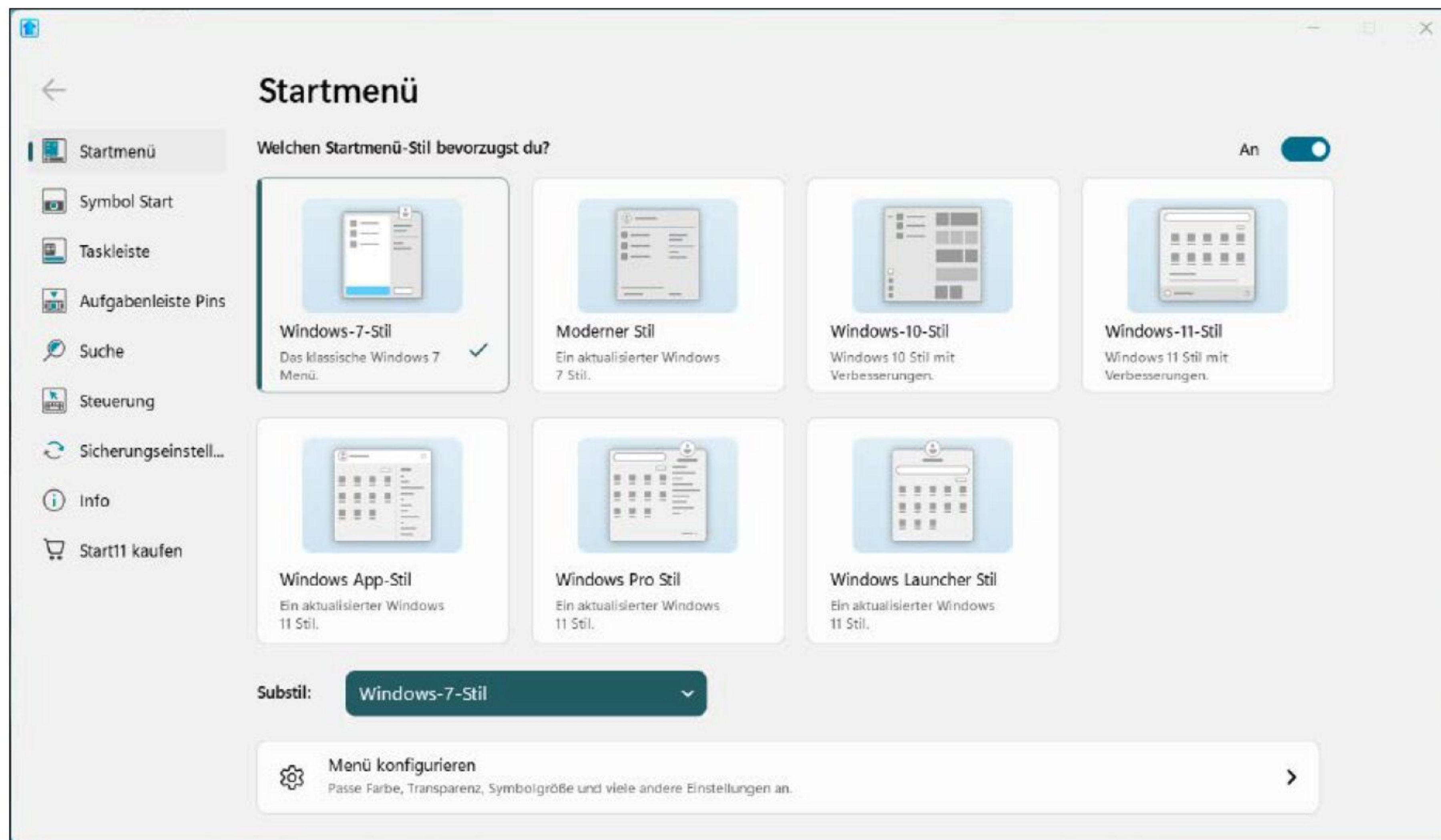
Wer mit dem Startmenü von Windows 11 gar nicht warm wird, kann es einfach ersetzen, ohne riskante Eingriffe in die Systemtiefe vornehmen zu müssen. Verschiedene

Tools bieten alternative Startmenüs mit mehr Funktionen, klassischer Optik und besserer Anpassbarkeit. **Start11** gilt hier als Platzhirsch unter den Startmenütools und bringt auf Wunsch das klassische Windows-7-Menü zurück, imitiert die Optik von Windows 10 oder kombiniert beides in einem modernen Hybriddesign. Nach der Installation haben Sie direkt die Möglichkeit, die Ausrichtung der Taskleiste festzulegen. Anschließend öffnet sich automatisch das Einstellungsfenster, in dem Sie das neue Startmenü Schritt für Schritt gestalten können. Wählen Sie im Bereich „Startmenü“ zunächst den gewünschten Stil aus. Jede Änderung wird sofort übernommen, sodass Sie direkt sehen, wie sich die Oberfläche verändert. Anschließend können Sie über das Feld „Menü konfigurieren“ Farben und Transparenzeffekte festlegen oder die Symbolgröße anpassen. Wenn Sie Layout und Erscheinung Ihres Startmenüs bis ins Detail anpassen möchten, wählen Sie unter „Startmenü → Menü konfigurieren“ den Eintrag „Individualisiere das Erscheinungsbild des Menüs“. Hier können Sie sich austoben: Unter „Schriftarten“ lassen sich beliebige System-Fonts ins Startmenü übertragen, inklusive eigener Einstellungen für Schriftgröße, Überschriften oder für

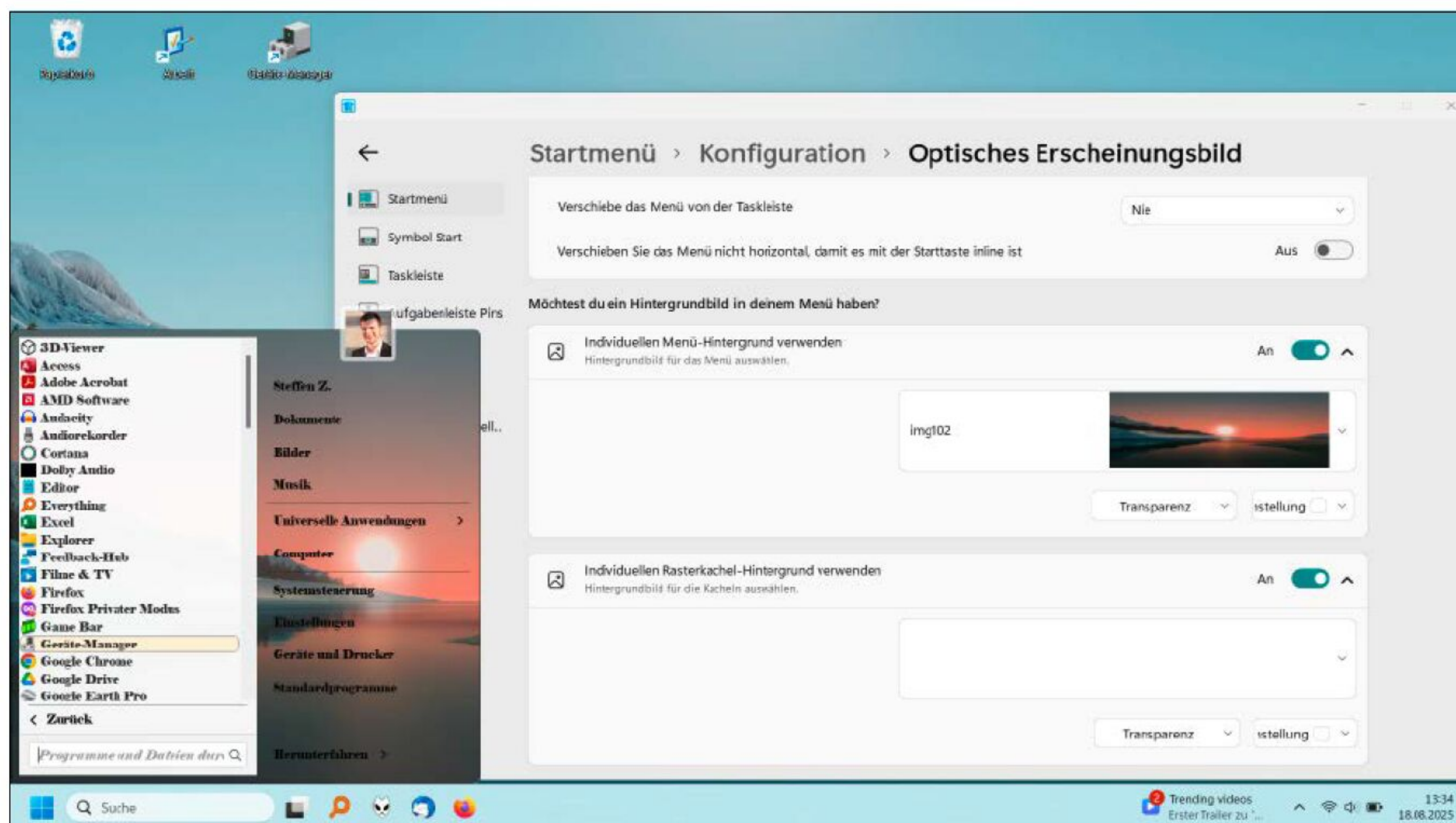
ÜBERBLICK: TOOLS FÜR DAS STARTMENÜ



Name	Beschreibung	URL	Auf	Sprache	Preis
Everything	Extrem schnelle lokale Dateisuche	www.voidtools.com/downloads/	Heft-DVD	Deutsch	Kostenlos
Start11	Ersetzt das Startmenü, bietet viele Anpassungen	www.stardock.com/products/start11/	Heft-DVD	Deutsch	Ca. 8 Euro
Start All Back	Bringt klassische Windows-Optik, sehr ressourcenfreundlich	www.startallback.com/	Heft-DVD	Deutsch	Ca. 5 Euro



Windows 10, Windows 7 oder ein übersichtlicher Launcher-Stil: Mit Start11 haben Sie viele Gestaltungsmöglichkeiten. Nach einer 30-tägigen Testphase wird das Tool aber kostenpflichtig (ca. 8 Euro).



Freie Schrift- und Hintergrundwahl: Der Kreativität sind bei Start11 kaum Grenzen gesetzt. Sogar eigene Fotos können Sie damit als Startmenü-Hintergrund festlegen.

die Menüschriftart. Unter „Optik“ (de-)aktivieren Sie abgerundete Kanten, heben das Menü von der Taskleiste ab oder legen Animationseffekte fest. Besonders ansprechend zeigt sich das Startmenü, wenn Sie den Menüpunkt „Individuellen Menü-Hintergrund verwenden“ aktivieren. Damit schmücken Sie das Menü mit Leder- oder Holzlook, fügen stimmungsvolle Hintergrundbilder ein oder sogar eigene Fotos.

Auch praktisch bei Start11: Sie haben die Möglichkeit, eigene Kategorien für Programme einzurichten, sodass häufig genutzte Apps in einem separaten Bereich zusammengefasst werden. Klicken Sie dazu im Hauptfenster auf den vierten Menüpunkt „Aufgabenleiste Pins“. Hier können Sie unter „Datei anheften“ wichtige Doku-

mente direkt an die Taskleiste heften oder mit der Option „Ordner anheften“ das Gleiche für wichtige (Arbeits-)Ordner tun. Sogar ganze Ordnermenüs lassen sich über das gleichnamige Feld verankern: So bringen Sie den Schnellstart unter, listen alle Apps auf oder lassen sich App-Vorschläge zeigen. Unter dem Menüpunkt „Suche“ können Sie im Startfenster auch die ungeliebte (und oft wenig erfolgreiche) Windows-Suche ersetzen oder mit der Einstellung „Use old Start10 style Search“ die Suchfunktion von Windows 7 zurückholen, wenn Sie sich nostalgisch fühlen.

Startmenü im Windows-10-Stil

Start All Back richtet sich vor allem an Nutzer, die den gewohnten Windows-10-Stil

vermissen, und ergänzt das klassische Startmenü um moderne Extras wie Dark Mode, Transparenzeffekte und flexible Symbolgrößen. Nach der Installation öffnet sich sogleich das Einstellungsfenster, in dem Sie zunächst das gewünschte Startmenü-Design auswählen. Sie können sich zwischen Windows 11, Windows 10 oder einem „Windows 7 Remaster“ entscheiden. Bei der Auswahl sehen Sie sofort die Veränderungen auf Ihrem Desktop.

Anschließend lassen sich Farben, Transparenzeffekte und Symbolgrößen anpassen, sodass das Erscheinungsbild genau Ihrem Geschmack entspricht. Wechseln Sie dafür zum zweiten Menüpunkt „Startmenü“. In der ersten Zeile legen Sie nun fest, wie sich Ihr Startmenü inhaltlich präsentieren soll. Hier bestimmen Sie das visuelle Design, die Symbolgrößen und wie viele Symbole gleichzeitig angezeigt werden sollen („Symbolanzahl“). Gehen Sie anschließend einmal die Einstellungsliste durch. Besonders praktisch sind hier die Möglichkeiten, große Symbole zu verwenden oder die Sortierreihenfolge zu ändern. Auch ein Flyout-Menü, sowohl für die Suche als auch für Ihre App-Liste, steht zur Verfügung. Unter „Elemente der rechten Seite“ können Sie den zweiten Fensterflügel flexibel individualisieren und praktische Menüs für die Einträge anheften.

Wer möchte, kann auch Ordner für Programme oder Dateien erstellen, um die Übersichtlichkeit zu verbessern. Klicken Sie dafür auf den blauen Text „Benutzerdefinierte Ordner...“. Der Befehl „Hinzufügen“ öffnet anschließend ein Explorer-Fenster, in dem Sie einen beliebigen Ordner auswählen können, beispielsweise einen Arbeitsordner oder einen Speicherort mit wichtigen Verknüpfungen. Über „Glyphen-Symbol ändern...“ legen Sie eigene Symbole dafür fest und machen Ihr Startmenü besonders individuell.

Bing aus dem Startmenü verbannen

Standardmäßig zapft Windows bei jeder Suchanfrage das Web an, meist via Bing. Wer damit nichts anfangen kann oder schlicht keine Webtreffer sehen möchte, kann die Websuche über einen kleinen Eingriff in die Registry abschalten. Öffnen Sie dazu zunächst den Registrierungs-Editor, indem Sie Windows-R drücken und *regedit* eingeben. Navigieren Sie anschließend zu „HKEY_CURRENT_USER\Software\Policies\

Microsoft\Windows“. Dort prüfen Sie, ob bereits ein Schlüssel namens „Explorer“ existiert. Falls nicht, legen Sie unter dem Windows-Ordner per Rechtsklick einen neuen Schlüssel an und nennen ihn „Explorer“. Innerhalb dieses Explorer-Ordners erstellen Sie dann mit einem erneuten Rechtsklick einen neuen DWORD-Wert (32-Bit) mit dem Namen „DisableSearchBoxSuggestions“ und setzen dessen Wert auf 1. Nach einem Neustart des PCs werden in der Startmenü-Suche fortan nur noch lokale Inhalte angezeigt, also Apps, Dateien und Einstellungen, während die Bing-Treffer verschwinden.

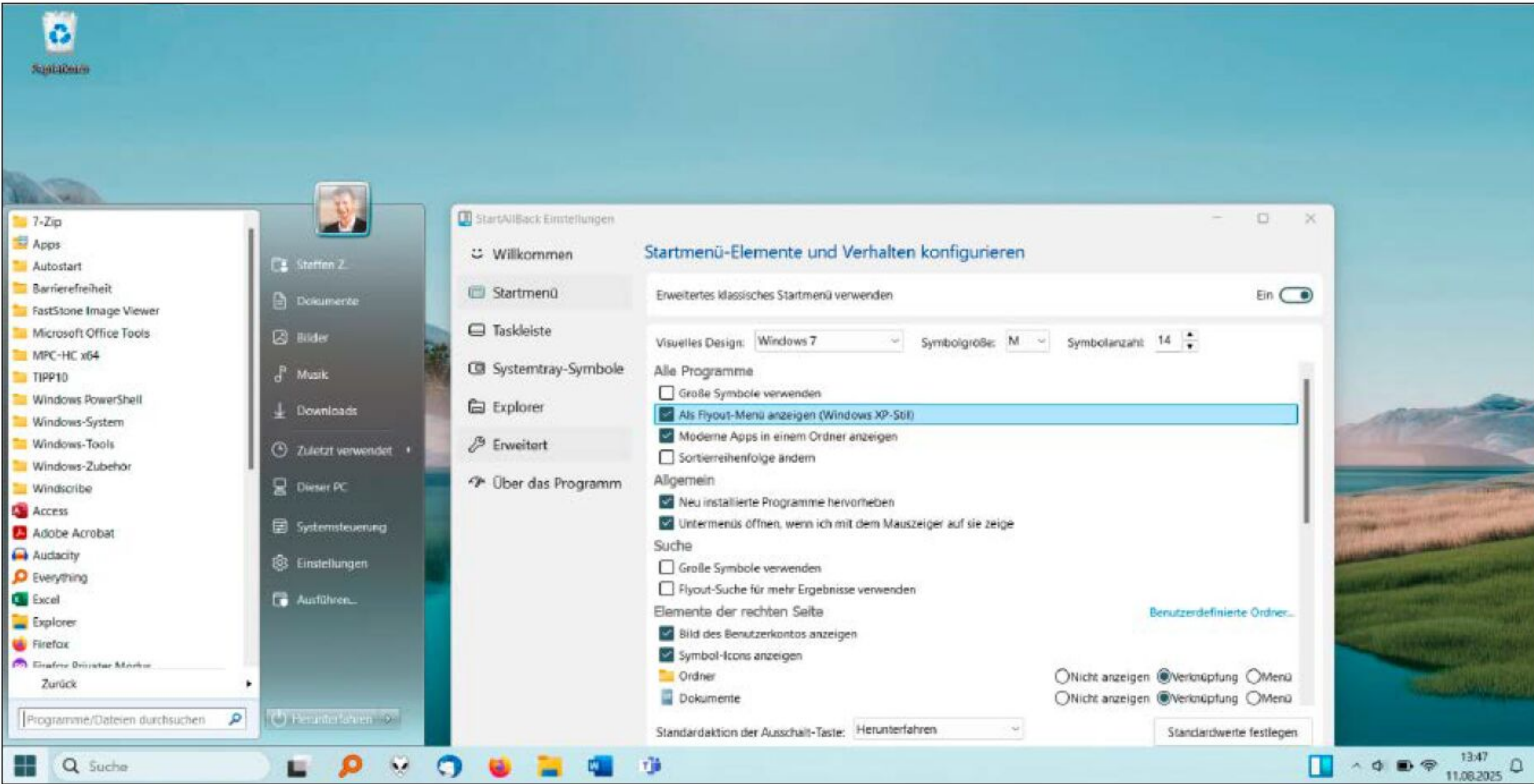
Hinweis: Die Deaktivierung der Websuche funktioniert nicht in allen Windows-11-Editionen oder Builds, und Microsoft kann dieses Verhalten per Update wieder ändern. Um Bing später erneut zu aktivieren, löschen Sie einfach den zuvor angelegten Registry-Wert und starten den PC erneut.

Alles sofort finden mit Everything

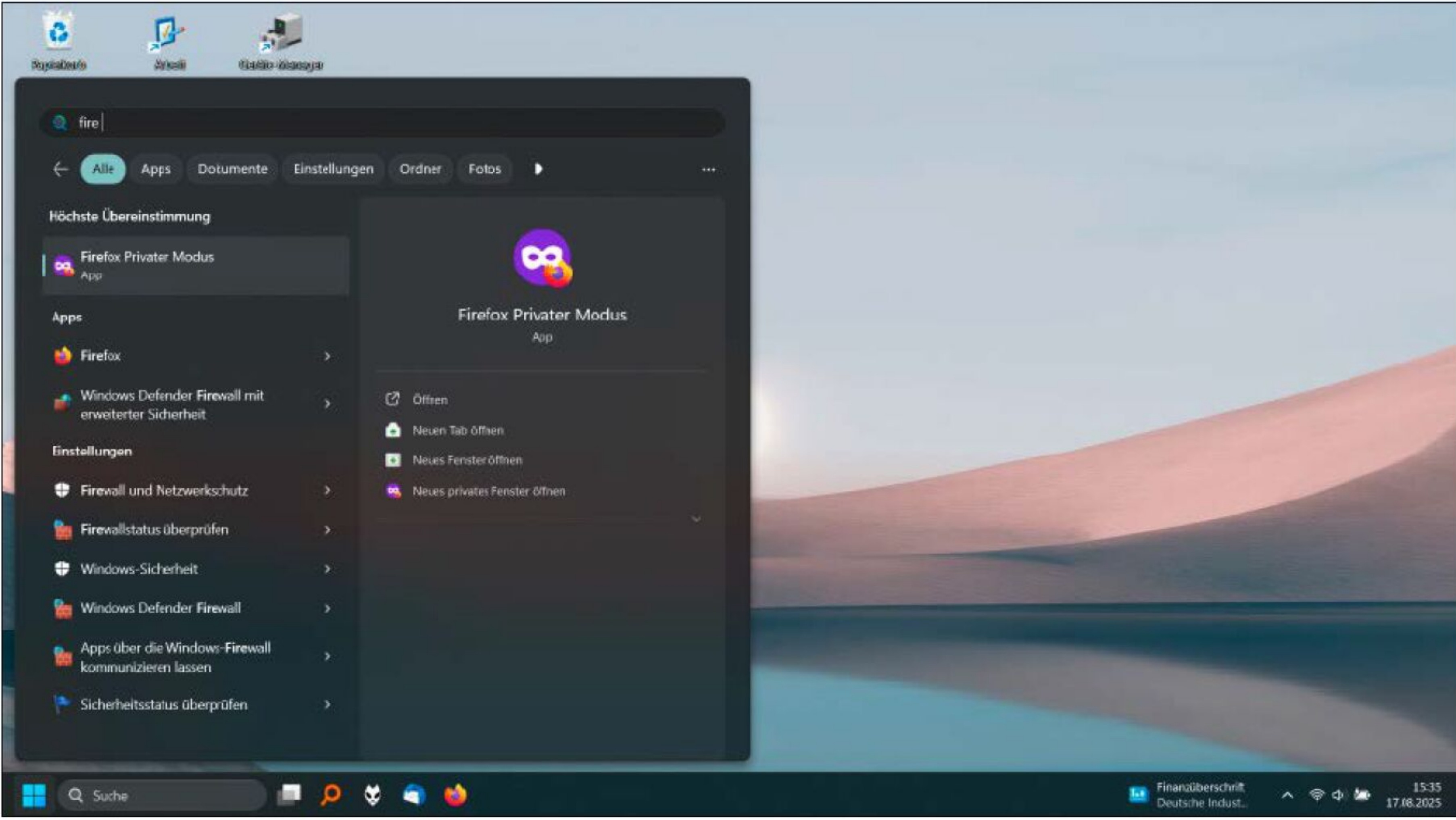
Wer unter Windows 11 Dateien zuverlässig finden möchte, kommt mit externen Suchwerkzeugen deutlich schneller ans Ziel als mit der halb blinden Standardsuche. Besonders leistungsfähig ist das kostenlose Open-Source-Tool **Everything**, das innerhalb von Sekunden einen Index aller Ihrer Dateien erstellt und Treffer sofort beim Tippen liefert. Schlank, blitzschnell und ohne unnötigen Ballast wie Werbung oder Websuche ist es ideal für alle, die häufig nach Dokumenten, Fotos oder Projektdaten suchen. Das Tool ist größtenteils selbsterklärend: Nach der Installation tippen Sie in der Suchleiste oben beliebige Begriffe ein, auch Fragmente von Dateinamen liefern exakte Treffer, und die Ergebnisse erscheinen unmittelbar. Über den Menüpunkt „Ansicht“ können Sie ein Vorschaufenster zuschalten oder ein Filtermenü für verschiedene Dateitypen aktivieren.

Fazit

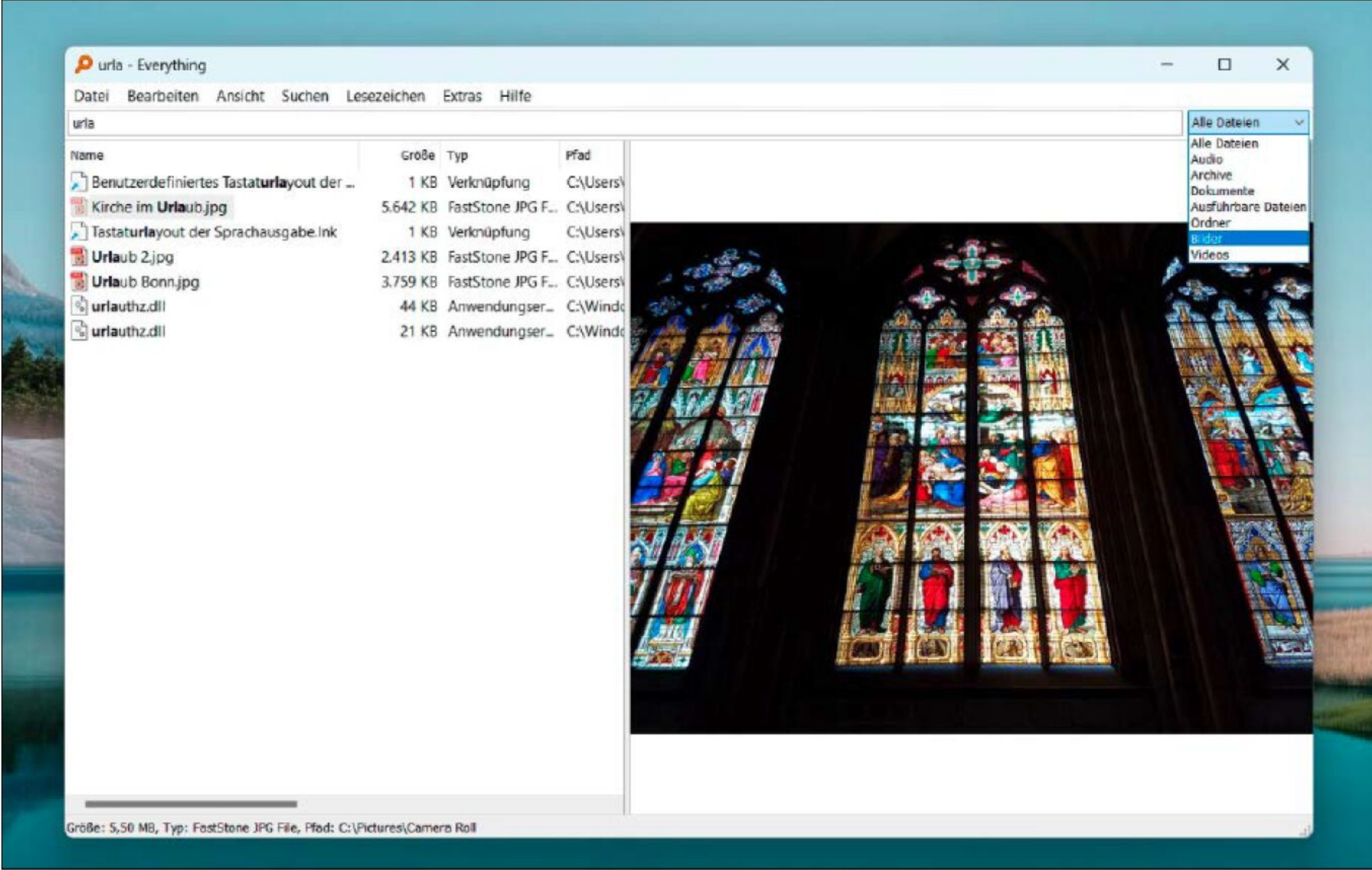
Mit Bordmitteln, gezielten Einstellungen und praktischen Tools lässt sich das Startmenü von Windows 11 deutlich übersichtlicher, effizienter und optisch ansprechender gestalten. Ob Sie nur aufräumen, den Empfehlungsbereich entschärfen oder das Menü komplett ersetzen möchten – mit den vorgestellten Methoden haben Sie freie Hand. ■



Aufgeräumt, effizient und frei konfigurierbar: Mit Start All Back lässt sich das Startmenü flexibel und übersichtlich anpassen. Alle Änderungen können per Deinstallation schnell wieder zurückgenommen werden.



Bye-bye Bing: Die oft nutzlosen Webtreffer der Windows-Suche deaktivieren Sie mit einem einfachen Registry-Schlüssel. Das sorgt sofort für einen „Aha“-Effekt – und für deutlich bessere Treffer.



Macht die schlappe Windows-Suche neidisch: Mit Everything spüren Sie Dateien in Echtzeit auf. Die Ergebnisse erscheinen schon während der Eingabe und lassen sich übersichtlich filtern.

Fernhilfe bei Umstieg auf Windows 11

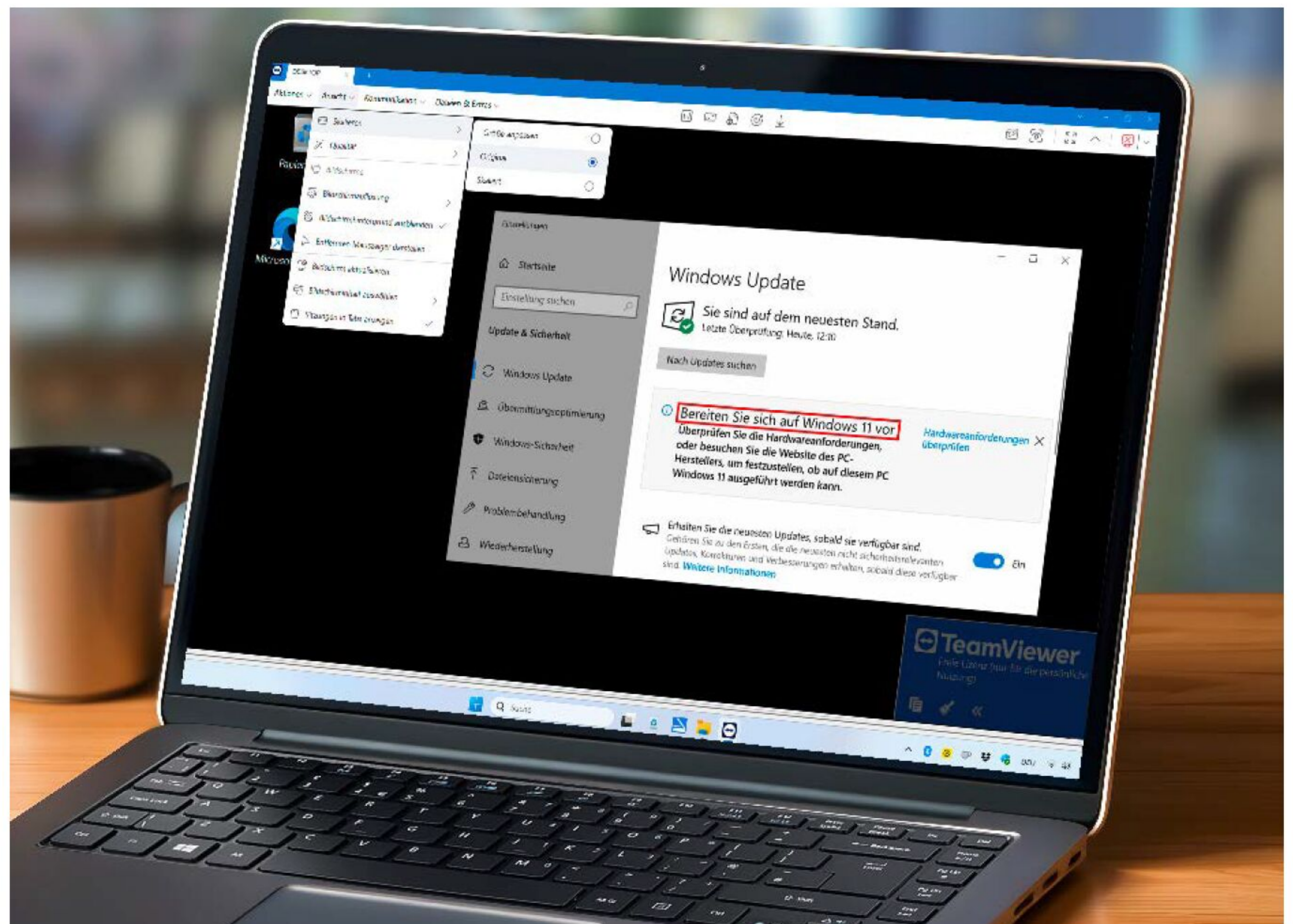
Der Umstieg von Windows 10 auf Windows 11 kann viele Anwender ängstigen. Ist beim Upgrade im Familien- oder Freundeskreis Ihre Hilfe gefragt, macht Onlineunterstützung es allen Beteiligten so einfach wie möglich.

VON PETER STELZEL-MORAWIETZ

Der Remote- oder Fernzugriff über das Internet auf einen anderen PC kann ein Segen sein, manches IT-Problem wird so schnell und unkompliziert gelöst. Schließlich kann sich der Helfer ein genaues Bild machen und das Problem im Idealfall sofort lösen, auch ohne dass er vor Ort ist. Die sonst mitunter schwierige Kommunikation per Telefon entfällt.

Absehbar viel Unterstützung wird für den Umstieg auf Windows 11 nötig. Selbst wenn der PC die passenden Hardwarevoraussetzungen hat, gibt es einige Stolpersteine an denen ein Upgrade scheitern kann (siehe auch Ratgeber „Windows-Upgrade: Jede Blo-

„PC-Erklärungsversuche am Telefon führen oft nicht weiter. Ein Fernwartungstool macht es Helfern und Hilfesuchenden einfach.“



© fluffyclouds - AdobeStock

ckade lösen“ in dieser Ausgabe). Wer seiner Familie, Freunden oder Bekannten behilflich sein möchte oder selbst Mithilfe benötigt, sollte sich daher vorbereiten.

Einfach und effizient unterstützen Sie andere per Fernhilfe. Das spart Fahrt- und Besuchszeit sowie Geld, zudem können Sie den Support auf mehrere Sitzungen verteilen. Auch wenn man einen Installationsstick per Post verschicken muss, kann es einige Tage dauern, bis es weitergeht. Das sollte man mit einplanen.

Unser Ratgeber erläutert die Vorbereitung, führt durch den Upgradeprozess, erklärt das Umgehen der Installationssperre auf älteren PCs und zeigt, wie Fernwartung selbst dann funktioniert, wenn Windows vor einer Neuinstallation noch gar nicht läuft. Schließlich ist es nicht ganz einfach, jeden Computer statt „normal“ von der Festplatte vom USB-Setup-Stick zu starten. Ohne Videounterstützung und -kontrolle kann das durchaus scheitern.

Mit **Teamviewer Remote** haben wir ein Fernwartungstool gewählt, das für den privaten Gebrauch kostenlos ist, problemlos funktioniert und es für diejenigen besonders einfach macht, die Ihre Hilfe benötigen: Bei der Variante **Teamviewer Quick-support** genügt es, auf einen per Mail zugeschickten Link zu klicken, schon kann es losgehen. Sie finden dieses Tool wie alle weiteren auf Heft-DVD.

So bereiten Sie die Unterstützung aus der Ferne optimal vor

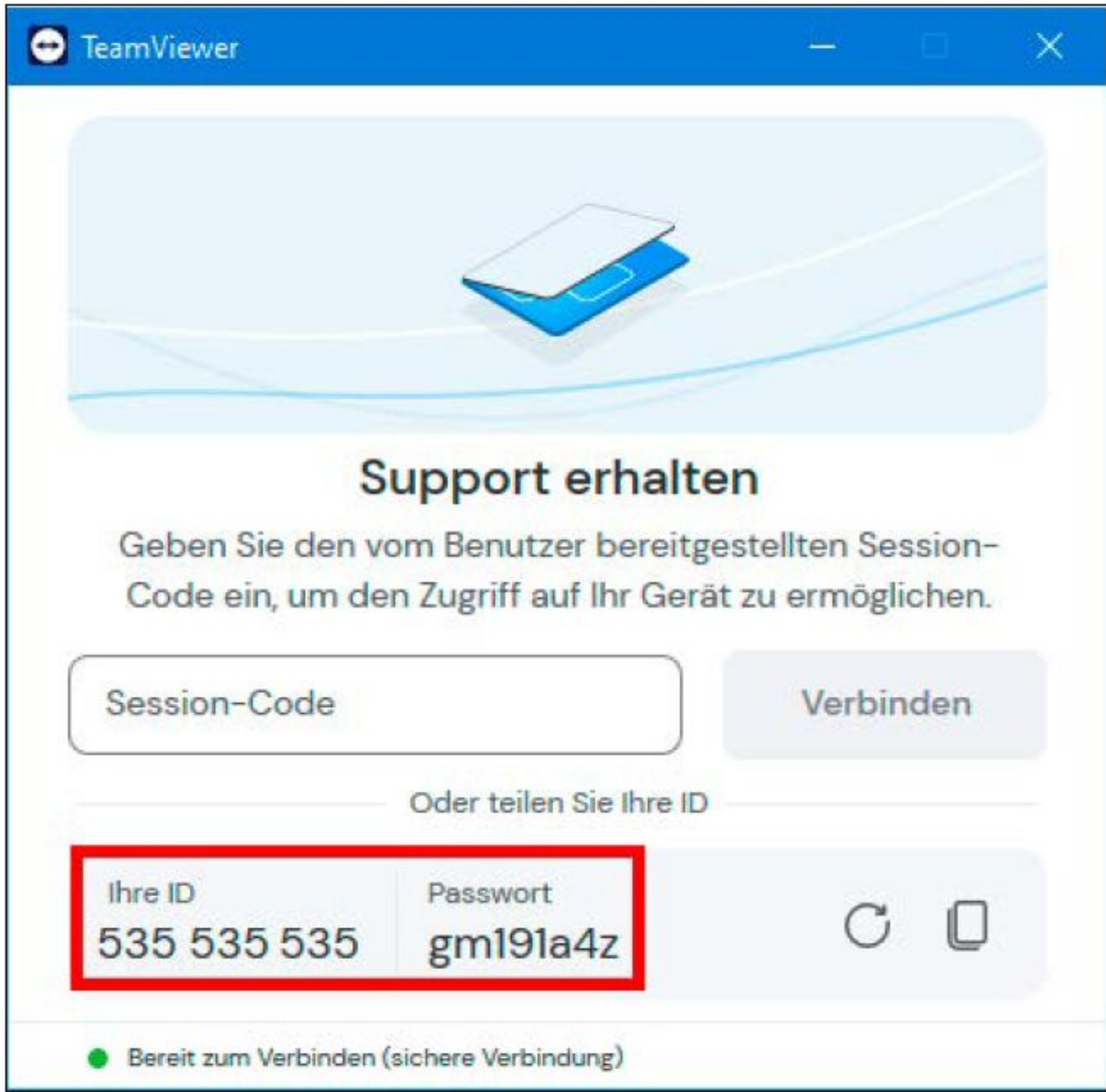
Vermutlich macht sich nicht jeder Windows-10-Anwender klar, was das Support-Aus wirklich bedeutet: Nämlich dass es ohne Sicherheitsupdates äußerst riskant ist, den PC wie bisher weiter zu nutzen. Entscheidend ist deshalb, Bewusstsein für den unter Sicherheitsaspekten zwingend notwendigen Wechsel auf das neue Betriebssystem zu schaffen. Immerhin läuft Windows 10 noch auf mehr als 30 Millionen Rechnern.



Während Microsoft den Hinweis auf das Support-Aus von Windows 10 im vergangenen Jahr häufig einblendete, erschien er auf unseren Systemen in den vergangenen Monaten nur ein einziges Mal.

Ferner gilt es zu prüfen, ob sich der vorhandene Computer für den Umstieg auf die aktuelle Version 25H2 von Windows 11 eignet oder ob – aus welchen Gründen auch immer – neue Hardware angeschafft werden muss oder soll. Davon hängt entscheidend das weitere Vorgehen ab. Die Voraussetzungen für die PC-Fernwartung sind denkbar gering: Beide Rechner müssen mit dem Internet verbunden sein, außerdem sollte man während der Unterstützung miteinander telefonieren, klassisch oder per Whatsapp. Das erleichtert Rückfragen und ermöglicht, die Hilfestellung zu erläutern. Als Helfer installieren Sie auf Ihrem Rechner die Clientversion, also Teamviewer Remote, und starten anschließend das Tool. Bestätigen Sie die Lizenzbestimmungen und warten Sie kurz ab, bis die Programm-

oberfläche erscheint. Sofern vorhanden, melden Sie sich mit Ihrem bestehenden Teamviewer-Konto an und klicken gegebenenfalls noch auf den Bestätigungslink „Vertrauenswürdige Geräte“ in der von Teamviewer zugeschickten Mail. Ansonsten legen Sie über „Konto erstellen“ einen neuen Account an. Nun zu Ihrem Gegenüber. Für ihn (oder sie) ist es am einfachsten, wenn Sie ihm (ihr) den Downloadlink für Teamviewer Quicksupport (https://download.teamviewer.com/download/TeamViewerQS_x64.exe) per E-Mail zusenden. Der muss dann nur noch angeklickt, das Tool heruntergeladen und per Doppelklick gestartet werden. Eine Installation ist nicht notwendig. Die Quicksupport-Oberfläche ist mit den beiden Angaben „Ihre ID“ und „Passwort“ stark reduziert. Die ID kennzeichnet den Computer, der übernommen



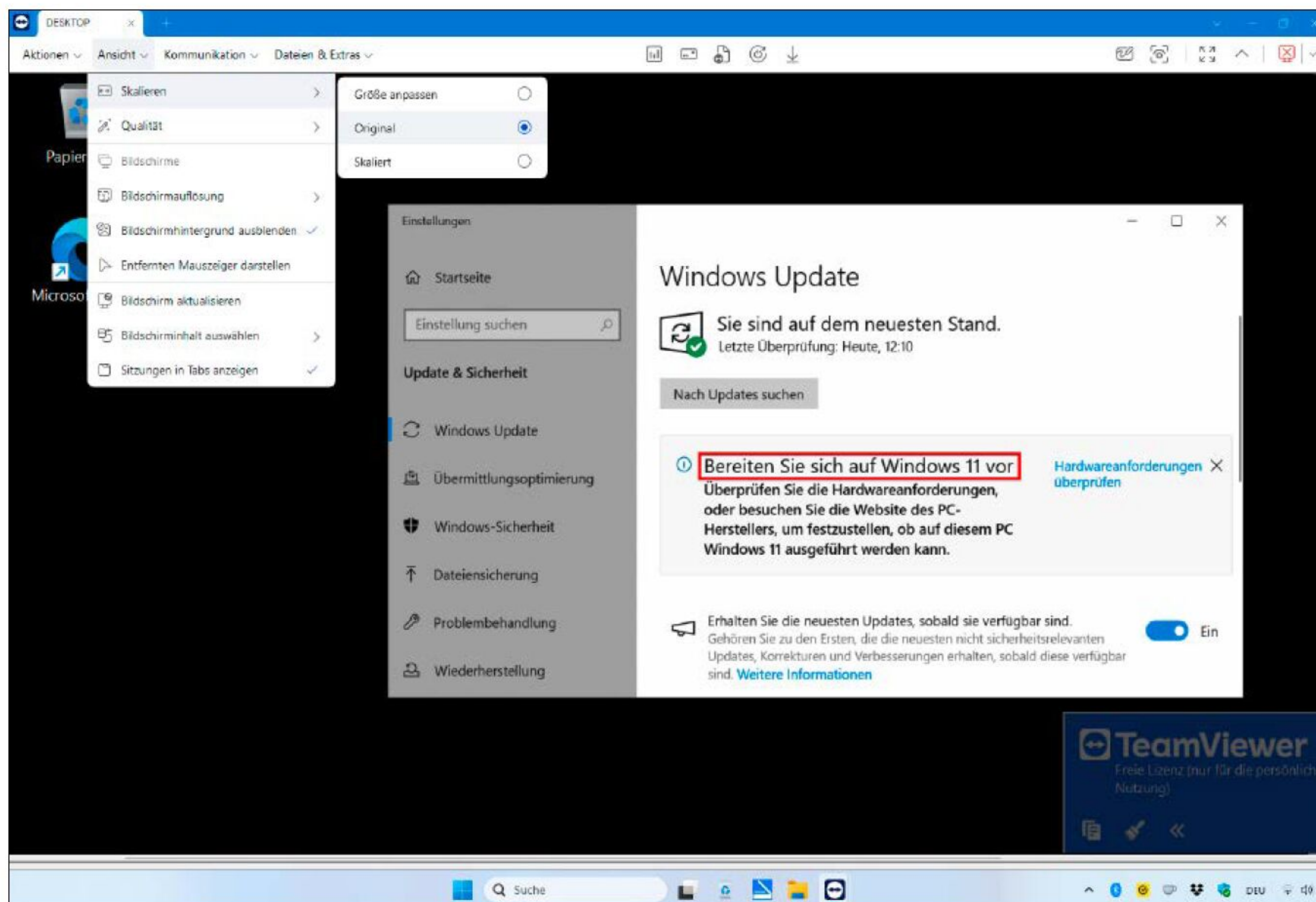
Teamviewer Quicksupport startet ohne Installation, die reduzierte Oberfläche macht die Fernwartung einfach: Rechner-ID und Passwort am Telefon durchgeben, schon geht's los.

werden soll, und ist fix. Das Passwort dagegen wird aus Sicherheitsgründen für jede Session neu generiert. Beides übermittelt Ihnen die zu unterstützende Person, entweder per Telefon oder über den Zwischenablage-Button rechts per E-Mail. Die ID des entfernten PCs übernehmen Sie in Ihrem Teamviewer-Client im Feld „Teilnehmer-ID“, klicken auf „Verbinden“, tippen im nächsten Fenster das Passwort ein und bestätigen mit „Anmelden“. Das startet die Verbindung automatisch, ohne dass Ihr Gegenüber etwas tun muss. Er erkennt Ihre Übernahme seines PCs am schwarz abgedunkelten Desktophintergrund. Sie selbst haben nun mit Maus und Tastatur die volle Kontrolle. Passen Sie, falls notwendig, die Desktopdarstellung des anderen Rechners in Teamviewer über „Ansicht → Skalieren“ an, meist ist die Option „Original“ richtig.

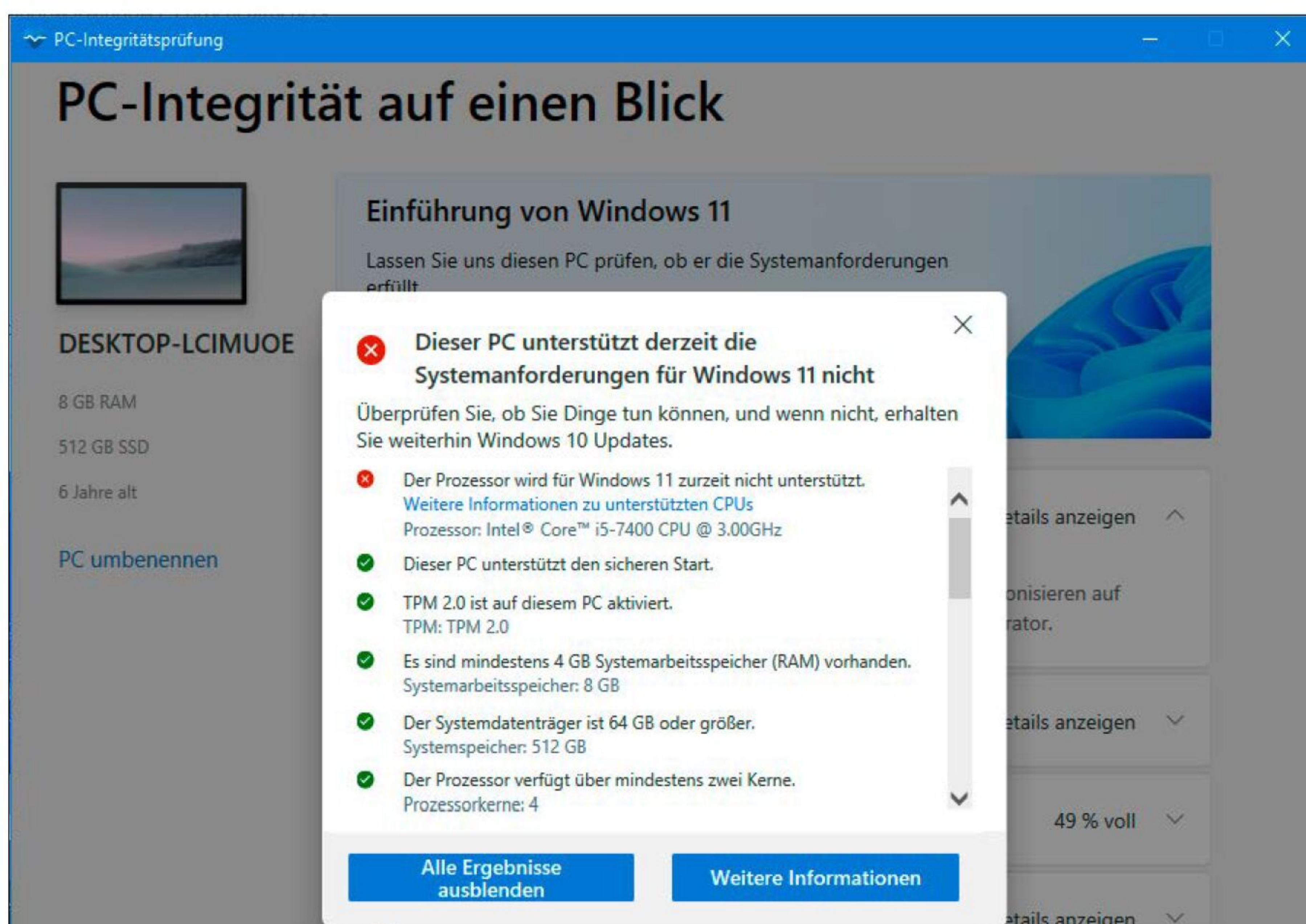
TOOLS FÜR DIE FERNHILFE UND INSTALLATION VON WINDOWS 11



Programm	Beschreibung	Auf	Internet	Sprache
Aomei Backupper Standard	Daten- und System-Backup	Heft-DVD	www.aomei.de/backup-software	Deutsch
App für die PC-Integritätsprüfung	Hardware-Check für Windows 11	-	https://aka.ms/GetPCHealthCheckApp	Deutsch
Easeus Todo Backup Free	Backup- und Kloningtool	Heft-DVD	www.easeus.de	Deutsch
Easeus Todo PC Trans Free	Softwaretransfer von PC zu PC	Heft-DVD	www.easeus.de	Deutsch
Media Creation Tool	Installationsdatenträger für Windows 11	-	https://go.microsoft.com/fwlink/?linkid=2156295	Deutsch
PC-WELT: Support-Aus Windows 10	Ratgeber zum Support-Aus von Windows 10	Heft-DVD	www.pcwelt.de/2591185	Deutsch
PC-WELT: Windows 11 auf alten PCs	Ratgeber zu Windows 11 auf alten PCs	Heft-DVD	www.pcwelt.de/1199049	Deutsch
PC-WELT: Windows 11 wie 10	Ratgeber zum Look and Feel von Windows 11	Heft-DVD	www.pcwelt.de/1203164	Deutsch
Rufus	USB-Sticks für die Windows-Installation	Heft-DVD	https://rufus.ie	Deutsch
Teamviewer	Teamviewer-Fernwartungstool	Heft-DVD	www.teamviewer.com/de/download	Deutsch
Teamviewer Quicksupport	Teamviewer-Schnellverbindung	Heft-DVD	www.teamviewer.com/de/download	Deutsch
UnigetUI	Oberfläche für Windows-Paketmanager	Heft-DVD	www.marticliment.com/unigetui	Deutsch
Windows-11-Installationsassistent	Upgradetool auf Windows 11	Heft-DVD	https://go.microsoft.com/fwlink/?linkid=2171764	Deutsch



Wenn Windows Update statt der Upgrademöglichkeit auf Windows 11 diese Meldung zeigt, können Sie den Umstieg auf das aktuelle Betriebssystem erzwingen – auch aus der Ferne.



PC-Integritätsprüfung: Erfüllt ein Rechner die Hardwareanforderungen an Windows 11 nicht, lässt sich das Setup des Betriebssystems über einen modifizierten Installationsstick erzwingen.

Kompatible Computer von Windows 10 auf 11 upgraden

Status quo prüfen: Falls auf dem anderen PC Windows 10 läuft und Sie die Hardware nicht im Detail kennen, checken Sie mit Microsofts **App für die PC-Integritätsprüfung**, ob der Rechner die Systemvoraussetzungen des neuen Betriebssystems erfüllt. Ist das nicht der Fall, zeigt die App auch den Grund. Heißt es dagegen „Dieser PC erfüllt die Anforderungen von Windows

11“, können Sie die Installation einfach über das Windows-Update vornehmen. Halten Sie davor aber bitte kurz Rücksprache, schließlich muss Ihr Gegenüber danach mit dem neuen System arbeiten und zurechtkommen.

Das Upgrade von Windows 10 auf 11 dauert abhängig von der Leitung der Komponenten maximal rund 30 Minuten. Da beim Umstieg alle Programme, Daten und Einstellungen erhalten bleiben, kann man im

Prinzip mit dem neuen System sofort weiterarbeiten. Auch die vorhandene Windows-10-Lizenz bleibt in den meisten Fällen für Windows 11 gültig, Sie müssen also keine neue kaufen. Mehr dazu lesen Sie unter www.pcwelt.de/article/1161247.

Upgrade erzwingen: Wird die Umstiegsoption auf Windows 11 im Windows Update trotz eigentlich kompatibler Hardware nicht angeboten, können Sie das Upgrade erzwingen: entweder über den **Windows-11-Installationsassistenten** oder über das **Media Creation Tool**. Mit einem dieser beiden Microsoft-Programme startet der Upgradeprozess in aller Regel, die Suche nach der Ursache können Sie sich also sparen. Auch hier übernimmt Windows 11 alle bestehenden Programme, Daten und Einstellungen.

Wenn das Upgrade an den Systemvoraussetzungen scheitert

Mühsamer wird es, wenn der Windows-10-PC den Hardwareanforderungen für Windows 11 nicht genügt. Zwar lässt sich die Setupsperre auf fast allen PCs aus den vergangenen zehn Jahren über einen mit **Rufus** modifizierten Installationsstick umgehen. Dieser muss jedoch am ferngewarteten PC in eine bootfähige USB-Buchse gesteckt werden, da sind Sie also auf Mithilfe angewiesen. Abhängig vom Kenntnisstand Ihres Gegenübers kann dabei Videotelefonie über das Smartphone helfen, zum Beispiel über Whatsapp.

Tipp: Eleganter funktioniert der Videosupport mithilfe der App Teamviewer Assist AR (Android und iOS). Damit können Sie Ihrem Partner auf dessen Smartphone im Livebild der Kamera genau zeigen, was wo zu tun ist. Die Unterstützung per Augmented Reality (AR) stellt jedoch hohe Anforderungen an das Mobiltelefon.

Alternativ bleibt die Möglichkeit, dass Sie den USB-Stick zu Hause so konfigurieren, dass Windows 11 auch auf formal nicht kompatibler Hardware läuft, und ihn anschließend per Post verschicken. Auch dann muss er in den Rechner eingesteckt werden, bevor Sie die Installation mit einem Doppelklick auf die Setup.exe-Datei auf dem Stick wieder über Teamviewer starten können. Hinweis: Wie Sie den Stick mit Rufus modifizieren und was sonst auf nicht kompatibler Hardware zu beachten ist, lesen Sie im PC-WELT-Ratgeber „**Windows 11 auf alten PCs**“ auf Heft-DVD.

Mehrere Optionen, um einen Computer ganz neu einzurichten

Noch schwieriger wird die Fernunterstützung, wenn der vorhandene Rechner durch einen neuen mit Windows 11 ersetzt werden soll. Prinzipiell lässt sich das bestehende System mit einem Image- und Kloning-tool wie **Easeus Todo Backup** eins zu eins auf die neue Hardware migrieren und danach auf Windows 11 aktualisieren. Das aber dauert wegen des Zwischenspeicherns der großen Datenmengen seine Zeit, erfordert eine externe Festplatte und diverse Handgriffe – die Erklärungen am Telefon können mühsam sein. Unter Umständen machen Sie das doch besser vor Ort oder lassen sich den alten Computer zuschicken und erledigen es zu Hause. Der Versand eines PCs ist ja durchaus praktikabel.

Alternativ zum Klonen migriert man nur die eigenen Daten und wichtige Programme vom alten auf den neuen PC, Windows 11 ist darauf ja meist vorinstalliert. Sofern am Ort des Geschehens eine ausreichend große Festplatte zur Verfügung steht, sichern Sie darauf über Teamviewer alle wichtigen Daten mit **Aomei Backupper** und übertragen sie von dort anschließend auf den neuen Rechner. Minimale Unterstützung beim Umstecken wird auch hier wieder vorausgesetzt.

Sollen neben den Daten auch die installierten Programme übernommen werden, hilft **Easeus Todo PC Trans Free**. Über die Option „Backup & Wiederherstellung“ sichert das Tool auf dem Windows-10-System die Anwendungen, Daten, Konten und Einstellungen. Dieses Backup wird anschließend auf einem Datenträger, einer Netzwerkfreigabe oder in der Cloud gespeichert und von dort auf den neuen PC wieder eingespielt. Die kostenlose Softwareversion ist auf zwei Gigabyte Daten und fünf Programme beschränkt. Die Pro-Version ohne Limitierung kostet knapp 40 Euro.

Neue Freeware in fast beliebiger Zahl und Auswahl installieren Sie bequem in einem Rutsch über die Funktion „Paket-Bündel“ in **UnigetUI**, das Tool fungiert als Oberfläche für den in Windows integrierten Paketmanager Winget.

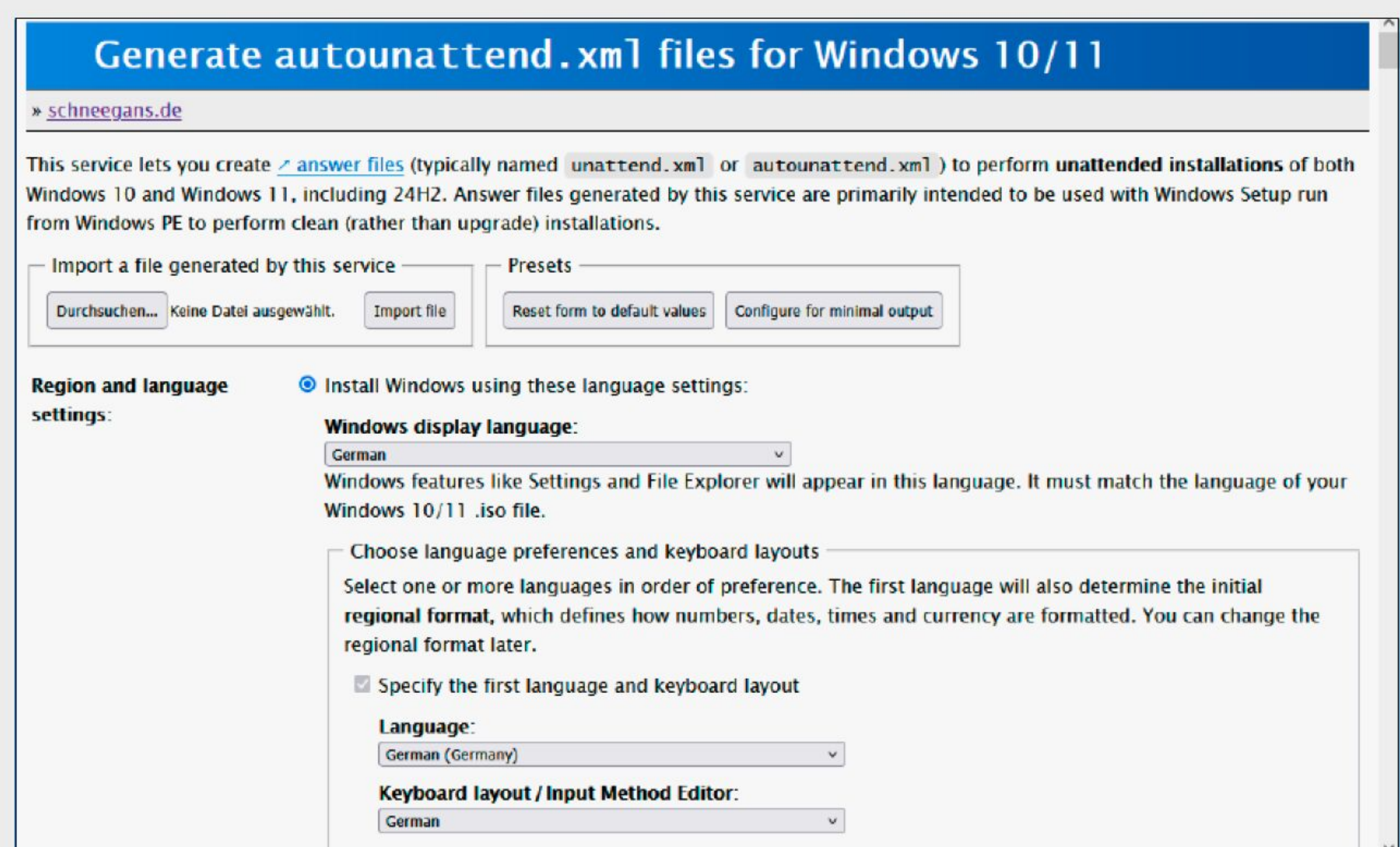
Ein Tipp für alle, die mit Windows 10 vertraut sind: Der Ratgeber „**Windows 11 wie Windows 10**“ auf Heft-DVD erläutert, wie Sie das neue Betriebssystem an das Look and Feel des Vorgängers anpassen. Das erleichtert die Umgewöhnung erheblich. ■



Die Software Easeus Todo PC Trans Free überträgt Daten und Software von einem PC auf einen anderen. Die Gratis-Version ist auf fünf Programme pro Durchgang beschränkt.

UNBEAUF SICHTIGTE WINDOWS-INSTALLATION

Soll Windows 11 ganz neu installiert werden, kommt man um einen Installationsdatenträger und das manuelle Booten vor Ort nicht herum. Der Start vom USB-Stick oder von DVD gelingt nicht per Remotezugriff, sehr wohl können Sie jedoch auch dabei helfen. Dazu recherchieren Sie zunächst die rechnerspezifische Taste zum Aufrufen des Bootmenüs, beim eigentlichen Setupprozess helfen Sie am Telefon. Möglichst einfach machen Sie es Ihrem Gegenüber mit einer unbeaufsichtigten Installation, die alle Einstellungen und Bestätigungen zu Konto, Datenschutz und anderem mehr überspringt. Einen Teil dessen spart bereits die Konfiguration des Setupsticks mit Rufus. Für die komplette Automatisierung nutzen Sie einen Unattended-Generator, zum Beispiel den unter <https://schneegans.de/windows/unattend-generator>. Er erzeugt nach Ihren Vorgaben eine Autounattended.xml-Datei, die Sie auf die oberste Ebene vom Installationsstick kopieren. Damit läuft das Setup von selbst durch.



Mithilfe eines Unattended-Generators im Internet konfigurieren Sie einen USB-Stick so, dass Windows 11 mit allen Wunschvorgaben automatisch ohne jede Bestätigung installiert wird.

PC-Upgrade für Windows 11

Komponenten tauschen statt neu kaufen: Auch wenn Ihr alter PC offiziell nicht mehr tauglich für Windows 11 ist, muss er nicht zu Elektroschrott werden. Bei vielen Rechnern genügt ein gezieltes Upgrade von Prozessor und Platine, um ihn mit dem neuen Betriebssystem weiter zu nutzen.

VON THOMAS RAU

Mit dem Supportende für Windows 10 müssen sich viele Nutzer nicht nur vom Betriebssystem verabschieden, sondern auch von ihrem Rechner. Selbst wenn dessen Komponenten leistungsfähig genug sind für Windows 11, kann er zu Elektroschrott werden: Denn Microsoft stellt strenge Vorgaben an die Hardware, auf der das neue Betriebssystem laufen darf – vor allem beim Prozessor. Die meisten PCs und Notebooks, die älter als acht Jahre sind, sind daher vom Upgrade ausgeschlossen – obwohl sie problemlos unter Windows 10 funktionieren und das sicher auch unter Windows 11 täten.

„Ein gezieltes Hardware-Upgrade für Windows 11 ist oft viel günstiger als ein neuer Komplett-PC.“

Um einen PC mit einem Intel-Prozessor tauglich für Windows 11 zu machen, genügt es nicht, nur den Prozessor auszutauschen. Die frische CPU benötigt auch eine neue Hauptplatine, weil sie ein unterschiedliches Sockelformat hat.



© ASUS

Doch mit kleinen Hardware-Upgrades können Sie Ihren Rechner offiziell fit für Windows 11 machen: Ob sich das lohnt, ob es überhaupt möglich ist und wie viel es kostet, hängt vom konkreten PC oder Notebook ab. Im besten Fall müssen Sie nur den Prozessor tauschen. Doch selbst die Investition in mehrere neue Hardwarekomponenten kann günstiger sein, als sich einen neuen Windows-11-Rechner zu kaufen. Sie müssen sich nur zutrauen, diese austauschen und einbauen zu können.

Wir geben Ihnen sinnvolle Upgrade-Tipps für Ihre Hardware, erklären, wie Sie bei Komponentenauswahl und -einbau am besten vorgehen und wie Sie Ihren Rechner so ausstatten, dass er auch für künftige Windows-Versionen gerüstet ist.

Das braucht Ihr Rechner für Windows 11

Die Anforderungen, die Microsoft für Windows 11 an einen Rechner stellt, sehen auf den ersten Blick gering aus: Der Prozessor mit 64-Bit-Unterstützung muss mindestens zwei Kerne und eine Taktrate von 1 GHz aufweisen, der Arbeitsspeicher 4 GB und das Laufwerk 64 GB groß sein. Das erfüllen viele alte Rechner ebenso wie den Anspruch an eine Grafikkarte mit DirectX 12: Selbst über zehn Jahre alte PCs warten mit passenden Komponenten auf.

Ähnliches gilt für Microsofts Verlangen nach einer Hauptplatine, die eine UEFI-Firmware mit der Funktion Secure Boot besitzt: Schon für Rechner mit Windows 8 war das vorgeschrieben, daher sollten Komplett-Systeme seit 2013 damit ausgestattet sein.

Problematischer ist die Forderung nach TPM 2.0: Im Trusted Platform Module speichert Windows Sicherheitsschlüssel, es überwacht außerdem den PC-Startvorgang, um sicherzustellen, dass keine Malware aktiv ist, bevor Windows lädt. Für Komplett-Systeme mit Windows 10 war TPM 2.0 Pflicht, sodass Rechner, die seit Ende 2016 verkauft wurden, entsprechend ausgestattet sein sollten. Vorher waren PCs und Notebooks üblicherweise mit TPM 1.2 ausgestattet – was sie aus Microsofts Sicht zu unsicher für Windows 11 macht.

An einer Hürde beim Umstieg auf Windows 11 werden aber die meisten Rechner scheitern: Sie brauchen laut Microsoft unbedingt einen Prozessor, der auf der offiziellen Kompatibilitätsliste steht, die es für Modelle von Intel (<https://tinyurl.com/pnk9pvvx>), AMD (<https://tinyurl.com/mtzws3ht>) und Qualcomm (<https://tinyurl.com/ydwwyxwv>) gibt. Damit scheiden alle für Privatanwender bestimmten Rechner aus, die mit einem Intel-Prozessor vor der 8. Core-Generation („Coffee Lake“, „Kaby Lake R“, „Kaby Lake G“, „Amber Lake Y“) ausgestattet sind oder einer

WhyNotWin11

v 2.6.1.1

Update suchen

ITMPTRFUJ1

FUJITSU D3223-A1 @ V4.6.5.4 R1.43.0 for D3223-A1x

Ihre Windows 11 Kompatibilitätsergebnisse

Architektur

64-Bit-CPU
64-Bit-Betriebssystem

Boot Methode

Legacy

CPU-Kompatibilität

nicht unterstützt

CPU-Kernanzahl

2 Kerne
4 Threads

CPU-Frequenz

3100 MHz

DirectX 12 und WDDM 2

DirectX 12 und WDDM 2

Partitionstyp

GPT nicht erkannt

Installierter RAM

8 GB

Secure Boot

deaktiviert oder nicht erkannt

Verfügbarer Speicher

C: 232 GB
Laufwerk(e) kompatibel

TPM-Version

deaktiviert oder nicht erkannt

Update suchen

ITMPTRFUJ1

FUJITSU D3223-A1 @ V4.6.5.4 R1.43.0 for D3223-A1x

Intel(R) Core(TM) i3-4160T

Intel(R) HD Graphics 4400

PC-Integritätsprüfung

PC-Integrität auf einen Blick

ITMPTRFUJ1

8 GB RAM

290 GB SSD

7 Jahre alt

PC umbenennen

Einführung von Windows 11

Lassen Sie uns diesen PC prüfen, ob er die Systemanforderungen erfüllt.

Wenn dies der Fall ist, können Sie das kostenlose Upgrade abrufen, wenn es verfügbar ist.

Jetzt überprüfen

Windows-Sicherung

Details anzeigen

Windows Update

Details anzeigen

Speicherkapazität

86 % voll

Startzeit

Details anzeigen

Info

Verwandter Link

Mehr über Windows 11

Auch bei sehr alten PCs sind fast nie RAM, SSD, die Prozessorakttrate oder die Zahl seiner Kerne der Grund, warum Windows 11 nicht installiert werden kann. Ihnen fehlen aber Sicherheitsfunktionen wie etwa Secure Boot.

Mit der PC-Integritätsprüfung von Microsoft testen Sie mit einem Klick, ob Ihr Rechner fit für Windows 11 ist. Das Tool checkt dafür unter anderem den Prozessor und die Uefi-Einstellungen.

AMD-CPU, deren Kerne nicht mindestens auf der Architektur Zen+ basieren. Komplet-Systeme mit einer unterstützten CPU gab es ab dem Frühjahr 2018 – ist Ihr Rechner also älter als sieben Jahre, lässt sich Windows 11 ohne Umwege nicht installieren. Konsequenter ist die Microsoft-Liste aber nicht: Als tauglich für Windows 11 stehen auch ältere Prozessoren darauf wie der Intel Core i7-7820HQ von Anfang 2017 oder jüngere wie der AMD Athlon 3000G von Ende 2019, der auf der Zen-Architektur basiert, obwohl andere Prozessoren mit dieser Architektur ausgeschlossen sind. Für das Windows-Update 24H2 hatte Microsoft im Februar 2025 neue Listen für die einzelnen Prozessorhersteller veröffentlicht: Sie enthalten vor allem aktuellere CPU-Modelle. Allerdings fallen auch einige CPUs weg, die zuvor als unterstützt gelistet waren – darunter auch einzelne Modelle aus Generationen, die eigentlich als kompatibel zu Windows 11 gelten. Ob das verse-

hentlich oder absichtlich geschah, ist unklar. Denn eigentlich richten sich diese Listen an PC-Hersteller (OEMs), nicht an Privatanwender. Gerade bei älteren Prozessoren geben sie Ihnen keine endgültige Gewissheit, ob eine bestimmte CPU von Windows 11 unterstützt wird – und selbst, falls es jetzt der Fall sein sollte, ob dies auch für künftige Updates des Betriebssystems gilt.

So prüfen Sie, ob der PC fit für Windows 11 ist

Wenn Ihr Rechner in seiner derzeitigen Ausstattung tauglich für Windows 11 ist, bekommen Sie in regelmäßigen Abständen die Aufforderung, auf das neue System umzusteigen. Auch in den Einstellungen unter „Windows Update“ weist Windows 10 mit einem großen Fenster darauf hin. Ist das bei Ihnen nicht der Fall, können Sie mit Tools prüfen, wie es um die Windows-11-Tauglichkeit Ihres PCs bestellt ist. Von Microsoft kommt dafür die PC-Integritäts-

prüfung (PC Health Check). Sie ist bei vielen Rechnern vorinstalliert, andernfalls laden Sie sie unter <https://tinyurl.com/9c6hb2fd> herunter. Den Check starten Sie über die blaue Schaltfläche „Jetzt überprüfen“. Erfüllt der Rechner die Anforderungen für Windows 11, sind das Gesamtergebnis und die Ergebnisse bei den einzelnen Komponenten grün markiert. Eine gelbe Markierung bedeutet, dass das Tool für eine bestimmte Anforderung den Test nicht durchführen konnte, weil die Komponenten oder die Funktion nicht erkannt oder bislang nicht aktiviert wurde – zum Beispiel, weil Secure Boot abgeschaltet ist. Ein Kreuz in einem roten Kreis zeigt, dass diese Komponente das Upgrade auf Windows 11 verhindert – in den meisten Fällen der Prozessor. Der Altersangabe, die im Startbildschirm des Tools links angezeigt wird, dürfen Sie übrigens nicht trauen – die Software rät sie einfach anhand bestimmter System-Infos, die aber nichts mit dem tatsächlichen Alter

WINDOWS 11: SO VIEL KOSTET DAS PC-UPGRADE

Plattform	Alte CPU-Generation (Beispiel)	Neue Plattform (Sockel, CPU-Generation)	Gesamtkosten (€)*	Neue CPU (Beispiel)	CPU (€)	Platine (€)	RAM (€)
Intel	Skylake / Kaby Lake (z. B. i7-6700, i5-7400), 2015-2017	LGA1200 (Rocket Lake), 2021	200	Core i5-11400	140	60	-
Intel	Skylake / Kaby Lake (z. B. i7-6700, i5-7400), 2015-2017	LGA1700 (Raptor Lake-R), 2024	230	Core i5-14400	160	70	-
Intel	Skylake / Kaby Lake (z. B. i7-6700, i5-7400), 2015-2017	LGA1851 (Arrow Lake), 2025	410	Core Ultra 5 225	260	110	40
AMD	Ryzen 1000 (Ryzen 7 1700), 2017	AM4 (Vermeer), 2021	200	Ryzen 7 5800X	200	-	-
AMD	Ryzen 1000 (Ryzen 7 1700), 2017	AM5 (Raphael), 2023	310	Ryzen 5 7600	190	80	40

* Die Gesamtkosten umfassen die notwendigen Komponenten für Windows 11. Je nach Rechner kommen Kosten für ein neues Netzteil, eine neue SSD oder RAM hinzu.

PC-WELT SONDERHEFT XXL 3/2026

53

!

Dieser PC unterstützt derzeit die Systemanforderungen für Windows 11 nicht

Überprüfen Sie, ob Sie Dinge tun können, und wenn nicht, erhalten Sie weiterhin Windows 10 Updates.

!

Dieser PC muss den sicheren Start unterstützen.
[Weitere Informationen zum Aktivieren des sicheren Starts](#)

!

TPM 2.0 muss auf diesem PC unterstützt und aktiviert sein.
[Weitere Informationen zum Aktivieren des TPM 2.0](#)
TPM: TPM nicht erkannt

✖

Der Prozessor wird für Windows 11 zurzeit nicht unterstützt.
[Weitere Informationen zu unterstützten CPUs](#)
Prozessor: Intel® Core™ i3-4160T CPU @ 3.10GHz

Alle Ergebnisse ausblenden

Weitere Informationen

Dieser PC mit einem Intel-Prozessor aus 2013 wird kein Upgrade auf Windows 11 erhalten. Neben CPU und TPM fehlt ihm zudem eine Platine mit Uefi-Firmware, die Secure Boot beherrscht.

nology“ Ausschau halten. Die entsprechenden Optionen bei einem AMD-Rechner heißen „AMD fTPM Switch“ oder „AMD PSP fTPM“. Stellen Sie sie auf „On“, „Enabled“ beziehungsweise „Aktiviert“.

Diese Hardware müssen Sie für Windows 11 tauschen

Für einen älteren PC führt der Weg zu Windows 11 meist über den Wechsel des Prozessors: An sich erfüllen auch ältere CPUs einige Anforderungen von Microsoft – sie bringen meist TPM 2.0 mit, und ihre Hauptplatine bietet eine Uefi-Firmware mit Secure Boot. Doch die Modelle auf der Kompatibilitätsliste verfügen über zusätzliche Funktionen, die ihre Vorgänger nicht besitzen und die sich nicht nachträglich per Update ergänzen lassen: Meist handelt es sich um Sicherheitsvorkehrungen gegen Malware-Angriffe auf das Betriebssystem. Am schnellsten und günstigsten machen Sie einen älteren PC deshalb fit für Windows 11, indem Sie ihn mit einem Prozessor ausstatten, den Microsoft erlaubt. Dazu müssen Sie zunächst klären, ob die CPU in Ihrem Rechner auf die Hauptplatine gelötet ist oder dort in einem Sockel sitzt – nur dann lässt sie sich überhaupt austauschen.

Bringen Sie die Modellbezeichnungen der CPU in Erfahrung – zum Beispiel über den Windows-Gerätemanager unter „Prozessoren“, in den Windows-Einstellungen unter „System → Info“ oder mit einem Hardware-Analysetool wie **HWinfo 64** (<https://www.hwinfo.com/download/>) oder **Speccy** (<https://www.ccleaner.com/de-de/speccy>; beide auch auf Heft-DVD).

Anschließend recherchieren Sie auf der Webseite des Prozessorherstellers – zum Beispiel ark.intel.com – nach den technischen Daten für dieses Modell. Hilfreich sind auch die Hardwaretools – bei HWinfo 64 schauen Sie nach „Hauptprozessor → CPU-Plattform“.

Tauchen dort Begriffe wie „Socket“, „PGA“ oder „LGA“ auf, handelt es sich um einen gesockelten Prozessor, der sich grundsätzlich ausbauen lässt. Sehen Sie dagegen das Kürzel „BGA“, auch in der Form „FC-BGA“, ist der Prozessor auf die Platine gelötet – Sie können ihn nicht tauschen.

Üblicherweise sitzt in einem Komplett-PC mit Desktop- oder Tower-Gehäuse ein gesockelter Prozessor, in vielen Notebooks ist die CPU hingegen gelötet. Es gibt aber Aus-

Merkmal	Beschreibung
Allgemeine Informationen	
Prozessorname:	Intel Core i3-3240
Originale Prozessorfrequenz:	3400.0 MHz
CPU ID:	000306A9
CPU-Markennamen:	Intel(R) Core(TM) i3-3240 CPU @ 3.40GHz
CPU-Hersteller:	GenuineIntel
CPU-Stufung:	L1/P0
CPU-Plattform:	Socket H2 (LGA1155)
CPU-Technologie:	22 nm
CPU S-Spec:	SR0RH

Nur wenn der Prozessor auf der Platine in einem Stecksockel sitzt, lässt er sich gegen einen neuen austauschen. Mit Check-Tools wie HWinfo 64 finden Sie heraus, ob das bei Ihrem Rechner der Fall ist.

der Hardware oder der Windows-Installation zu tun haben. Auch die Freeware **Why Not Win 11** (auf DVD, Download unter <https://github.com/rcmaehl/WhyNotWin11>) prüft die Windows-11-Kompatibilität der einzelnen Komponenten und Funktionen: Grün bedeutet bestanden, Rot durchgefallen. Bemängelt das Check-Tool, dass Secure Boot nicht entdeckt werden konnte, kann es daran liegen, dass Sie diese Funktion nicht aktiviert haben. Starten Sie zunächst die Windows-Systeminformation, indem Sie *msinfo32* in das Suchfenster eingeben: In der Zeile „Bios-Modus“ muss „UEFI“ stehen. Wenn bei „Sicherer Startzustand“ die Anzeige „Aus“ steht, unterstützt das Uefi Secure Boot, aber es ist nicht aktiviert. Um Secure Boot einzuschalten, rufen Sie die Uefi-Einstellungen auf: Am zuverlässigsten funktioniert das, indem Sie in den Windows-Einstellungen unter „Update & Sicherheit → Wiederherstellung → Erweiterter Start“ auf „Jetzt neu starten“ klicken. Nach kurzer Zeit erscheint die blaue Pre-Bootumgebung von

Windows: Wählen Sie dort „Problembehandlung → Erweiterte Optionen → UEFI-Firmwareeinstellungen → Neu starten“. Nun ruft der Rechner das Uefi-Setup auf: Je nach Hersteller finden Sie die Optionen für Secure Boot im Kapitel „Boot“, „Sicherheit“ oder „Security“. Dort stellen Sie Secure Boot auf „Enabled“, „Eingeschaltet“, „Uefi“ oder „Windows Uefi Mode“. Nach dem Neustart sollte in den Systeminformationen bei „Sicherer Startzustand“ die Angabe „Ein“ stehen. Ähnlich gehen Sie bei der Prüfung für TPM vor: Geben Sie ins Windows-Suchfenster *tpm.msc* ein. Erscheinen die Infos für ein TPM sowie die Angabe „Spezifikationsversion 2.0“ ist alles in Ordnung, Version „1.2“ genügt für Windows 11 nicht – hier brauchen Sie einen neuen Prozessor. Sehen Sie „Es wurde kein kompatibles TPM gefunden“, ist das TPM möglicherweise kompatibel, aber nicht aktiv. Jetzt müssen Sie erneut das Uefi aufrufen und nach einer Option wie „Security Device“, „TPM State“ oder bei einem Rechner mit Intel-CPU nach „Intel PTT“ beziehungsweise „Intel Platform Trust Tech-

nahmen: All-in-One-PCs oder kleine Mini-PCs nutzen häufig gelötete Notebook-CPUs, während in großen Notebooks – zum Beispiel Spiele- und High-End-Laptops – oft ein gesockelter Prozessor sitzt.

Intel: So wählen Sie einen passenden Prozessor aus

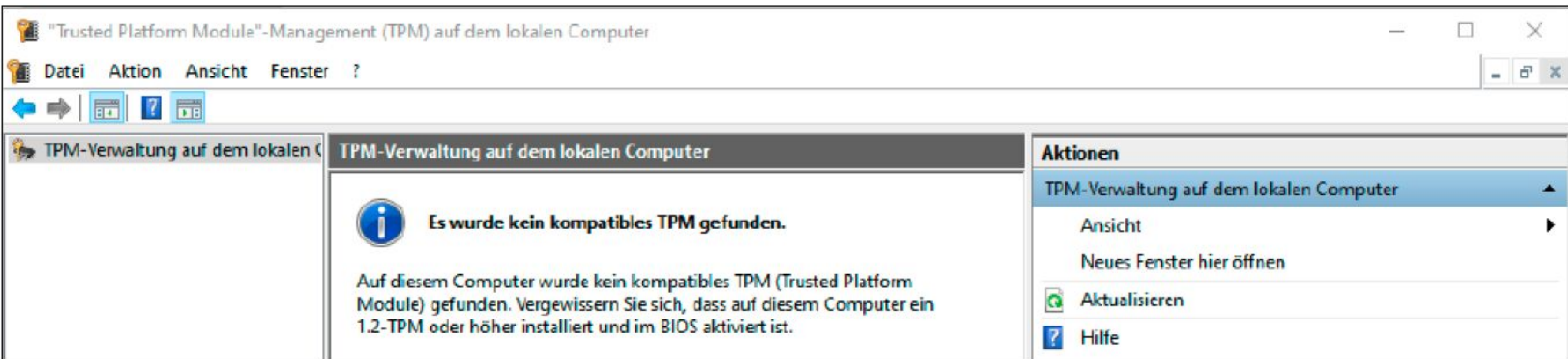
Lässt sich der Prozessor wechseln, ist im nächsten Schritt die Frage zu klären, ob sich stattdessen ein Windows-11-kompatibles Modell einsetzen lässt. Der neue Prozessor muss dazu in den vorhandenen Steckplatz auf der im PC eingebauten Hauptplatine passen.

Bei älteren Rechnern mit Intel-Prozessor stehen Ihre Chancen schlecht: Die gesockelten Modelle aus den CPU-Generationen, die für Windows 11 tauglich sind – ab Coffee Lake –, nutzen einen anderen Steckplatz als ihre Vorgänger. Der heißt zwar auch LGA1151 – aber die Version 1 unterscheidet sich in den elektrischen Anschlüssen von der Version 2 für Coffee Lake: Sie können einen neueren Prozessor daher einsetzen, aber er wird nicht funktionieren. Beim Umstieg auf Windows 11 benötigen Sie bei der Intel-Plattform also einen neuen Prozessor und eine neue Hauptplatine.

Je nachdem, wie leistungsfähig Ihr Rechner nach dem Upgrade sein soll, kostet Sie das Aufrüsten zwischen rund 200 und 500 Euro. Außerdem können Sie beim Neukauf von Prozessor und Platine mehrere CPU-Generationen von Intel überspringen, denn neuere Modelle sind kaum teurer als ältere: Das macht den aktualisierten Rechner nicht nur fit für Windows 11, sondern verschafft ihm einen üppigen Tempozuwachs.

Nutzt Ihr alter PC DDR4-RAM, können Sie den Arbeitsspeicher selbst auf einer Platine für die 14. Core-Generation „Raptor Lake-R“ aus dem letzten Jahr einsetzen: Ein passendes Mainboard wie das Asus Prime H610M kostet rund 70 Euro, einen soliden Mittelklasse-Prozessor wie den Core i5-14400 bekommen Sie als Boxed-Variante mit Kühler für rund 160 Euro.

Deutlich teurer wird es, wenn Sie Ihren alten PC mit der aktuellen CPU-Generation Arrow Lake ausstatten wollen: Günstige Prozessoren wie ein Core Ultra 5-225 kosten rund 260 Euro, eine passende Platine knapp über 100 Euro. Außerdem benötigen Sie dafür DDR5-Arbeitsspeicher, was für 16 GB Kapazität rund 40 Euro ausmacht. Wer nur ein knappes Upgrade-Budget hat, kann bei



Wenn Sie unter Windows die TPM-Verwaltung mit dem Befehl `tpm.msc` öffnen, zeigt Ihnen das System, ob ein entsprechendes Sicherheits-Modul vorhanden und auch eingeschaltet ist. Findet Windows kein TPM im System, müssen Sie es möglicherweise zunächst in den Einstellungen des Uefi-Setups aktivieren.

B450M H (rev. 1.x)											
Key Features Specification Support News & Awards Buy											
CPU Support											
Socket AM4 - AMD B450											
N/A = Not support											
Socket AM4											
Motherboard										Model	B450M H
										PCB	1.x
Vendor	CPU Model	Cores/Thread	Frequency	L2 Cache	L3 Cache	GPU Info.	Core Name	Process	Stepping	Wattage	Since BIOS Version
AMD	Ryzen 9 5950X	16C/32T	3.4GHz / 4.9GHz	8MB	64MB	N/A	Vermeer	7nm	B0	105W	F60
AMD	Ryzen 9 5900XT	16C/32T	3.3GHz / 4.8GHz	8MB	64MB	N/A	Vermeer	7nm	B0	105W	F60
AMD	Ryzen 9 5900X	12C/24T	3.7GHz / 4.8GHz	6MB	64MB	N/A	Vermeer	7nm	B0	105W	F60
AMD	Ryzen 9 3950X	16C/32T	3.5GHz / 4.7GHz	8MB	64MB	N/A	Matisse	7nm	B0	105W	F1
AMD	Ryzen 9 3900XT	12C/24T	3.8GHz /	6MB	64MB	N/A	Matisse	7nm	B0	105W	F2

Bei vielen alten PCs mit AMD-CPU genügt deren Austausch, um sie kompatibel zu Windows 11 zu machen. Prüfen Sie zuvor, ob es für die eingebaute Platine ein Uefi-Bios-Update gibt, das den neuen Prozessor unterstützt.

einem Intel-PC zu einer Platine mit Steckplatz LGA1200 greifen: Dort lassen sich CPUs bis zur 11. Generation Rocket Lake einsetzen, etwa ein Core i5-11400, der mit Lüfter rund 140 Euro kostet. Dazu kommt noch eine LGA1200-Platine wie etwa die Gigabyte H510M v2 für rund 60 Euro.

Kosten für ein neues Laufwerk entstehen in keinem Fall: Alle Platinen für die dargestellten Upgrade-Optionen besitzen M.2- und SATA-Anschlüsse, sodass Sie eine vorhandene SSD weiter nutzen können – außer, Sie benötigen einen Flash-Speicher mit größerer Kapazität. Die günstigsten M.2- und SATA-SSDs mit 512 GB liegen bei rund 30 Euro – für M.2 genügt eine SSD mit PCI-Express 3.0, weil die empfohlenen Platinen keine höhere PCIe-Version für das Laufwerk unterstützen.

In vielen Fällen können Sie Ihr vorhandenes Netzteil weiter nutzen: Dessen Anschlüsse sollten für die neue Platine und die neuen Komponenten passen, sofern Sie keine leistungsfähige Grafikkarte einsetzen. Allerdings ist der Austausch des Netzteils bei einem Rechner, der sechs Jahre oder älter ist, grundsätzlich empfehlenswert.

Hardware-Upgrade bei einem AMD-Rechner

Günstiger ist der Upgrade-Weg zu Windows 11, wenn Sie einen Rechner mit AMD-Prozessor besitzen: Den Sockel AM4 für die älteren Prozessoren führte der Hersteller bis 2022 weiter. Deshalb lässt sich zum Beispiel ein Ryzen 7 1700, der nicht mit Windows 11 funktioniert, durch einen Prozessor aus der Ryzen-5000er-Serie ersetzen, wie den Ryzen 7 5700 oder den Ryzen 7 5800XT. Diese Modelle sind immer noch gut verfügbar und kosten zwischen 120 und rund 180 Euro mit Kühler.

Bevor Sie den neuen Prozessor kaufen, prüfen Sie, ob Ihre vorhandene Hauptplatine ihn unterstützt: Der Hersteller muss ein passendes Uefi-Update bereitstellen, was sich auf den Support-Seiten für die entsprechende Platine herausfinden lässt. Den eingebauten Arbeitsspeicher und eine vorhandene SSD können Sie weiter nutzen. Wie bei Intel unterstützen neuere AMD-Prozessoren zwar höhere Taktraten für DDR4: Im PC-Alltag fällt es aber meist kaum auf, dass der vorhandene DDR4-Speicher im alten Rechner etwas langsamer läuft. ■

Der perfekte Notfall-Stick

Die Tools auf der Heft-DVD eignen sich für die Analyse und Beseitigung von Windows-Problemen. Packen Sie alles auf einen USB-Stick, damit bei Bedarf eine nützliche Werkzeugsammlung sofort bereitsteht.



© Mit Material von fluffy clouds - AdobeStock

VON THORSTEN EGGELING

Nicht immer läuft bei Windows alles reibungslos, und die möglichen Problemquellen sind zahlreich. Besonders häufig sind Fehler beim automatischen Windows-Update, ein verlangsamer Start oder Bootprobleme. Vieles kann mit Windows-Bordmitteln untersucht und behoben werden, zusätzliche Tools (auf Heft-DVD) bieten mehr Funktionen und Möglichkeiten. Fast alle im Artikel genannten Programme sind portabel. Das bedeutet, die Tools lassen sich direkt starten und eignen sich daher hervorragend für einen USB-Stick, den man für Notfälle bereithält. Eine externe USB-Festplatte oder ein beliebiges anderes Laufwerk können Sie ebenfalls verwenden. Ein USB-Stick hat den Vorteil, dass Sie ihn einfach mitnehmen können, etwa um einem Bekannten bei PC-Problemen zu helfen.

„Ein USB-Stick mit portablen Tools für die Analyse und Reparatur hilft bei Windows-Problemen.“

Den USB-Stick für die Toolsammlung vorbereiten

Sie können jeden USB-Stick mit ausreichend freier Kapazität und dem Dateisystem exFAT, NTFS oder FAT32 verwenden. Neben den portablen Tools kann der USB-Stick auch andere Daten enthalten.

Die gewünschten Tools können Sie einzeln auf dem USB-Stick einrichten. Die meisten stammen von <https://portableapps.com> und werden mit einem Installer geliefert, der das Programm in das Zielverzeichnis entpackt. Sie können auch den Programmstarter **PortableApps.com Platform** auf dem Stick einrichten und dann die Tools zum Download wählen. Der Vorteil: Der Starter bietet auch Updates an, und Sie halten damit die Toolsammlung stets aktuell.

PC-WELT Windows Cleaner-Kit ist ein Starter für ausgewählte Programme. Der Schwerpunkt liegt bei Aufräumtools wie CCleaner und Bleachbit, es sind aber auch Programme für die Hardware-Analyse und die Windows-Reparatur dabei. Jedes Tool ist mit einer Beschreibung versehen, die in die grundlegenden Funktionen einführt.

Windows System Control Center (WSCC) ist ein weiterer Programmstarter für den USB-Stick. Beim ersten Start wählen Sie aus, was Sie herunterladen möchten. WSCC bietet vor allem Tools der Sysinternals Suite wie **Autoruns** und **Process Explorer** an, aber auch von Nirsoft und Mitec.

Bootfähiger USB-Stick: Wenn der Stick auch bootfähig sein soll, etwa um die Windows-Wiederherstellungsumgebung oder das Lazesoft-Rettungsmedium zu starten, muss er neu formatiert werden. Die darauf befindlichen Dateien müssen Sie vorher sichern. Verwenden Sie **Rufus**, um einen USB-Stick für die Windows-Installation und -Reparatur zu erzeugen. Die ISO-Datei für Windows 11 erhalten Sie von Microsoft über <https://tinyurl.com/dw11iso>.

Ein mit **Ventoy** erstellter USB-Stick ist flexibler. Er kann mehrere ISO-Dateien aufnehmen, die sich direkt booten lassen. Der USB-Stick muss einmal neu formatiert werden. Sichern Sie deshalb alle darauf befindlichen Dateien.

Starten Sie Ventoy2Disk.exe und wählen Sie unter „Device“ den USB-Stick. Unter „Option“ deaktivieren Sie „Secure boot support“, und im Firmware-Setup des PCs muss Secure Boot ebenfalls deaktiviert sein. Andernfalls müssen Sie den Ventoy-Sicherheitsschlüssel umständlich importieren (siehe www.ventoy.net/en/doc_secure.html).

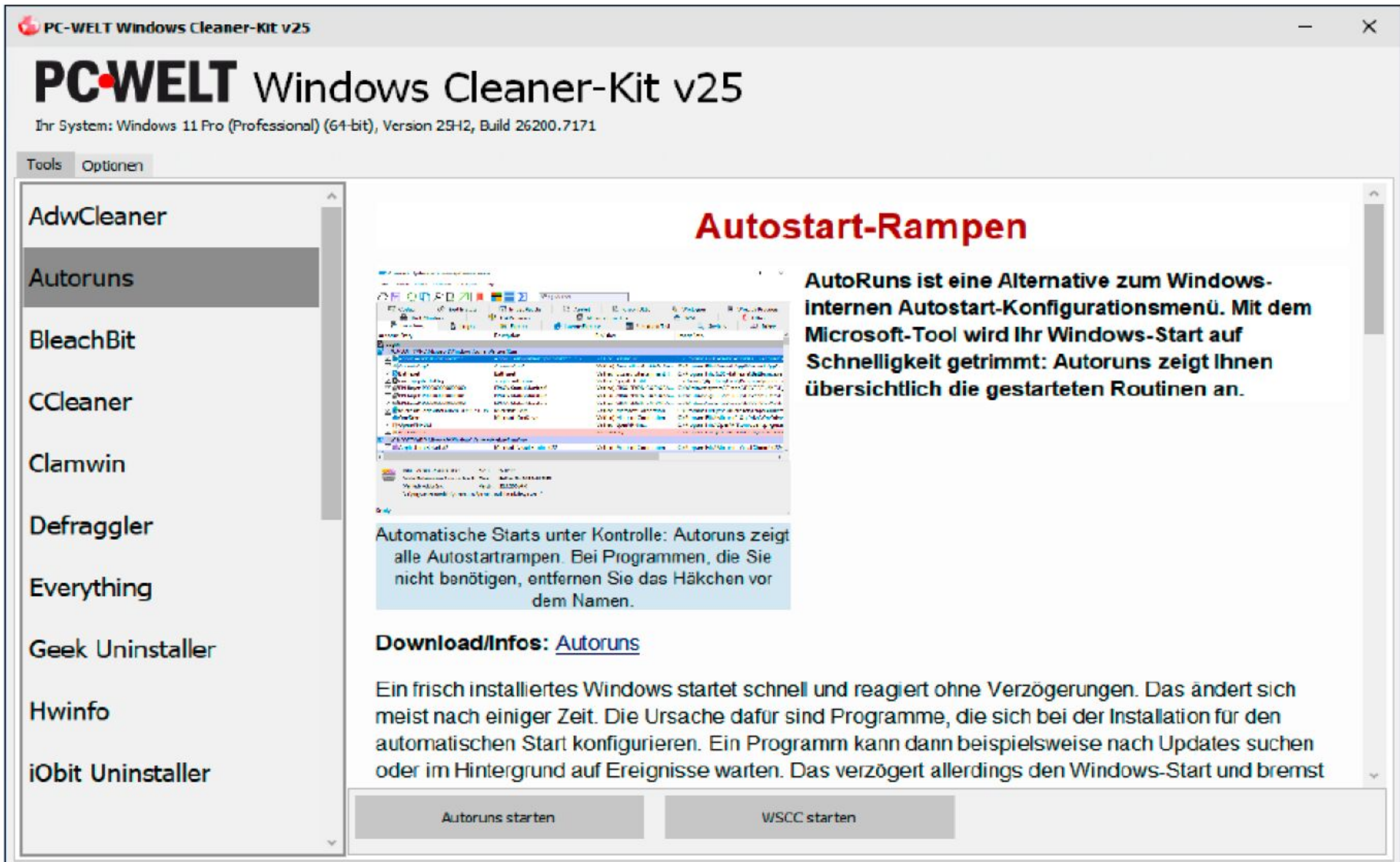
Klicken Sie auf „Install“. Der Stick wird neu formatiert, alle enthaltenen Daten gehen verloren. Kopieren Sie die gewünschten ISO-Dateien und andere benötigte Tools auf den Stick.

Booten Sie den PC vom USB-Stick. Im Menü wählen Sie anschließend die gewünschte ISO-Datei aus.

Ein Tool für die Analyse und Windows-Reparatur

Windows Repair Free kann zahlreiche Windows-Probleme beheben, etwa Dateiberechtigungen zurücksetzen, Systemdateien neu registrieren oder das Windows-Update reparieren. Richten Sie das Tool von der Heft-DVD ein oder starten Sie es über PC-WELT Windows Cleaner-Kit. Nach dem Start wählen Sie als Sprache „German | Deutsch“. Windows Repair empfiehlt, alle Reparaturen im abgesicherten Modus durchzuführen. Das ist zwar nicht zwingend erforderlich, verspricht aber mehr Erfolg. Sie sollten dem Vorschlag daher folgen. Klicken Sie auf „Neustart im abgesicherten Modus“ und bestätigen Sie mit „Ja“. Sobald Windows wieder läuft, starten Sie Windows Repair erneut.

- Schritt 1:** Folgen Sie dem Assistenten, indem Sie auf „Zu Schritt 1 gehen“ klicken. Sie erhalten die Empfehlung, Windows neu zu starten. Wenn Sie Windows – wie empfohlen – im abgesicherten Modus neu gestartet haben, ist das bereits erledigt.
- Schritt 2:** Klicken Sie auf die Schaltfläche mit dem Pfeil nach rechts, dann auf „Vorab-Scan aufrufen“ und auf „Scan starten“. Sollten im Ergebnis Informationen über nicht vorhandene „reparse points“ auftauchen, ignorieren Sie das. Gemeint sind Verknüpfungen im Benutzerprofil, etwa zu „Start-



Toolsammlung für den USB-Stick: Über PC-WELT Windows Cleaner-Kit starten Sie Aufräum- und Wartungstools vom Stick. Die Beschreibungen erläutern die Funktionen der Tools.

menü“ und „Anwendungsdaten“. Das Tool kennt jedoch nur die englischsprachigen Bezeichnungen und zeigt daher bei einem deutschsprachigen Windows Fehler an. Sie sollten deshalb auch nicht auf „Reparse-Punkte reparieren“ klicken. Verwaiste Pfade in Umgebungsvariablen zeigt Windows Repair ebenfalls an, was Sie nach einem Klick auf „Umgebungsvariablen reparieren“ beheben können. Ungültige Pfade verursachen zwar keine Fehler, die Länge der Variablen ist jedoch auf 2048

Zeichen begrenzt. Sollte diese Länge überschritten werden, schneidet Windows den darüber hinausgehenden Teil einfach ab, und die Pfadangaben fehlen dann. Um die Länge zu reduzieren, sollten Sie daher überflüssige Pfade entfernen.

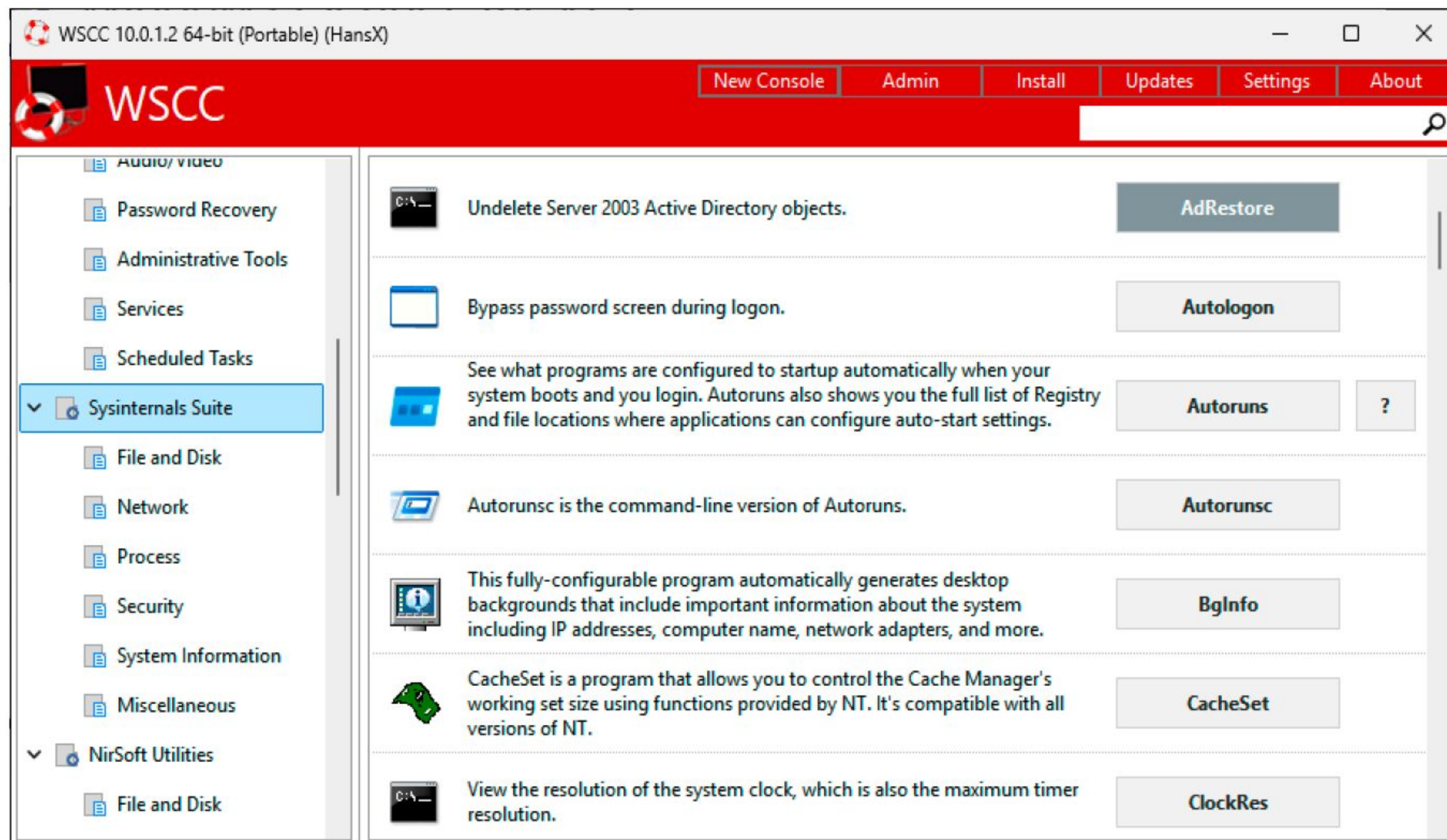
Schritt 3: Im nächsten Schritt klicken Sie auf „Prüfen“, um einen Check des Dateisystems einzuleiten. Dieser sollte ohne Fehler abgeschlossen werden. Andernfalls klicken Sie auf „Beim nächsten Booten Datenträger prüfen aufrufen“ und wählen die erste Op-

IM ÜBERBLICK: TOOLS FÜR DEN USB-STICK



Name	Beschreibung	Auf	Internet	Sprache
AS SSD Benchmark	Benchmark-Test für Laufwerke	Heft-DVD	www.alex-is.de	Englisch
Autoruns	Autostart-Programme deaktivieren	Heft-DVD*	https://tinyurl.com/SIAUTOR	Englisch
Clam Win Portable	Virens scanner	Heft-DVD*	https://clamwin.com	Englisch
CPU-Z Portable	Infos zum Prozessor ermitteln	Heft-DVD	www.cpuid.com	Englisch
Crystal Disk Info Portable	Laufwerksinformationen ermitteln	Heft-DVD	https://crystallmark.info	Deutsch
Crystal Disk Mark Portable	Benchmark für Laufwerke	Heft-DVD	https://crystallmark.info	Deutsch
Emsisoft Emergency Kit	Virens scanner	Heft-DVD	www.emsisoft.com	Deutsch
GPU-Z	Infos zum Grafikchip abrufen	Heft-DVD	www.techpowerup.com	Englisch
Hwinfo Portable	Informationen zur Hardware ermitteln	Heft-DVD*	www.hwinfo.com	Deutsch
Lazesoft Recovery Suite	Rettungssystem mit Backup- und Reparaturfunktionen	Heft-DVD	www.lazesoft.com	Englisch
PC-WELT Windows Cleaner-Kit	Starter für einige portable Tools	Heft-DVD	www.pcwelt.de/1158389	Deutsch
PCI-Z	Infos zu Hardware am PCI-Bus	Heft-DVD	www.pci-z.com	Englisch
PortableApps.com Platform	Starter für portable Programme	Heft-DVD	https://portableapps.com	Deutsch
Process Explorer Portable	Laufende Prozesse untersuchen	Heft-DVD*	https://learn.microsoft.com/de-de/sysinternals	Englisch
Rufus Portable	Bootfähigen USB-Stick erzeugen	Heft-DVD	https://rufus.ie	Deutsch
SSD-Z	Zeigt Informationen zu SSDs	Heft-DVD	http://aezay.dk	Englisch
Ventoy	Multiboot-Stick erzeugen	Heft-DVD	www.ventoy.net	Deutsch
Windows Repair Free Portable	Windows-Reparaturen durchführen	Heft-DVD*	www.tweaking.com	Deutsch
Windows System Control Center (WSCC)	Tool von Microsoft und Nirsoft herunterladen	Heft-DVD*	www.kls-soft.com	Englisch

*auch in PC-WELT Windows Cleaner-Kit enthalten.



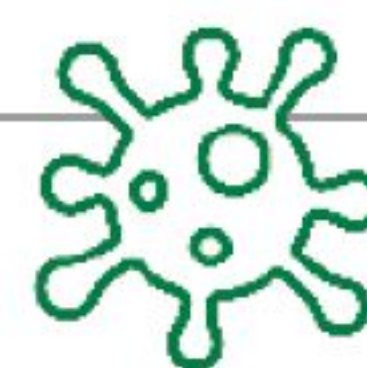
Windows System Control Center: Mit WSCC laden Sie nützliche Tools von Microsoft-Sysinternals und Nirsoft herunter, die Sie über die grafische Oberfläche starten können.

tion mit der Bezeichnung „(/F) Behebt Fehler auf dem Datenträger“. Klicken Sie auf die Schaltfläche „Zum nächsten Boot hinzufügen“ und starten Sie Windows neu. Nachdem die Datenträgerreparatur abgeschlossen ist, starten Sie Windows über Windows Repair erneut im abgesicherten

Modus, rufen das Tool wieder auf, überspringen die ersten drei Schritte und fahren mit dem letzten Schritt fort.

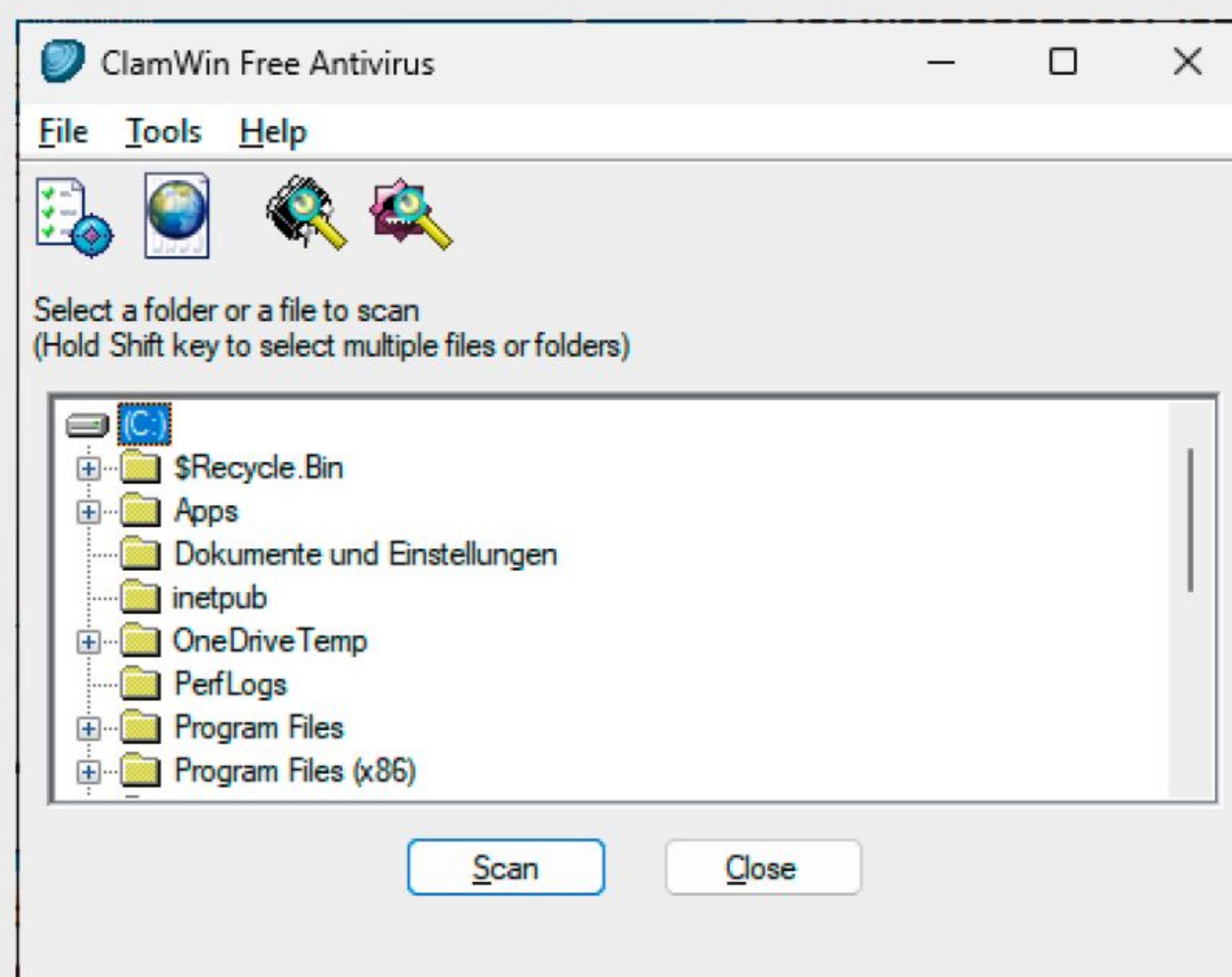
Schritt 4: Klicken Sie auf „Prüfen“. Jetzt kommen „sfc /scannow“ und einige dism-Befehle zum Einsatz, mit denen die Systemdateien überprüft werden.

SCHADSOFTWARE AUF DEM PC FINDEN



Ein Virens Scanner sollte auf jedem Windows-PC installiert sein. Manchmal kann es jedoch sinnvoll sein, eine zweite Meinung einzuholen, etwa nach dem Download einer Datei. Dafür können Sie **Clam Win** verwenden, einen kostenlosen Open-Source-Virens Scanner. Beim ersten Start laden Sie die Virendefinitionen herunter. Danach klicken Sie das Laufwerk an, das Sie untersuchen wollen. Per Doppelklick öffnen Sie den Verzeichnisbaum, und Sie können dann auch einen einzelnen Ordner wählen. Nach einem Klick auf „Scan“ startet der Virens Scan. Der Vorgang kann bei umfangreichen Verzeichnissen eine lange Zeit dauern. Nach dem Scan gehen Sie auf „Tools → Display Reports → Scan Report“. Damit öffnen Sie eine Textdatei, die Informationen zu den infizierten Dateien enthält.

Emsisoft Emergency Kit kann auf einem USB-Stick eingerichtet werden. Das Programm bietet einen Schnelltest, mit dem Sie nur die gerade aktiven Programme prüfen. Nach einem Klick auf „Eigener Scan“ können Sie einzelne Laufwerke oder Ordner angeben, in denen das Tool nach Schadsoftware suchen soll.



Clam Win Portable: Der einfache Virens Scanner kann ganze Laufwerke oder nur einzelne Ordner auf Schadsoftware prüfen. Das Ergebnis des Scans finden Sie in einer Report-Datei.

Schritt 5: Der letzte Schritt im Assistenten bietet „Sicherungswerkzeuge“. Sie sollten zumindest das angebotene Backup der Registry wahrnehmen. Bei Problemen lässt sich die Registry im abgesicherten Modus nach Klicks auf „Wiederherstellen“ und „Restore Registry“ zurücksichern.

Mit diesen Vorbereitungen haben Sie die grundlegenden Fehlerquellen beseitigt, etwa defekte Systemdateien. Gehen Sie jetzt auf „Reparaturen – Hauptteil“. Klicken Sie beispielsweise auf „Voreinstellung: Windows-Update“, wenn Sie die Update-Funktionen reparieren möchten. Unter „Reparaturen“ ist vor allen Optionen ein Häkchen gesetzt, die Auswirkungen auf das Windows-Update haben. Klicken Sie auf „Reparaturen starten“. Nach Abschluss der Reparaturen starten Sie Windows neu.

Windows Repair bietet auch Voreinstellungen für „Malware Cleanup Repairs“, was Sie nach der Entfernung von Schadsoftware durch einen Virens Scanner verwenden. Oder Sie wählen „Common Repairs“, über das sich mehrere bekannte Problembereiche reparieren lassen. Bei Bedarf können auch gezielt einzelne Reparaturfunktionen aktiviert werden.

Die Windows-Wiederherstellungsumgebung verwenden

Einige Reparaturen sind im laufenden System nicht möglich, etwa bei Problemen mit der Bootumgebung. Auch wenn Windows nicht mehr startet, benötigen Sie ein Zweitsystem. Für dessen Nutzung sind in der Regel keine zusätzlichen Tools erforderlich, weil ein Reparatursystem mit dem Namen WinRE (Windows Recovery Environment, Wiederherstellungsumgebung) standardmäßig auf einer eigenen Partition eingerichtet ist. Es wird automatisch aktiv, wenn Windows nach mehreren Versuchen nicht startet oder der Start mehrfach – etwa über den Resetknopf des PCs – abgebrochen wird. Sie erkennen WinRE an der Meldung „Automatische Reparatur wird vorbereitet“. Windows kann dann zum Beispiel Defekte im Dateisystem beheben sowie die Bootumgebung reparieren.

Wie es nach der automatischen Reparatur weitergeht, hängt vom behobenen Fehler und der Windows-Version ab:

- Der PC startet automatisch neu, und das Problem wurde behoben. Wenn nicht, brechen Sie den Windows-Start wieder ab und rufen in WinRE „Erweiterte Optionen“ auf.

- Sie sehen die Meldung „Der PC wurde nicht korrekt gestartet“. Sie können auf „Neu starten“ klicken und prüfen, ob der Fehler behoben wurde. Oder Sie klicken auf „Erweiterte Optionen“.
- Windows 11 24H2/25H2 zeigt nach den Updates im November 2025 auf schwarzem Hintergrund „Ihr Gerät kann zurzeit nicht automatisch repariert werden“, wenn keine Reparatur möglich war. Ein Countdown zählt 30 Minuten herunter, danach sucht Windows erneut nach Lösungen für das Problem. Per Mausklick oder über die Eingabetaste gelangen Sie zu „Weitere Wiederherstellungsoptionen“. Danach geht es über „Problembehandlung“ zu „Erweiterte Optionen“.

Unter „Erweiterte Optionen“ können Sie Updates deinstallieren und das System auf einen vorherigen Wiederherstellungspunkt zurücksetzen. Erfahrene Benutzer verwenden die Eingabeaufforderung für manuelle Reparaturen.

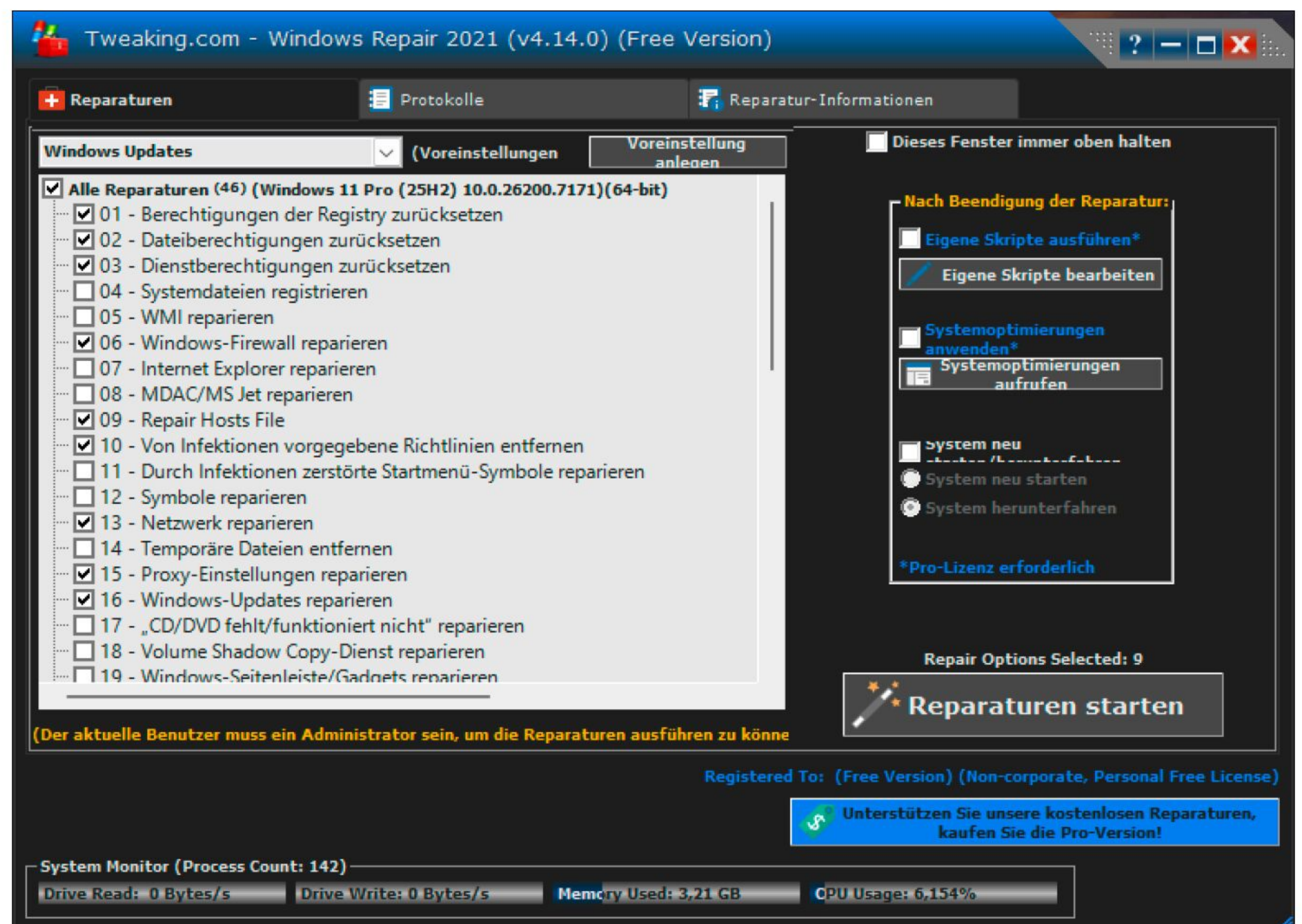
Windows-Reparaturen über ein Zweitsystem

Wenn weder Windows noch WinRE starten, ist wahrscheinlich die Bootumgebung defekt, oder es liegt ein Hardwareproblem vor. In diesem Fall starten Sie WinRE vom Windows-Installationsmedium, für das Sie einen USB-Stick mit Rufus oder Ventoy vorbereitet haben. Im Installationssystem von Windows 11 wählen Sie nach der Sprachauswahl und Tastatureinstellung die Option „Meinen PC reparieren“ und dann das Tastaturlayout.

Nach einem Klick auf „Problembehandlung“ gehen Sie für die Reparatur der Bootumgebung auf „Starthilfe“. Sie können außerdem einen Wiederherstellungspunkt sichern, Updates deinstallieren und die Eingabeaufforderung nutzen.

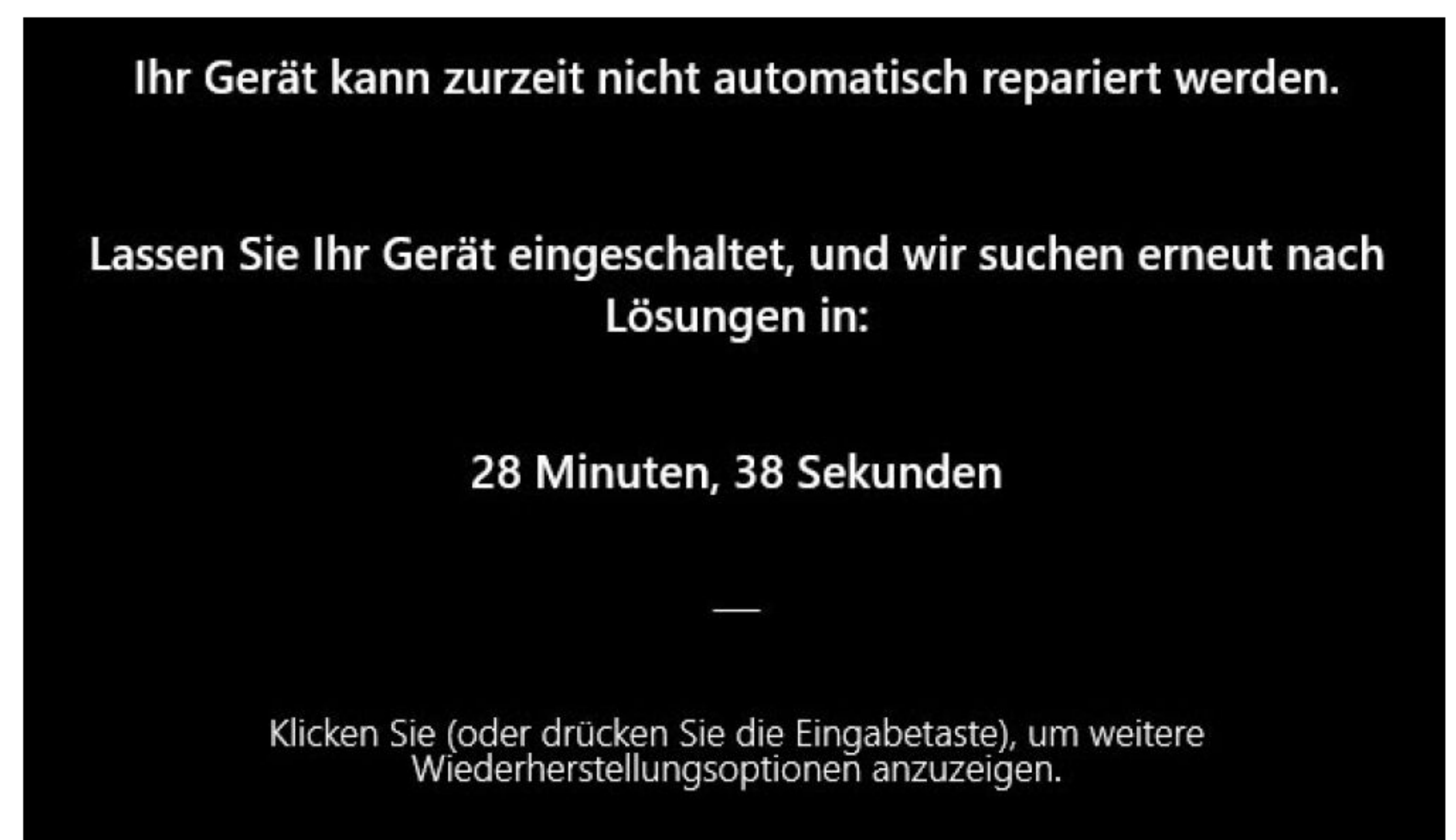
Lazesoft Recovery Suite müssen Sie auf der Festplatte installieren, und Sie können damit Backups erstellen und gelöschte Dateien wiederherstellen. Für unseren Zweck ist der enthaltene Lazesoft Recovery Suite Media Builder von Interesse, mit dem Sie ein Rettungssystem erstellen. Erzeugen Sie damit eine ISO-Datei, die Sie etwa über Ventoy von einem USB-Stick booten.

Im Rettungssystem klicken Sie auf „Windows Recovery“, wählen die Windows-Installation aus und klicken auf „OK“. Die meisten Boot-Reparaturoptionen beziehen sich auf ältere Systeme mit einer MBR-



Windows reparieren: Windows Repair bietet Voreinstellungen für häufige Reparaturaufgaben. Sie können aber auch gezielt nur einzelne Reparaturen durchführen.

Aktualisierte Reparaturumgebung: WinRE von Windows 11 kann jetzt auch online nach Lösungen suchen. Starten Sie die Wiederherstellungsoptionen für weitere Tools.



Partition. Bei einem aktuellen Uefi-System starten Sie auf der Registerkarte „Reparaturwerkzeuge“ das Programm BCD Doctor. Hier klicken Sie dann auf „Wiederaufbau/Reparatur“.

Im Notfall besonders nützlich ist der Lazesoft File Manager. Über ihn erhalten Sie Zugriff auf die Windows-Partition, und Sie können dann wichtige Dateien etwa auf den USB-Stick retten.

Im Startmenü können Sie unter „Microsoft Tools“ auch die Microsoft-Wiederherstellungsumgebung starten. Ihnen stehen dann alle Tools aus WinRE zur Verfügung.

Die Hardware des Rechners untersuchen

Die Ursache von Windows-Problemen ist nicht immer bei der Software zu finden.

Manchmal arbeitet auch die Hardware nicht ordnungsgemäß. Die Überhitzung von Komponenten beispielsweise führt nicht nur zu einem vorzeitigen Verschleiß, sondern auch zu einem instabilen Betriebssystem. Mit einer Analyse der Hardware ermitteln Sie außerdem, was im PC steckt. Das kann vor allem bei fremden Geräten die Suche nach Treibern erleichtern.

Hwinfo zeigt Details zur Hardware besonders ausführlich an. Die Informationen etwa zu CPU, Hauptplatine und Speicher werden in einer Baumstruktur im Hauptfenster angezeigt. Produktbezeichnungen erscheinen – soweit verfügbar – als Link. Ein Klick darauf öffnet ein Menü, über das Sie im Browser Produktinformationen abrufen können oder zur Webseite mit Treiber-Downloads gelangen.



Windows-Wiederherstellungsumgebung: Im Notfallsystem können Sie fehlerhafte Windows-Updates deinstallieren oder einen Wiederherstellungspunkt zurücksichern.



Mini-Windows vom USB-Stick starten: Wenn Windows nicht mehr bootet, verwenden Sie „Starthilfe“ im Windows-Installationssystem. Problematische Updates lassen sich ebenfalls entfernen.

AUTOSTARTS UND LAUFENDE PROZESSE UNTERSUCHEN



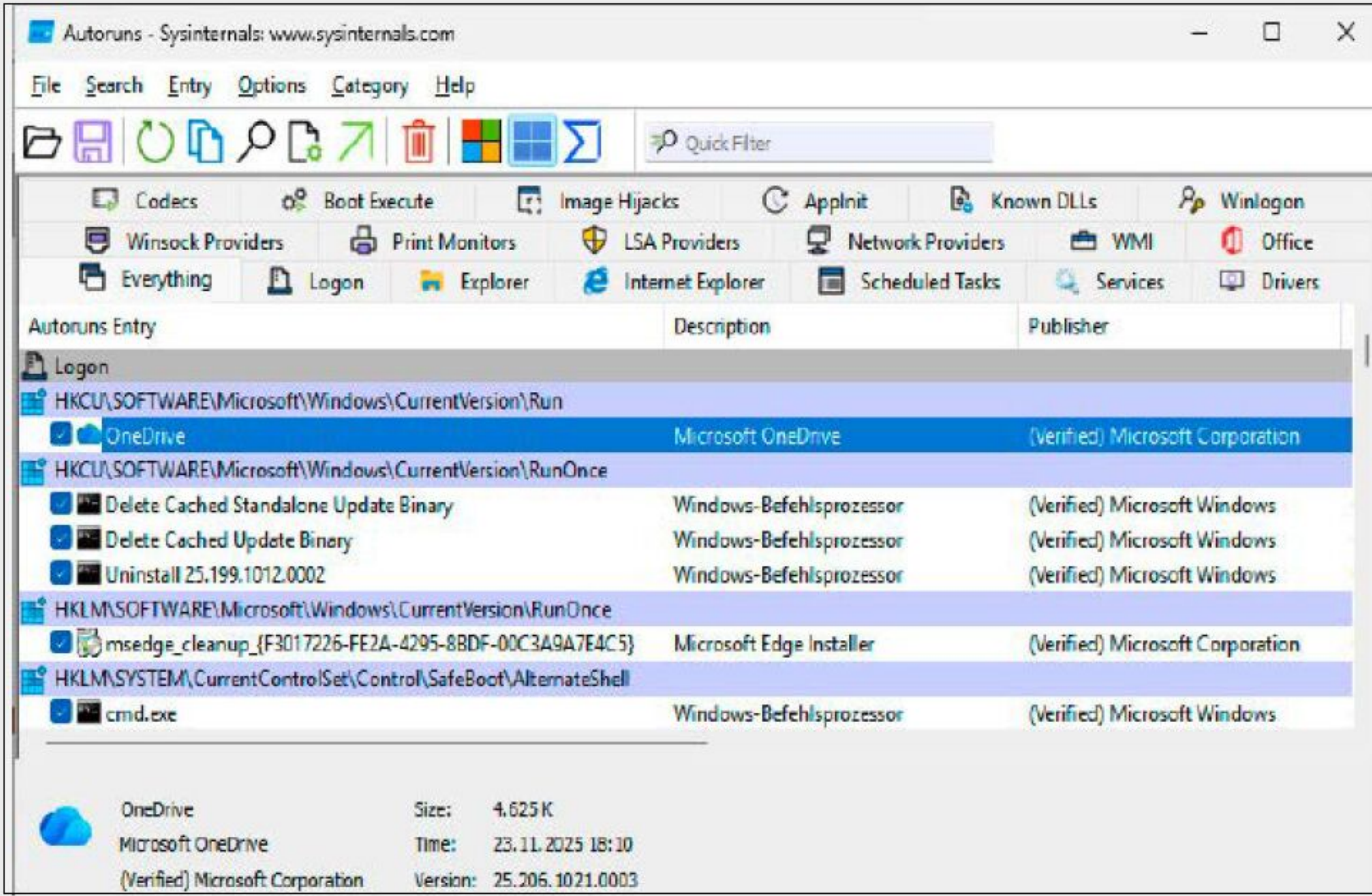
Wenn Windows zu langsam startet, können Autostart-Programme die Ursache sein.

Was alles automatisch startet, kann man mit dem Microsoft-Tool **Autoruns** herausfinden. Autoruns zeigt auf der Registerkarte „Everything“ alle Autostart-Rampen an. Die Liste ist ziemlich lang, lässt sich aber über „Options → Hide Windows Entries“ auf Produkte beschränken, die nicht von Microsoft stammen und daher später über Software anderer Hersteller hinzugekommen sind.

Entfernen Sie die Häkchen bei allen Einträgen, die Sie nicht benötigen. Gelöscht wird dadurch nichts. Sollte sich später herausstellen, dass ein Programm doch automatisch gestartet werden soll, setzen Sie das Häkchen wieder.

Process Explorer ermöglicht Ihnen in Echtzeit einen detaillierten Überblick über alle aktiven Prozesse auf Ihrem Computer. So haben Sie jederzeit im Blick, welche Dienste, Programme, Apps, DLLs und sonstigen Anwendungen gerade ausgeführt werden oder geladen sind.

Autoruns und Process Explorer können beide eine Datei an Virustotal senden, wo deren Inhalt mit mehreren Virensclannern geprüft wird. Verwenden Sie den Kontextmenüpunkt „Submit File to VirusTotal“ beziehungsweise „Check VirusTotal.com“.



Autostarts stoppen: Autoruns findet alles, was Windows automatisch startet. Deaktivieren Sie unnötige Programme, um den Windows-Start zu beschleunigen.

Klicken Sie in der Symbolleiste auf „Überblick“. Das Fenster „System-Überblick“ liefert genauere Daten zu Prozessor (CPU), Hauptplatine und Grafikchip (GPU). Per Klick auf „Sensoren“ öffnen Sie das Fenster „Sensorstatus“, das Daten zu Systemspannung, Taktfrequenz, Temperatur und Lüfterdrehzahl liefert. Es sind jeweils die aktuellen Werte sowie Minimal-, Maximal- und Durchschnittswerte angegeben. Sie können so ermitteln, ob Ihre CPU, GPU oder Laufwerke zu heiß werden und deshalb zu Fehlfunktionen neigen. Die Ursache sind meist verschmutzte Lüfter oder Lüftungsschlitze. Eine gründliche Reinigung des PCs oder Notebooks sollte das Problem beheben. Es ist auch möglich, dass ein Lüfter durch Verschleiß schwergängig wird und nicht mehr die nötige Leistung liefert. Tauschen Sie dann den Lüfter aus.

Wem die Informationen von Hwinfo nicht ausreichen, der kann zu Spezialisten für einzelne Komponenten greifen: **CPU-Z**, **GPU-Z**, **SSD-Z** und **PCI-Z** zeigen die Daten von Prozessor, Grafikchip, SSD und PCI-Bus an.

Die Fitness von Laufwerken ermitteln

Mechanische Festplatten sind Verschleißteile. Der Elektromotor hält nicht ewig, meist sind es jedoch Beschädigungen auf den magnetischen Platten, die zu Ausfällen führen. Eine begrenzte Menge defekter Sektoren kann eine Festplatte verkraften, weil Reservesektoren vorhanden sind. Mit zunehmenden

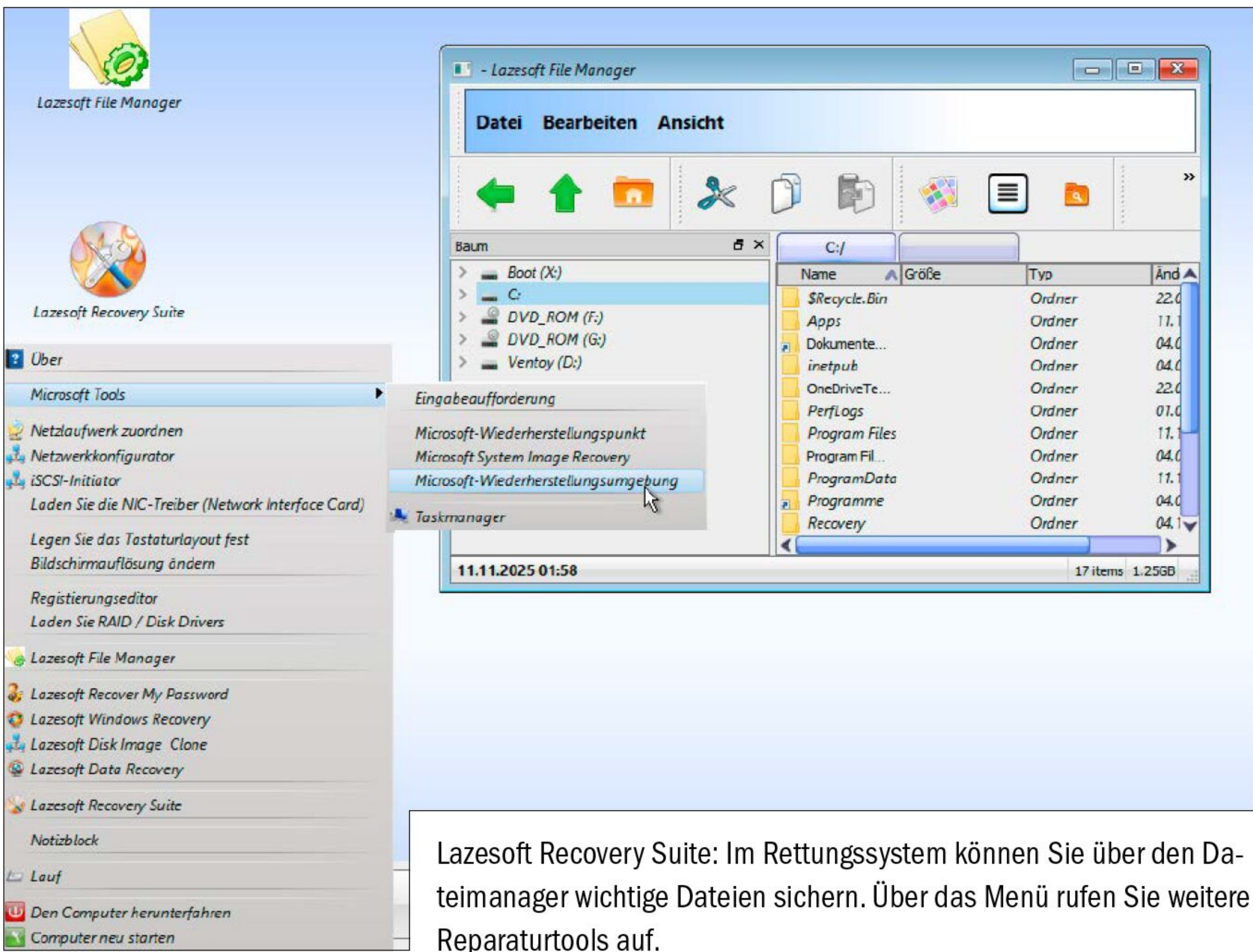
dem Alter und bei intensiver Nutzung erhöht sich jedoch die Anzahl der Defekte, was dann zu Datenverlust führen kann. Mechanische Einwirkungen oder hohe Temperaturen können die Alterung beschleunigen. Die Lebensdauer einer Festplatte liegt bei fünf bis zehn Jahren. Es ist wichtig, Probleme frühzeitig zu erkennen und das Laufwerk auszutauschen, wenn nötig.

Bei SSDs gibt es keinen mechanischen Verschleiß, die Speicherzellen altern aber auch. Entscheidend ist hier die Anzahl der Schreib- und Löschvorgänge, die jede Zelle nur begrenzt verkraftet. Reservezellen sorgen dafür, dass Ausfälle nicht zu früh auftreten. Bei durchschnittlicher Nutzung sollte eine SSD bis zu zehn Jahre durchhalten.

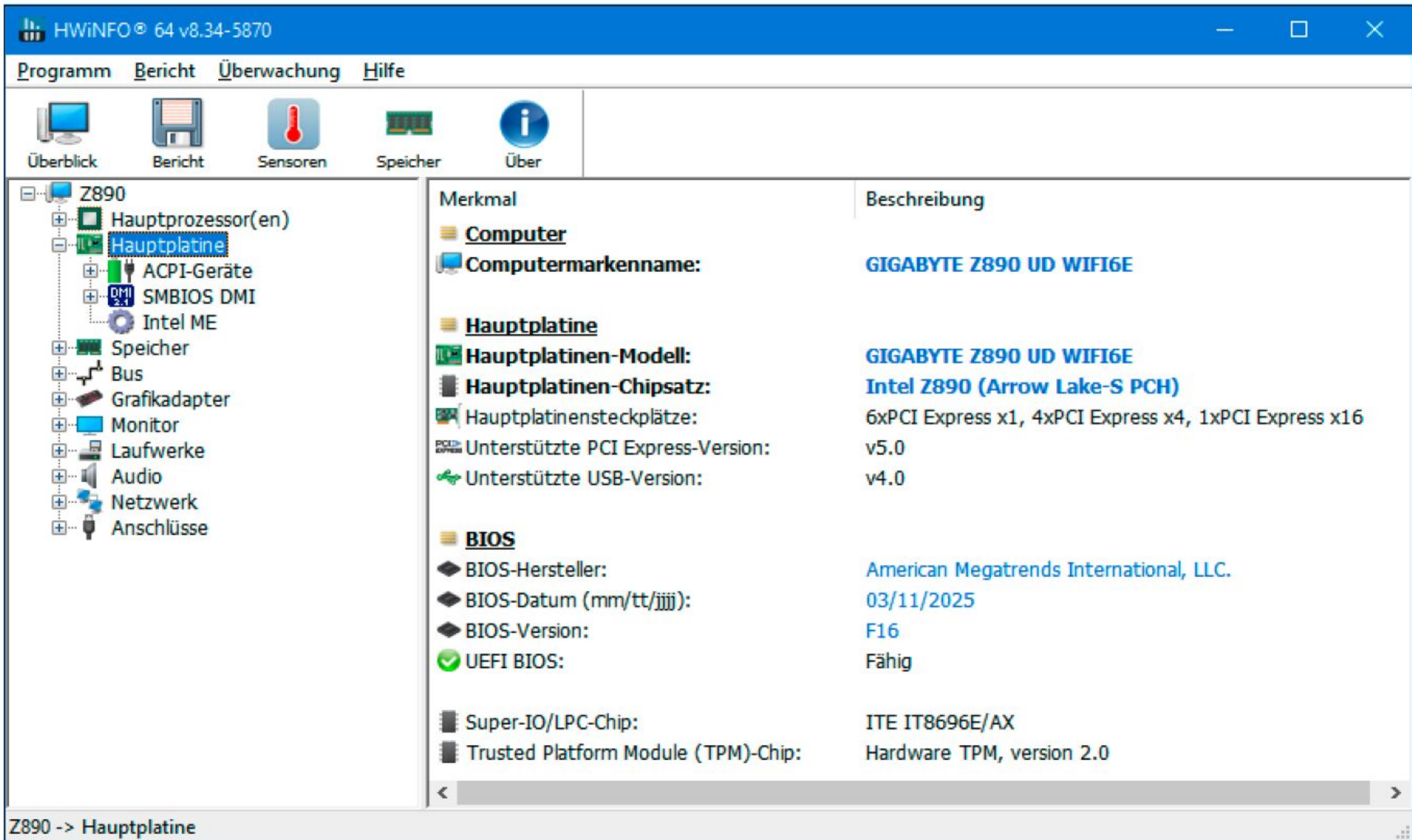
Alle Laufwerke verfügen mit S.M.A.R.T. über eine integrierte Diagnosefunktion. Hwinfo zeigt unter „Laufwerke“ die wichtigsten Daten für jede Festplatte und SSD an. In der Rubrik „Self-Monitoring, Analysis and Reporting Technology“ sehen Sie die einzelnen Werte, die nicht standardisiert und dadurch nicht einfach zu interpretieren sind. Jedes Laufwerk liefert andere Werte, die zudem auch noch vom Anschlusstyp abhängen (SATA, NVMe, USB). Aussagekräftiger ist die Angabe hinter „Anzahl der gemeldeten nicht korrigierbaren Fehler“ unter „Gerätestatistiken“, die bei „0“ liegen sollte. Der Wert hinter „Betriebsstunden“ ist ebenfalls hilfreich. Ab 26.280 Stunden (drei Jahre) sollte man eine Festplatte etwas häufiger prüfen. Hwinfo liefert im Fenster „Sensorstatus“ für die Laufwerke außerdem eine Kurzeinschätzung hinter „Festplattenfehler“ und „Festplattenwarnung“. Wenn hier etwas anderes als „Nein“ steht, sollten Sie die Daten sichern und über einen Austausch des Laufwerks nachdenken.

Crystal Disk Info ist eine Alternative zu Hwinfo. Das Tool ist auf Laufwerksdaten spezialisiert und daher etwas übersichtlicher. Die Liste der einzelnen S.M.A.R.T.-Werte bedarf auch hier der Interpretation. In der Regel genügt aber die Angabe unter „Gesamtzustand“, die „Gut“ lauten sollte. Die Anzahl der Betriebsstunden und bei SSDs auch die gesamte geschriebene Datenmenge liefert Crystal Disk Info ebenfalls.

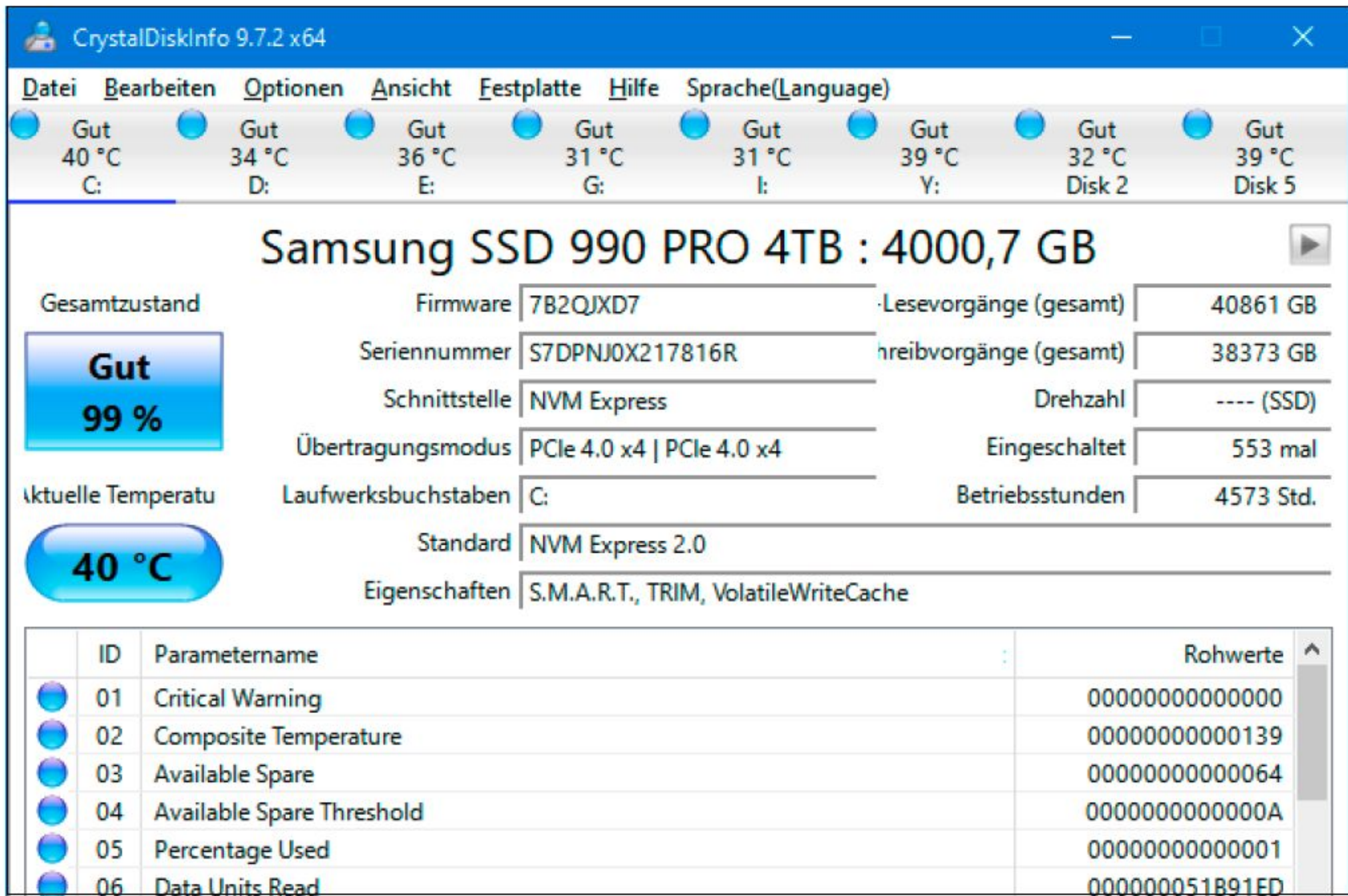
Crystal Disk Mark und **AS SSD Benchmark** bieten einen Leistungstest für Laufwerke und können die Übertragungsrate mit unterschiedlichen Dateigrößen ermitteln. Damit kann festgestellt werden, ob etwa eine SSD so schnell arbeitet, wie sie sollte. ■



Lazesoft Recovery Suite: Im Rettungssystem können Sie über den Dateimanager wichtige Dateien sichern. Über das Menü rufen Sie weitere Reparaturtools auf.



Was im PC steckt: Hwinfo zeigt Daten zu allen Hardwarekomponenten an. Links führen zu den Support-Seiten des jeweiligen Herstellers, etwa für Treiber-Downloads.



Laufwerksinfos: Crystal Disk Info liest die S.M.A.R.T.-Werte von Festplatten und SSDs aus. Das Tool informiert außerdem über den Gesamtzustand und die Betriebsstunden insgesamt.

Für jeden Stick das richtige Dateisystem



Wenn etwas bei USB-Sticks nicht funktioniert, liegt es oft am Dateisystem: Mal hakt es bei FAT32, mal aber auch bei NTFS. Jedes Formatierungsformat hat eben seine Vorteile, Nachteile und Einschränkungen. Wir erklären, welches Dateisystem für welches Betriebssystem, Gerät und Einsatzszenario am besten passt.

VON PETER STELZEL-MORAWIETZ

Technisch war es nie ein Problem, USB-Datenträger mit einer Speicherkapazität von mehr als 32 GB mit dem Dateisystem FAT32 zu formatieren. Nur Windows selbst

„Microsoft will beim verbreiteten Dateisystem FAT32 die maximale Größe der Speichersticks von 32 auf künftig 2000 GB hochsetzen.“

ist dazu seit jeher nicht der Lage, man muss also stets auf externe Tools zurückgreifen. Das soll sich in Zukunft ändern. Im Sommer 2024 kündigte Microsoft an, dass der betriebssysteminterne Format-Befehl auch Speichermedien bis zwei Terabyte mit FAT32 unterstützen soll. Im Vergleich zu dem bisherigen 32-GB-Limit ist das mehr als 60-mal so viel.

Aktuell steckt die neue Funktion zwar erst in einigen Insider-Vorabversionen von Windows 11, doch wenn sie in den Preview-Builds problemlos läuft, soll sie in den kommenden Monaten in das normale Betriebssystem übernommen werden. Dieser Schritt macht es insbesondere für viele technisch weniger versierte PC-Nutzer einfacher, mobile Datenträger mit 64 und

mehr Gigabyte Speicherkapazität universeller als bisher einzusetzen.

Da sind wir mittendrin im Thema, denn der wichtigste Pluspunkt von FAT32 gegenüber vielen anderen Dateisystemen ist seine große Kompatibilität: Auf diese Weise formatierte Datenträger garantieren auf praktisch allen Geräten sowie mit den wichtigsten Betriebssystemen problemlos Schreib- und Lesezugriff.

Das Dateisystem ist bei mobilen Datenträgern besonders wichtig

In aller Regel braucht man über Dateisysteme und Formatierungsoptionen gar nicht nachzudenken, denn interne wie auch externe Datenträger funktionieren einfach. So wird die PC-Festplatte bei der Windows-

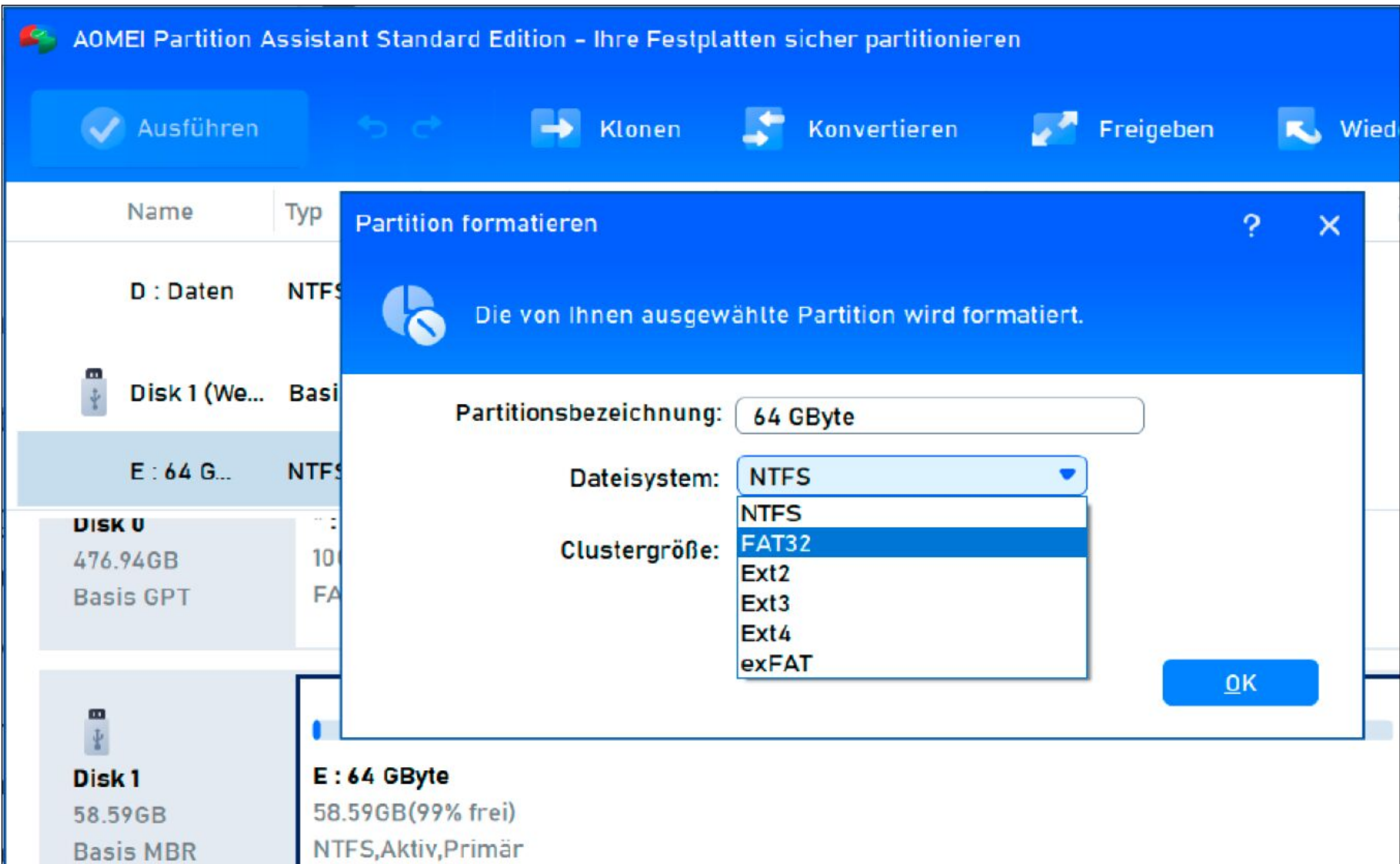
Neuinstallation automatisch richtig formatiert. Und USB-Sticks und (Mikro-) SD-Speicherkarten sind bereits vorformatiert, sodass man sie meist einfach anstecken beziehungsweise einlegen kann.

Doch insbesondere bei mobilen Speichern funktioniert dann plötzlich und unerwartet irgendetwas nicht. Beispielsweise, weil Sie Stick oder Speicherkarte an einem Rechner mit anderem Betriebssystem, einem Router, einem Fernseher oder sonst einem Gerät aus dem Bereich Unterhaltungselektronik verwenden möchten. Mit einer Fehlermeldung quittiert Windows auch jeden Versuch, eine über vier Gigabyte große Datei auf einem FAT32-formatierten USB-Stick zu speichern – in diesem Fall ist schlicht die maximale Dateigröße dieses Dateisystems überschritten.

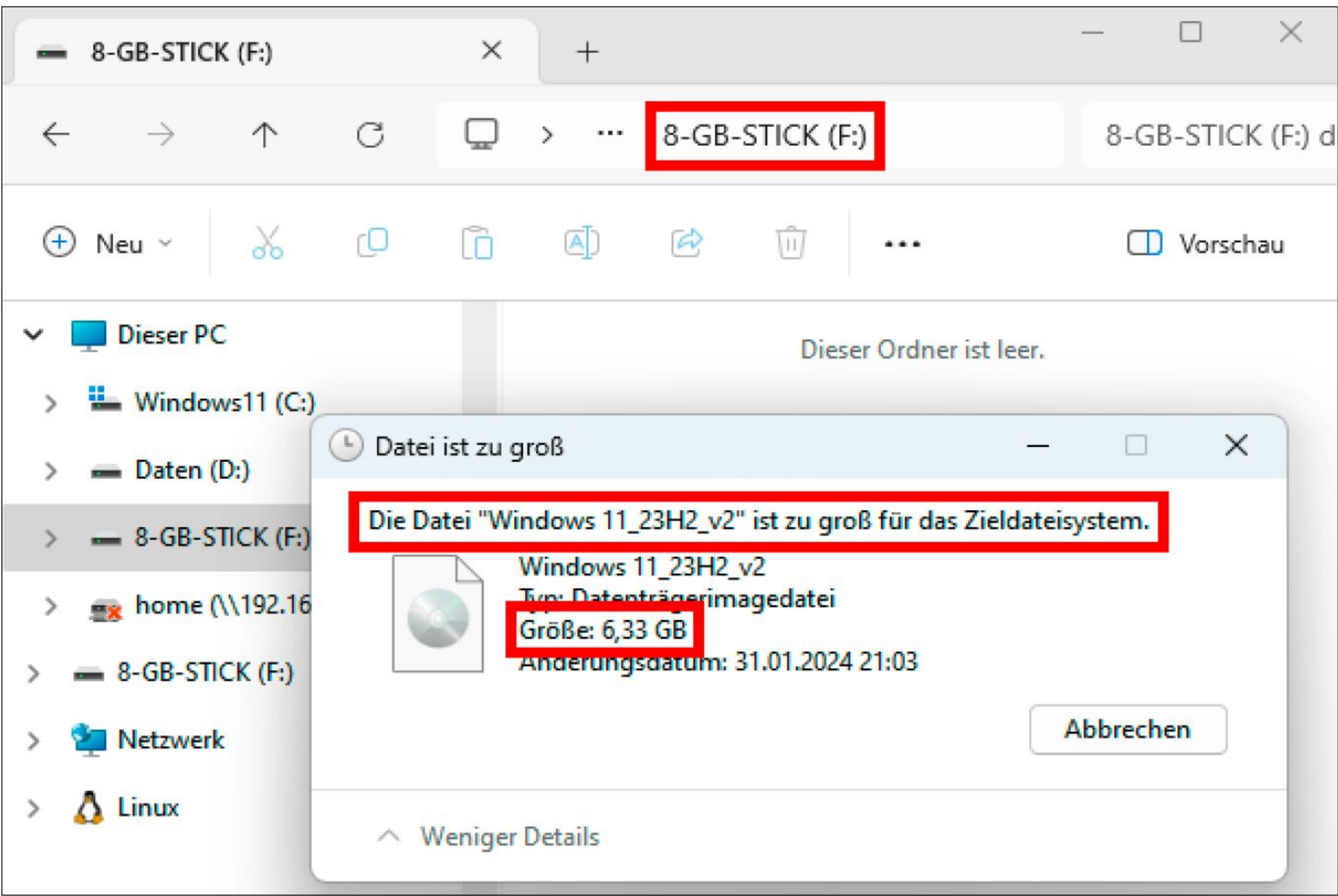
Dies sind nur zwei Beispiele aus einer ganzen Reihe von Szenarien, in denen Funktionen beeinträchtigt sind oder Fehler auftreten. Und zwar nicht deshalb, weil das Speichermedium, die Gerätebuchse oder sonst etwas defekt wäre, sondern nur, weil das verwendete Dateisystem nicht passt und falsch gewählt ist. In solchen Fällen genügt es meist, zum für den jeweiligen Verwendungszweck richtigen Format zu wechseln. Unser Ratgeber erläutert, wie Sie solche Probleme lösen, und stellt dabei die praktischen Fragen in den Vordergrund. Welches Dateisystem eignet sich für welchen Anwendungszweck, wie lösen Sie Formatierungsprobleme und wie umgehen Sie die Windows-Beschränkungen. Die Tools auf der Heft-DVD unterstützen Sie dabei.

Ein bisschen Theorie: Was genau ist denn ein Dateisystem?

Etwas Hintergrundwissen hilft bei der Erklärung, welches Dateisystem sich denn



Während Windows die Auswahl bei den Dateisystemen unnötig stark einschränkt, bieten Partitionierungsprogramme wie Aomei Partition Assistant deutlich mehr Optionen.

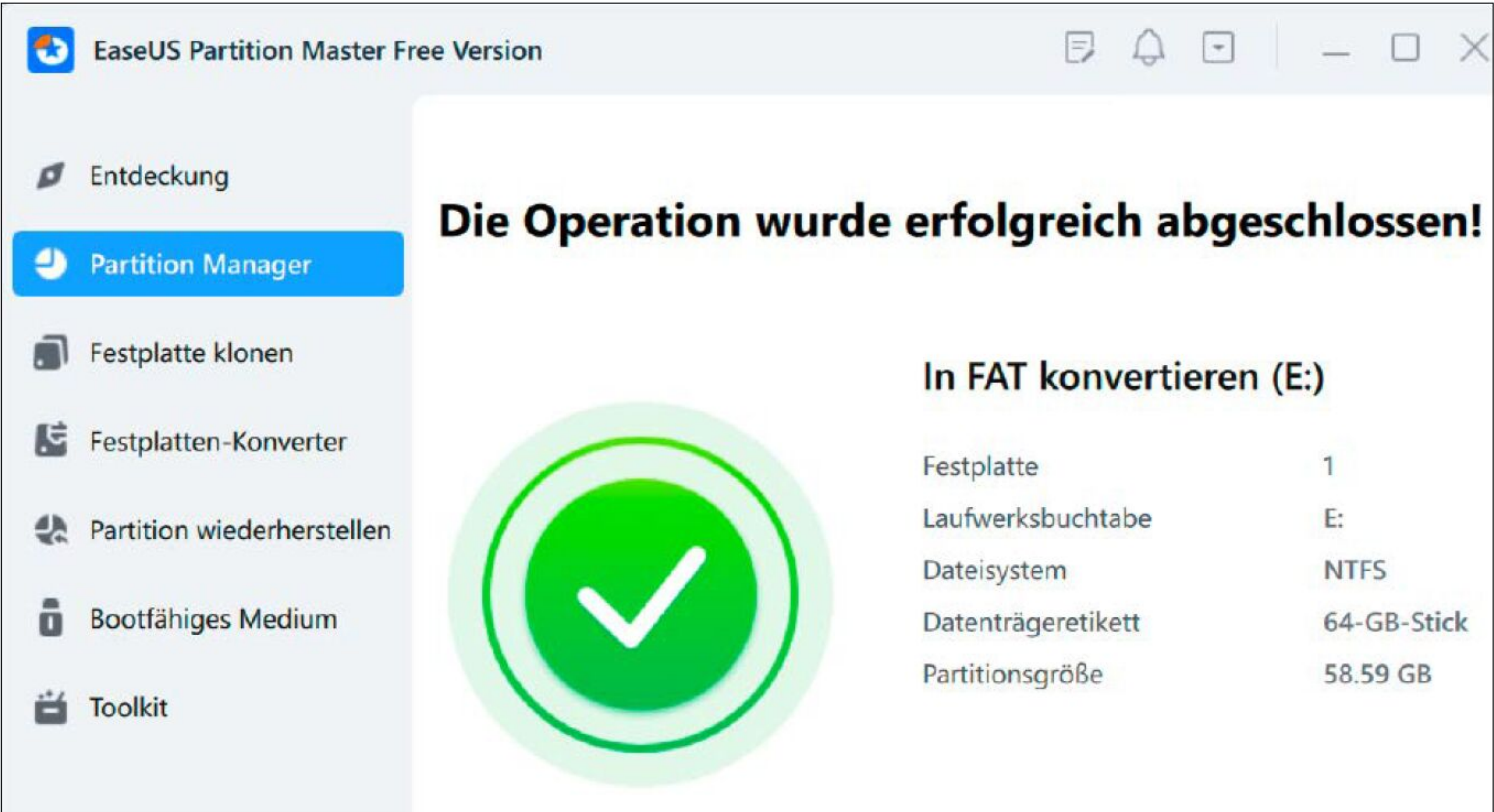


Inkompatibilitätshinweis: Diese gut 6 GB große ISO-Datei passt zwar prinzipiell auf den 8-GB-Stick, das verwendete Dateisystem FAT32 erlaubt jedoch nur Dateigrößen bis 4 GB.

DIE WICHTIGSTEN DATEISYSTEME FÜR WINDOWS UND MOBILE DATENTRÄGER



	FAT32	exFAT	NTFS
Maximalgröße Partition bzw. Datenträger	8 TB	512 TB	8 PB
Maximale Dateigröße	4 GB	512 TB	8 PB
Zugriffskontrolle / Benutzerverwaltung	Nein	Eingeschränkt	Ja
Komprimierung	Nein	Nein	Ja
Verschlüsselung (EFS)	Nein	Nein	Ja
Lese- und Schreibzugriff unter	Windows, Chrome OS, Linux und Mac-OS	Windows, Chrome OS, Linux und Mac-OS	Windows, Chrome OS, Linux und Mac-OS
Verwendungszweck, Einsatzgebiet	Kompatibel mit allen Betriebssystemen und sehr vielen Geräten aus allen Bereichen. Ideal zum Dateiaustausch über mobile Datenträger.	Konzipiert für Flash-Speichermidien wie USB-Sticks, nicht kompatibel vor allem mit älteren Geräten.	Standardformat für interne und externe Datenträger unter Windows, nicht kompatibel zu vielen anderen Geräten.



Änderungen am Dateisystem ohne Datenverlust sind nicht mit Windows, sondern nur mit externen Programmen möglich. Hier gezeigt am Beispiel von Partition Master Free von Easeus.



Dateisystem unbekannt: Die am Fernseher zum Aufzeichnen formatierte Festplatte arbeitet mit einem Format, das weder von Windows noch von gängigen Partitionierungstools erkannt wird.

nun für welche Geräte beziehungsweise Zwecke eignet. Entscheidend beim Formatieren und Partitionieren von Datenträgern ist das schon mehrfach genannte Dateisystem. Darunter versteht man das Ablagesystem eines Speichermediums: also wo und wie welche Daten gespeichert, geändert, gelöscht oder auch verschlüsselt werden. Sowohl aus historischen Gründen als auch wegen ständig steigender Anforderungen existieren mittlerweile weit über 100 verschiedene Dateisysteme. Wir beschränken uns deshalb auf die wichtigsten für den PC

und Geräte aus der IT und Unterhaltungselektronik, die in zahlreichen Haushalten im Einsatz sind. Dazu zählen unter anderem Router, Fernseher, smarte TV-Zuspieler, Digitalkameras, Spielekonsolen und auch Smartphones. Geradezu universell nutzbar sind die beiden Dateisysteme FAT32 und exFAT. Die Abkürzung FAT steht für „File Allocation Table“ und lässt sich mit Dateizuordnungstabelle übersetzen. FAT-formatierte Datenträger werden von sehr vielen Geräten sowie allen wichtigen PC-Betriebssystemen

erkannt, inklusive voller Zugriffsrechte beim Beschreiben. Das prädestiniert sie unter anderem zum Datenaustausch über mobile Datenträger wie USB-Sticks, Speicherkarten und teilweise auch Festplatten. Andererseits bietet FAT praktisch keine Zugriffskontrolle, Benutzerverwaltung, Komprimierung und Verschlüsselung. Das alles unterstützt das NTFS-Standarddateisystem für Festplatten in Windows-PCs, zudem eignet sich das „New Technology File System“ viel besser für große Datenträger und Dateien. Bisher nicht durchsetzen konnte sich Microsofts jüngstes Dateisystem ReFS (Resilient File System).

Hinweis: Beim Konfigurieren eines Bootsticks als Livesystem beziehungsweise für die Windows-Installation wird das Dateisystem in aller Regel automatisch passend gewählt. Das gilt sowohl für die Funktion zum Erstellen von Bootmedien in diverser Software wie auch bei **Rufus** für Bootsticks.

Immer das passende Dateisystem für USB-Sticks und Speicherkarten

FAT32 funktioniert so universell, dass man damit zunächst kaum etwas falsch macht. Die größte Einschränkung, darauf haben wir bereits hingewiesen, ist das Dateigrößenlimit auf 4 GB. An diese Beschränkung stößt man bei Backups, ISO-Dateien und Videos nicht nur am PC immer häufiger, sondern auch auf sonstigen Geräten. Das gilt vor allem für solche, die Videos aufnehmen oder speichern. Manche Fernseher, Film- und Actioncams splitten längere Aufnahmen deshalb automatisch, bei anderen kann und muss man auf exFAT (extended FAT) umstellen. Für neuere Geräte ist deshalb exFAT unter Umständen die bessere Wahl. Ob ein älteres Gerät dieses Dateisystem unterstützt, entnehmen Sie bitte den technischen Daten, der Bedienungsanleitung oder probieren es einfach aus. Die Tabelle „Die wichtigsten Dateisysteme für Windows und mobile Datenträger“ nennt einige Eigenschaften und bevorzugte Einsatzzwecke der verschiedenen Standards.

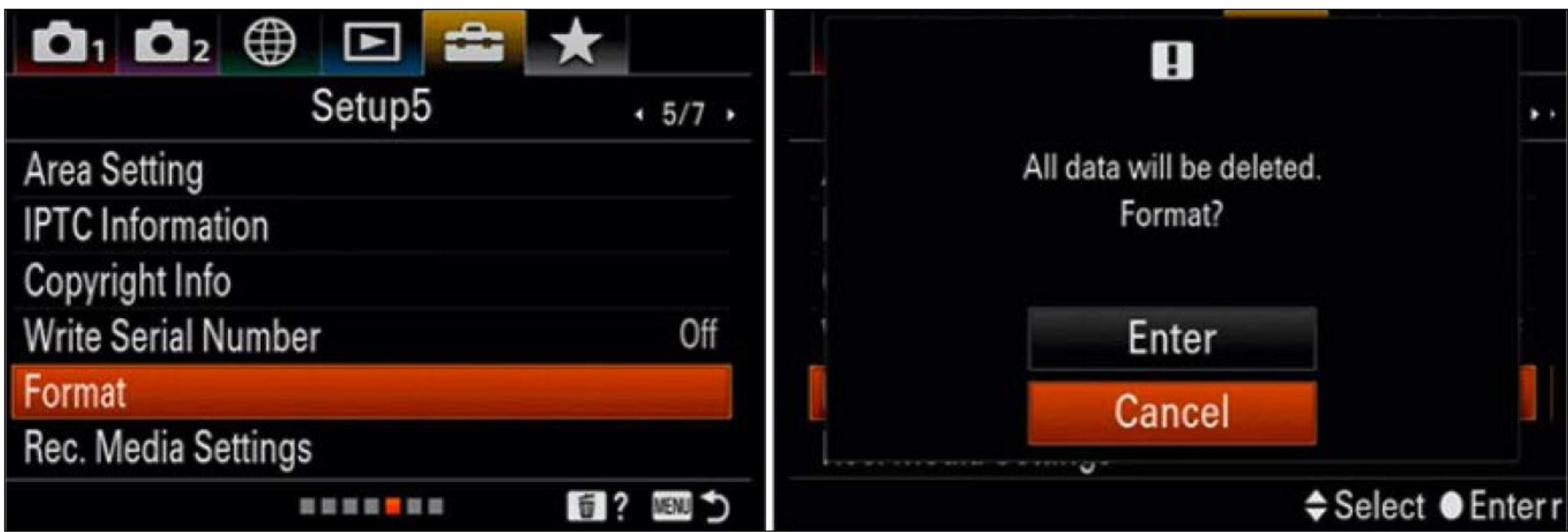
Am PC ändern Sie das Dateisystem von mobilen Datenträgern mit Windows-Bordmitteln (siehe Kasten „Vorsicht, Datenverlust!“) oder mit einem der folgenden Partitionierungstools: **Aomei Partition Assistant Standard**, **Easeus Partition Master Free** oder **Minitool Partition Wizard Free**. Letzteres unterstützt nur FAT zu NTFS. Diese Programme löschen, anders als die Win-

dows-internen Funktionen, keine Daten, Sie müssen sie also vor dem Konvertieren des Dateisystems nicht separat sichern.

Viele Kameras, Fernseher und weitere Geräte bieten zudem im Bedienmenü die Möglichkeit, den eingelegten oder angesteckten Datenträger zu formatieren. Dieser Weg gewährleistet automatisch das richtige Format. Manchmal ist dies sogar die einzige Option, einen Datenträger am spezifischen Gerät zu verwenden. Wo Sie die interne Formatierungsfunktion finden, entnehmen Sie bitte wieder der jeweiligen Geräteanleitung. Beachten Sie, dass am Fernseher gespeicherte Aufnahmen stets verschlüsselt und damit an das individuelle TV-Gerät gebunden sind. Auf dem PC lassen sich die Videos nicht abspielen.

Die verbreiteten Fritzbox-Router von AVM akzeptieren bei USB-Datenträgern als Netzwerkfestplatte alle gängigen Dateisysteme: NTFS, exFAT, FAT32 und die Linux-Formate ext2, ext3 und ext4. Für andere Router informieren Sie sich bitte beim Gerätehersteller. Und wie steht es um die Spielekonsolen? Die Playstation von Sony unterstützt externe Datenträger mit FAT32 und exFAT, die Xbox-Modelle von Microsoft zusätzlich NTFS, und Nintendo empfiehlt für seine Switch ausschließlich FAT32.

Zum Schluss fehlt noch die Beschreibung, wie sich USB-Sticks ans Android-Smartphone anschließen lassen. Dazu überprüfen Sie mithilfe der App **USB OTG Checker** aus dem Google Play Store zunächst, ob Ihr Telefon die Funktion überhaupt unterstützt. Das ist nämlich keineswegs immer der Fall. Die Abkürzung OTG steht für „On the Go“ und beschreibt die Möglichkeit, Peripheriegeräte wie USB-Sticks, Maus oder Tastatur, Drucker und Ähnliches anzuschließen. Unterstützt Ihr Mobiltelefon OTG, benötigen Sie ferner einen sogenannten OTG-Adapter. Das ist ein kurzes Kabel mit einem USB-Stecker (meist USB-C) an einem Ende



Die Funktion zum Formatieren der Speicherkarte in Digitalkameras differiert zwar von Hersteller zu Hersteller, im Grunde ähnelt sich der Vorgang aber immer.

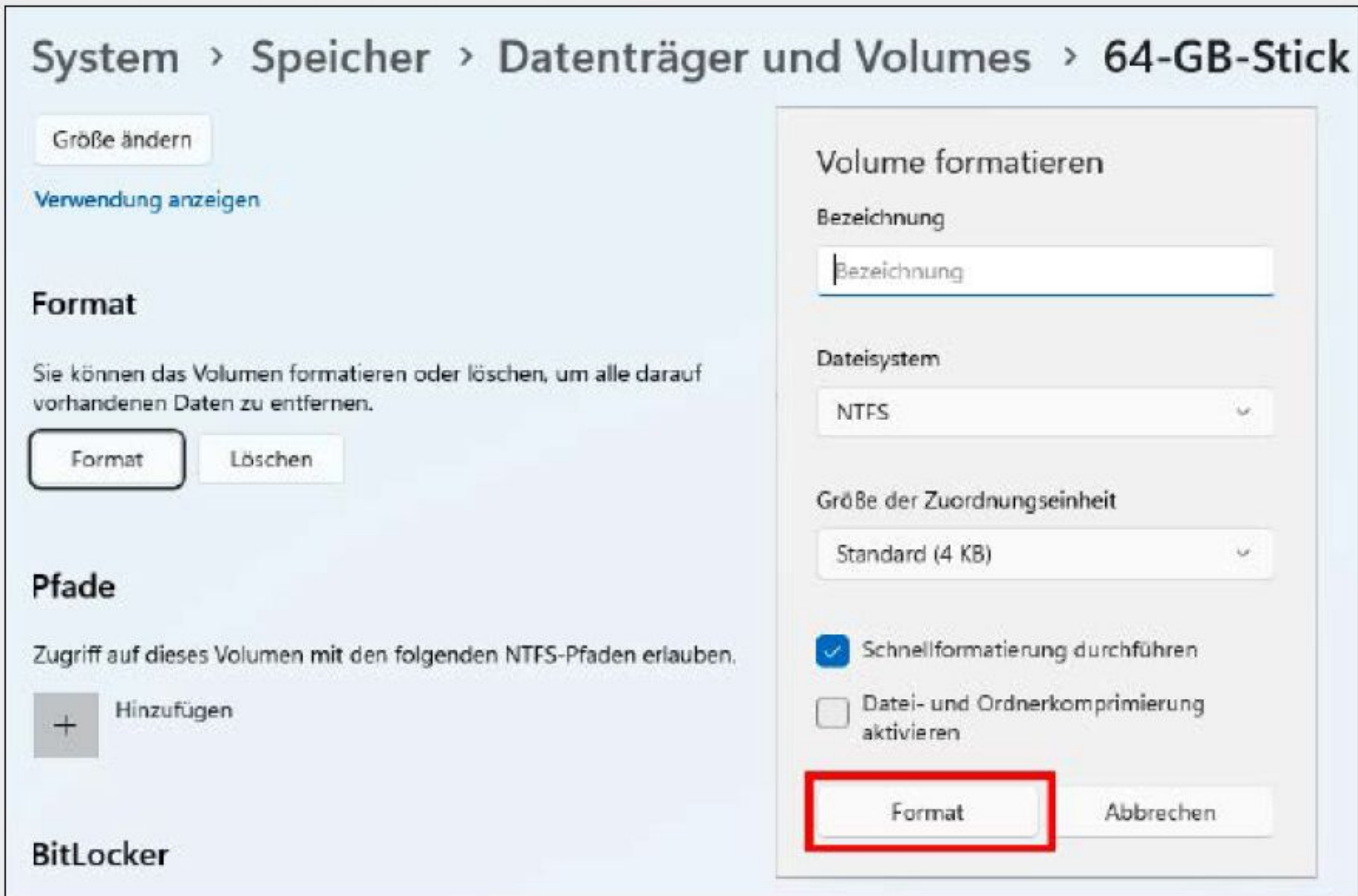
und einer USB-A-Buchse zum Einstecken des USB-Sticks am anderen. OTG-Adapter gibt es bei Amazon und Co. ab etwa fünf Euro. Ausführliche Informationen dazu finden Sie bei uns online unter www.pcwelt.de/2426443. ■

VORSICHT, DATENVERLUST!



Mit Windows-Bordmitteln können Sie das Dateisystem eines Datenträgers auf verschiedene Art und Weise ändern. Am einfachsten per Rechtsklick auf das Explorer-Laufwerk und „Formatieren“ im Kontextmenü. Zweitens über die klassische „Datenträgerverwaltung“ und drittens in Windows 11 zusätzlich über „System → Speicher → Datenträger und Volumes“ in der Einstellungen-App. Während Windows bei den ersten beiden Wegen ausdrücklich auf den Datenverlust bei der Neuformatierung hinweist, fehlt diese Warnung bei Option drei unter Windows 11!

Wichtig: Anders als die Konvertierungsfunktion von Aomei Partition Assistant Standard, Easeus Partition Master Free und Mini-tool Partition Wizard Free löscht die Neuformatierung mit Windows-Bordmitteln stets alle auf einem Datenträger beziehungsweise einer Partition gespeicherten Daten. Sichern Sie deshalb vor dem Ändern des Dateisystems sämtliche darauf gespeicherten Daten auf einer Festplatte.



Vorsicht! Bei der Neuformatierung über die Einstellungen-App in Windows 11 fehlt jeglicher Warnhinweis, dass dieser Vorgang sämtliche Dateien auf dem Datenträger löscht.

WINDOWS-TOOLS ZU DEN DATEISYSTEMEN



Programm	Beschreibung	Auf	Internet	Sprache
Aomei Partition Assistant Standard	Partitionierungstool für Festplatten und Datenträger	Heft-DVD	www.aomei.de/partition-manager	Deutsch
APFS für Windows	Schreib- und Lesezugriff auf Mac-formatierte Laufwerke (Testversion 10 Tage)	Heft-DVD	www.paragon-software.com/home/	Deutsch
Easeus Partition Master Free	Partitionierungstool für Festplatten und Datenträger	Heft-DVD	www.easeus.de/partition-manager	Deutsch
Minitool Partition Wizard Free	Partitionierungstool für Festplatten und Datenträger	Heft-DVD	www.partitionwizard.com	Deutsch
Paragon HFS+ für Windows	Schreib- und Lesezugriff auf Mac-formatierte Laufwerke (Testversion 10 Tage)	Heft-DVD	www.paragon-software.com/home/	Deutsch
Paragon Linux File Systems	Schreib- und Lesezugriff auf Linux-formatierte Laufwerke	Heft-DVD	www.paragon-software.com/home/	Deutsch
Rufus	Erstellt bootfähige USB-Sticks	Heft-DVD	https://rufus.ie	Deutsch

PC-WELT Rettungssystem 2026

Großes Update: Die neue Version des Rettungssystems der PC-WELT setzt auf verbesserte Tools für PC-Notfälle und auf frische Linux-Komponenten für umfassenden Hardware-support. Außerdem lassen sich jetzt auch per Bitlocker verschlüsselte Laufwerke leichter integrieren.



VON DAVID WOLSKI

Hardwarehavarien kündigen sich heutzutage nicht mehr auffällig an. Wenn bei einem älteren Rechner die betagte Festplatte vernehmbar rattert, das Bios schrille Pfeiftöne von sich gibt oder der Geruch verbrannter Elektronikteile unmissverständlich auf einen Geräteschaden schließen lässt, ist der PC-Notfall eindeutig.

Doch bei modernen PCs oder Notebooks mit lautlosen SSD-Laufwerken sind die Ursachen für einen Rechnerausfall schwieriger zu ermitteln – besonders unter Windows: Bluescreens, Systemabstürze und Bootprobleme können vielfältige Gründe haben. Besonders schwierig gestaltet sich die Fehleranalyse, wenn Windows nicht

mehr funktioniert. Jetzt sollten Sie schnell handeln, um die Schadensursache auf physische Komponenten oder Programme einzugrenzen: Dazu benötigen Sie ein spezialisiertes Zweitsystem, das eigenständig von DVD oder USB-Stick startet.

Das ist der Anspruch unseres Rettungssystems auf Heft-DVD, das Sie dieses Jahr als neue Version 11 erhalten: ein intuitives und kompaktes Livesystem, das unabhängig von Windows arbeitet – mit aktuellen Rettungstools, Bitlocker-Entschlüsselung, Partitionierer und Browser. Die Inspiration dafür lieferte Parted Magic, das aber seit 2013 nicht mehr frei verfügbar ist.

Zwar richten sich einige der im Rettungssystem enthaltenen Tools an fortgeschrittene Anwender. Doch die Benutzeroberfläche „Mate“ des PC-WELT-Systems ist einladend und einfach gehalten: So finden Sie im Notfall immer schnell die passende Lösung für Ihr PC-Problem. Wir zeigen, wie Sie das PC-WELT-Rettungssystem verwenden, und präsentieren seine Tools mit praktischen Anleitungen sowie verständlichen Anwendungsbeispielen.

Aufgefrischtes System mit vielen neuen Programmen

Das PC-WELT-Rettungssystem arbeitet als alternatives Betriebssystem, das Sie direkt von der Heft-DVD oder einem erzeugten USB-Stick starten können, um die Funktion der meisten Hardwarekomponenten zu überprüfen. Zudem können Sie damit jene Aufgaben erledigen, die nur mit einem Livesystem funktionieren, wenn das installierte Windows nicht mehr startet: den Zugriff auf Dateien, die Wiederherstellung gelöschter Dateien, die Neu-Partitionierung der Datenträger und das Klonen oder Speichern sowie Wiederherstellen von Datenträgern aus Abbilddateien (Images) für komplette Backups. Dafür bringt das neue PC-WELT-Rettungssystem 2026 (64 Bit) viele Diagnose- und Wiederherstellungswerkzeuge mit. Bei diesen Tools handelt es sich um bewährte Open-Source-Programme aus der Datenforensik sowie um Eigenentwicklungen. Auch die Basis des Betriebssystems haben wir selbst entwickelt auf der Grundlage von Arch Linux: Alle Komponenten haben in der diesjährigen Version große Updates erhal-

„Die neue Version des Rettungssystems wappnet Sie für jeden PC-Notfall.“

ten, um die Unterstützung für aktuelle Hardware wie NVMe-Laufwerke, CPUs und Chipsätze zu verbessern.

Zu den Highlights gehört das Entschlüsselungsprogramm **Dislocker** für Windows-Bitlocker-Partitionen, das jetzt in einer neuen Version vorliegt, die zu Windows 11 kompatibel ist. So müssen Sie nicht mehr auf die Kommandozeile ausweichen, um Bitlocker-Laufwerke zu entsperren. Denn der integrierte Dateimanager kann Bitlocker-Laufwerke mit bekanntem Passwort sowie Bitlocker to go direkt per Doppelklick öffnen. Zudem gibt es ein grafisches Werkzeug zum einfachen Ein- und Aushängen von Laufwerken per Mausklick. Auch das inzwischen weitverbreitete Dateisystem exFAT wird unterstützt.

Das grafische Werkzeug **Qphotorec** setzen Sie zur Dateirettung ein und durchsuchen damit Laufwerke mit dem bewährten Forensik-Tool **Photorec**. Zur Abwehr von Malware setzt das Rettungssystem auf Clam-AV-GUI, das mit dem freien Virens Scanner **Clam AV 1.4.2** arbeitet, der dank der Unterstützung von Cisco konkurrenzfähiger ist.

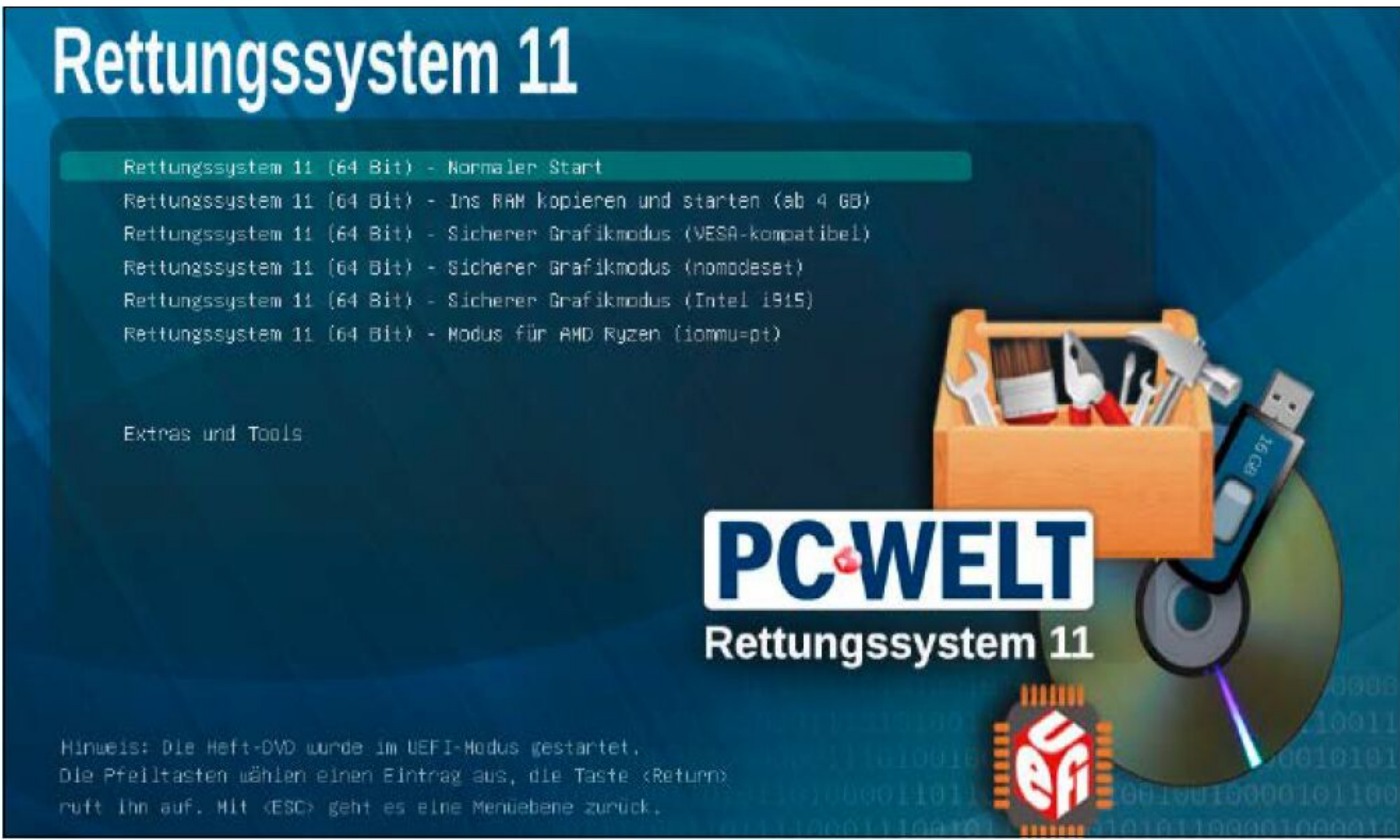
Neben diesen verbesserten Programmen bietet das Rettungssystem 2026 auch viele Neuzugänge: **Baobab** ist ein formidables Tool, um die Datenträgerbelegung anzuzeigen, **Gnome Disks** ein Laufwerksmanager, der auch Images einer Partition anlegen kann, und **Filezilla** ein Übertragungswerkzeug für Dateien im Netzwerk über die Protokolle SFTP, SSH und FTP(S). Ein weiteres Netzwerktool ist **Zenmap**, das den Portscanner **Nmap** um eine grafische Oberfläche erweitert: Damit erstellen Sie einen Plan der Netzwerktopologie mit allen erreichbaren Hosts.

Los geht's: So starten Sie das Rettungssystem von Heft-DVD

Das Rettungssystem gibt sich aufgrund seiner schlanken Linux-Komponenten mit wenig Rechenleistung zufrieden: Es läuft auch auf einer 20 Jahre alten 64-Bit-CPU und mit 1 GB RAM anständig – Sie können es daher auch auf sehr alten Systemen mit Pentium-4-CPU oder einem frühen AMD-64-Prozessor einsetzen. Beachten Sie, dass das Livesystem Secure Boot nicht unterstützt: Sie müssen diese Funktion deshalb vor dem Einsatz in den Bios-Einstellungen abschalten.

Von Heft-DVD lässt sich das Rettungssystem im Bios- oder im Uefi-Modus starten. Legen

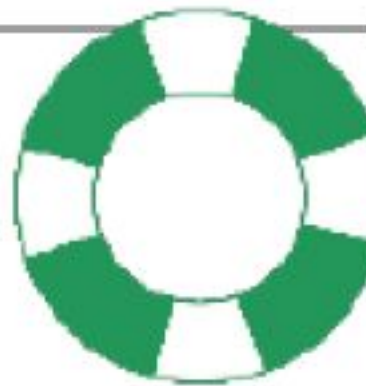
Multibootmenü: Beim Start von Heft-DVD oder vom USB-Stick zeigt dieses Menü alle Startoptionen des Rettungssystems an. Es startet je nach Hardware unter Bios und natürlich mit Uefi.



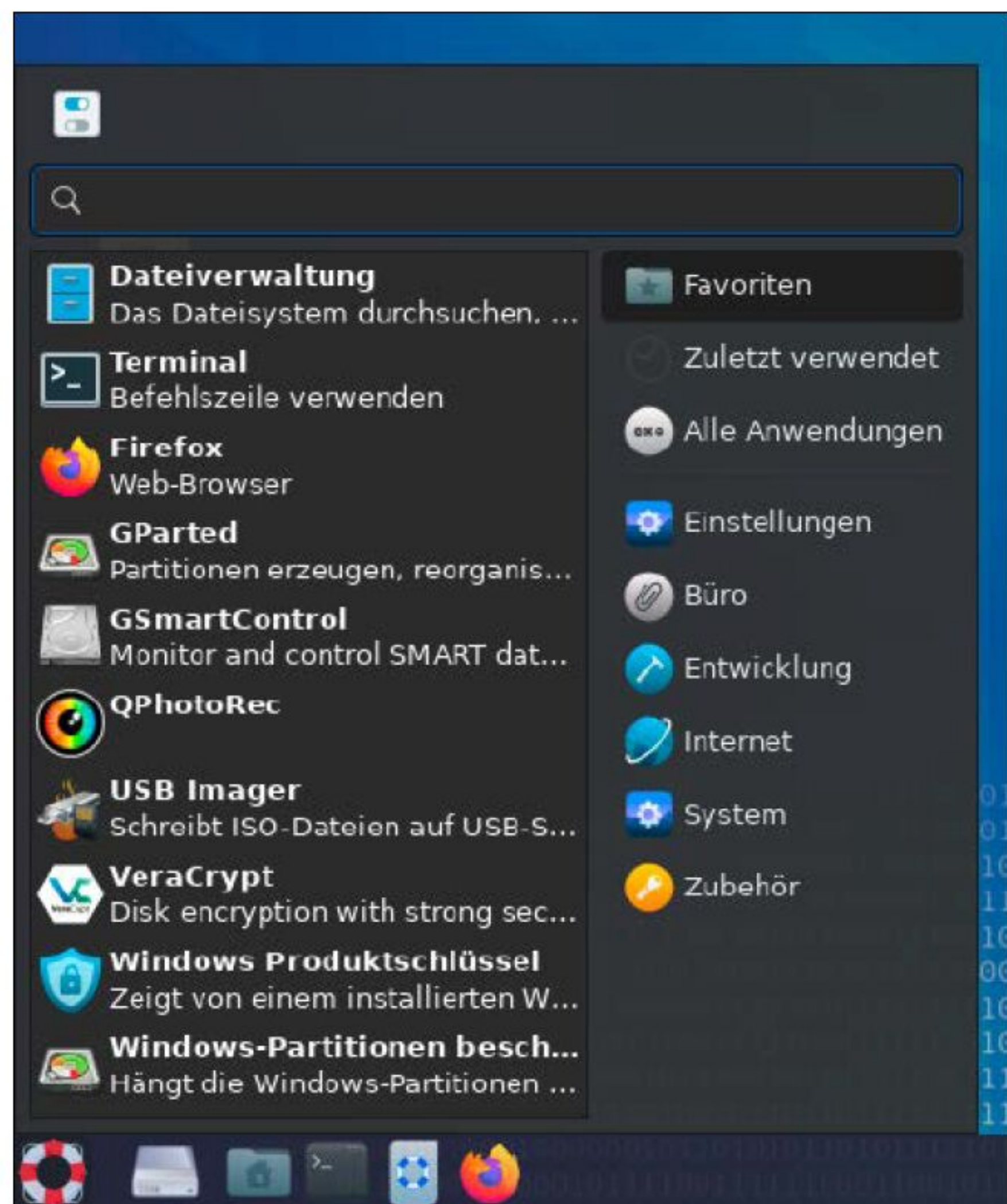
Sie dazu die Heft-DVD ins Laufwerk und starten Sie den Rechner neu. Damit der PC von der Heft-DVD bootet, müssen Sie bei den meisten Rechnern die Taste F8 oder F12 drücken. Die DVD zeigt nun ein Bootmenü: Der oberste Eintrag „Rettungssystem 11 (64 Bit) – Normaler Start“ bootet das Livesys-

tem. Außerdem bietet das Bootmenü als Unterpunkt „Ins RAM kopieren und starten (ab 4 GB)“ an: Diese Startmethode empfiehlt sich für aktuelle Rechner mit viel Arbeitsspeicher. Dabei lädt sich das Linux-System komplett ins RAM. Dies dauert zwar etwas länger, dafür reagiert das laufende System

PC-WELT RETTUNGSSYSTEM 2026: DIE WICHTIGEN TOOLS



Programm (grafisch)	Funktion	Aufruf über
ATA Secure Erase	Löscht SSDs am SATA-Port komplett	Menü → Favoriten
Baobab (neu)	Visualisiert die Datenträgerbelegung	Menü → Zubehör → Baobab
Chromium 135	Deutschsprachiger Webbrowser	Schnellstartleiste
Filezilla 3.69 (neu)	Dateiübertragung im Netzwerk	Menü → Internet
Firefox ESR 128.9	Deutschsprachiger Webbrowser	Schnellstartleiste
Gnome Disks 46.1 (neu)	Datenträgerverwaltung und Mounter	Menü → Zubehör → Laufwerke
Gparted 1.7	Grafischer Partitionierer	Schnellstartleiste
Gsmartcontrol 2.0	Überprüft SMART-Werte von Festplatten	Menü → Favoriten
Hardinfo 0.6	Liefert detaillierte Hardwareinformationen	Menü → Favoriten
NVME Secure Erase	Löscht NVMEs sicher und komplett	Menü → Favoriten
Opera 118	Webbrowser mit eigenem VPN	Menü → Internet
Qphotorec 7.1	Wiederherstellung gelöschter Dateien	Menü → Favoriten
USB Imager 1.0.10	Überträgt das System auf USB-Sticks	Menü → Favoriten
Veracrypt 1.26.7	Verschlüsseler im Stil von Truecrypt	Menü → Favoriten
Zenmap 7.94 (neu)	Grafischer Netzwerkscanner	Menü → Favoriten
Programm (Terminal)	Funktion	Aufruf über
Clam AV 1.4.2	Virens Scanner von Cisco	"clamscan" im Terminal
Clam AV Updater	Aktualisiert Virensignaturen	"sudo freshclam" im Terminal
Clonezilla 3.35	Backup- und Wiederherstellungstool	Schnellstartleiste
Ddrescue 1.2.8	Liest Laufwerke als Image-Datei aus	"sudo ddrescue" im Terminal
Dislocker 0.7.3	Entschlüsselt Bitlocker-Partitionen	"sudo dislocker" im Terminal
Ext4Magic 0.3.2	Wiederherstellung gelöschter Dateien	"sudo ext4magic" im Terminal
Fight Flash Fraud 8.0	Überprüft USB-Sticks und SD-Karten	"f3probe" im Terminal
Midnight Commander 4.8	Dateimanager und Netzwerkclient	"mc" im Terminal
Nmap 7.92	Adress- und Portscanner im Netzwerk	"nmap" im Terminal
Photorec 7.2	Wiederherstellung gelöschter Dateien	"sudo photorec" im Terminal
Testdisk 7.2	Stellt gelöschte Partitionen wieder her	"sudo testdisk" im Terminal
Wimlib 1.14	Öffnet WIM-Archive von Windows	"wiminfo" im Terminal



Alles immer im Blick und sofort per Klick erreichbar: Die Arbeitsfläche des Rettungssystems ist in Version 11 neu gestaltet. Unter „Favoriten“ liegen Verknüpfungen zu den am häufigsten benötigten Tools.

aber sehr schnell, da es nicht mehr auf die DVD zugreifen muss. Für Hardware mit exotischen, sehr alten oder aber besonders neuen Grafikchips ist der Eintrag „Sicherer Grafikmodus (VESA-kompatibel)“ gemacht: In diesem Fall nutzt das System einen kompatiblen Grafiktreiber mit geringer Auflösung, falls der normale Start nicht gelingen sollte. Als weitere Bootoptionen finden sich zudem spezielle Einträge für problematische Grafikchips von Intel, AMD und Nvidia – darauf sollten Sie aber nur zurückgreifen, wenn der normale Start nicht gelingt. Neben dem Bootmenü zeigt das Logo

„BIOS“ oder „UEFI“ stets an, in welchem Modus der Rechner gerade gestartet wurde. Auf dem Desktop des Rettungssystems finden Sie unten eine Taskleiste mit einer Schnellstartleiste. Die wichtigsten Tools sind links daneben im ausklappenden Anwendungsmenü unter „Favoriten“ untergebracht. Sie benötigen für keine Aktion im Livesystem ein Passwort – auch dann nicht, wenn eigentlich Admin-Rechte verlangt werden. Ist Ihr Rechner per Ethernet-Kabel mit einem Internetrouter verbunden, geht das Rettungssystem automatisch online. Für eine WLAN-Verbindung finden Sie unten rechts einen Netzwerkmanager hinter dem Symbol mit den gegengleichen Pfeilen, mit dem Sie sich bei Ihrem Funknetz anmelden.

Dateimanager: Einfach auf Windows-Partitionen zugreifen

Die häufigste Aufgabe für ein Livesystem ist der Zugriff auf Laufwerke und Dateien, wenn das installierte Windows nicht mehr startet. Das Rettungssystem verfügt über einen NTFS-Treiber (NTFS-3G) für das Windows-Dateisystem und kann damit Windows-Partitionen direkt zum Lesen per Klick öffnen sowie Dateien auf einen angeschlossenen USB-Datenträger kopieren. Die erkannten Partitionen sehen Sie in der linken Leiste unter „Geräte“: Sie tragen als Bezeichnung den vorhandenen Partitionsnamen oder die unter Linux übliche Laufwerksbezeichnung, bei der die Partition „sda1“ der ersten Partition (1) auf dem ersten SATA-Laufwerk (Namensteil „sda“) ent-

spricht. Sind Sie sich hier unsicher, hilft ein schneller Klick auf die Partition, um deren Inhalt im Hauptfenster anzuzeigen. Um Dateien und Ordner von der beschädigten Windows-Partition zu retten, ziehen Sie sie einfach mit der Maus von einem Fenster des Dateimanagers in ein anderes mit dem geöffneten Zielort.

Neu im Rettungssystem 2026 ist ein Laufwerk-Symbol links unten neben dem Anwendungsmenü: Ein Klick darauf zeigt die erkannten Partitionen in einer Liste an, ein weiterer hängt die jeweilige Partition ein oder aus. Dieser Mount-Vorgang ist typisch für Linux und ermöglicht dem System den Zugriff aufs Laufwerk, was unter Windows üblicherweise automatisch passiert.

NTFS-Zugriff: Lesen und Schreiben auf Laufwerke ermöglichen

Das neue Rettungssystem behandelt NTFS-Dateisysteme vorsichtiger als der Vorgänger: Es öffnet NTFS-Datenträger zunächst nur zum Lesen. Das ist sinnvoll, da bei allen aktuellen Windows-Versionen die Funktion „Fast Startup“ (Schnellstart) aktiviert ist: Windows verzichtet dann darauf, den Dateisystem-Cache zu leeren und Datenträger vor dem Herunterfahren sauber auszuhängen. Währenddessen darf kein Livesystem auf die noch geöffneten Datenträger schreiben, weil es sonst geöffnete Dateien beschädigen könnte.

Der NTFS-Treiber im Rettungssystem erkennt entsprechende NTFS-Partitionen und weigert sich, sie im Schreibmodus ein-

RETTUNGSSYSTEM PER USB-STICK STARTEN



Sie können das Rettungssystem auch dann nutzen, wenn Ihr PC oder Notebook kein optisches Laufwerk besitzt. Denn unser Livesystem bringt alles mit, um es auf einen USB-Stick zu übertragen: Sie können es dazu am Rechner eines Freundes mit Laufwerk starten oder dafür ein externes optisches Laufwerk am eigenen PC nutzen. Verbinden Sie außerdem einen Stick, dessen Inhalt Sie nicht mehr benötigen, mit dem Rechner. Im gestarteten Rettungssystem gehen Sie im ausklappenden Anwendungsmenü links unten über „Favoriten“ zum Programm „USB Imager“. Nach dem Start wählen Sie im ersten Eingabefeld mit einem Klick auf die drei nebenstehenden Punkte die ISO-Datei des Rettungssystems aus. Sie findet sich beim Start von der Heft-DVD im Dateibrowser im Pfad „sr0 → Image-Dateien → pcw_rettungssystem_11.iso“. Im unteren Feld listet der USB Imager die angeschlossenen Laufwerke mit Namen und Kapazität auf. Nach einem Klick auf „Schrei-

ben“ dauert der Vorgang nur etwa eine Minute. Von diesem USB-Stick können Sie nun das Rettungssystem wie von Heft-DVD starten. Auf dem Stick ist dann allerdings kein Platz mehr frei, auch wenn es die Kapazität zuließe. Dies ist eine Nebenwirkung des verwendeten ISO-9660-Dateisystems.

Rettungsstick unter Windows erstellen: Das Open-Source-Tool **USB Imager 1.0.10** gibt es auch für Windows (auf Heft-DVD, Download unter <https://gitlab.com/bztsrc/usbimager>, deutschsprachig). Es sieht beinahe genauso aus wie die Linux-Version und verfügt über die gleichen Funktionen. Um das Rettungssystem unter Windows auf einen USB-Stick zu übertragen, muss dieser ab 2 GB Kapazität haben. Außerdem benötigen Sie die Heft-DVD dieser PC-WELT-Ausgabe mit der ISO-Datei des Rettungssystems: Sie befindet sich gepackt als „pcw_rettungssystem_11.zip“ im Unterordner „pcwsoft“.

zuhängen. Um mit dem Rettungssystem auf Windows-Partitionen zu schreiben, müssen Sie deshalb die Schnellstart-Funktion zuerst abschalten oder das System sauber herunterfahren. Das erledigen Sie in der Eingabeaufforderung, die Sie mit Administrator-Rechten starten. Geben Sie dort den Befehl

```
shutdown /s /t 0
```

ein, um Windows sauber herunterzufahren. Im Rettungssystem gehen Sie anschließend auf „Menü → Favoriten → Windows-Partitionen (RW)“, um ein Script auszuführen, das die Windows-Datenträger mit NTFS beschreibbar macht. Das Script prüft auch, ob die Partitionen tatsächlich korrekt eingehängt sind.

Das Schreiben auf NTFS-Partitionen erfolgt auf eigene Gefahr. Aber manchmal müssen Sie dieses Risiko eingehen, wenn beispielsweise das Windows-System nicht mehr booten will und die NTFS-Partitionen in einem inkonsistenten Zustand verbleiben. In diesem Fall können Sie im Terminal mit dem Befehl

```
sudo ntfsfix /dev/sda3
```

die Sperre vom NTFS-Laufwerk /dev/sda3 entfernen und dabei Cache-Informationen verwerfen. Dies kann zu Dateiverlust führen, wenn Dateien im Windows-System noch geöffnet waren, ist aber nur nötig, um Schreibrechte zu erlangen.

Bitlocker entsperren per Passwort oder Schlüssel

Unter Windows sind Laufwerke normalerweise per Bitlocker verschlüsselt. Das neue Rettungssystem kann damit einfach umgehen: Ein Klick im Dateimanager auf ein Bitlocker-Laufwerk mit Passwort und auf einen Datenträger mit Bitlocker to go fragt das entsprechende Kennwort ab.

Wenn statt des Passworts nur der Wiederherstellungsschlüssel für die Bitlocker-Partitionen bereitsteht, nutzen Sie im Rettungssystem das Programm „dislocker“ in der Kommandozeile. Es erlaubt, Bitlocker-Laufwerke mit einem korrekten Schlüssel einzuhängen, ebenfalls im Schreib-Lese-Modus. Dazu müssen Sie zunächst im laufenden Rettungssystem die Bitlocker-Laufwerke mit ihrer Partitionskennung identifizieren. Einfach geht das über den grafischen Partitionseditor **Gparted**, der verschlüsselte Partitionen deutlich mit dem Dateisystemtyp „Bitlocker“ kennzeichnet. Wenn Sie die korrekte Partition gefunden haben, beispiels-

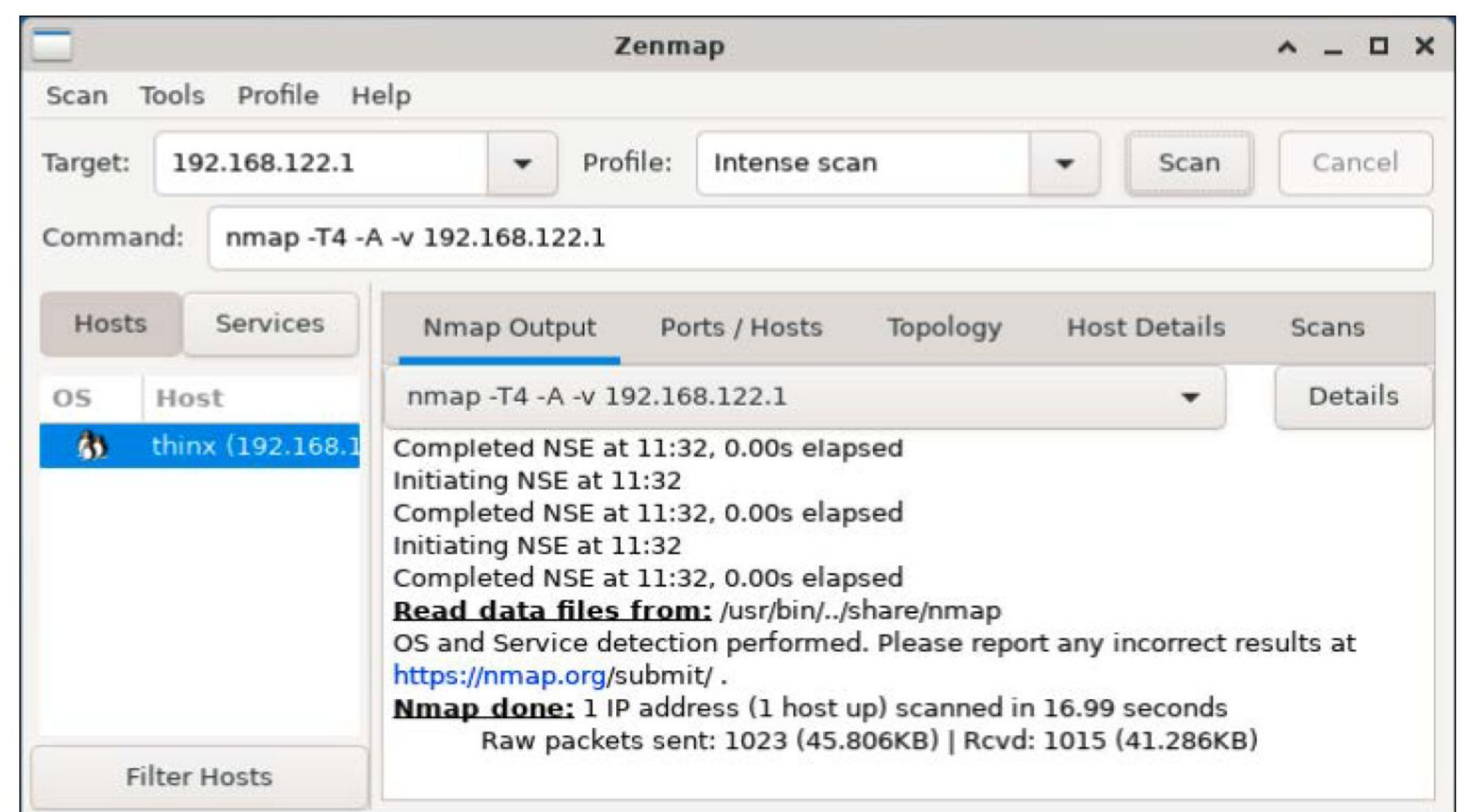
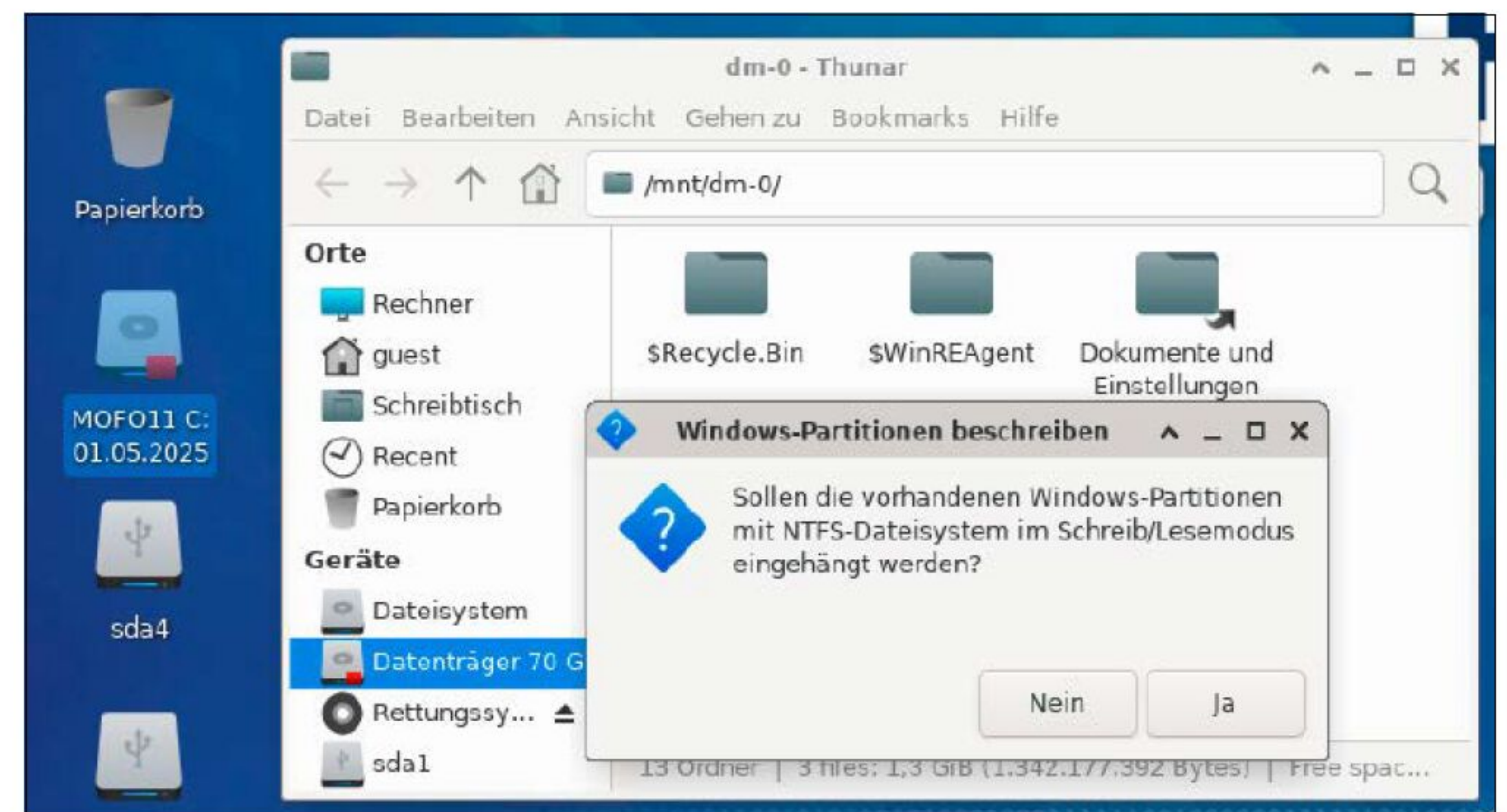
weise „/dev/sda3“, öffnen Sie ein Terminalfenster, und zwar über das erste Symbol von links in der Schnellstartleiste. Geben Sie dort das Kommando

```
sudo dislocker-metadata -V /dev/sda3
```

ein, um den Inhalt der angegebenen Partitionen zu analysieren. Dies dient zur Bestätigung, dass es sich um die richtige Partition handelt. Zum Entschlüsseln und Einhängen der verschlüsselten Partition verlangt Dislocker zwei Einhängpunkte, also Verzeichnisse. Diese erstellen Sie am besten unterhalb des Ordners „/mnt“ mit den folgenden Befehlen im Terminal:

```
sudo mkdir /mnt/bitlocker
sudo mkdir /mnt/laufwerk
```

In das Verzeichnis wird zunächst mittels Dislocker die Bitlocker-Partition als entschlüsseltes NTFS-Image eingehängt. Dazu benötigen Sie den numerischen Wiederherstellungsschlüssel („Recovery-Key“/„Recovery-Passwort“) einer chiffrierten Windows-Partition, den ein Windows-System bei der ersten Erstellung eines Bitlo-



Zenmap im Netzwerk: Dieser Portscanner arbeitet als grafische Oberfläche für Nmap. Es ist damit möglich, in einem Netzwerk eine Topologie der anderen erreichbaren Hosts zu erstellen.

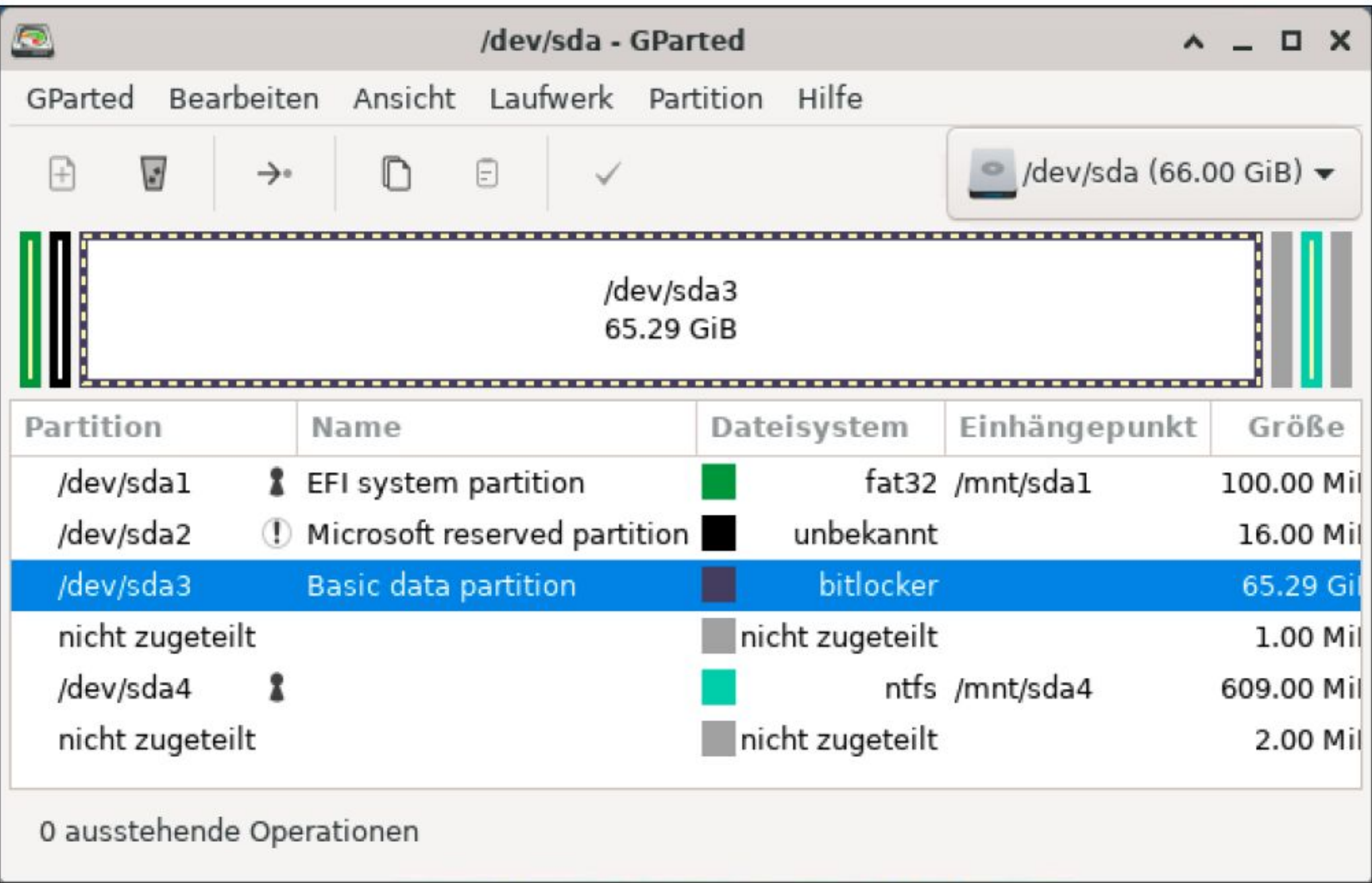
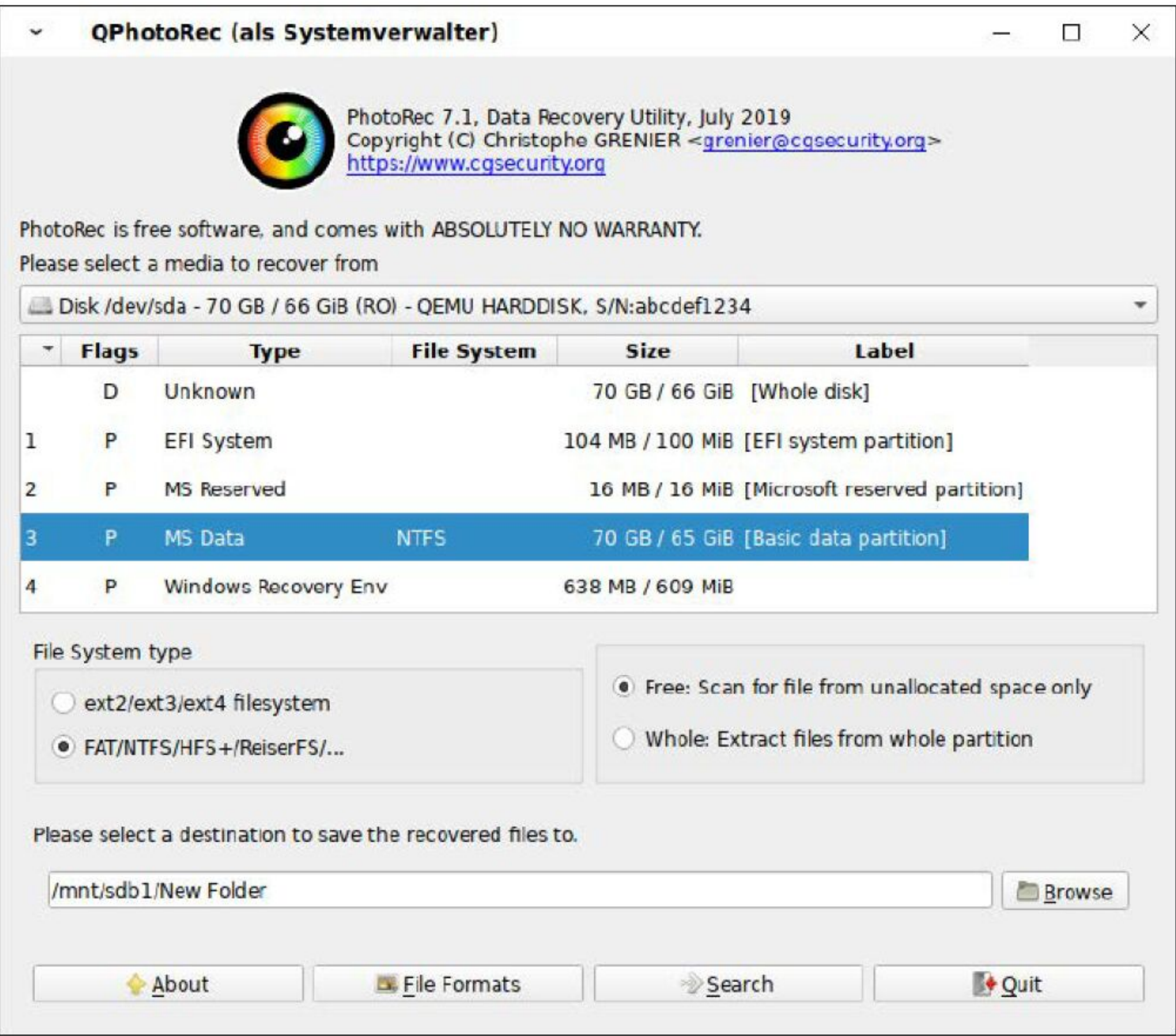
cker-Laufwerks zur Sicherung anbietet. Das Kommando

```
sudo dislocker -v -V /dev/sda3 -p /mnt/bitlocker/
```

entschlüsselt die Partition „/dev/sda3“ und fragt dafür das sudo-Passwort und anschließend das Bitlocker-Kennwort beziehungsweise den Wiederherstellungsschlüssel mit 55 Stellen ab. Stimmen die Eingaben, zeigt der Befehl

```
sudo ls /mnt/bitlocker/
```

die Datei „dislocker-file“ im Zielverzeichnis an. Dieses Image müssen Sie jetzt als Loopback-Gerät einhängen. Das Kommando `sudo mount -o loop /mnt/bitlocker/dislocker-file /mnt/laufwerk` hängt das NTFS-Laufwerk in der Datei „dislocker-file“ im Schreib- und Lesemodus nach „/mnt/laufwerk“ ein. Mit dem vorhandenen Dateimanager kann das Rettungssystem nun lesend auf den gesamten Inhalt der Bitlocker-Partition zugreifen. Auch hier gilt: Soll ein Bitlocker-Laufwerk beschrieben werden, müssen Sie zunächst Windows komplett beenden.



Wiederbelebung: Gelöschte Dateien retten

Selbst IT-Experten passiert das manchmal: Eine noch benötigte Datei landet unter Windows nicht im Papierkorb, sondern wird irrtümlicherweise direkt vom Speichermedium entfernt. Nun gilt es, unverzüglich Schreibvorgänge auf dem Speichermedium zu stoppen und mit der Datei-Wiederherstellung zu beginnen – Sie sollten also sofort Windows beenden und das Rettungssystem starten, um die Datei zurückzuholen. Dafür nutzen Sie das Programm **Qphotorec** (Menü → Favoriten → Qphotorec): Es durchsucht die freien Bereiche von ganzen Dateisystemen und stellt von dort Dateien anhand ihres Typs und einer heuristischen Suche in einem Zielverzeichnis auf einem anderen Datenträger wieder her. Welche Bezeichnungen die Quell- und Zielpartitionen haben, ermitteln Sie im Partitionierer Gparted. Im Beispiel soll das Quelllaufwerk mit Windows

und den gelöschten Dateien die Kennung „/dev/sda“ haben. In Qphotorec wählen Sie oben im Feld dieses Laufwerk aus und darunter die einzelne Partition, die analysiert werden soll. Bei Windows ist dies üblicherweise die Partition, die mit „MS Data“ beschrieben ist und das Dateisystem NTFS hat. **Wichtig:** Diese Partition darf im Livesystem nicht eingehängt sein, nur dann ist eine Suche nach gelöschten Dateien erfolgreich. Unter „File System Type“ ist die Standardauswahl „FAT/NTFS/HFS+“ korrekt. Danach können Sie den freien Platz („Free“) oder das gesamte Laufwerk („Whole“) nach gelöschten Dateien durchsuchen, wobei „Free“ schnell und zuverlässig genug ist. Wichtig ist ganz unten die Auswahl eines eingehängten Ziellaufwerks im Feld „Please select a destination to save the recovered files to“. Hier müssen Sie einen anderen, eingehängten Datenträger angeben, der genügend Platz für die wiederhergestellten Dateien hat.

Heuristische Suche nach gelöschten Dateien: Das grafische Programm Qphotorec arbeitet rigoros und findet viel. Ein Ziellaufwerk sollte deshalb ausreichend groß sein, denn Hunderte Megabyte sind schnell zusammen.

Weiterhin eines der wichtigsten Programme im Rettungssystem: Der Partitionierer Gparted liegt jetzt in der neuen Version 1.7 vor und ändert Partitionen ohne Datenverlust.

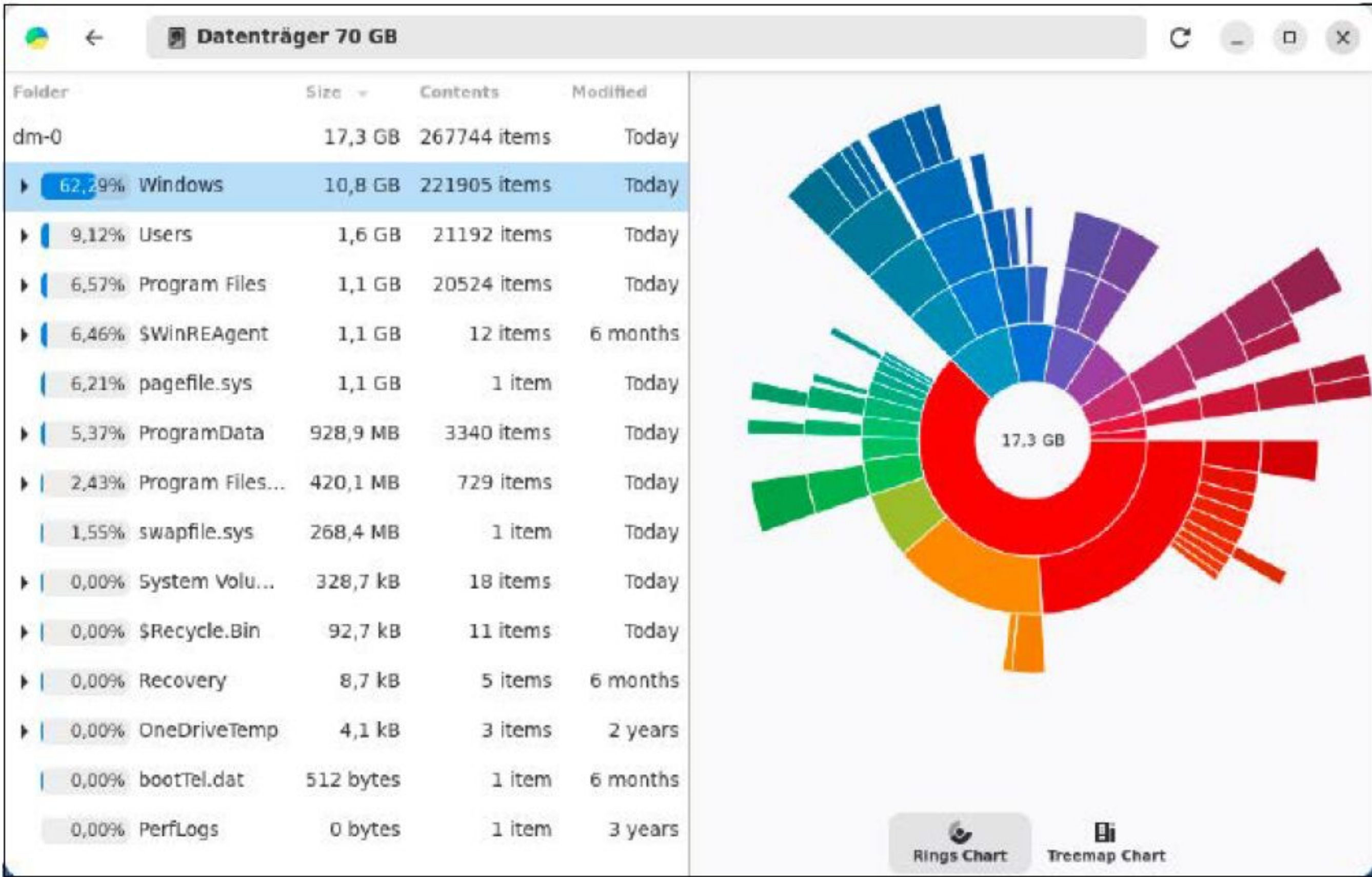
Die heuristische Suche von Qphotorec analysiert die Datei-Header, um Dateitypen zu unterscheiden. Je genauer Sie den jeweils gesuchten Dateityp einschränken, desto schneller arbeitet das Programm bei der Wiederherstellung. In der Standardeinstellung stellt Qphotorec alle gelöschten Dateien wieder her, was aufgrund der Datenmenge nicht sinnvoll ist. Klicken Sie aus diesem Grund auf die Schaltfläche „File Format“ ganz unten. In der Liste entfernen Sie mit „Reset“ zuerst die Haken vor allen bekannten Dateitypen, um anschließend gezielt nur die zu markieren, die gesucht werden sollen. Unter den Typ „zip“ fallen übrigens auch Dokumente von Microsoft Office und Libre Office, da diese ZIP-komprimiert sind. Je nach Größe des Datenträgers kann der Suchlauf einige Stunden dauern: Er findet meist sehr viele wiederherstellbare Dateien, die Sie danach auf dem Zieldatenträger im angelegten Unterverzeichnis „recup_dir.1“ prüfen sollten. Denn Dateinamen stellt Qphotorec nicht wieder her.

Partitionieren & Formatieren: Tools für Festplatten und SSDs

Das Rettungssystem enthält den Partitionierer **Gparted** in der neuesten Version 1.7: Sie rufen ihn auf über „Menü → Favoriten → Gparted“ oder in der Schnellstartleiste. Das Tool ist auch für die Repartitionierung von (unverschlüsselten) Windows-Dateisystemen ein unverzichtbarer Helfer. Gparted eignet sich zur Neupartitionierung, Partitionsänderung und Formatierung. Es unterstützt eine große Anzahl von Dateisystemen und Partitionstabellen aus dem Umfeld von Linux, Unix, Apple und Windows. Die SMART-Werte von SATA-Laufwerken zeigt das Tool **Gsmartcontrol** an, das sich ebenfalls in den „Favoriten“ findet. Um den aktuellen Zustand eines Laufwerks zu erfahren, rufen Sie das Untermenü „Self-Tests“ auf, das dafür einen kurzen „Short Self-Test“ oder einen ausführlichen, stundenlangen „Extended-Test“ bietet. Das neue Tool **Baobab** analysiert und visualisiert die Datenträgerbelegung durch verschiedene Diagramme, die Verzeichnisse als farbige Elemente darstellen. Ein Klick auf ein Verzeichnis steigt in diese Ebene herab und berechnet die Belegung ab diesem Punkt neu. Um nicht mehr benötigte Laufwerke sicher zu löschen, bietet die ATA-Spezifikation bei SSDs am SATA-Bus das spezielle Kommando

ATA Secure Erase. Es überschreibt bei einem Format-Befehl den gesamten Datenträger inklusive reservierter Bereiche der „Sector Reallocation“, die im normalen Betrieb nicht zugänglich sind. Bei SSDs setzt dieser Befehl den Datenträger in den Werkszustand zurück – die SSD ist damit wieder so schnell wie am ersten Tag. Ein grafisches Tool für ATA Secure Erase und die Auswahl einer SSD enthält das Rettungssystem unter „Menü → Favoriten“. Seien Sie besonders vorsichtig bei der Auswahl und der Identifikation des Datenträgers anhand der angezeigten Geräte-ID sowie der Modellbezeichnung: Denn die Dateien auf dem ausgewählten Laufwerk gehen nach den nächsten Schritten unwiederbringlich verloren. Sehen Sie in der Liste die Spalte „Eingefroren“ zu einer SSD mit dem Eintrag „ja“, lässt sich dieses Laufwerk nicht sofort löschen. Hier hilft der Trick, den Rechner kurz in den Ruhezustand zu versetzen und wieder aufzuwecken. NVMe-SSDs nutzen nicht mehr SATA, sondern PCI-Express als Bussystem. Trotzdem lassen sich viele NVMe-Laufwerke ebenfalls komplett löschen mit dem Befehl „User Data Format“. Ob er sich nutzen lässt, hängt von der Firmware des Laufwerks ab – bei Marken-Laufwerken ist dies meist der Fall. Im Rettungssystem gehen Sie zum Löschen von NVMe-SSDs zu „Menü → Favoriten → **NVME**

So steht es um die Auslastung Ihrer Datenträger: Das Tool Baobab ist ein Neuzugang im Rettungssystem und visualisiert die Datenbestände auf verschiedenen Verzeichnisebenen.



Secure Erase – der Befehl funktioniert auf die gleiche Weise wie ATA Secure Erase.

Clam AV: Nach Malware suchen

Auch ein Virens scanner darf im Rettungssystem nicht fehlen: Es ist das freie Programm **Clam AV**, das Sie im Livesystem einfach über eine Onlineverbindung mit den neuesten Viren-Signaturdateien aktualisieren. Bei Tests von Antivirenprogrammen liegt es zwar meist hinter der kommerziellen Konkurrenz, erkennt mittlerweile aber über 8,5 Millionen Schadprogramme. Trotzdem ist der Viren-Check per Livesystem sinnvoll: Denn dann kann sich fortgeschrittene Malware nicht in einem laufenden Windows-System verstecken, indem sie ei-

nen aktiven Virenschutz per Windows-API manipuliert. Für eine zweite Meinung ist Clam AV daher in jedem Fall empfehlenswert. Der Virens scanner findet sich unter „Menü → Favoriten → Clam AV GUI“. Wenn Sie ihn aufrufen, erscheint unten rechts im Infobereich ein Symbol: Ein Klick darauf öffnet das Programmfenster, wo Sie zuerst über die Schaltfläche „Update now!“ die Virendefinitionen aktualisieren sollten. Im Untermenü „Scan“ markieren Sie dann zum Scannen einen Ordner auf einem eingehängten Laufwerk und starten den Check mit „Start“. Clam AV 1.4.2 ist wegen der wachsenden Menge der Malware-Signaturen recht speicherhungrig und läuft daher nur auf Rechnern ab 4 GB RAM. ■

EXTRAS: NOCH MEHR BOOTFÄHIGE TOOLS



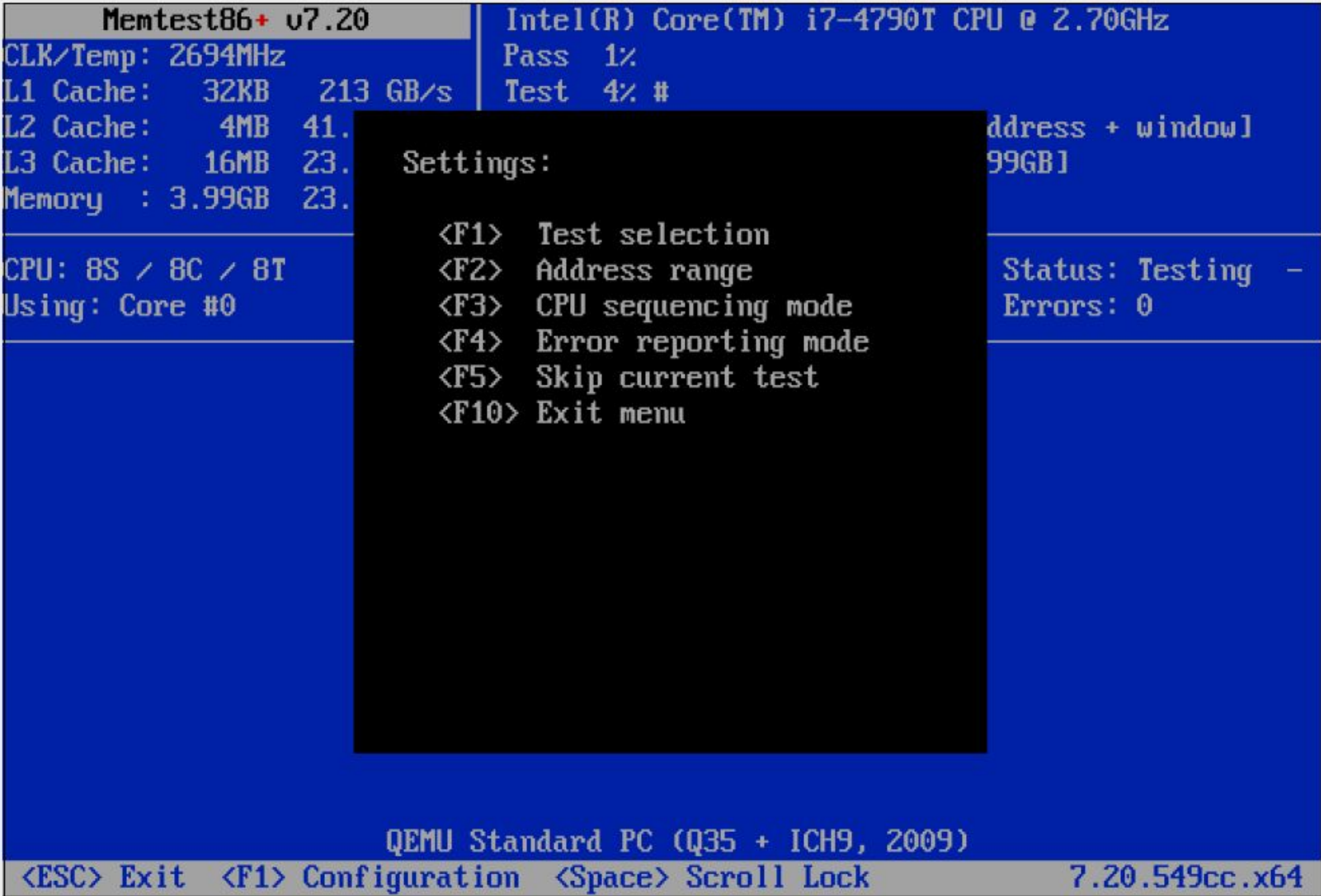
Neben dem Rettungssystem finden Sie im Multibootmenü der Heft-DVD noch drei weitere startfähige Tools, die unverzichtbare Hilfestellungen bei einem PC-Notfall leisten können. Im Menü der DVD sind diese Werkzeuge unter „Extras & Tools“ verfügbar.

Memtest 86+ 7.2: Unzuverlässige und überhitzte RAM-Bausteine sorgen für plötzliche Abstürze und instabile Systeme. Memtest 86+ überprüft den Arbeitsspeicher eines Rechners anhand vergleichender Muster und findet damit nach längeren Testreihen auch minimale Fehler. Neu im Rettungssystem ist jetzt die Unterstützung für DDR4-RAM.

Hardware Detection Tool 0.5.2: Dieses Tool hilft, schnell den Überblick zur Hardware eines Systems zu bekommen. Es ist ideal, wenn Sie die Konfiguration eines PCs untersuchen möchten, auf dem noch kein Betriebssystem installiert ist. Dieses Tool startet nur im Bios-Modus und nicht unter Uefi.

Shred OS 2021.08.2: Dies ist ein bootfähiges Löschwerkzeug für komplette Festplatten. Es löscht Daten auf magnetischen Laufwerken endgültig, sodass auch forensische Wiederherstellungstools keine Information mehr von der Platte kratzen können.

nen. Shred OS unterstützt mehrere Löschmethoden mit Überschreibmodus, um eine Festplatte unwiderruflich zu löschen.



Memtest 86+ 7.20: Das Speichertestprogramm hat ein Update für DDR4-RAM und den AMD Zen erhalten. Es ist über das Untermenü „Extras & Tools“ im Bootmenü der Heft-DVD startfähig.

Datenrettung leicht gemacht

Seit SSDs die mechanischen Festplatten abgelöst haben, ist die Wiederherstellung gelöschter Dateien deutlich schwieriger geworden. Doch Windows hat immer noch einige Tricks auf Lager. Die nötigen Programme finden Sie auf der Heft-DVD.

VON ROLAND FREIST

Einmal nicht aufgepasst, und schon ist es passiert: Mit einem Druck auf die Entf-Taste hat man eine Datei gelöscht, die man eigentlich noch benötigt. Zum Glück gibt es in Windows Sicherheitsmechanismen, die einen Datenverlust in den meisten Fällen auffangen. So landen gelöschte Dateien zunächst im Papierkorb, aus dem man sie mit wenigen Klicks wieder an ihren alten Speicherort zurückkopieren kann.

Doch wenn Sie Dateien von einer Freigabe auf einem anderen Rechner in Ihrem Netzwerk oder in der Eingabeaufforderung löschen, versagt dieser Mechanismus, und

„Wer sein Windows richtig konfiguriert und zusätzlich ein externes Backup-Tool einsetzt, kann sich bei der Datenrettung entspannt zurücklehnen.“



die Daten sind weg. In der Vergangenheit leisteten Datenrettungsprogramme wie **Re-cuva** gute Arbeit beim Rekonstruieren auch dieser Dateien. Doch aufgrund der Eigenheiten moderner SSD-Laufwerke funktioniert das nur noch eingeschränkt. Die Sicherung wichtiger Daten gewinnt daher eine deutlich größere Bedeutung.

Den Dateiversionsverlauf nutzen

Windows bringt zum Sichern von Dateien den Dateiversionsverlauf mit. Sie rufen ihn über die Systemsteuerung auf. Tippen Sie „system“ ins Suchfeld der Taskleiste und gehen Sie in der Symbolansicht auf „Dateiversionsverlauf“. In der Kategorie-Ansicht klicken Sie unter „System und Sicherheit“ auf „Speichern von Sicherungskopien Ihrer Dateien mit ‚Dateiversionsverlauf‘“. Beginnen Sie mit einem Klick auf „Laufwerk auswählen“ und markieren Sie das Laufwerk, das die Sicherungen aufnehmen soll. Falls kein passendes Laufwerk zur Verfügung steht, klicken Sie auf „Netzwerkadres-

se hinzufügen“ und geben Sie eine Freigabe auf einem anderen Rechner an. Klicken Sie danach auf „Einschalten“, um den Dateiversionsverlauf zu aktivieren.

Weiter geht es mit „Erweiterte Einstellungen“. Hier können Sie zum einen einstellen, wie oft das Programm Ihre Dateien sichern soll. Da das Tool dafür entworfen wurde, die Rückkehr zu früheren Versionsständen zu ermöglichen, ist eine Stunde voreingestellt. Außerdem können Sie an dieser Stelle angeben, wie lange der Dateiversionsverlauf die verschiedenen Versionen aufheben soll. Über „Versionen bereinigen“ können Sie zudem eine Frist einstellen, nach der ältere Versionen gelöscht werden.

In der Voreinstellung sichert das Programm die Dateien aus Ihren lokalen Bibliotheken und vom Desktop sowie die in Windows gespeicherten Kontakte und Favoriten. Um den Sicherungen weitere Dateien und Ordner hinzuzufügen, weisen Sie sie einer Bibliothek zu. Dazu klicken Sie einen Ordner mit der rechten Maustaste an und gehen

auf „Weitere Optionen anzeigen → In Bibliothek aufnehmen“ und wählen dann eine der angezeigten Bibliotheken aus. Über „Ordner ausschließen“ im Fenster des Dateiversionsverlaufs können Sie wiederum einzelne Bibliotheken oder darin enthaltene Ordner aus den Sicherungen herausnehmen. Um später eine Datei oder eine frühere Version zurückzuholen, klicken Sie auf „Persönliche Dateien wiederherstellen“.

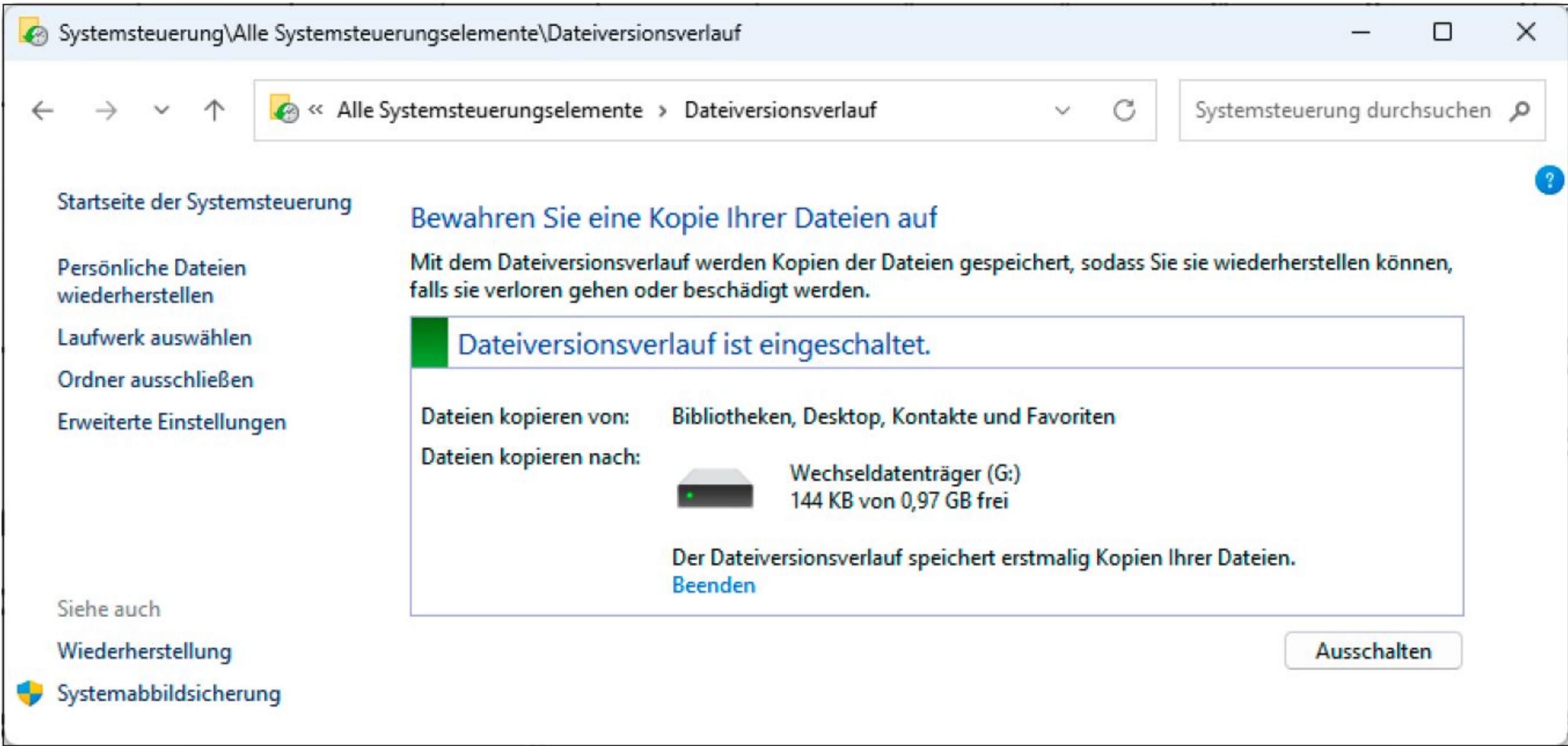
Der Dateiversionsverlauf ist allerdings kein Allheilmittel, das Sie vor allen Datenverlusten durch versehentliche Löschungen und das Überschreiben älterer Versionen sicher schützt. Dennoch ist es sinnvoll, das Programm zu aktivieren. **Doch Achtung:** Die Zeitspanne zwischen den Sicherungen sollte nicht zu klein gewählt werden, und auch ein dauerhaftes Speichern älterer Versionen ist nicht zu empfehlen. Denn der Dateiversionsverlauf beherrscht keine Komprimierung, so dass schnell große Datenvolumen zusammenkommen.

Sie öffnen den Dateiversionsverlauf in der Systemsteuerung in der Ansicht „Kategorien“, unter „System und Sicherheit → Dateiversionsverlauf → Persönliche Daten wiederherstellen“.

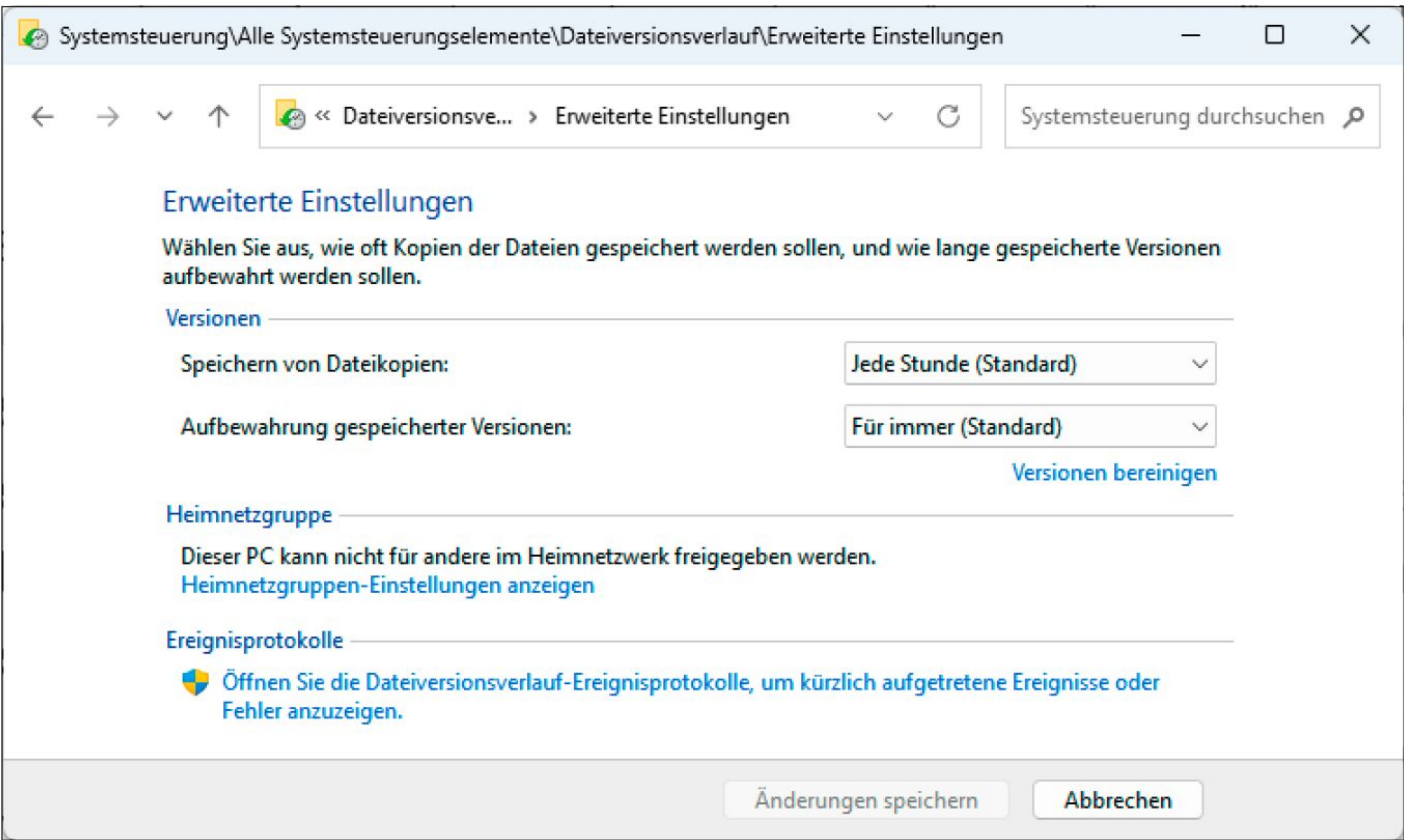
Dateiwiederherstellung mit Recuva

Ein anderes Werkzeug zur Wiederherstellung gelöschter Dateien kommt aus der Freeware-Szene. **Recuva** erweist sich bereits seit Jahren in Tests immer wieder als unschlagbar, wenn es um die Rettung von Daten geht. Das Tool funktioniert auf internen Festplatten genauso wie auf den Speicherkarten von Fotoapparaten, auf USB-Sticks und externen USB-Disks. Auf SSDs kann es allerdings zu Problemen kommen, dazu gleich mehr.

Recuva liest in einem ersten Schritt die Master File Table (MFT) des gewählten Laufwerks ein und sucht dort nach Gelöscht-Flags. Darüber hinaus bietet es einen Tiefenscan an, bei dem die Software auf Da-



Der Dateiversionsverlauf muss zunächst aktiviert werden und sichert dann Dateien aus ausgewählten Ordnern auf ein zweites Laufwerk. Eine zweite Partition genügt nicht, es muss ein weiteres Laufwerk sein.



Per Voreinstellung sichert der Dateiversionsverlauf jede Stunde eine Kopie Ihrer Dokumente und bewahrt sie unbegrenzt lange auf. Beides lässt sich in den Einstellungen ändern.

tenmuster achtet, die auf Dateiformate wie etwa DOCX oder JPG hinweisen. Entdeckt sie einen Datei-Header, der auf ein bekanntes Format schließen lässt, erscheint das File in Recuva in einer Liste, die alle gelöschten und eventuell wiederherstellbaren Files aufführt. Nach einem Doppelklick auf einen dieser Namen versucht das Programm, die Datei wieder nutzbar zu ma-

chen. Das funktioniert im Allgemeinen ausgezeichnet und mit guten Erfolgsaussichten. Der Trim-Befehl moderner SSDs macht Tools wie Recuva jedoch häufig einen Strich durch die Rechnung.

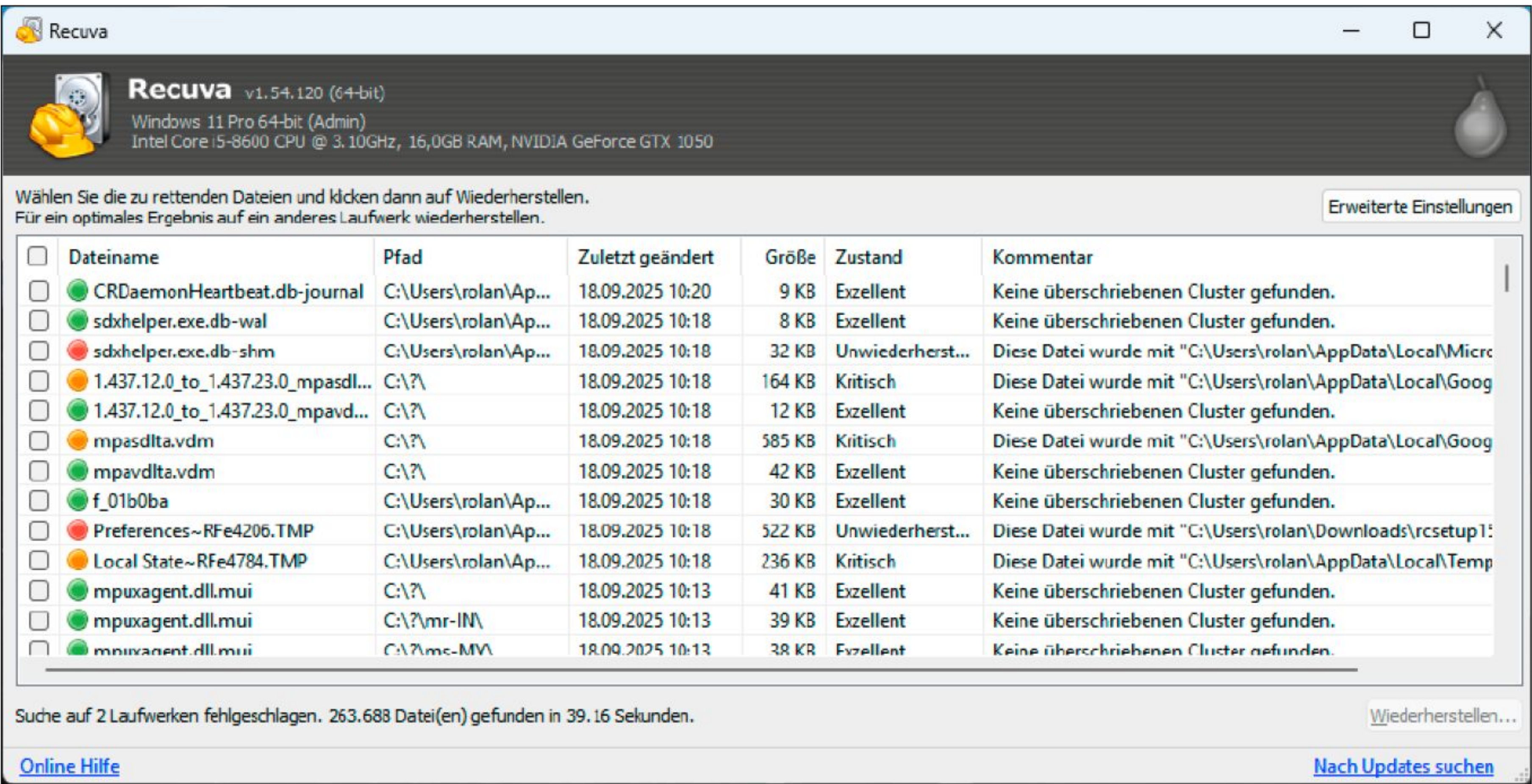
Wie der Trim-Befehl funktioniert

Jede moderne SSD mit ATA-Schnittstelle beherrscht den Trim-Befehl zur Verwaltung

IM ÜBERBLICK: TOOLS FÜR DIE DATENRETTUNG



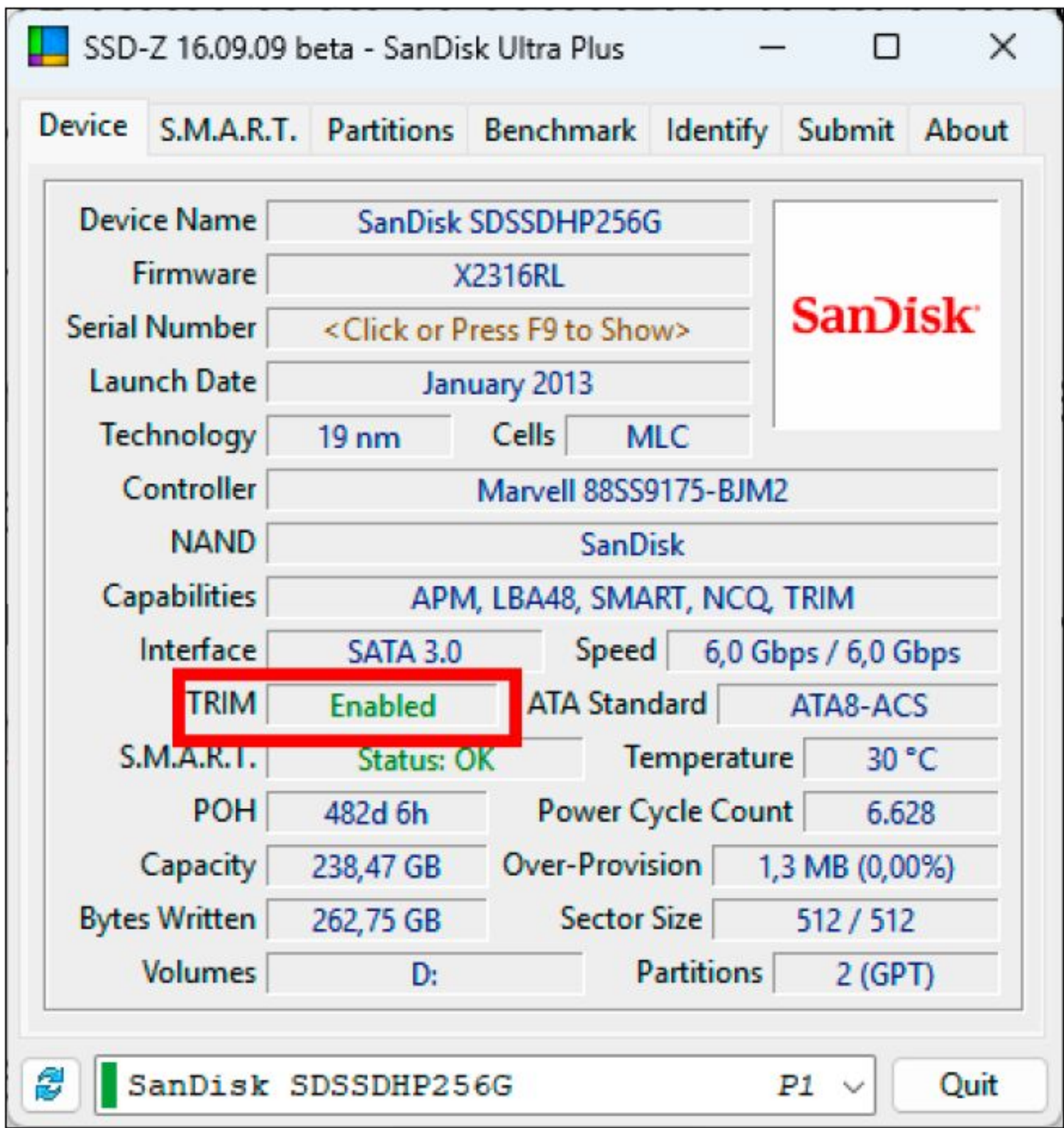
Name	Beschreibung	Auf	Internet	Sprache	Preis
Aomei Backupper Standard	Backup-Programm	Heft-DVD	www.pcwelt.de/1686627	Deutsch	kostenlos
Ashampoo Backup Pro	Backup-Programm	Heft-DVD	www.pcwelt.de/1143745	Deutsch	kostenlos
Easeus Todo Backup Free	Backup-Programm	Heft-DVD	https://tinyurl.com/3rvcsnb9	Deutsch	kostenlos
Paragon Backup & Recovery	Backup-Programm	Heft-DVD	https://tinyurl.com/mr3a5kr8	Deutsch	kostenlos
Recuva	Dateiwiederherstellung	Heft-DVD	www.pcwelt.de/1134926	Deutsch	kostenlos
SSD-Z	SSD-Analyse	Heft-DVD	www.pcwelt.de/1152107	Englisch	kostenlos



Recuva sucht in der Master File Table nach gelöschten Dateien und untersucht deren Beschaffenheit. Grün bedeutet, dass es gute Chancen für eine Wiederherstellung gibt.

der Inhalte ihrer Speicherzellen. Normalerweise ist dieser Befehl bereits ab Werk aktiviert. Auch SSDs mit NVMe-Schnittstelle können „trimmen“. Bei diesen Modellen nennt sich der Befehl „Deallocate“, die Funktionsweise ist jedoch die gleiche.
Darum geht es: Wenn Sie auf einer SSD eine oder mehrere Dateien löschen, werden die zugehörigen Speicherbereiche als frei gekennzeichnet. Das heißt jedoch nicht, dass Windows oder eine Anwendung dort wie bei einer mechanischen Festplatte sofort wieder Daten ablegen könnten. Stattdessen müssen diese Speicherbereiche zunächst geleert werden.

Solange auf der SSD noch genügend bislang nicht genutzter Speicher frei ist, ist alles in Ordnung. Doch sobald der freie Speicher knapp wird, und Windows auf die als frei gekennzeichneten Speicherbereiche zurückgreifen muss, senkt das notwendige Leeren dieser Bereiche von alten Daten die Zugriffsgeschwindigkeit. Um das zu verhindern, haben die Hardware- und Software-Hersteller den Trim-Befehl entwickelt. Wenn sich der PC im Leerlauf befindet, teilt Windows der SSD mit, welche Speicherbereiche gelöscht wurden und befiehlt ihr, diese Bereiche vorsorglich schon einmal von den Restdaten zu



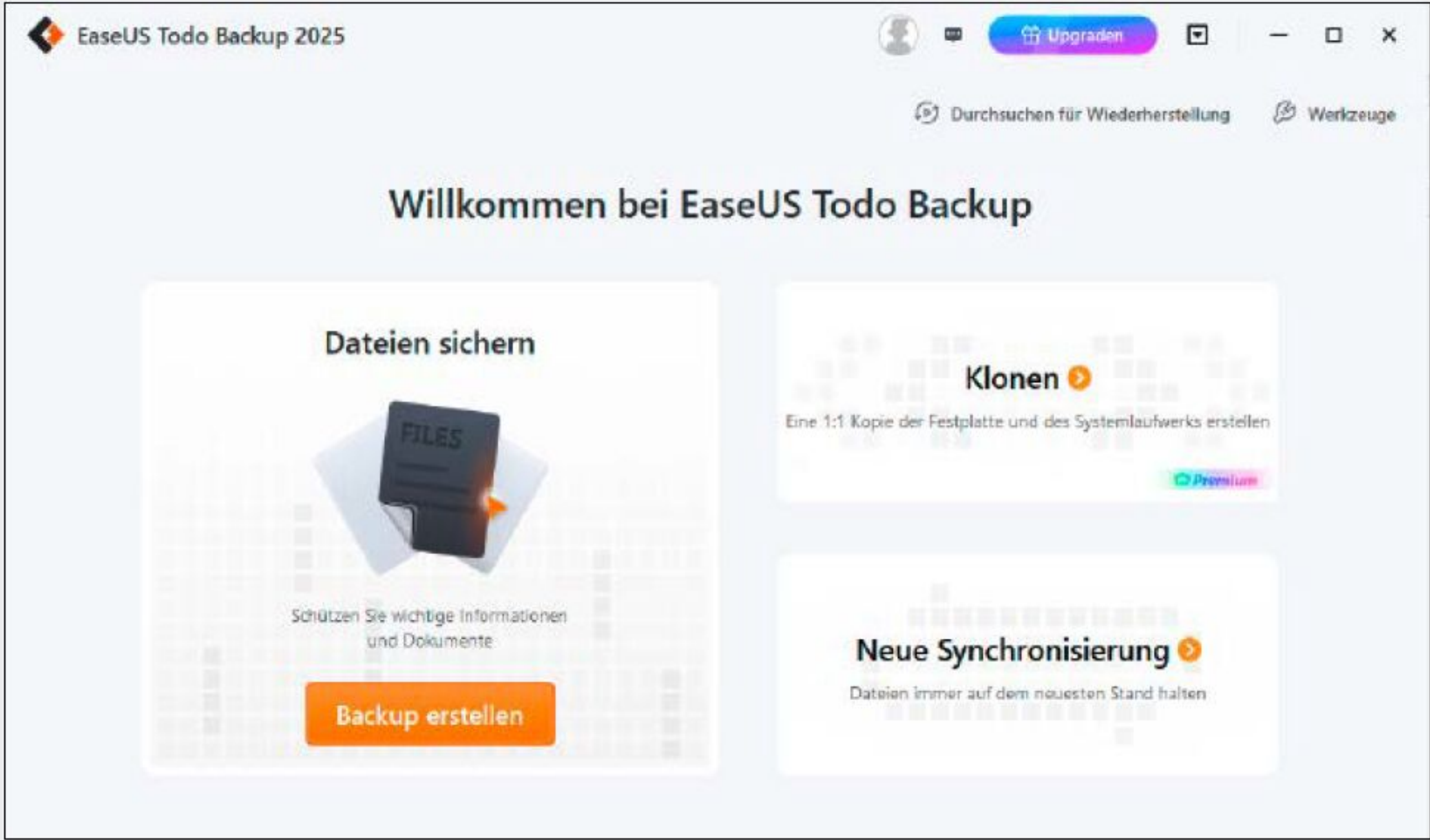
Mit dem Utility SSD-Z ermitteln Sie, ob Ihre SSD den Trim-Befehl unterstützt, und ob er aktiv ist.

befreien. Auf diese Weise steht dieser Speicher wieder für das Befüllen mit Dateien zur Verfügung, und es kommt bei Speichervorgängen zu keinen Verzögerungen. Was sich allerdings positiv auf die Geschwindigkeit der SSD auswirkt, hat einen negativen Effekt auf die Chancen zur Wiederherstellung der gelöschten Dateien. Denn sobald die SSD Dateifragmente nach Aufforderung durch den Trim-Befehl entfernt hat, gibt es keine Möglichkeit mehr, die Files zu rekonstruieren. Der Trim-Befehl muss sowohl von der Hardware, also der SSD, wie auch vom Betriebssystem unterstützt werden. Heute

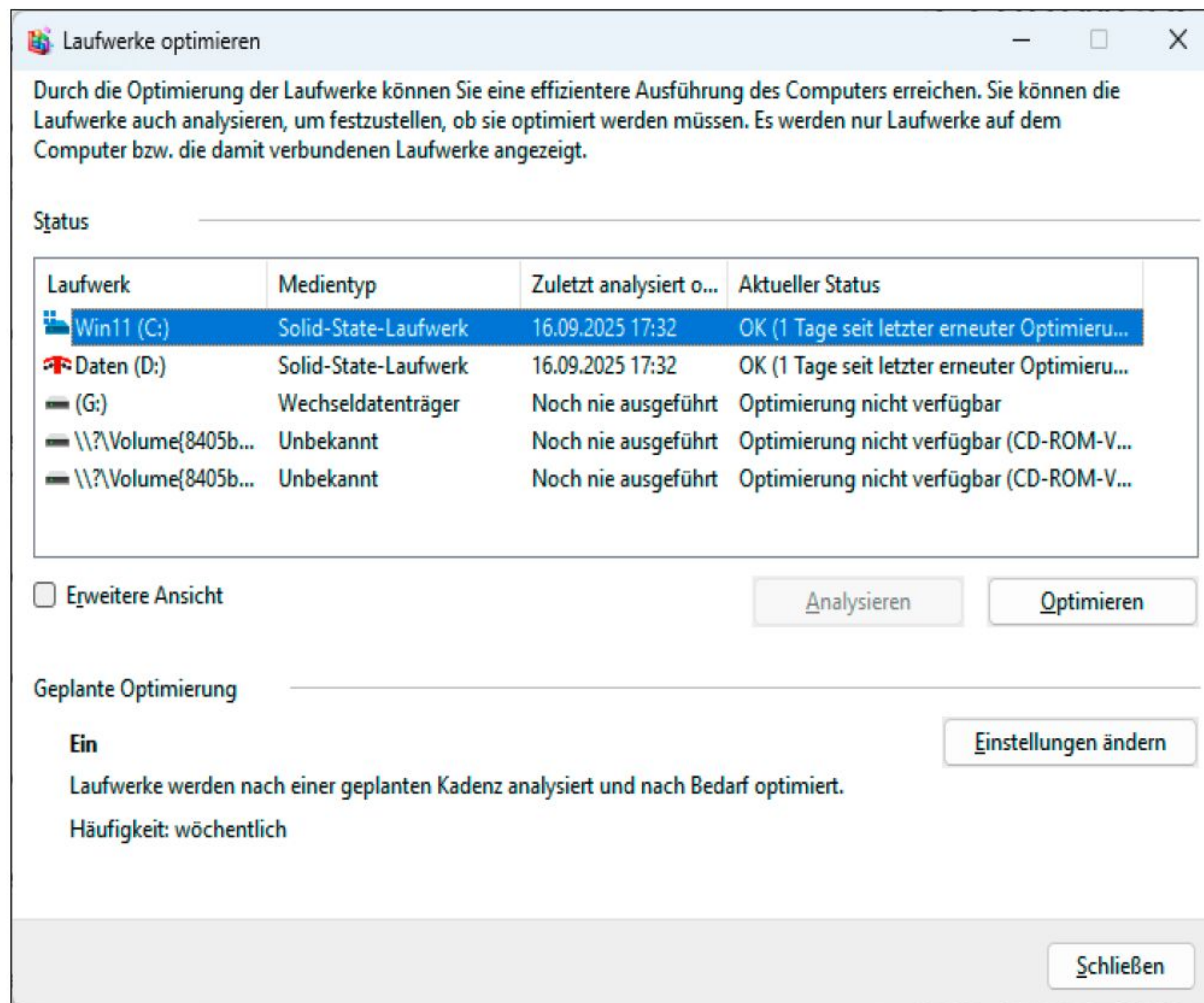
KOSTENLOSE BACKUP-PROGRAMME

- Aomei Backupper Standard:** Der Aomei Backupper überzeugt bereits in der kostenlosen Variante durch eine klar gegliederte Oberfläche und Möglichkeiten zum Sichern einzelner Dateien, Partitionen, Festplatten sowie des gesamten Windows-Systems. Hinzu kommen Funktionen zum Synchronisieren und Klonen.
- Ashampoo Backup Free:** Das Ashampoo-Backup zeichnet sich durch ein Sicherungssystem aus, mit dem Sie auch bei einem defekten, nicht mehr bootfähigen Windows auf Ihre Sicherungen zugreifen können. In der kostenlosen Version fehlen unter anderem ein Cloudbackup und die Möglichkeit zum Verschlüsseln der Sicherungen. Auf der Heft-DVD finden Sie daher auch die Vollversion **Ashampoo Backup Pro**.
- Easeus Todo Backup Free:** Das Backup-Programm von Easeus sichert Dateien, Ordner und ganze Partitionen sowie komplette Images der Festplatte. Es kann inkrementelle und differentielle Sicherungen anlegen und Backup-Sätze verschlüsseln.
- Paragon Backup & Recovery Community Edition:** Paragon bietet ein Rettungssystem, mit dem Sie ein gesichertes Windows-System auf eine andere Festplatte mit abweichender Größe kopie-

ren können. Beim Sichern unterstützt die Software ganze Festplatten und Partitionen, einzelne Dateien und Ordner und ein inkrementelles Backup.



Die kostenlose Version des Backup-Programms von Easeus kann nicht nur Dateien und Ordner sichern, sondern auch komplette Partitionen und Images der Festplatte. Dabei beherrscht es inkrementelle und differentielle Sicherungen.



Die Laufwerkoptimierung von Windows sagt Ihnen, wann der Trim-Befehl für ein bestimmtes Laufwerk zuletzt ausgeführt wurde.

beherrschen alle SSD-Laufwerke diese Technik, lediglich einige sehr alte Modelle können nicht trimmen. Ob Ihre SSD dazu gehört, ermitteln Sie mit der Freeware **SSD-Z**. Sie zeigt Ihnen im Register „Device“ im Feld „TRIM“ an, ob der Befehl in der SSD aktiv ist oder nicht. In Windows ist der Trim-Befehl seit Version 7 integriert.

Einstellungen für den Trim-Befehl

Windows gibt den Trim-Befehl in der Voreinstellung einmal pro Woche. Außerdem kommt der Befehl automatisch zum Einsatz, wenn Sie auf einem SSD-Laufwerk Dateien löschen. In beiden Fällen ist Voraussetzung, dass sich der Rechner im Leerlauf befindet. Zum dritten können Sie die Ausführung auch manuell anstoßen. Ob und wie oft Windows 11 der SSD den Befehl zum Trimmen gibt, steuern Sie über die Einstellungen des Betriebssystems: Öffnen Sie das Startmenü und wählen Sie „Einstellungen → System“. Gehen Sie auf der rechten Seite auf „Speicher“ und klicken Sie im nächsten Fenster auf „Erweiterte Speichereinstellungen“. Scrollen Sie nach unten und gehen Sie auf „Laufwerkoptimierung“.

Klicken Sie im Fenster „Laufwerk optimieren“ im Abschnitt „Geplante Optimierung“ auf „Einstellungen ändern“. Im darauffolgenden Fenster ist standardmäßig die „Ausführung nach Zeitplan“ aktiv, als „Häufigkeit“ ist „Wöchentlich“ eingestellt. Wenn Sie das Häkchen bei „Ausführung nach Zeitplan“ entfernen, deaktivieren Sie

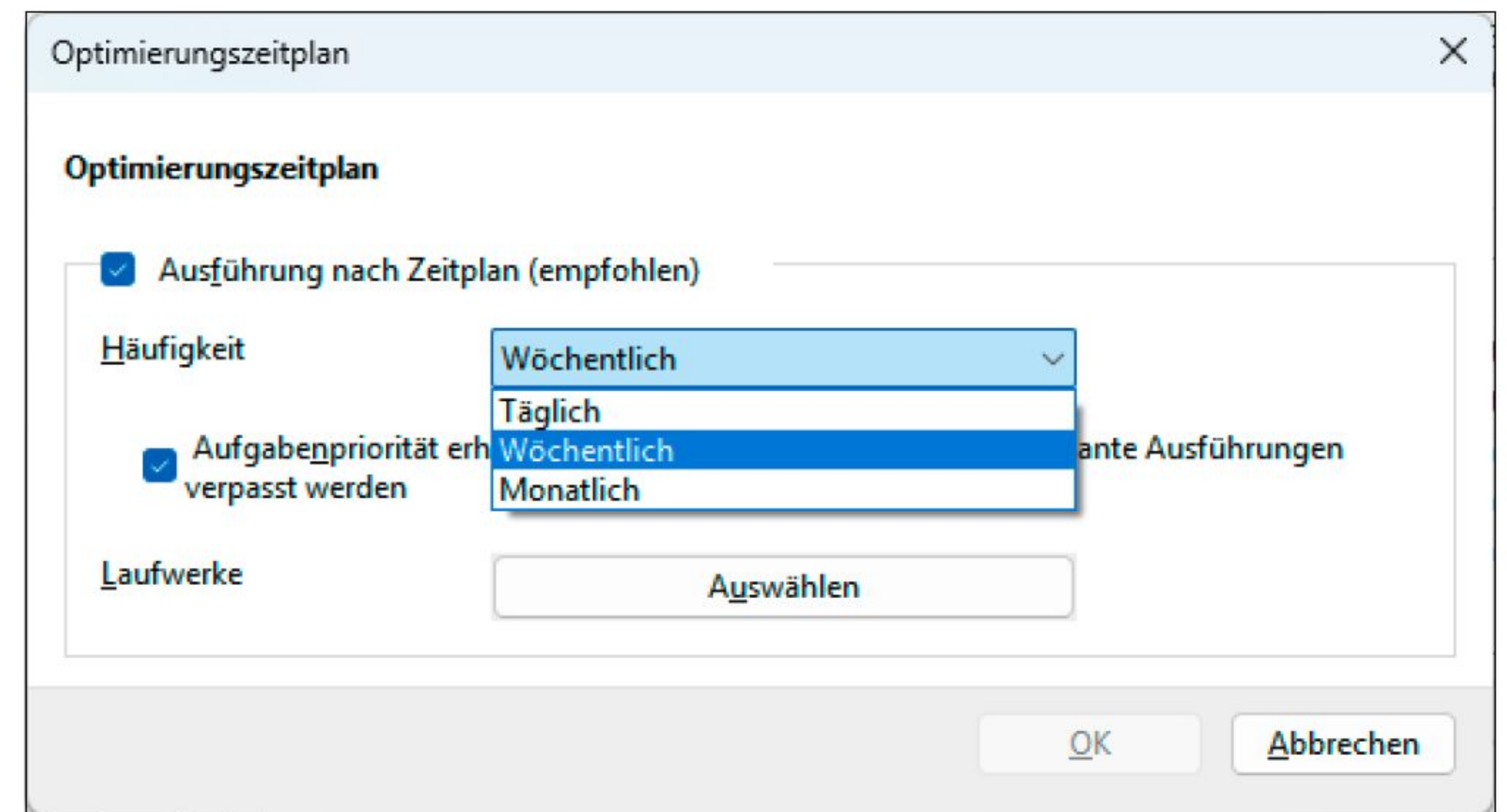
Der Maildienst Web.de umfasst in seiner kostenlosen Version 2 GB freien Onlinespeicher für Backups von Dokumenten, Fotos und Videos. Bei anderen Diensten erhalten Sie bis zu 10 GB.

den Trim-Befehl. Damit bleibt der Inhalt der Speicherzellen Ihrer SSD länger erhalten, und gelöschte Dateien lassen sich mit Tools wie Recuva wiederherstellen. So lange noch genügend Platz auf der SSD ist, bildet das kein Problem. Erst wenn der Speicher stark gefüllt ist, nimmt die Geschwindigkeit beim Schreiben von Daten langsam etwas ab.

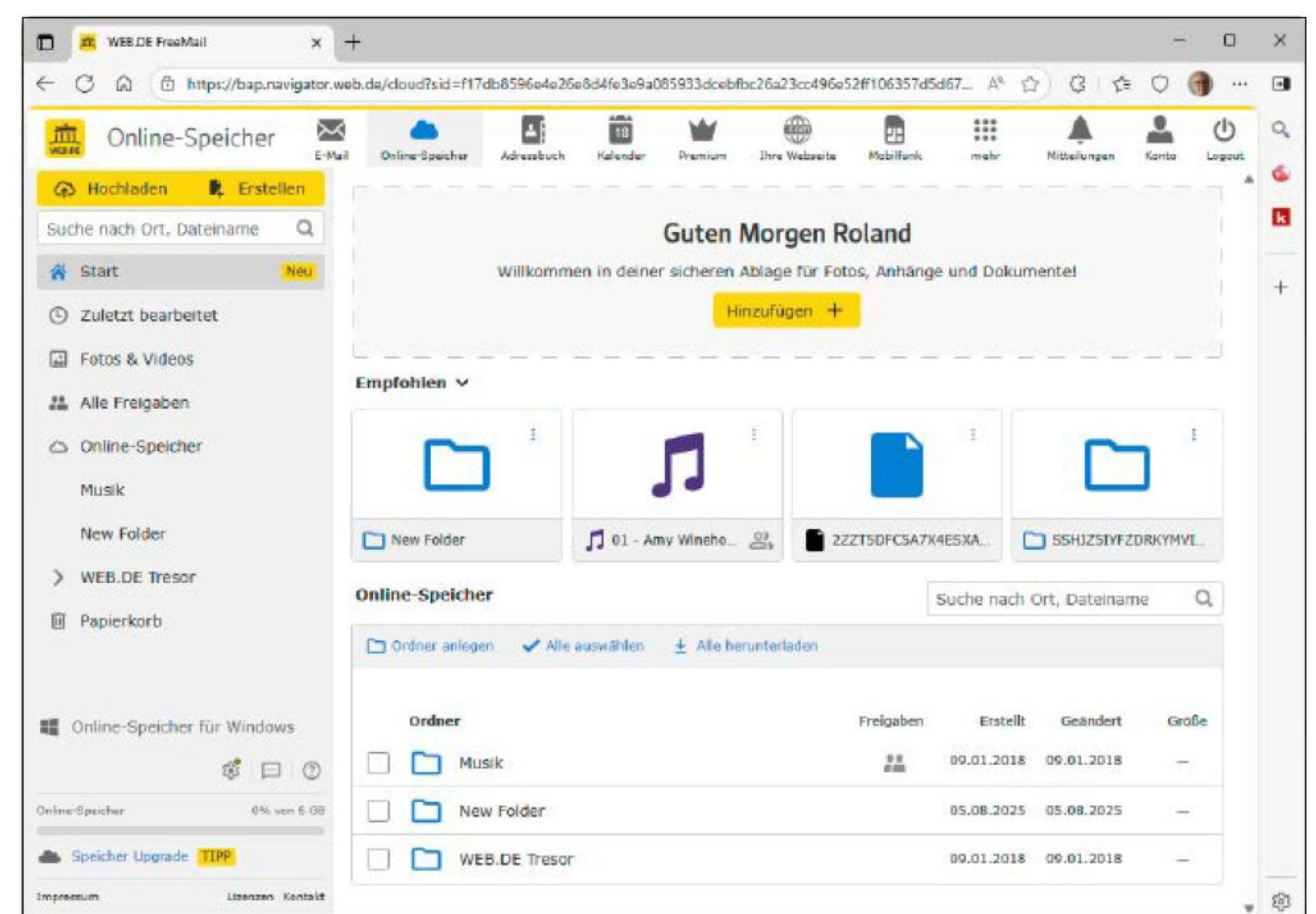
Daten regelmäßig sichern

Durch den Trim-Befehl gibt es beim Speichern von Daten auf einer SSD einen Konflikt zwischen bestmöglicher Datensicherheit auf der einen Seite und optimierter Geschwindigkeit auf der anderen. Dieses Dilemma lässt sich am besten lösen, indem Sie Ihre Daten regelmäßig sichern, so dass Sie sie nach einem versehentlichen Löschen einfach und sicher wiederherstellen können.

Die einfachste Form der Sicherung ist das manuelle Kopieren wichtiger, noch benötigter Dateien auf ein externes Medium wie etwa eine USB-Festplatte oder einen USB-Stick. Wer ein privates Netzwerk ein-



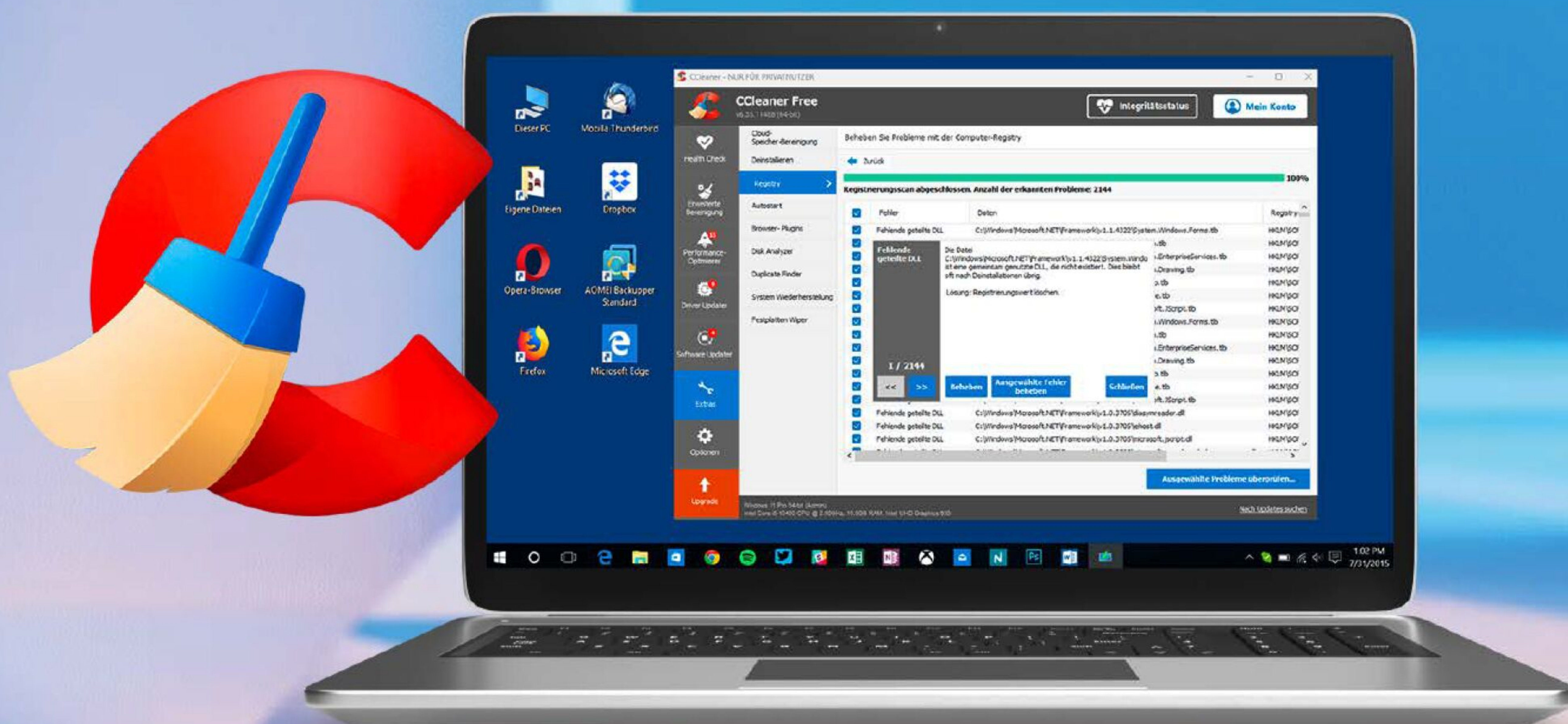
In der Laufwerkoptimierung von Windows stellen Sie ein, ob und wie oft der Trim-Befehl bei Ihren SSDs tätig werden soll.



gerichtet hat, kann die zu sichernden Daten auch in eine Freigabe auf einem anderen Computer übertragen.

Eine andere Möglichkeit ist die Synchronisierung ausgewählter Ordner mit einem Clouddienst. Registrierte Windows-Nutzer bekommen von Microsoft 5 GB freien Speicher bei Onedrive, Dienste wie Web.de, GMX, Dropbox und die Telekom geben 2 bis 10 GB kostenlos ab. Platz genug, um wichtige Office-Dokumente und eine Auswahl an Fotos zu sichern. Für wenig Geld lässt sich dieser Speicherplatz auf 100 oder mehr Gigabyte erweitern.

Die bequemste Lösung ist jedoch ein Backup-Programm, denn es erledigt die Sicherungen selbsttätig und automatisch. Tools wie **Aomei Backupper**, **Easeus Todo Backup Free**, **Ashampoo Backup Free** und **Paragon Backup & Recovery Community Edition** erlauben die gezielte Auswahl zu sichernder Dateien und Ordner, bieten einen Zeitplan für ihre Sicherungen und beherrschen neben einem Vollbackup auch die platzsparenden Varianten Differential- und inkrementelles Backup. ■



© Mit Material von adobestock3d - AdobeStock

CCleaner für mehr Platz und Leistung

Weniger Datenmüll, mehr Speicherplatz, bessere Performance und weniger PC-Probleme verspricht der Hersteller von CCleaner. Wir zeigen die Funktionen zur Windows-Optimierung im Detail und bieten Gratis-Alternativen für Features der kostenpflichtigen Pro-Version.

VON PETER STELZEL-MORAWIETZ

CCleaner ist längst ein Klassiker unter den Systemoptimierern für Windows, in diesem Jahr feiert das Tool sein 20-jähriges Jubiläum. Mittlerweile wurde die Freeware nach

„Die individuelle Systemanalyse von CCleaner entdeckt und löscht überflüssige Dateien, die schon seit Jahren die Festplatte zumüllen.“

Angaben des Anbieters weltweit fast drei Milliarden Mal heruntergeladen. Zeit also, das Programm ausführlich vorzustellen. Nur zur Erklärung: Das große Doppel-C am Wortanfang ist kein Schreibfehler, die Schreibweise stammt vielmehr von der früheren Toolbezeichnung Crap Cleaner, auf Deutsch „Sch...wegräumer“. Ausgesprochen wird der Name übrigens englisch, in Lautschrift also ['si:kli:nər].

Die Software geht beim Löschen sehr behutsam und ziemlich intelligent vor. So löscht das Programm weder Dateien, die die Systemstabilität beeinträchtigen würden, noch Log-in-Daten für E-Mail und Ähnliches, die Sie anschließend wieder erneut eingeben müssten.

Die Installation von **CCleaner** ist einfach und im Kasten „CCleaner-Setup“ erläutert.

Dort weisen wir auf die portable Version hin, die ohne Installation startklar ist, und die Sie auch auf einem USB-Stick für die Nutzung auf anderen Windows-Rechnern mitnehmen können.

Bevor es gleich richtig losgeht, ein erster Tipp: Deaktivieren Sie in CCleaner unter „Optionen → Privatsphäre“ alle angeklickten Häkchen. Damit unterbinden Sie das Senden jeglicher Daten an den Hersteller.

System und Festplatte mit wenigen Mausklicks aufräumen

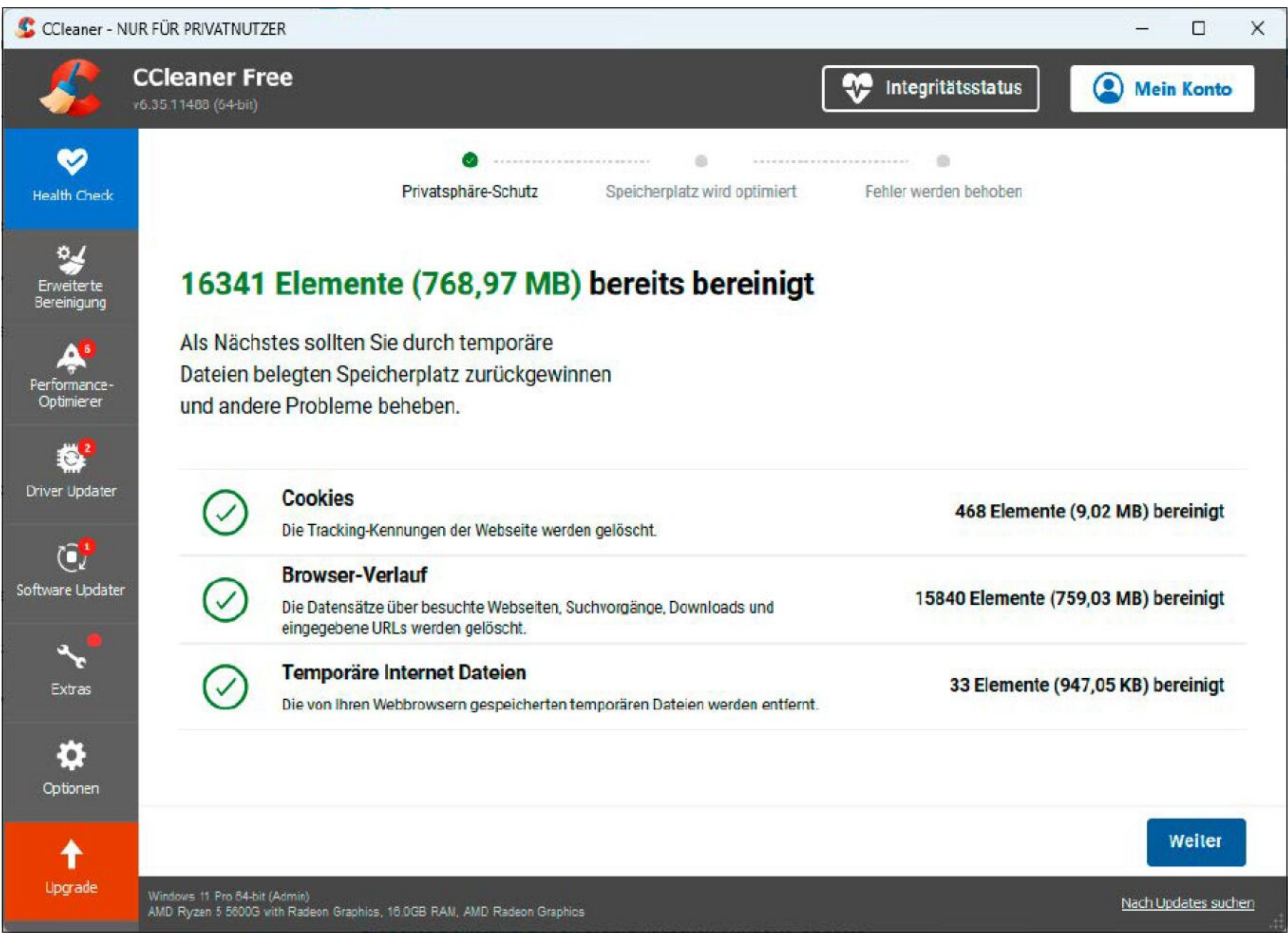
Beim Starten schlägt CCleaner vor, einen ersten Systemscan durchzuführen. Dem folgen Sie bitte mit einem Klick auf den zentralen Button. Später können Sie das System über „PC scannen“ jederzeit erneut überprüfen. Falls Sie dabei bestimmte Pro-

gramme wie einen Browser geöffnet haben, werden Sie aufgefordert, diese zu schließen. Als Ergebnis der Analyse schlägt das Tool in aller Regel Hunderte oder Tausende Elemente zum Löschen vor. Gleichzeitig sehen Sie, wie viel zusätzlicher Platz auf der Festplatte dabei frei wird. Mit einem Klick auf „Bereinigen“ folgen Sie den Vorschlägen und räumen so die Festplatte Ihres Rechners auf.

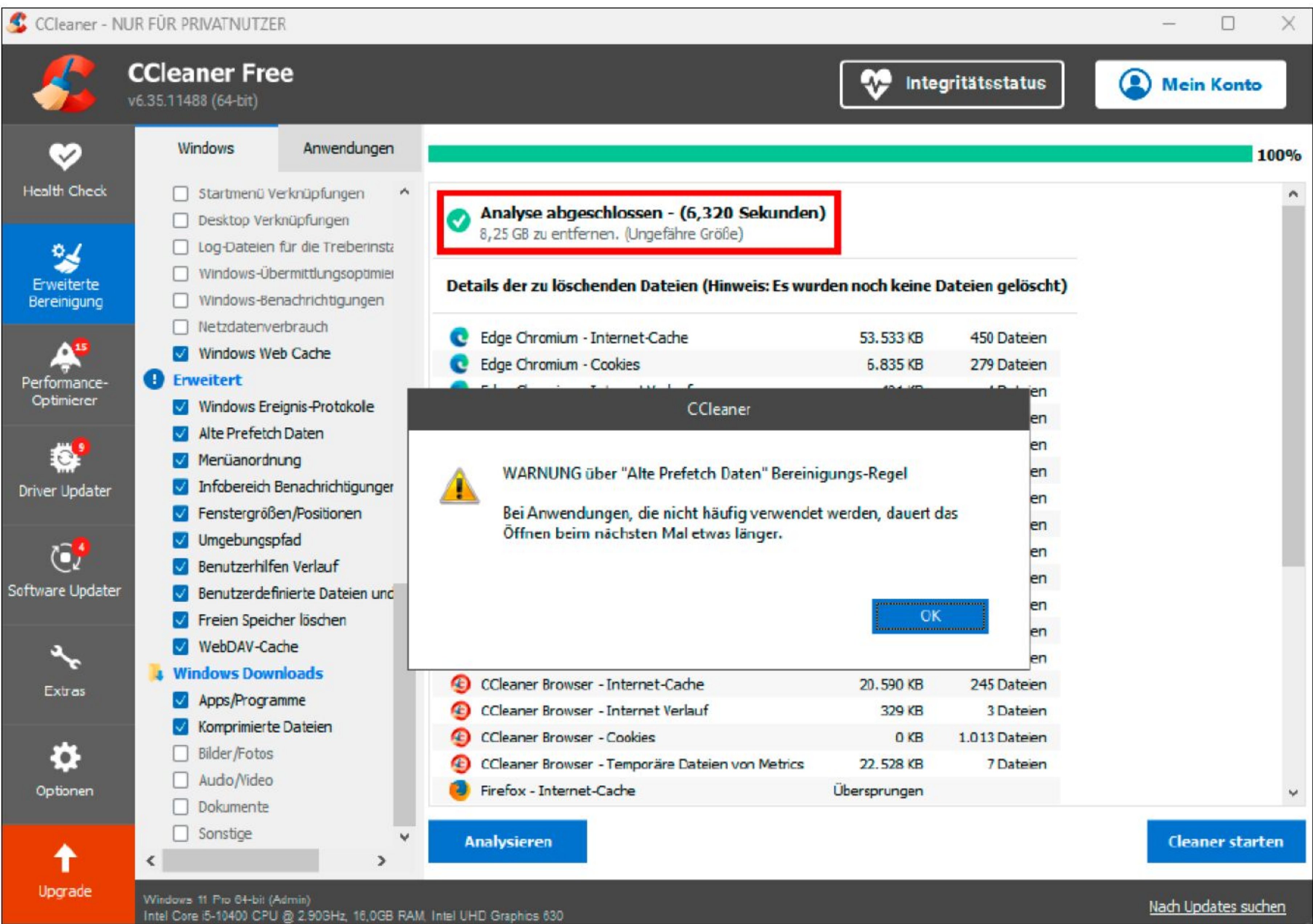
Neben diesem „Health Check“ genannten Schnelldurchlauf bietet die „Erweiterte Bereinigung“ links in der Aufgabenleiste weitere und detailliert einstellbare Möglichkeiten zum Aufräumen. Unterteilt sind diese Optionen in die beiden Bereiche „Windows“ und „Anwendungen“.

In der ersten Rubrik können Sie kleinteilig auswählen, was CCleaner im Betriebssystem löschen soll und was eben nicht. So ist es beispielsweise durchaus sinnvoll, heruntergeladene Programme und komprimierte Dateien aus dem Download-Ordner zu löschen. Denn diese Daten benötigen Sie nach dem Installieren beziehungsweise Extrahieren in aller Regel nicht mehr, während Sie Bilder oder Dokumente aus dem Internet vielleicht behalten möchten. Die meisten Optionen sind selbsterklärend und haben auf das Funktionieren des Rechners keinen unmittelbaren Einfluss. Anders verhält es sich bei den als „Erweitert“ markierten Einstellungen. Hier blendet CCleaner deshalb jeweils eine kurze Erläuterung der gewählten Funktion ein, sobald Sie einen Eintrag markieren.

Bei den „Anwendungen“ glänzt das Programm damit, dass der Anwender nach der Untersuchung wirklich das und nur das sieht, was für seinen individuellen Rechner relevant ist. Was nicht installiert und damit ohne Belang ist, wird und bleibt ausgeblendet. Das erleichtert die Auswahl der zu löschenden Objekte erheblich. Markieren Sie unter den einzelnen Programmen das, was Sie löschen



Über die Aufgabenleiste links ist die Programmoberfläche von CCleaner gut strukturiert und die Bedienung damit einfach. Das Hauptfenster zeigt Infos zur aktuell gewählten Funktion.

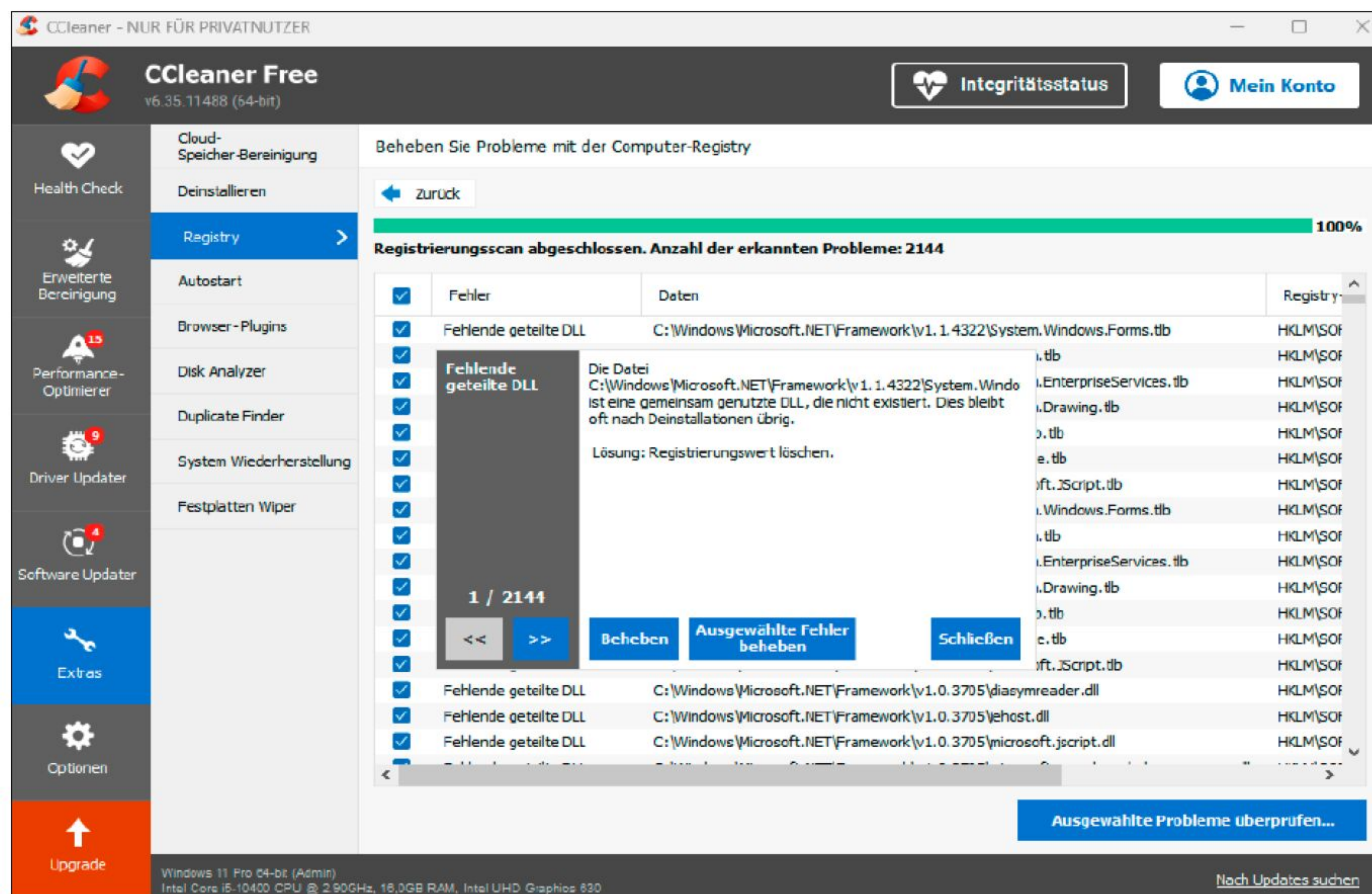


In „Erweiterte Bereinigung“ legen Sie detailliert und teilweise mit Erläuterung fest, was CCleaner löschen soll. Im Beispiel-Screen gewinnt man gut 8 GB mehr Speicherplatz.

CCLEANER UND ERGÄNZENDE TOOLS



Programm	Beschreibung	Auf	Internet	Sprache
AllDup	Doppelte Dateien aufspüren und löschen	Heft-DVD	www.allsync.de	Deutsch
CCleaner	Windows-PC aufräumen und optimieren	Heft-DVD	www.ccleaner.com	Deutsch
CCleaner Portable	Windows-PC aufräumen und optimieren (ohne Installation)	Heft-DVD	www.ccleaner.com	Deutsch
Revo Uninstaller	Programme restlos deinstallieren	Heft-DVD	www.revouninstaller.com	Deutsch
Snappy Driver Installer (SDI Lite)	Treiber installieren und updaten	-	https://sdi-tool.org	Deutsch
UnigetUI	Software installieren und updaten (Oberfläche für Winget-Paketmanager)	Heft-DVD	www.marticliment.com/unigetui	Deutsch



CCleaner erkennt auf diesem Rechner über 2000 „Probleme“ in der Windows-Registry. Beheben sollte man sie jedoch erst, nachdem man zuvor die Registry-Datei gesichert hat.

möchten, und klicken Sie anschließend unten erst auf „Analysieren“ und danach zum tatsächlichen Bereinigen auf „Cleaner starten → Fortfahren“.

Die Extras: Diverse Zusatzfunktionen in CCleaner Free

Über das Optimieren und Platzschaffen hinaus bietet die Gratis-Version eine Reihe

weiterer Tools und Funktionen. Diese finden Sie links in den „Extras“.

„Deinstallieren“ listet die auf dem Computer installierten Programme auf. Sie erreichen sie prinzipiell auch in der Windows-Systemsteuerung unter „Programme deinstallieren“ sowie in der Einstellungen-App unter „Apps → Installierte Apps“. Zum Ersten sollte man die Liste von Zeit zu Zeit immer mal wieder nach nicht mehr benötigten Einträgen oder Softwaredoubletten überprüfen und dabei überflüssige Apps löschen. Zum Zweiten zeigt CCleaner hier durchaus auch manchen Microsoft-Dienst, der sich über das Betriebssystem nicht entfernen lässt: „Hilfe anfordern“ ist ein solches Beispiel.

„Registry“ ist die einzige Reparaturfunktion, von deren Benutzung wir eher abraten. Zwar zeigt CCleaner da mitunter über 1000 „erkannte Probleme“. Doch die Gefahr, dass das Betriebssystem dabei beschädigt wird, ist deutlich höher als der potenzielle Nutzen. Falls Sie „Registry“ unbedingt ausprobieren möchten, bestätigen Sie im nächsten Schritt auf jeden Fall den Hinweis und sichern zuvor die komplette Registrierungsdatenbank.

„Autostart“ zeigt unter anderem das, was Sie auch im Windows-Taskmanager unter „Autostart von Apps“ sehen. Weitere Einträge kommen in den beiden Registern „Geplante Aufgaben“ und „Kontextmenü“ hinzu. Positiv anzumerken ist hier: Überambitionierte Anwender können die Einträge in CCleaner unter „Dienste“ nur deaktivieren, aus dem System jedoch nicht komplett entfernen.

Die „Browser-Plugins“ zeigen die installierten Erweiterungen, und zwar nach Browser getrennt. Die Plug-ins lassen sich deaktivieren, wieder aktivieren oder auch vollständig entfernen.

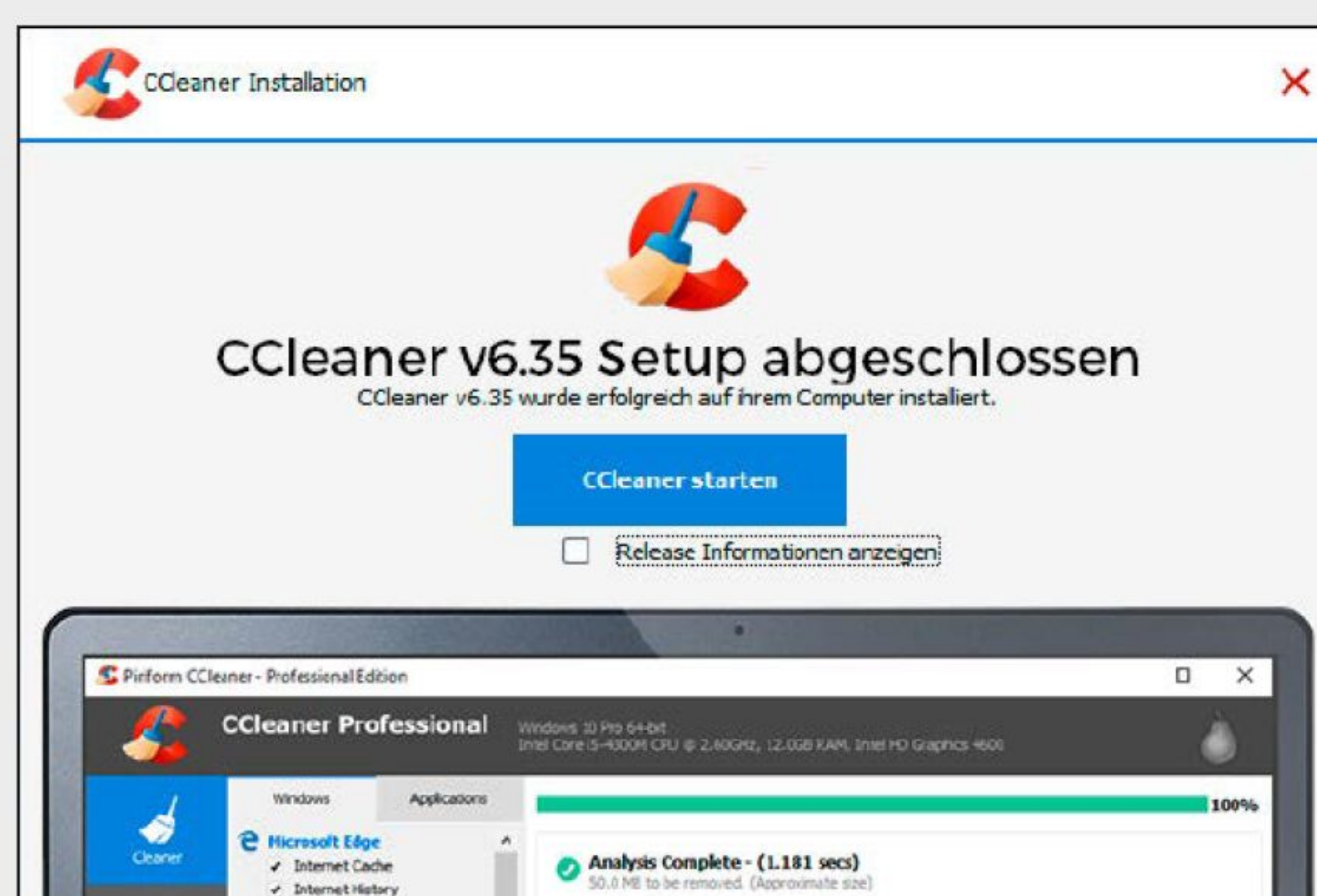
„Disk Analyzer“ gibt einen Überblick, welche Arten von Daten die einzelnen Laufwerke beziehungsweise Partitionen am stärksten belegen. CCleaner unterscheidet dabei zunächst zwischen Bildern, Musik, Dokumenten, Videos, E-Mail und komprimierten Dateien. Nach der Analyse können Sie zudem nach einzelnen Dateiformaten filtern, bei Bildern also nach JPG, PNG und so weiter. Über das Kontextmenü lassen sich so gezielt bestimmte Dateien löschen.

„Duplicate Finder“ spürt mehrfach abgespeicherte Files auf, die unnötig Platz auf dem Datenträger beanspruchen und die deshalb

CCLEANER-SETUP

Die Installation von CCleaner ist unkompliziert und mit zwei Mausklicks schnell vollzogen. Nach dem Start des Setups klicken Sie auf die Schaltfläche „Installieren“. Den Umweg über „Benutzerdefiniert“ können Sie sich sparen, der Hersteller hat die Voreinstellungen bereits sinnvoll angepasst. Nach wenigen Sekunden startet CCleaner über den gleichnamigen Button, fertig. Etwaig angebotene Zusatztools wie AVG Anti-Virus oder einen weiteren Browser lehnen Sie ab. Schließen Sie auch zunächst den Hinweis auf die kostenpflichtige Pro-Version, wir kommen auf die erweiterten Funktionen der Abovariante am Schluss dieses Ratgebers zurück. Neben der Version für die permanente PC-Optimierung steht CCleaner in einer portablen Version zum Mitnehmen auf einem USB-Stick zur Verfügung.

Nach dem Entpacken kopieren Sie das gesamte Verzeichnis auf einen externen Datenträger, von dem Sie **CCleaner Portable** über die Datei „Ccleaner64.exe“ auf jedem Windows-Rechner starten können. Die Bedienoberfläche der portablen Version stellen Sie auf Deutsch um, indem Sie unter „Options → Settings → Language“ den Eintrag „Deutsch“ auswählen.



Die Installation von CCleaner ist schnell abgeschlossen. Daneben existiert auch eine portable Version, unter anderem zum Mitnehmen auf einem USB-Stick.

gelöscht werden sollten. Über die Einstellungen der Dateigröße unter „Ignorieren“ lässt sich die Suche gezielt auf besonders große Duplikate beschränken. Viel mehr Optionen bei der Dublettensuche bietet jedoch die Freeware **AllDup**, die CCleaner für diesen Zweck deshalb vorzuziehen ist.

„Systemwiederherstellung“ macht es einfach und übersichtlich, alte und nicht mehr benötigte Wiederherstellungspunkte zu löschen. Damit erzeugen Sie unter Umständen etliche Gigabyte zusätzlichen freien Speicherplatz auf der Festplatte.

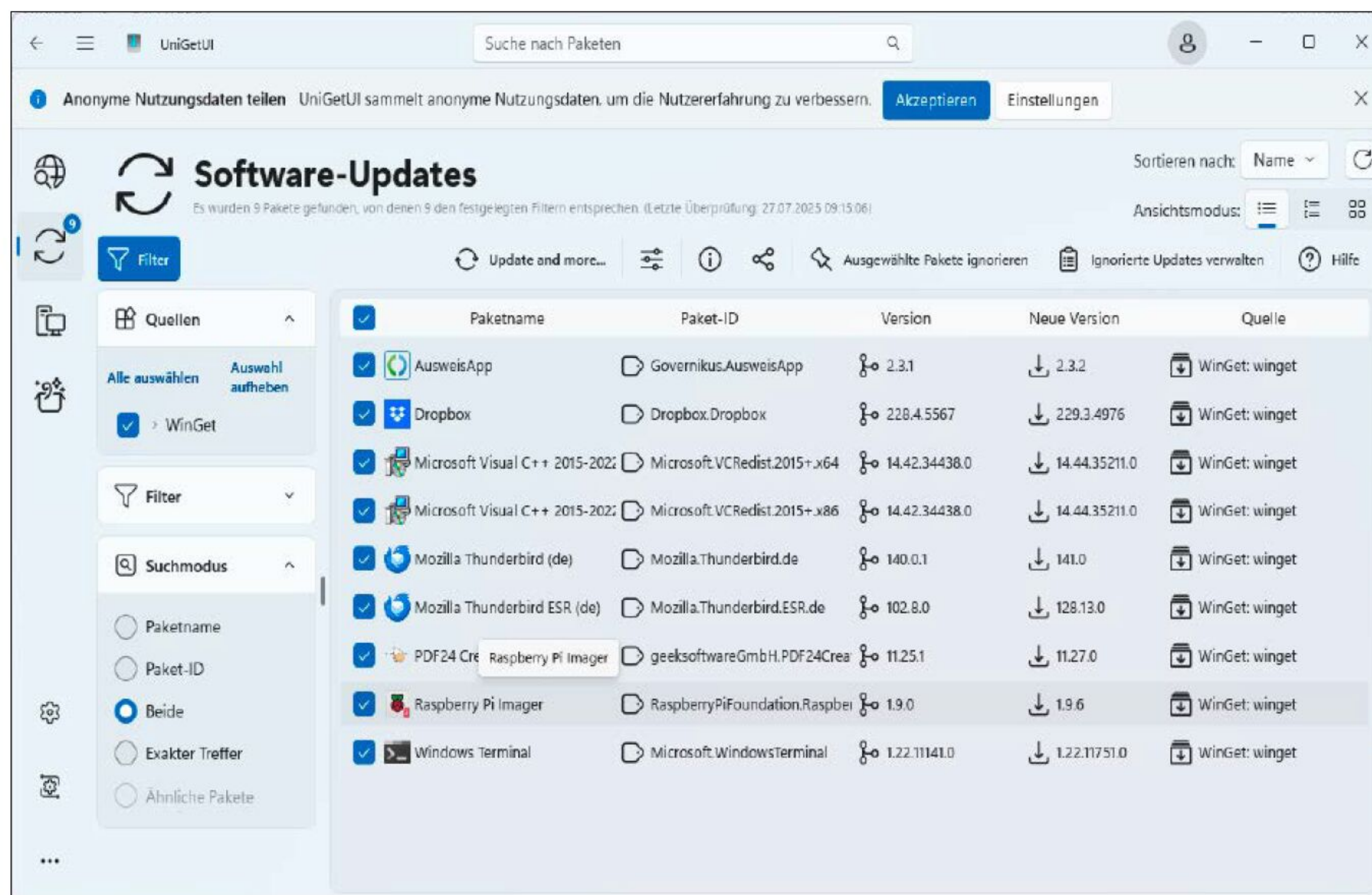
„Festplatten Wiper“ löscht Daten von der Festplatte. Hier sind zwei Szenarien zu unterscheiden: das „Löschen“ des freien Speichers und das komplette Löschen des gesamten Datenträgers beziehungsweise einer Partition. „Frei“ bedeutet hier nur, dass Windows den Speicherplatz zum Abspeichern neuer Daten verwenden kann. Frei im engeren Sinn ist er meist jedoch nicht, weil dort noch Reste zuvor gelöschter Dateien vorhanden sind. Möchten Sie sicherstellen, dass sich nichts davon wiederherstellen lässt, werden diese Bereiche von CCleaner gelöscht, indem sie zwischenzeitlich mit anderen Daten überschrieben werden – auf Wunsch auch mehrfach.

Das Löschen ganzer Laufwerke arbeitet im Prinzip genauso, funktioniert unter Windows systembedingt aber nicht mit der Systempartition, sondern nur mit weiteren Festplattenbereichen und anderen (externen) Datenträgern. Die Warnung beim Löschen auf vorzeitigem SSD-Verschleiß können Sie bei gelegentlicher Nutzung ignorieren.

Lohnt das CCleaner-Abo der kostenpflichtigen Pro-Version?

Neben den hier zuvor beschriebenen Funktionen sehen Sie auf der Bedienoberfläche drei weitere Rubriken: den „Performance-Optimierer“, den „Driver-Updater“ und den „Software-Updater“. Diese Funktionen sind meist mit einem roten Punkt sowie Ziffern für die Zahl der erkannten Probleme markiert. Nutzen lassen sich diese Funktionen jedoch nur in der kostenpflichtigen Pro-Version, in der Gratis-Variante von der Heft-DVD sind sie gesperrt.

Da stellt sich die Frage, ob sich die Ausgabe für das erforderliche Pro-Abo lohnt. Kauft man die Lizenz direkt aus der CCleaner-App, zahlt man für das Jahresabo zunächst nur vergleichsweise günstige 14,28 Euro



Die Funktion zum Aktualisieren der installierten Software gibt es nur im kostenpflichtigen CCleaner Pro. Eine gute Update-Alternative ist der kostenlose Paketmanager UniGetUI.

(12 Euro plus Mehrwertsteuer). Der angefügte Zusatz „erstmalig“ deutet jedoch in Verbindung mit dem regulären Abopreis von knapp 40 Euro darauf hin, dass sich die Gebühren nach den ersten zwölf Monaten fast verdreifachen, sofern man nicht rechtzeitig kündigt.

Wer sich die Ausgabe sparen möchte, kann zu den kostenlosen Alternativen **Snappy**

Driver Installer (SDI Lite) und **UniGetUI** greifen, wenn es um das Aktualisieren der Hardwaretreiber und installierten Programme geht. Kostenlos sind auch das schon genannte AllDup sowie **Revo Uninstaller**. Beide Tools bieten mehr und ausgefeiltere Funktionen als die Dublettensuche und die Deinstallieren-Option in der CCleaner-Freeware. ■

CCLEANER AM SMARTPHONE

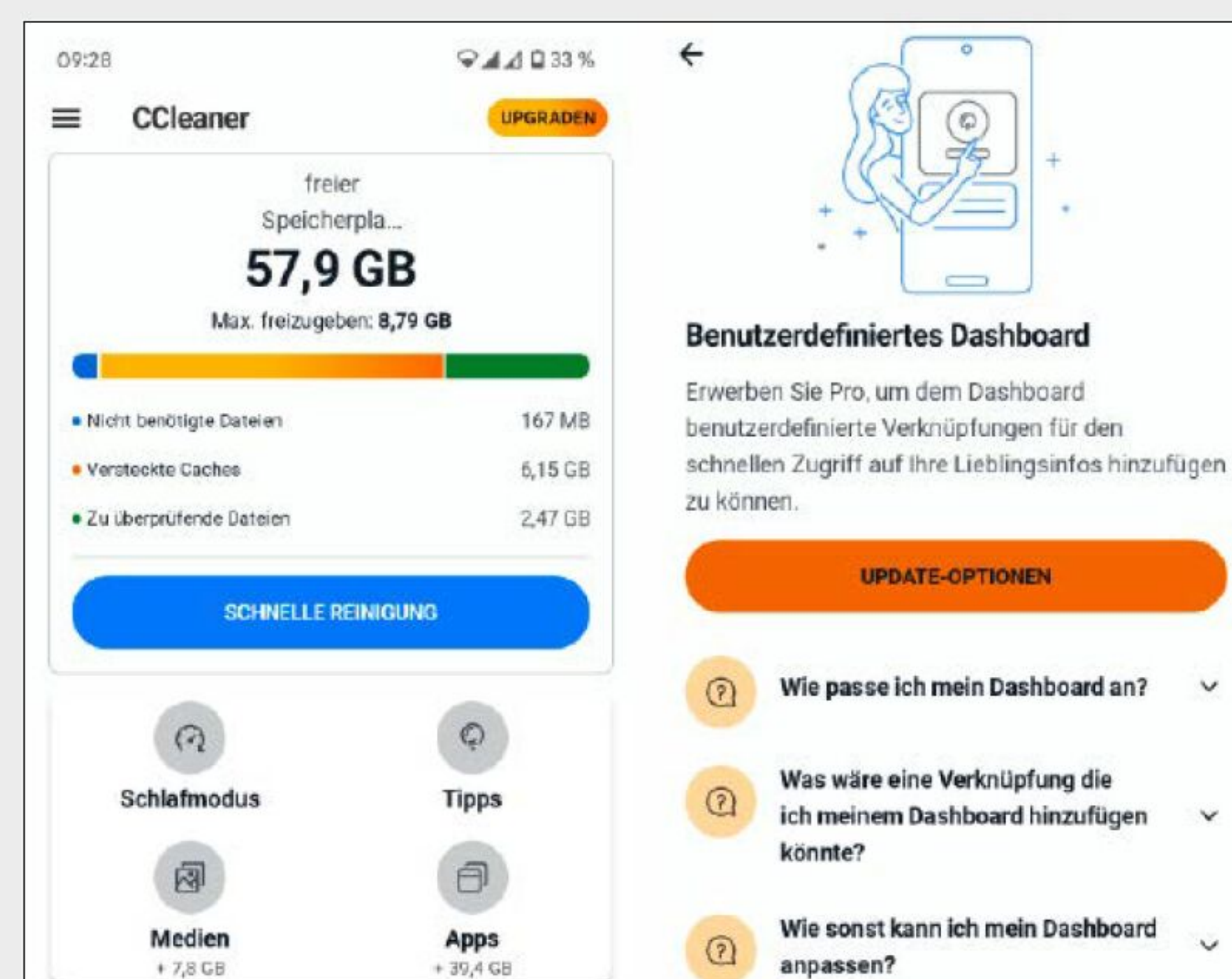


CCleaner gibt es auch für Android-Smartphones und iPhones, die Apps installieren

Sie wie gewohnt über die App Stores von Google und Apple. Ähnlich wie die Windows-Version macht es die Mobil-App dem Nutzer einfach, überflüssige Daten zu löschen und damit mehr freien Platz auf dem internen Gerätespeicher beziehungsweise auf der eingelegten SD-Karte zu schaffen.

Praktisch ist auch der schnelle Zugriff auf die „Speicherfresser“, wenngleich die App dabei nur zu der ohnehin in Android und iOS vorhandenen Übersicht und Löschmöglichkeit weiterleitet.

Einige weitergehende Funktionen sind auch in der Mobil-App auf die kostenpflichtige Pro-Version beschränkt – der Hersteller weist in der Gratis-Version ziemlich penetrant darauf hin.



Die CCleaner-App fürs Smartphone löscht überflüssige Daten auf dem Mobilgerät und schafft so neuen Speicherplatz für Fotos, Apps und mehr.

Sofort-Update für jede Software

Während Paketmanager unter Linux, am Mac und am Smartphone längst Standard sind und alle Apps selbstständig aktualisieren, musste man seine Software am Windows-PC lange manuell pflegen. Endlich funktioniert das auch hier automatisch, und zwar ganz komfortabel.

VON PETER STELZEL-MORAWIETZ

Werfen Sie einmal einen Blick auf die Liste all der Programme, die auf Ihrem Rechner installiert sind: entweder in der Systemsteuerung unter „Programme → Programme und Features“ oder in den Windows-Einstellungen unter „Apps“. In aller Regel sind es Dutzende, darunter vermutlich auch einige, die Sie schon längere Zeit nicht mehr verwendet und folglich auch nicht aktualisiert haben.

Derzeit bietet Windows keine Option, die auf dem Rechner installierte Software jenseits der Store-Apps auf Aktualität zu prü-

„Nie war es unter Windows so einfach, sämtliche am PC installierten Programme automatisch auf den neuesten Stand zu bringen.“



© Mer_Studio - AdobeStock

fen und zu aktualisieren – immerhin hat Microsoft eine solche Funktion kürzlich in Aussicht gestellt. Noch aber beschränkt sich das Windows-Update auf „andere Microsoft-Produkte“ wie das Office-Paket, Software anderer Anbieter wird beim Update-Check nicht berücksichtigt. Sofern die Programme nicht wie zum Beispiel die Browser selbst überprüfen, ob eine neue Version vorliegt, müssen Sie das regelmäßig selbst erledigen. Immerhin bieten dazu einige Programme die Möglichkeit, dies mit zwei oder drei Mausklicks zu tun.

Andere Anbieter haben keinen solchen Updatemechanismus integriert und bieten auch keine Möglichkeit, sich per E-Mail auf neue Software- oder Firmwareupdates hinweisen zu lassen. Das populäre Packtool 7-Zip ist ein solcher Fall: Da wurden im vergangenen Jahr gleich mehrere gefährliche

Sicherheitslücken durch neue Versionen geschlossen, die aber musste man manuell herunterladen und installieren. Selbst ein knappes Jahr später dürfte 7-Zip deshalb auf vielen PCs noch in veralteten und Schadcode-anfälligen Versionen laufen.

Paketmanager für Auto-Updates unter Windows wenig verbreitet

Mit einem sogenannten Paketmanager wäre das nicht passiert, er spielt neue Programmversionen selbstständig und ohne Zutun ein. Also so, wie man es vom Smartphone, von Linux und vom Mac schon lange kennt. Das Gleiche gilt unter Windows für die Apps aus dem Microsoft Store, sofern in den Store-Einstellungen die Option „App-Updates“ aktiv ist. Nicht automatisch aktualisiert werden dagegen die auf gewöhnlichem Weg installierten Programme.

Während also Paketmanager auf anderen Systemen längst Standard sind, führten sie unter Windows lange ein Schattendasein. Tools wie Iobit Software Updater, Patch my PC, Secunia Personal Update Inspector, SUMo (Software Update Monitor) oder Updatestar existieren zwar schon seit geraumer Zeit, haben jedoch jeweils ihre Schwachpunkte oder sind in der Gratisversion stark funktionslimitiert. Mit **Iobit Software Updater Pro** erhalten Sie in dieser Ausgabe eine Jahreslizenz der nicht eingeschränkten Vollversion, auf die wir gleich zurückkommen.

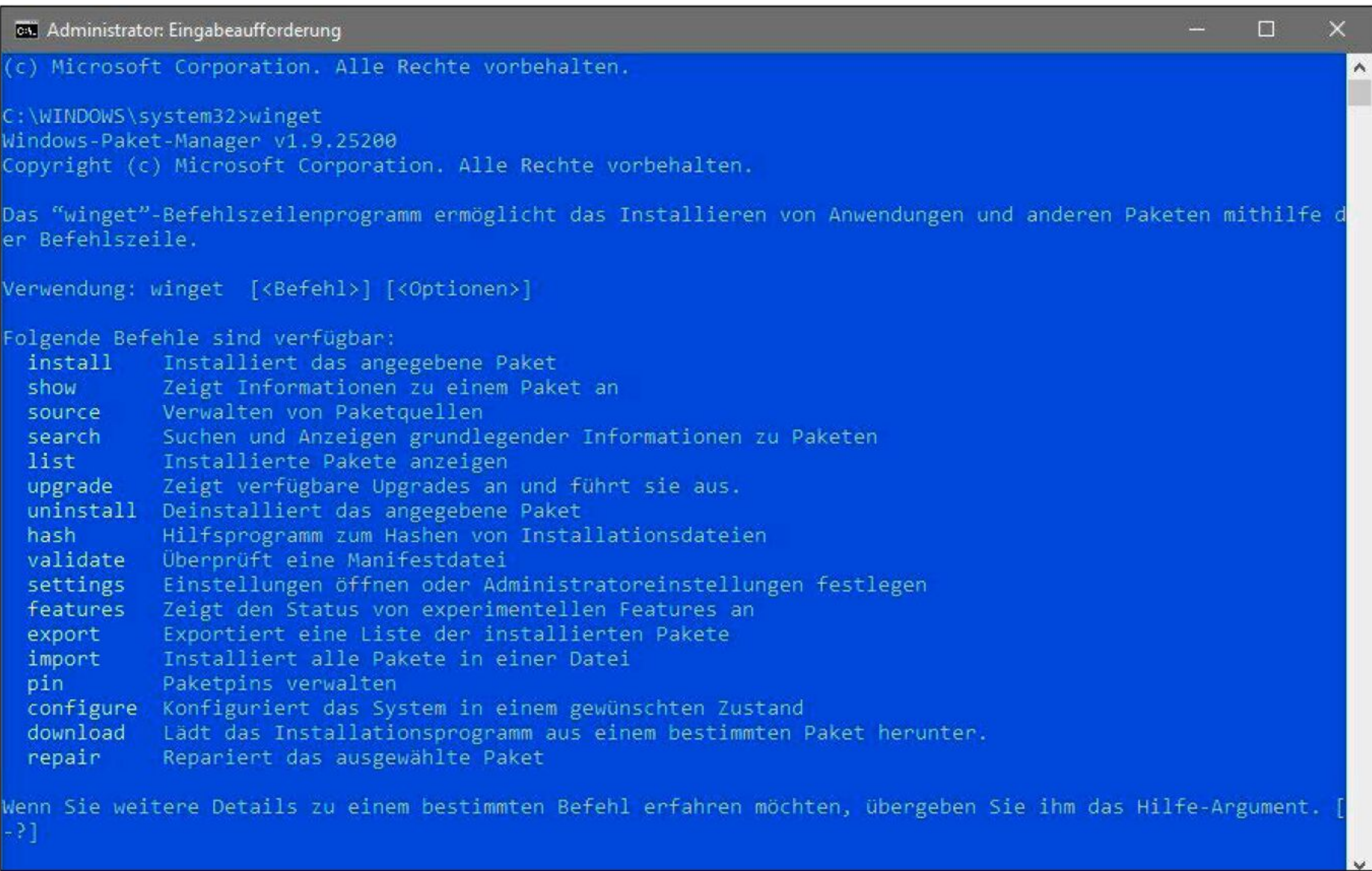
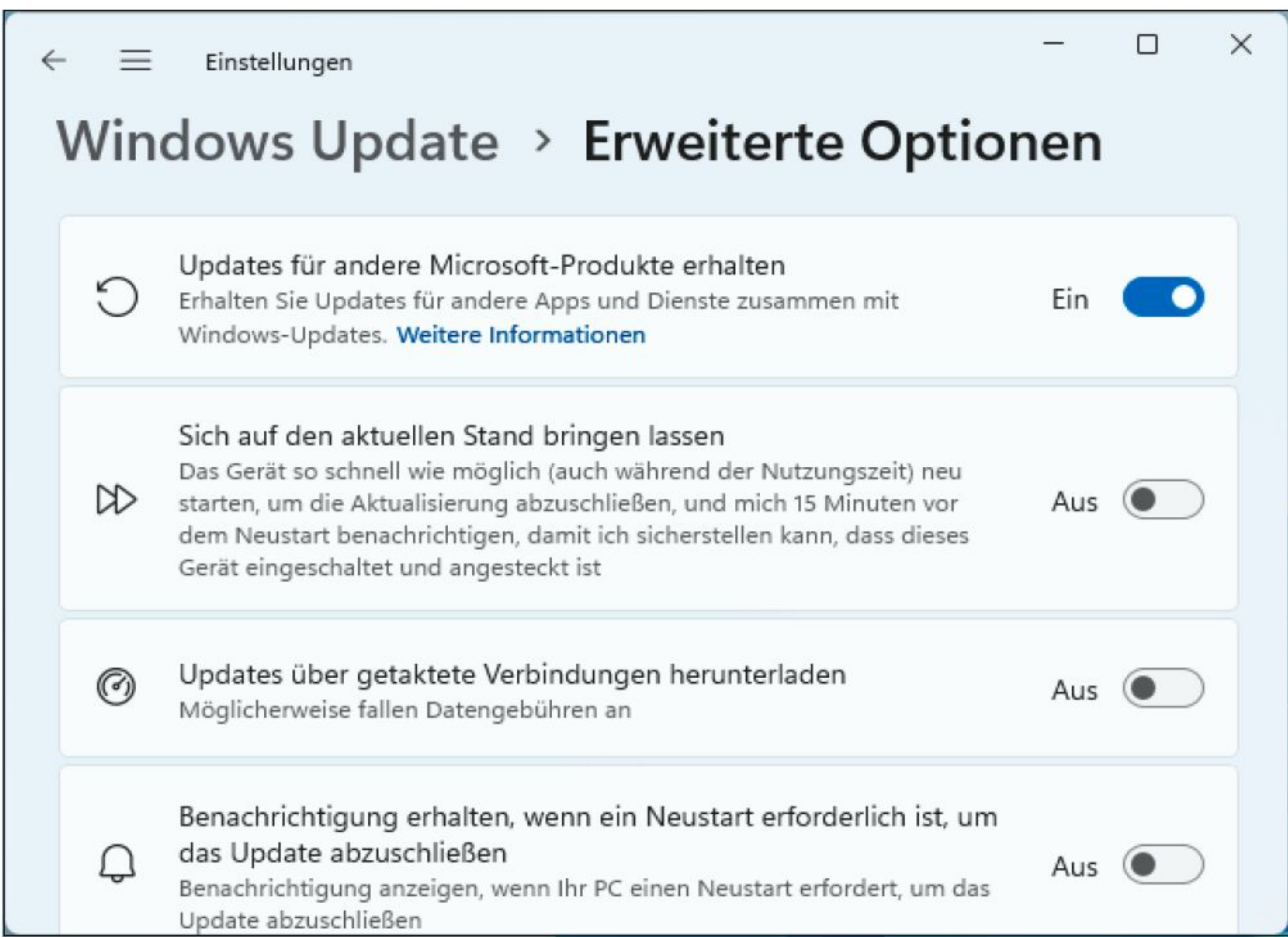
Zunächst aber erläutern wir den in Windows 10 und 11 integrierten Microsoft-eigenen Paketmanager Winget, den man eigentlich etwas umständlich per Kommandozeile steuern muss (<https://learn.microsoft.com/de-de/windows/package-manager>).

UnigetUI macht die Nutzung von Winget ganz einfach

Viel einfacher wurde die Bedienung mit der WingetUI genannten grafischen Benutzeroberfläche, die Abkürzung steht für „Winget User Interface“. Dieses Tool machte es plötzlich möglich, neue Software bequem per Maus und ohne die üblichen „Weiter“-Bestätigungen zu installieren und bereits am PC laufende Programme automatisch up to date zu halten. Weil sich WingetUI inzwischen nicht mehr nur auf Winget beschränkt, sondern auch andere Konsolen-Paketmanager unterstützt, wurde es in der Zwischenzeit in **UnigetUI** umbenannt.

Installation: Da Microsofts Paketmanager Winget selbst Bestandteil von Windows 10 und 11 ist, brauchen Sie nur die UnigetUI-Oberfläche zu installieren. Beim Setup achten Sie im ersten Schritt darauf, das Tool für alle Benutzerkonten zu installieren. Je nach Einstellung müssen Sie dazu in der Benutzerkontensteuerung (UAC) zulassen, dass UnigetUI Änderungen am System vornehmen darf. Die übrigen Schritte können Sie mit allen Voreinstellungen übernehmen. Dazu zählt insbesondere, auch den weiteren Paketmanager Chocolatey einzu-

Windows Update erlaubt unter „Erweiterte Optionen“ nur, Microsoft-eigene Programme zu aktualisieren. Die übrige installierte Software bleibt beim Update-Check außen vor.



Als Microsoft seinen Paketmanager für Windows herausbrachte, war das Tool anfangs nur über die Kommandozeile zu bedienen. Das erforderte beträchtliche Einarbeitung.

beziehen. Zum Abschluss klicken Sie auf „Fertigstellen“, UnigetUI startet daraufhin automatisch.

Bevor wir gleich genauer auf die Funktionen eingehen, sollten Sie links unten unter „Einstellungen → Einstellungen für Administratorenrechte“ die Option „Nur einmal nach Administratorrechten fragen“ unter „Einstellungen für Administratorenrechte“ aktivieren. Das erspart später so manche Rückfrage. Falls gewünscht, können Sie UnigetUI unter „Aktualisierungseinstellungen“ zudem anweisen, alle verfügbaren Updates automatisch aufzuspielen. Stellen Sie die Option aber erst einmal zurück, denn so haben Sie die Aktualisierungen stets im Blick und machen sich mit dem Paketmanager vertraut.

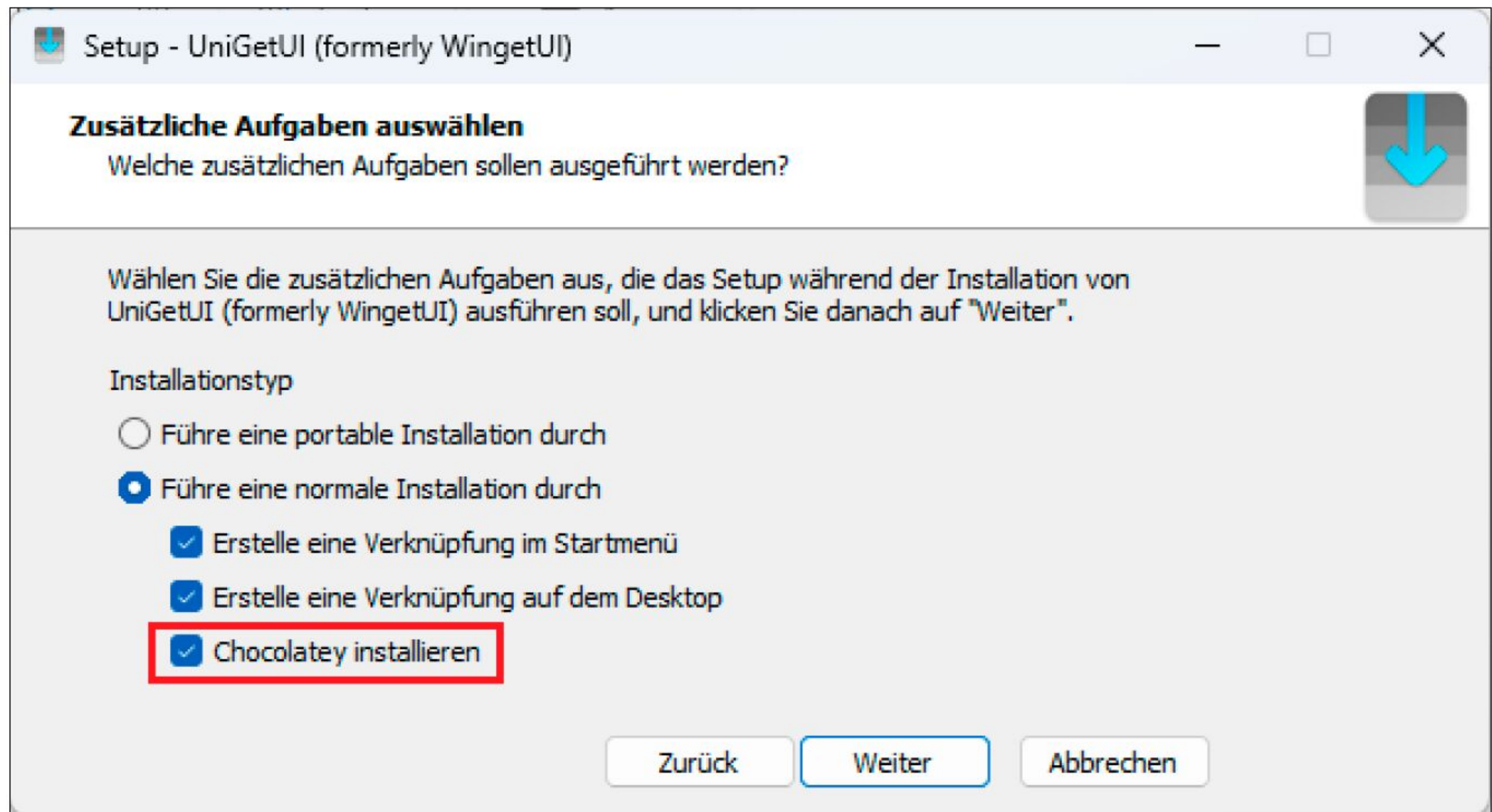
Die wichtigen Funktionen auf der Bedienoberfläche UnigetUI

UnigetUI wird beim Setup so konfiguriert, dass es beim Einschalten des Computers automatisch mitstartet. Sie erkennen dies

PAKETMANAGER FÜR WINDOWS



Programm	Beschreibung / Alternative zu	Auf	Internet	Sprache
Iobit Software Updater Pro	Paketmanager (Vollversion)	Heft-DVD	www.iobit.com/de/iobit-software-updater.php	Deutsch
UnigetUI	Oberfläche für Winget und weitere Paketmanager	Heft-DVD	www.marticliment.com/unigetui	Deutsch



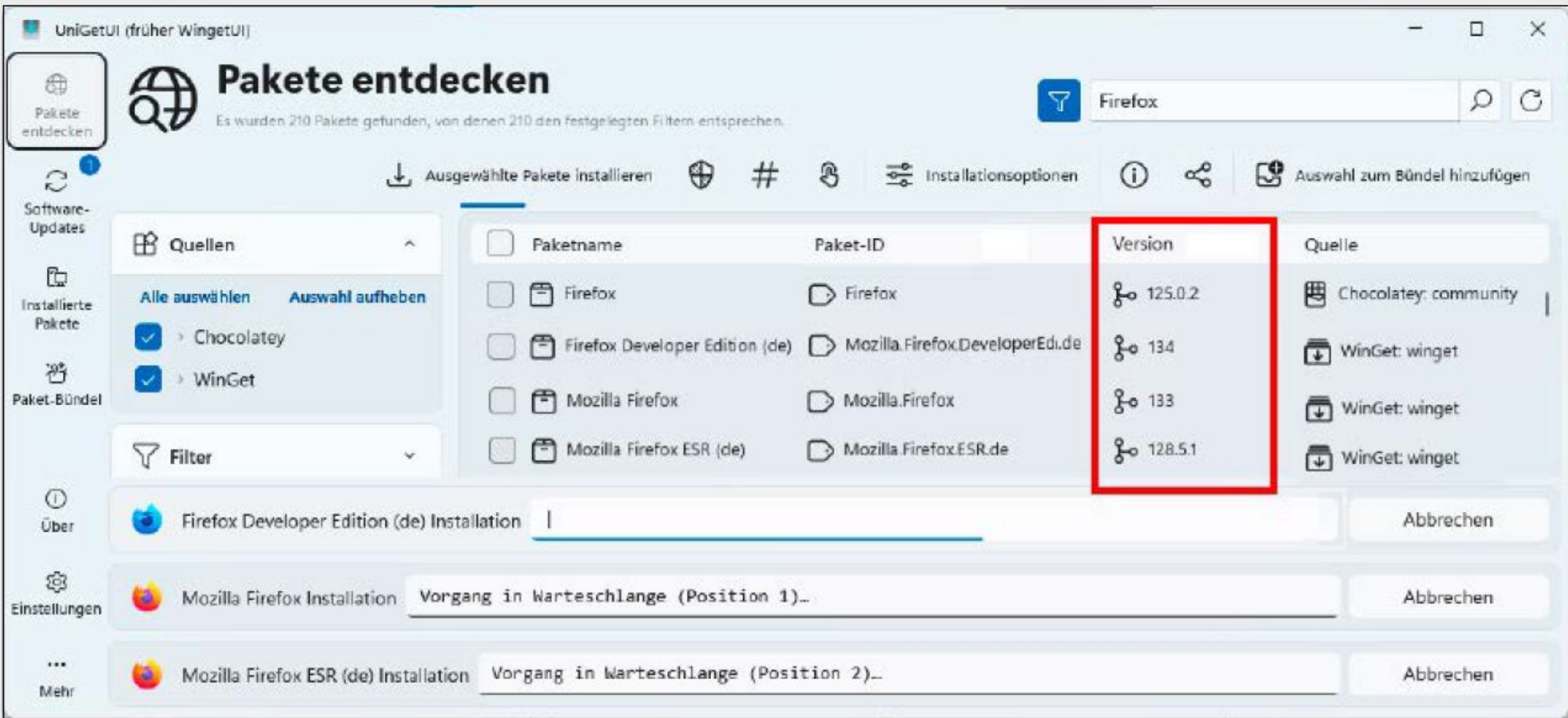
Während Microsofts eigener Paketmanager Winget bereits in Windows integriert ist, kann und sollte die Alternative Chocolatey zusammen mit UniGetUI installiert werden.

NEUE PROGRAMME INSTALLIEREN

Neben den automatischen Updates der installierten Programme bietet UniGetUI eine weitere clevere Funktion, den „Silent Install“. Hinter dem Begriff verbirgt sich das Installieren von Software ohne Rückfrage: Statt im Setup-Prozess mehrfach auf „OK“ oder „Weiter“ zu klicken, installiert UniGetUI die Software autonom.

So geht's: Um ein Programm auf diese Art und Weise zu installieren, öffnen Sie UniGetUI, klicken in der linken oberen Ecke auf „Pakete entdecken“, tippen im Suchfeld rechts den Namen des gewünschten Programms ein und bestätigen mit der Enter-Taste. Nach einem kurzen Augenblick erscheint das gesuchte Programm. Das markieren Sie und installieren es mit einem Klick auf „Ausgewählte Pakete installieren“. Abhängig von der Software wird diese in mehreren Versionen angeboten, die sich hinsichtlich der Sprache, Versionsnummer und mehr unterscheiden. Aus diesen wählen Sie die gewünschte Version aus.

Zwei Hinweise zum Schluss: Auf die Möglichkeit, mehrere Programme zu einem „Paket-Bündel“ zusammenzufassen und zu speichern, um diese so in einem Rutsch zu installieren, wurde im Artikel schon hingewiesen. Zweitens: Möchten Sie bei einem bestimmten Programm etwas an den Installationseinstellungen ändern, deaktivieren Sie den Silent Install von UniGetUI über die Schaltfläche „Interaktive Installation“ oben in der Mitte. Dann erscheinen beim Setup die üblichen Bestätigungen mit ihren Änderungsoptionen.



UniGetUI installiert neue Software automatisch ohne die üblichen Bestätigungen. Je nach Programm stehen zudem mehrere unterschiedliche Versionen zur Verfügung.

am neuen Icon rechts unten in der Taskleiste. Ein grüner Punkt im Symbol weist darauf hin, dass neue Softwareupdates vorliegen. Oben links auf der Programmoberfläche sehen Sie vier wichtige Bereiche. Über „Pakete entdecken“ installieren Sie neue Programme, mehr dazu lesen Sie im Kasten „Neue Programme installieren“. Im Mittelpunkt der nachfolgenden Ausführungen stehen die „Software-Updates“. Der dritte Bereich „Installierte Pakete“ zeigt ähnlich wie die Windows-interne Apps-Liste in den Windows-Einstellungen, welche Programme installiert sind. Hier listet UniGetUI teilweise jedoch deutlich mehr Einträge auf. Das kann wichtig sein, weil sich die Tools über die UniGet-UI-Funktion „Ausgewählte Pakete deinstallieren“ aus dem System entfernen lassen.

„Paket-Bündel“ schließlich dient ebenfalls dazu, Software zu installieren. Doch statt sie einzeln aufzuspielen, lassen sich hier mehrere Programme zu einem „Bündel“ zusammenfassen, speichern und damit später auf einem anderen Rechner in einem Rutsch installieren.

Alle installierten Programme mit einem Mausklick up to date

Die Software auf Ihrem Rechner per Hand auf Updates zu überprüfen gehört mit UniGetUI der Vergangenheit an. Das erledigt das Tool automatisch. Sobald im Programm-Icon der Taskleiste der grüne Punkt oder zusätzlich eine Windows-Benachrichtigung erscheint, öffnen Sie die Tooloberfläche. Alle vorliegenden Updates sind darin bereits ausgewählt und markiert, mit einem weiteren Klick auf die Schaltfläche „Ausgewählte Pakete installieren“ bringen Sie alles auf den aktuellen Stand.

UniGetUI lädt daraufhin die Updates herunter und spielt sie ein, den Stand beziehungsweise Fortschritt zu jeder Software können Sie unten verfolgen. Eventuell unterbrochen wird der Prozess nur, wenn die Benutzerkontensteuerung (UAC) Ihre Zustimmung verlangt. Vollautomatisch und ohne jeden Eingriff läuft es, wenn Sie den UAC-Schieberegler ganz nach unten auf „Nie benachrichtigen“ ziehen und diese Einstellung mit „OK“ bestätigen. Abhängig von Umfang und Zahl der Updates dauert das Herunterladen und Installieren seine Zeit. Zum Schluss erscheint die Bestätigung „Hurra! Es wurden keine Updates gefunden“.

Falls Sie ein oder mehrere Programme vorübergehend vom Updaten ausschließen möchten, deaktivieren Sie diese in der Liste und starten die Aktualisierung erst danach. Möchten Sie ein oder mehrere Updates ganz zurückstellen, erreichen Sie dies über die Schaltfläche „Ausgewählte Pakete ignorieren“. Über „Ignorierte Updates verwalten“ lassen sich die zurückgestellten Updates wieder ausführen.

Hinweis: Lassen Sie sich nicht davon irritieren, wenn beim Updaten unter „Quellen“ mal nur eine und mal mehrere erscheinen. Voreingestellt und aktiv in UnigetUI sind insgesamt neun Paketmanager beziehungsweise Repositories, das Tool wählt die zu jeder Software jeweils passende Quelle selbstständig aus.

Fazit: Das Tool UnigetUI ist eine uneingeschränkte Empfehlung

Die Oberfläche für Winget, Chocolatey und Co. macht die Verwendung der Paketmanager endlich auch unter Windows komfortabel. Statt Befehle in die Kommandozeile einzutippen, erledigt man mit UnigetUI alles per Mausklick. Das Tool installiert und aktualisiert jenseits kommerzieller Software fast alles und schließt somit bestehende Sicherheitslücken, behebt Fehler oder schaltet zusätzliche Funktionen frei.

Neue Versionen von Bezahlsoftware können die Paketmanager naturgemäß nicht installieren, sie zeigen sie deshalb zumeist nicht einmal an. Hier hilft die Vollversion **Iobit Software Updater Pro** weiter: Die Software bietet uneingeschränkte Updates für mehr als 700 Programme und erledigt das auf Benutzerwunsch sogar automatisch. Dazu vergleicht das Tool die installierten Versionen mit einer Datenbank und spielt die fehlenden Updates gegebenenfalls selbstständig ein. Sie erhalten die Jahreslizenz nach einer kostenlosen Registrierung beim Anbieter unter <https://id.iobit.com/de/giveaway/isu/pcwelt20260227.html>.

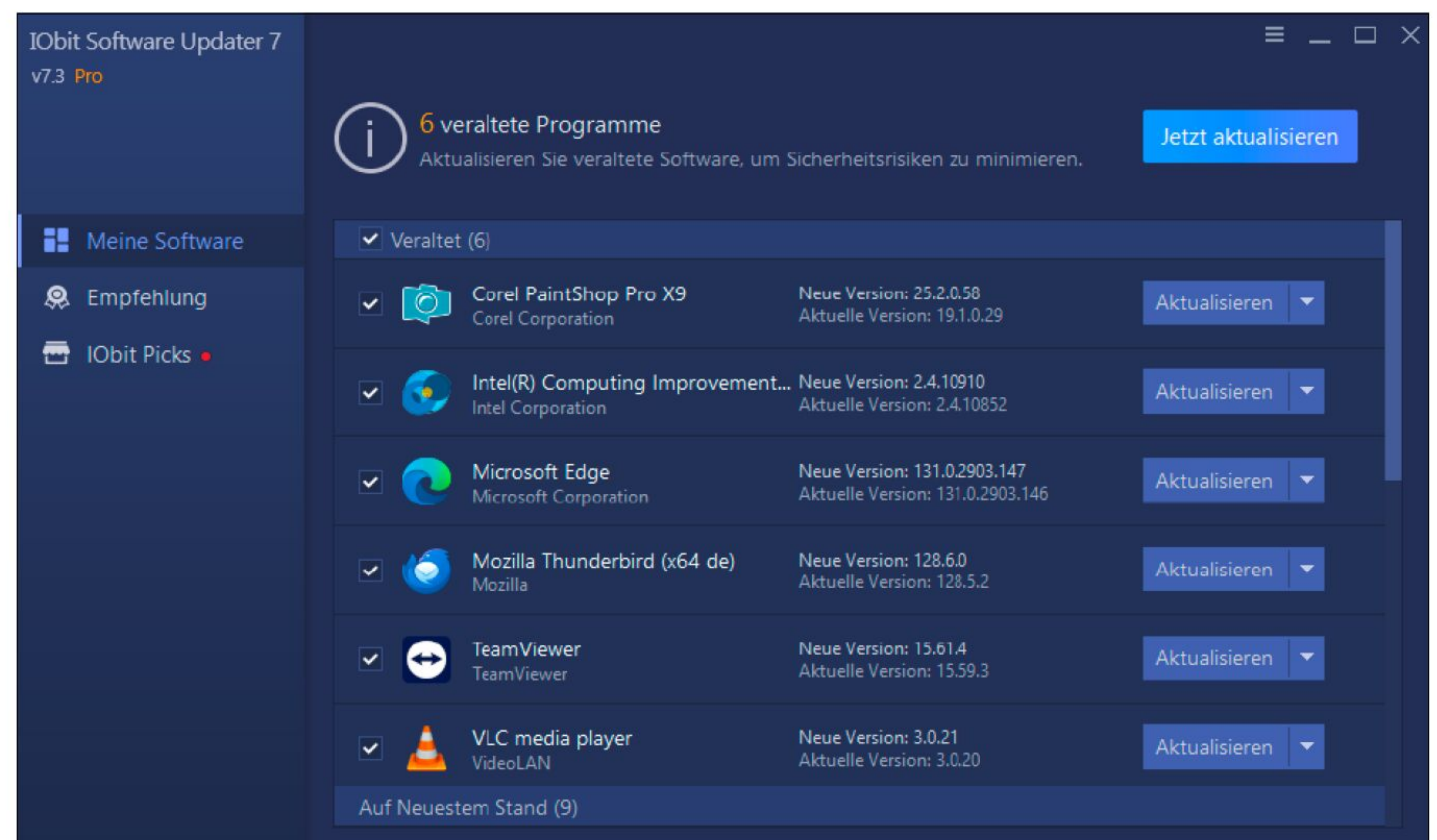
Hinweis: Falls Sie zwei oder mehr Paketmanager einsetzen, können sich die Ergebnisse im Detail unterscheiden. Mal zeigt eines der Tools eine neue Softwareversion, die in der Datenbank des anderen noch fehlt. Mal handelt es sich auch um verschiedene Bereitstellungszyklen, beispielsweise um Standard- und Langzeitversionen (ESR). Dies ist kein „Fehler“ der Paketmanager, sondern der vom Nutzer installierten Version geschuldet. ■



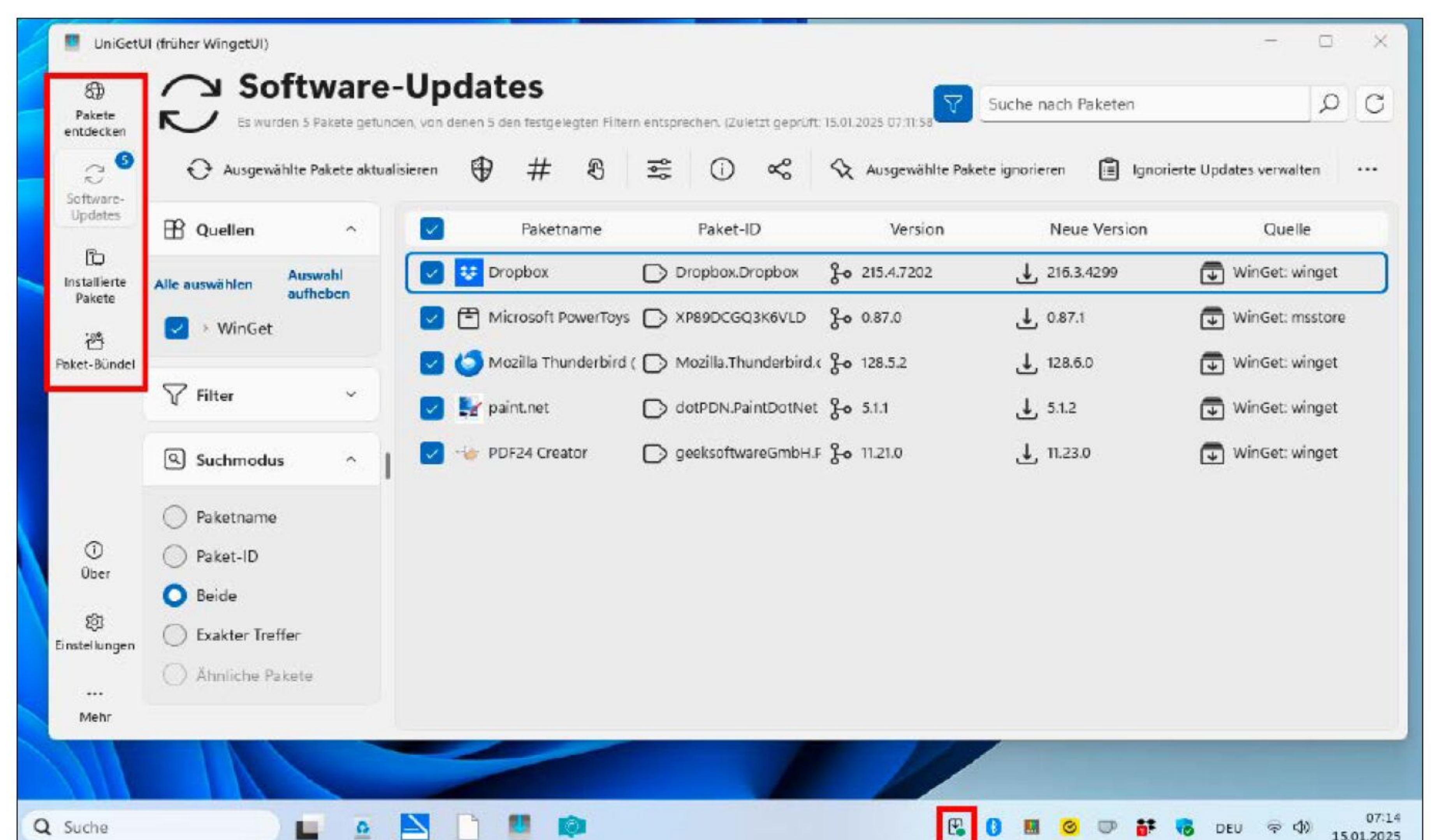
KOMMENTAR: „DER LETZTE SCHRITT FEHLT NOCH“

Peter Stelzel-Morawietz,
Redakteur PC-WELT

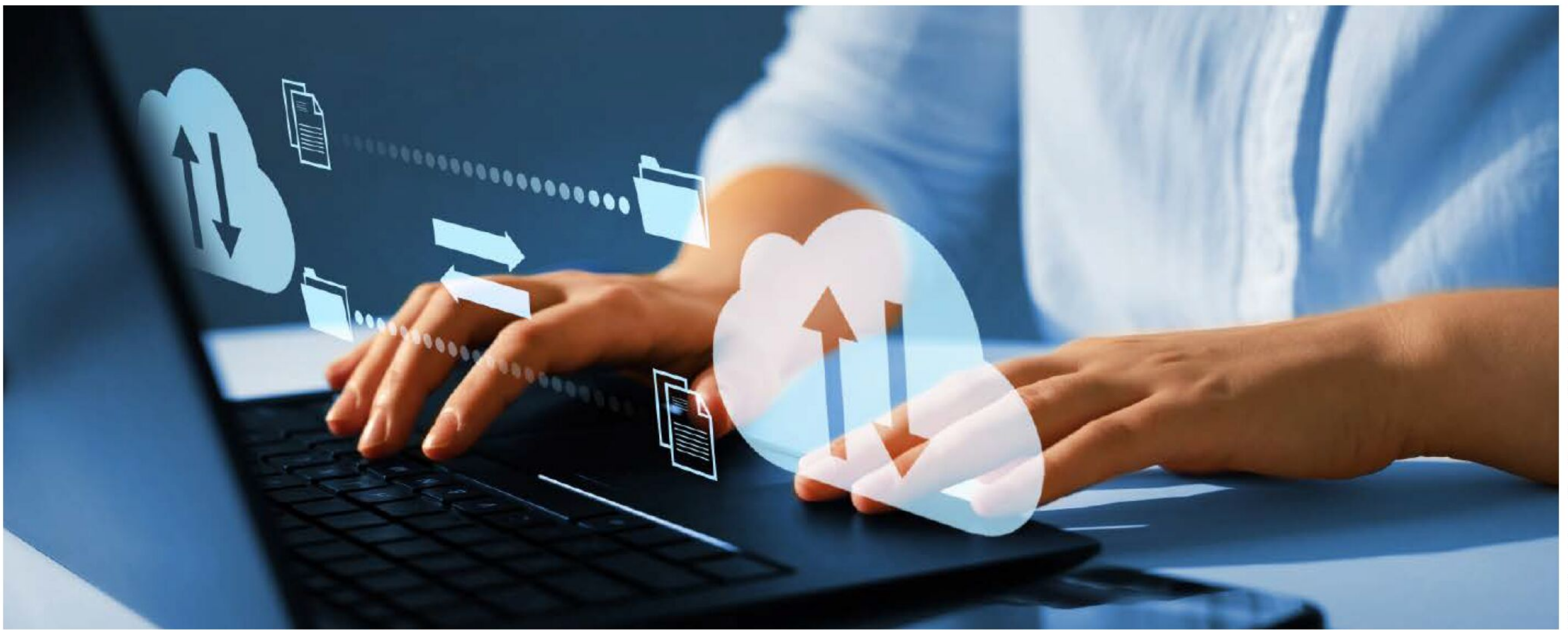
Das Windows-Update bringt und hält nicht nur das Betriebssystem auf dem neuesten Stand, sondern aktualisiert auch weitere Programme von Microsoft und zunehmend sogar Hardwaretreiber. Parallel dazu bietet der ebenfalls in Windows integrierte Paketmanager Winget die Möglichkeit, die auf dem PC installierte Software automatisch zu aktualisieren. Jetzt muss Microsoft nur noch eins und eins zusammenzählen und die beiden bisher getrennten Prozesse zu einer Funktion zusammenführen – kürzlich wurde diese Funktion immerhin angekündigt. Wenn das Windows-Update dann meldet „Sie sind auf dem neuesten Stand“, wüsste man, dass das auch wirklich stimmt.



Iobit Software Updater weist auch auf veraltete Vollversionen wie hier Paintshop Pro (oben) hin und bietet eine Aktualisierung an. Unter Umständen benötigt man aber eine neue Lizenz.



Die Bedienoberfläche UnigetUI zeigt links oben vier wichtige Funktionsbereiche. Wenn das Tool Updates bereit hält, erkennen Sie das am grünen Punkt im Icon in der Taskleiste.



© Mit Material von Miha Creative - AdobeStock

Daten perfekt sichern und synchronisieren

Regelmäßige Backups verhindern, dass wichtige Daten nach einem Crash, Virenangriff oder auch durch versehentliches Löschen verloren gehen. Gerade diese Gefahr droht beim Synchronisieren in der Cloud: Denn ohne zusätzliche Vorkehrung bedeutet das Entfernen von Inhalten an einem Computer, dass Sie sie von allen Geräten löschen.

VON ROLAND FREIST

Backups schützen zuverlässig vor Datenverlust! Das gilt für die „klassischen“ Katastrophenfälle wie versehentliches Löschen, Speicherfehler, Defekte an Festplatte oder SSD genauso wie für die Bedrohung durch Ransomware, die ganze Partitionen verschlüsselt und Lösegeld fürs Entschlüsseln fordert. Deshalb sollten Sie von wichtigen Dateien immer eine aktuel-

le Kopie besitzen, auf die Sie im Notfall zurückgreifen können.

Passende Backuptools sind als Freeware in nahezu jeder gewünschten Komplexität verfügbar. Darüber hinaus bieten viele Softwarehersteller ihre Backupprogramme im Rahmen von Aktionen immer mal wieder als kostenlose Version an. Microsoft hat im vergangenen Jahr ein neues Tool namens Windows-Sicherung per Update an alle Windows-Rechner verteilt, das seither Apps, Einstellungen und Anmeldeinformationen auf Microsofts Clouddienst OneDrive speichert.

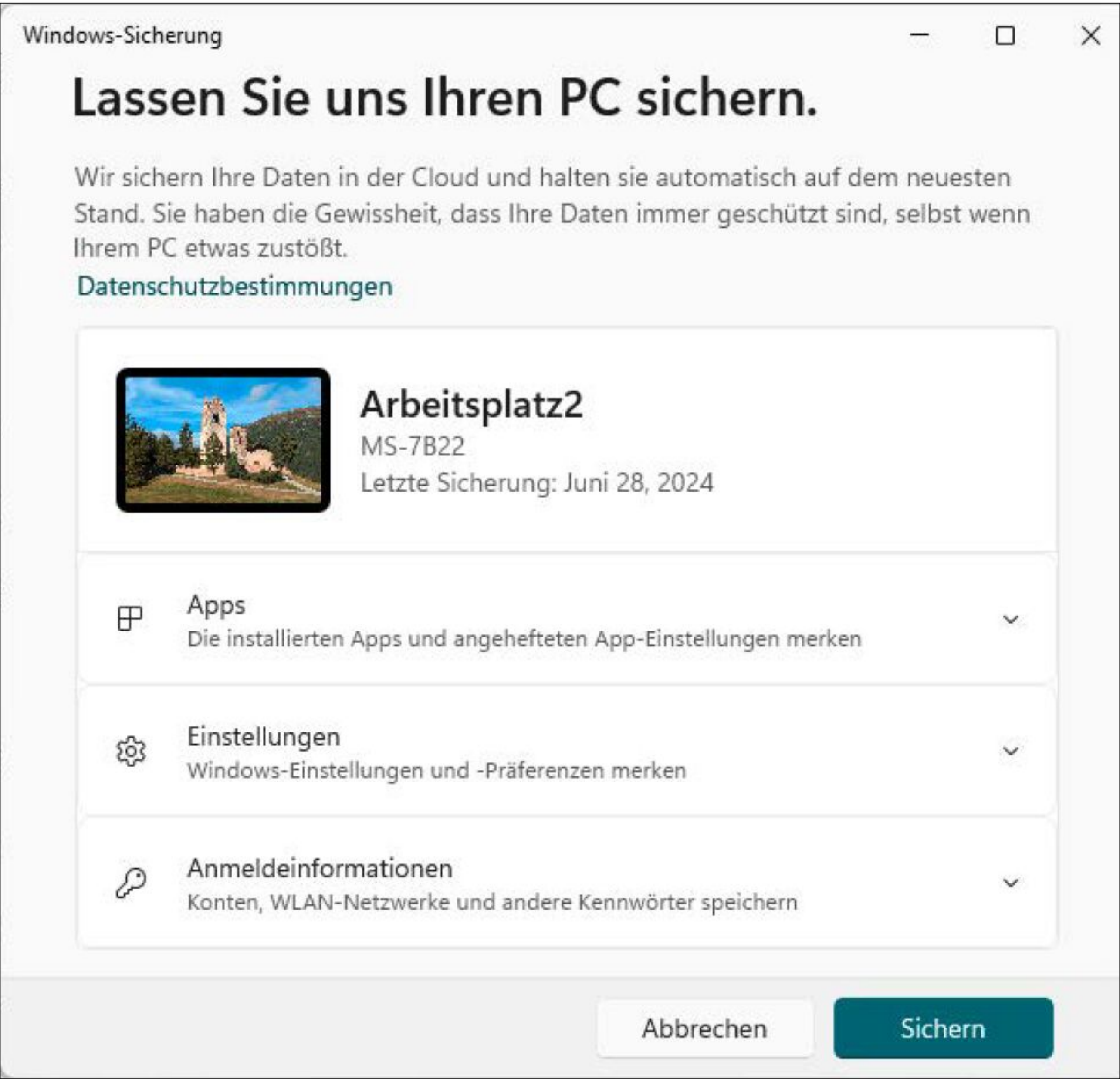
Bei Abonnenten von Microsoft 365 wird automatisch die Synchronisierung wichtiger Ordner mit OneDrive eingerichtet. Schließlich hat Microsoft in Windows 11 das Tool „Sichern und Wiederherstellen (Windows 7)“ wieder aktiviert, das zwischenzeitlich nur noch aus Kompatibilitätsgründen im Betriebssystem enthalten war. Doch bei diesem Tool hat es in der Vergangenheit

immer wieder gehakt. Gerade bei wichtigen Daten sollte man also keineswegs alleine darauf setzen.

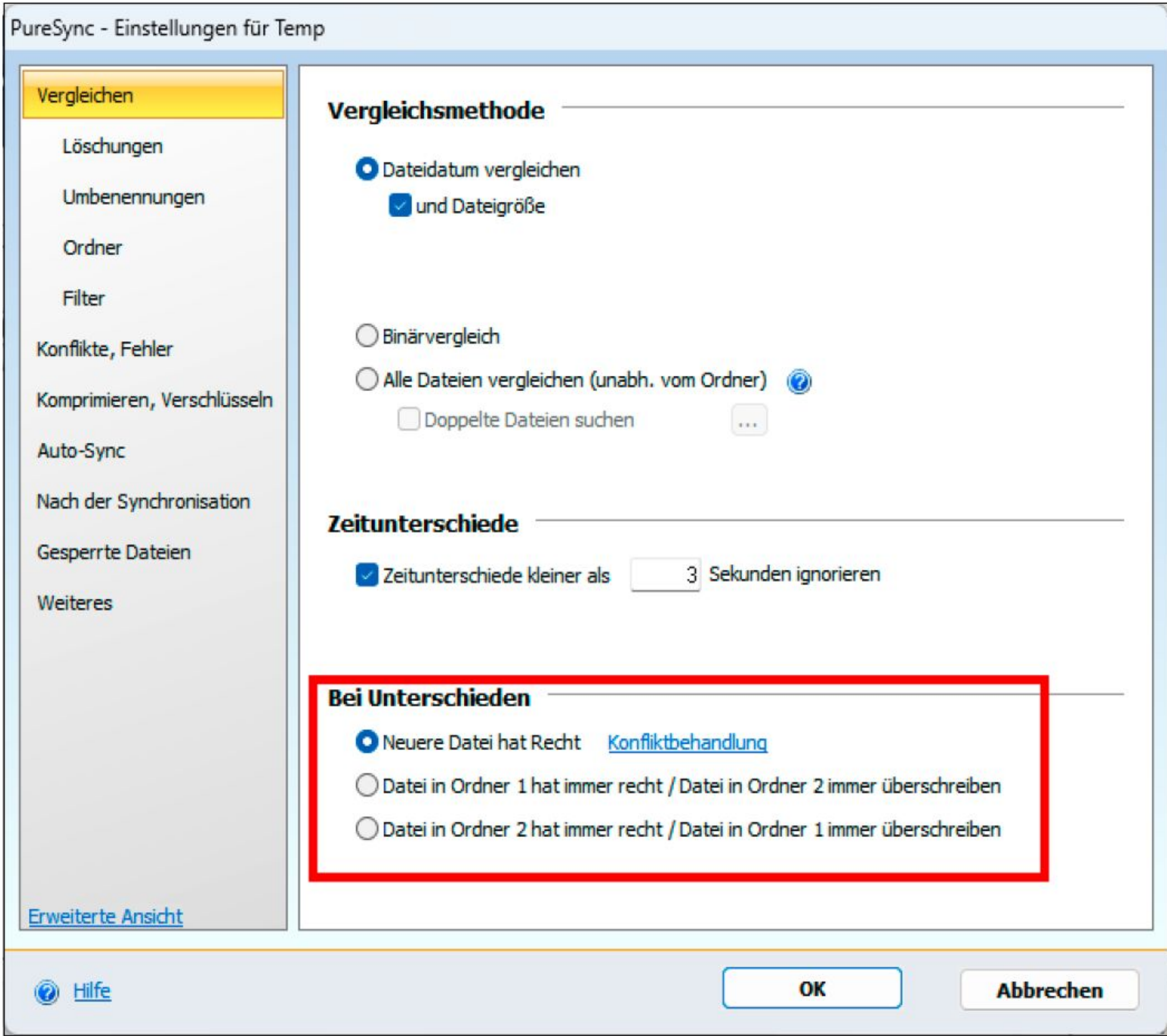
Backup und Synchronisieren immer wieder verwechselt

Im Vertrauen darauf, schon nicht von Datenverlusten betroffen zu sein, schenken viele Anwender den Sicherungsmechanismen von Windows oder auch den Einstellungen ihres Backuptools kaum Beachtung. Das aber ist ein Fehler, so wird beispielsweise häufig Backup mit Synchronisierung verwechselt. Dies führt dazu, dass ältere Dateiversionen nicht mehr verfügbar sind. Oder dass die Software lediglich die Windows-Standardbibliotheken sichert, nicht jedoch das Verzeichnis, in dem man seine Dokumente tatsächlich speichert. Oder dass das Sicherungsmedium voll ist, dass man sich mit einem lokalen Konto bei Windows anmeldet und die Verbindung zu OneDrive deshalb nicht funktioniert, oder oder oder.

„Windows bietet diverse Backuptools, doch manche Funktion hat ihre Tücken und beim Wiederherstellen ernste Probleme.“



Die Windows-Sicherung überträgt automatisch die Liste der installierten Apps, aktuelle Einstellungen und Anmeldeinformationen in die Onedrive-Cloud.



In Puresync können Sie für jeden Synchronisationsjob einstellen, ob die Daten in beide Richtungen oder nur in eine Richtung synchronisiert werden sollen.

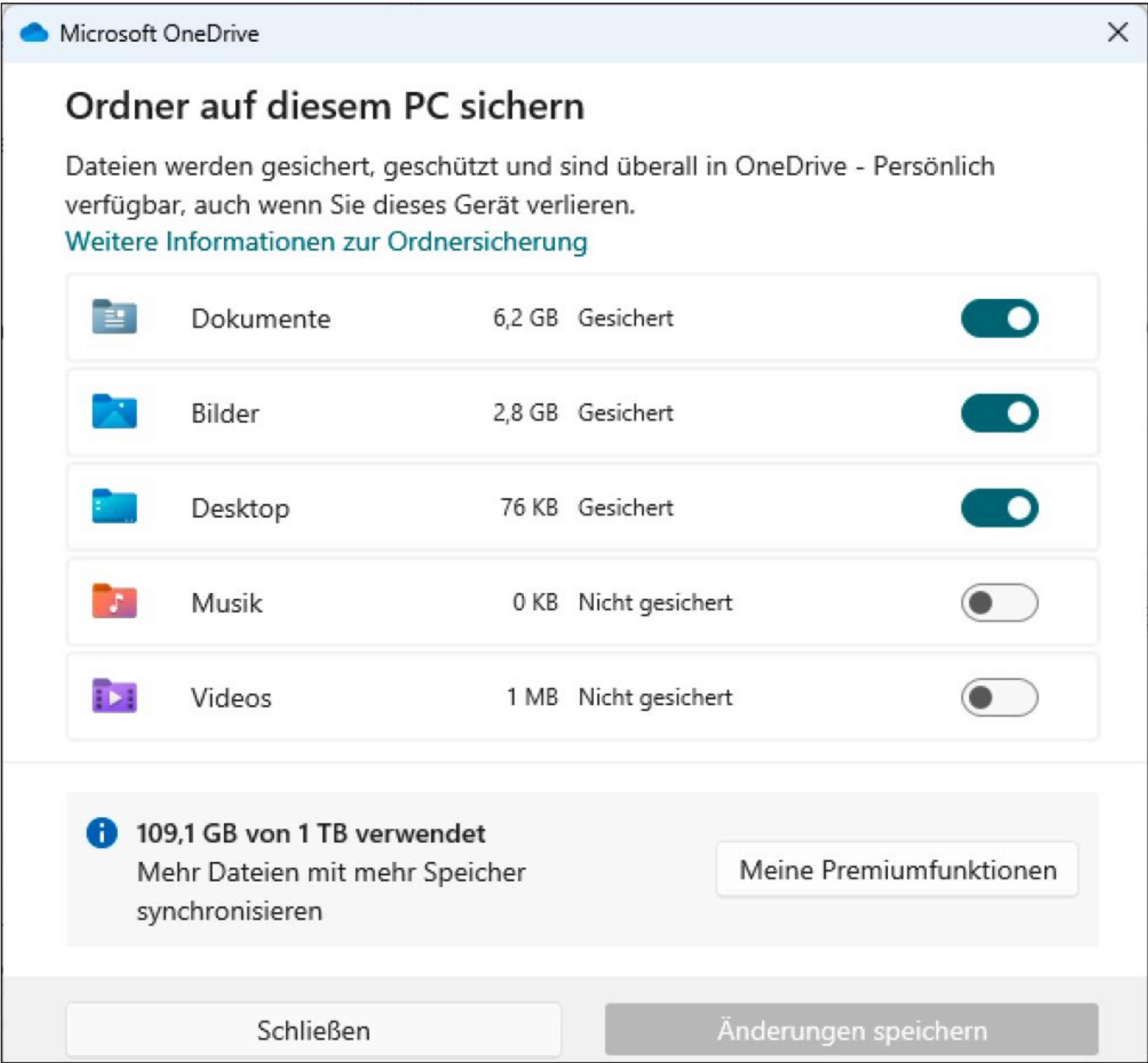
Deshalb zunächst nochmals zur Definition von Backup und Synchronisierung: Ein Backup ist eine Kopie von Dateien, Einstellungen und mehr auf einem anderen Medium. Die meisten Backupprogramme fassen die gesicherten Dateien und Ordner in einer einzigen Datei zusammen. Bei jeder Sicherung legt das Sicherungstool einen neuen Backupsatz an. Das bedeutet, dass es mehrere Versionen Ihrer Dateien und Ordner speichert. Sollten Sie aus Versehen die aktuelle Version eines Dokuments, an dem Sie schon seit mehreren Tagen arbeiten, durch eine ältere Variante überschrieben haben, können Sie aus dem jüngsten Backup zumindest die Version beispielsweise vom Vortag wiederherstellen. Auch eine Synchronisationssoftware speichert beim ersten Ausführen eine Kopie Ihrer Dateien und Ordner auf einem anderen Medium. Doch statt wie beim Backup mehrere Versionen zu speichern, sorgt das Synchronisieren dafür, dass auf dem Original- und dem Sicherungslaufwerk stets die gleiche und aktuelle Version vorhanden ist. Ist die Dateiversion auf dem Siche-

rungslaufwerk neuer, wird sie von dort auch wieder zurückkopiert. Bei der Synchronisation mit Onedrive geschieht das automatisch und lässt sich nicht ändern. Bei speziellen Programmen wie **Freefile-sync** oder **Puresync** dagegen können Sie die Synchronisation auf eine Richtung beschränken: Original → Sicherung oder Sicherung → Original. Bei Freefilesync klicken Sie dazu auf das grüne Zahnrad und wählen im folgenden Fenster unter „Variante“ die Option „Spiegeln“ oder „Aktualisieren“. In Puresync richten Sie zunächst einen neuen Synchronisationsjob ein und klicken im Assistentenfenster „Fertigstellen“ auf „Alle Einstellungen“. Klicken Sie im folgenden Fenster im Abschnitt „Bei Unterschieden“ auf „Datei in Ordner 1 hat immer recht / Datei in Ordner 2 immer überschreiben“ oder auf „Datei in Ordner 2 hat immer recht / Datei in Ordner 1 immer überschreiben“ und bestätigen Sie mit „OK“. Damit werden die Daten auf dem Sicherungsspeicher jedes Mal überschrieben, während bei einem Backup die älteren Versionen verfügbar bleiben.

Daten auch jenseits des Onedrive-Ordners synchronisieren
Onedrive synchronisiert nur die Ordner, die als Unterordner in seinem Synchronisationsordner eingetragen sind. Dieser Ordner liegt in der Voreinstellung in „C:\Benutzer\[Benutzername]“ und heißt schlicht „OneDrive“. Möchten Sie weitere Verzeichnisse in die Synchronisation einbeziehen, müssen Sie diese prinzipiell in den Onedrive-Ordner verlegen. Es gibt jedoch einen Trick: Über eine symbolische Verknüpfung können Sie beliebige Ordner mit der Onedrive-Cloud synchronisieren. Eine solche Verknüpfung erstellen Sie mithilfe des in Windows enthaltenen Kommandozeilenbefehls `mklink`. In einem ersten Schritt müssen Sie die absoluten (tatsächlichen) Pfade sowohl des Ordners, den Sie synchronisieren wollen, wie auch des Onedrive-Ordners ermitteln. Rufen Sie den Explorer auf und gehen Sie zum Ordner für die Synchronisation. Sobald Sie in die Eingabezeile klicken, zeigt Ihnen der Explorer den Pfad an und markiert ihn im gleichen Zug. Möchten Sie bei-

TOOLS FÜR SYNCHRONISATION UND BACKUP

Name	Beschreibung	Auf	Internet	Sprache	Preis
Aomei Backupper	Backupsoftware	Heft-DVD	www.pcwelt.de/1686627	Deutsch	kostenlos
Freefilesync	Synchronisationssoftware	Heft-DVD	www.pcwelt.de/1144358	Deutsch	kostenlos
Puresync	Synchronisationssoftware	Heft-DVD	www.pcwelt.de/1144300	Deutsch	kostenlos



Onedrive erstellt auch automatische Backups. Die App sichert auf Wunsch die wichtigsten Windows-Ordner in die Cloud, darunter die Ordner „Dokumente“, „Bilder“ und „Desktop“.

und speichern Sie ihn mit Strg-V in einer Textdatei zwischen. Mit dem Synchronisationsordner von Onedrive verfahren Sie auf die gleiche Art.

Nun tippen Sie *cmd* ins Suchfeld der Taskleiste und öffnen die Eingabeaufforderung. Geben Sie dort den Befehl `mklink /d "[Sync-Ordner von Onedrive]" "[Quellordner]"` ein. Wenn Onedrive also im Standardpfad liegt und Sie den Benutzerordner „Öffentlich“ verknüpfen wollen, geben Sie folgenden Befehl ein:

```
mklink /d "C:\Users\[Benutzername]\OneDrive" "C:\Users\Public"
```

Windows legt nun im Synchronisationsordner von Onedrive eine exakte Kopie des Quellordners an und synchronisiert beide. Alles, was Sie im Quellordner speichern, daraus löschen oder dort hineinkopieren, erscheint auch im zweiten Ordner „C:\Benutzer\[Benutzername]\OneDrive“. Auf die gleiche Weise können Sie beliebige andere Ordner, selbst solche auf anderen Partitionen, mit Onedrive synchronisieren.

Backup mit Onedrive: So sichern Sie Bilder, Dokumente & Co.

Onedrive synchronisiert nicht nur, es führt auch Datensicherungen von Ihrem PC in den Cloudspeicher durch. Dabei nutzt es die fünf GB freien Speicher, die jeder Windows-Nutzer gratis hat, der sich an seinem Rechner mit seinem Microsoft-Konto anmeldet. Haben Sie zusätzlich Microsoft 365 abonniert, können Sie mit Onedrive sogar auf ein Terabyte Speicher zurückgreifen. Das Onedrive-Backup sichert auf Wunsch die Benutzerordner „Dokumente“, „Bilder“, „Desktop“, „Musik“ und „Videos“. Welche dieser Ordner in die Sicherung einbezogen werden sollen, steuern Sie über die Onedrive-App: Dazu klicken Sie auf das Wolken-symbol in der Taskleistenecke und fahren mit einem Klick auf das Zahnradsymbol, gefolgt von „Einstellungen“, fort. Stellen Sie auf der linken Seite sicher, dass Sie sich im Register „Synchronisieren und sichern“ befinden, und klicken Sie auf „Sicherung verwalten“ – fertig.

Windows 11 bietet verschiedene Funktionen zum Datensichern

Windows bietet gleich mehrere Backup-tools: Die klassische Datensicherung, also das Backup von Dateien und Ordnern in

spielsweise „C:\Benutzer\Öffentlich“ synchronisieren, so zeigt Ihnen der Dateima-nager als absoluten Pfad „C:\Users\Public“ an. Kopieren Sie diesen Pfad mit Strg-C

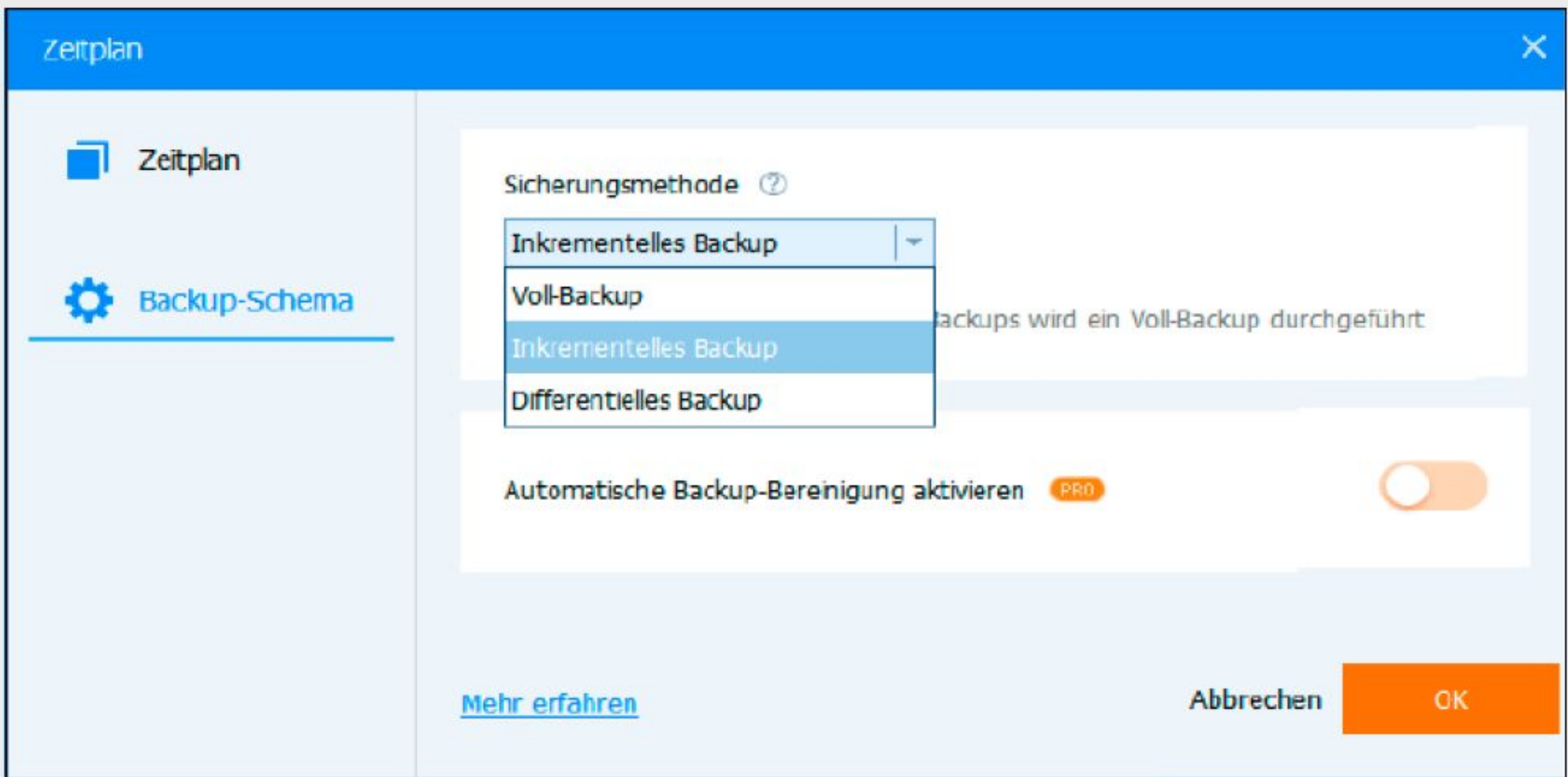
DIE RICHTIGE BACKUPMETHODE WÄHLEN

Die Software **Aomei Backupper** bietet unter „Schema → Backup-Schema“ ein inkrementelles, ein differentielles und ein Voll-Backup an. Bei einem Voll-Backup werden alle für die Sicherung gekennzeichneten Dateien und Ordner auf das Sicherungsziel kopiert. Diese Backupmethode ist daher zeitaufwendig und erfordert viel Speicherplatz.

Ein inkrementelles Backup sichert hingegen nur die seit dem letzten Backup neu hinzugekommenen und geänderten Dateien, und das jeden Tag. Erfolgte etwa am Sonntag ein Voll-Backup, gibt es am Montag ein inkrementelles Backup mit den geänderten Dateien und am Dienstag ein weiteres inkrementelles Backup mit den seit Montag geänderten Files. Das setzt sich bis zum nächsten Voll-Backup fort. Ein inkrementelles Backup ist schneller und benötigt weniger Speicherplatz als ein Voll-Backup. Allerdings dauert die Wiederherstellung der Dateien länger, da man von einer inkrementellen Sicherung zur nächsten zurückgehen muss.

Ein differentielles Backup sichert am Montag die seit dem letzten Voll-Backup neu hinzugekommenen und geänderten Dateien, am Dienstag die am Montag und Dienstag hinzuge-

kommenen Dateien und so weiter. Es ist umfangreicher als eine inkrementelle Sicherung, aber kleiner als ein Voll-Backup und erlaubt eine schnellere Wiederherstellung.



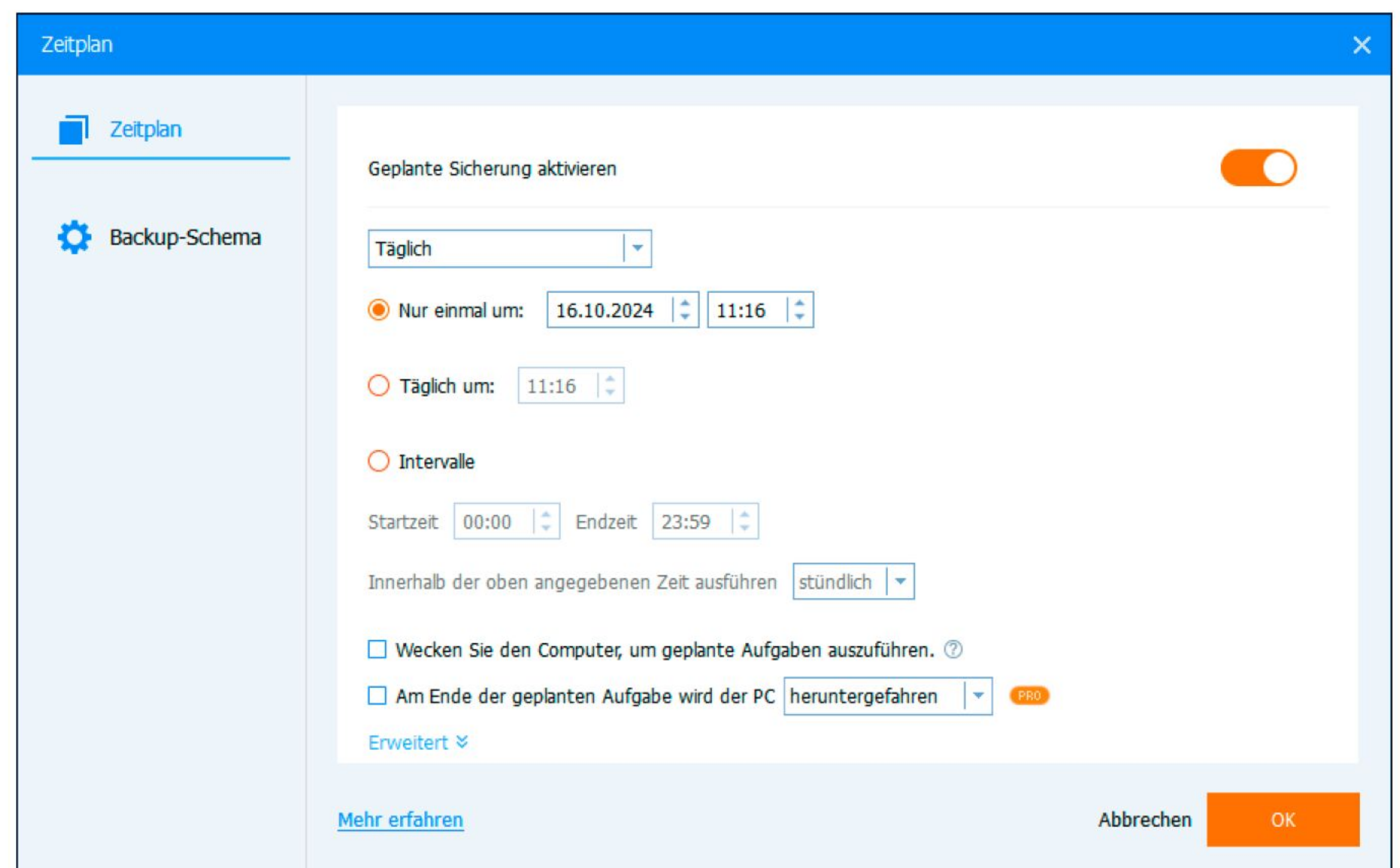
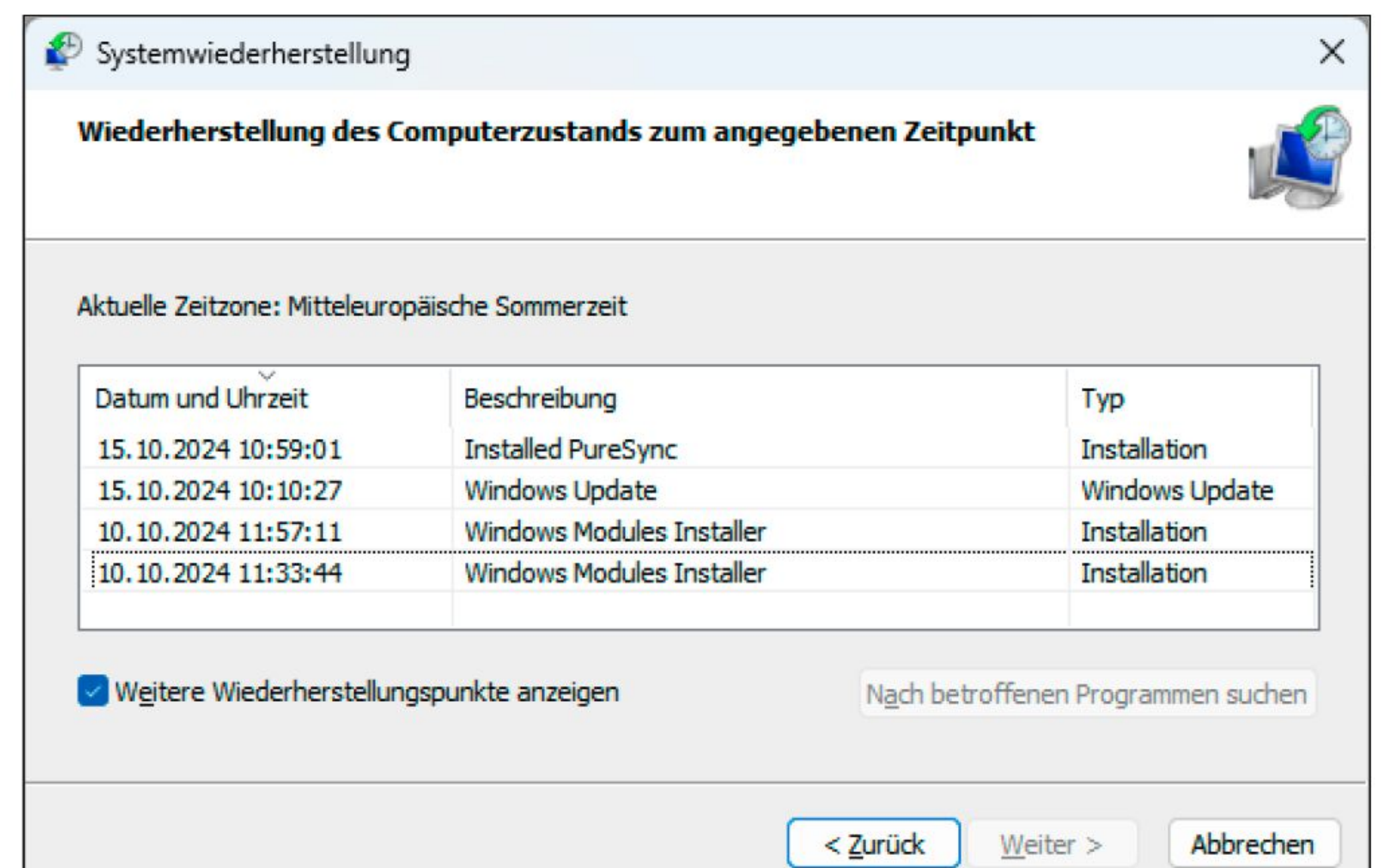
Die Software Aomei Backupper beherrscht mehrere Sicherungsmethoden: vom umfassenden Voll-Backup bis zur schnellen, aber beim Wiederherstellen langsamen inkrementellen Sicherung.

eine Sicherungsdatei auf einem anderen Laufwerk, erledigen Sie über „Sichern und Wiederherstellen (Windows 7)“ in der Systemsteuerung. Von diesem Tool ist allerdings, wie schon erwähnt, abzuraten. Zahlreiche Berichte zeigen, dass sich die Daten nicht mehr wiederherstellen lassen. Über das Fenster von „Sichern und Wiederherstellen“ erreichen Sie darüber hinaus die nur wenigen bekannte Funktion „Systemabbild erstellen“. Damit legen Sie eine Imagedatei an, die Sektor für Sektor die komplette Verzeichnisstruktur einer Partition inklusive der enthaltenen Dateien abbildet. Ein solches Image ist vor allem dann hilfreich, wenn Sie tiefgreifende Änderungen an Windows oder am Dateisystem vornehmen möchten und eine Versicherung brauchen, dass Sie jederzeit wieder zum Ausgangszustand zurückkehren können. Das Anlegen einer Imagedatei kann dauern und erfordert viel Speichervolumen. Zum Dritten gibt es in Windows die Systemwiederherstellung: Sie dient zum Sichern der Systemeinstellungen und der aktuellen Konfiguration von Windows mitsamt den installierten Programmen. Um ein echtes Backup handelt es sich dabei jedoch nicht! Für eine zuverlässige Datensicherung empfehlen wir ein dediziertes Backuptool wie **Aomei Backupper**.

Backup auf USB-Festplatten, Netzspeichern und -freigaben

Ein Backup darf niemals auf dem gleichen Datenträger landen, auf dem die Originaldateien liegen. Ansonsten bietet es keinen Schutz vor Fehlern auf dem Datenträger und vor Hardwaredefekten. Falls in Ihrem PC eine zweite Festplatte/SSD steckt, können Sie diese zum Sichern verwenden. Auch Netzwerkfreigaben oder NAS-Geräte, die mit einem Laufwerksbuchstaben ins Dateisystem eingebunden sind, eignen sich für Backups. Bei Netzwerkfreigaben muss der Rechner, auf dem die Freigabe eingerichtet ist, während des Backups eingeschaltet sein. Optimal ist ein externes Laufwerk, das Sie nur für das eigentliche Backup anschließen, anschließend wieder entfernen und sicher verwahren: beispielsweise USB-Festplatten oder -SSDs. Zur Not geht auch ein ausreichend großer USB-Stick, doch deren Speicherchips sind häufig von minderer Qualität, es besteht also Gefahr von Datenverlusten! Externe Speichermedien bieten zudem Schutz vor Ransomware-Angriffen,

Mit der Systemwiederherstellung von Windows können Sie die Systemeinstellungen, die Registry und Treiber automatisch sichern lassen und später wiederherstellen.



Aomei Backupper erlaubt tägliche Sicherungen. Die Liste der Voll-Backups sollte mehrere Wochen in die Vergangenheit zurückreichen, um zuverlässig vor Ransomware zu schützen.

bei denen Erpresser Ihre Daten auf dem internen Datenträger verschlüsseln. Wenn Sie darauf achten, dass das Speichergerät nach dem Backup stets wieder vom Computer getrennt wird, verringern Sie die Gefahr, dass auch die darauf gesicherten Dateien verschlüsselt werden. Moderne Ransomware-Angriffe versuchen diesen

Schutz jedoch zu hintertreiben, indem sie tage- oder sogar wochenlang im Dateisystem auf der Lauer liegen, sodass sie in die Sicherungen einbezogen werden und diese ebenfalls infiziert sind. Sie sollten aus diesem Grund immer Sicherungssätze bereithalten, die mehrere Wochen in die Vergangenheit zurückreichen. ■

VORSICHT BEIM ZUSCHALTEN VON ONEDRIVE!

Wenn Sie beispielsweise mit Word an einem lokal gespeicherten Dokument arbeiten, sollten Sie nicht zwischendurch die Onedrive-Synchronisierung einschalten. Denn dann geschieht Folgendes: Der aktuelle Stand des Dokuments wird synchronisiert, und Word arbeitet automatisch – und ohne Sie darüber zu informieren – auf dem Onedrive-Laufwerk weiter. Dort wird die Datei dann auch gespeichert. Auf dem lokalen Rechner verbleibt jedoch die Version, die bis zum Einschalten von Onedrive aktuell war. Häufig genug passiert es dann, dass man mit der „alten“ Dateiversion weiterarbeitet.

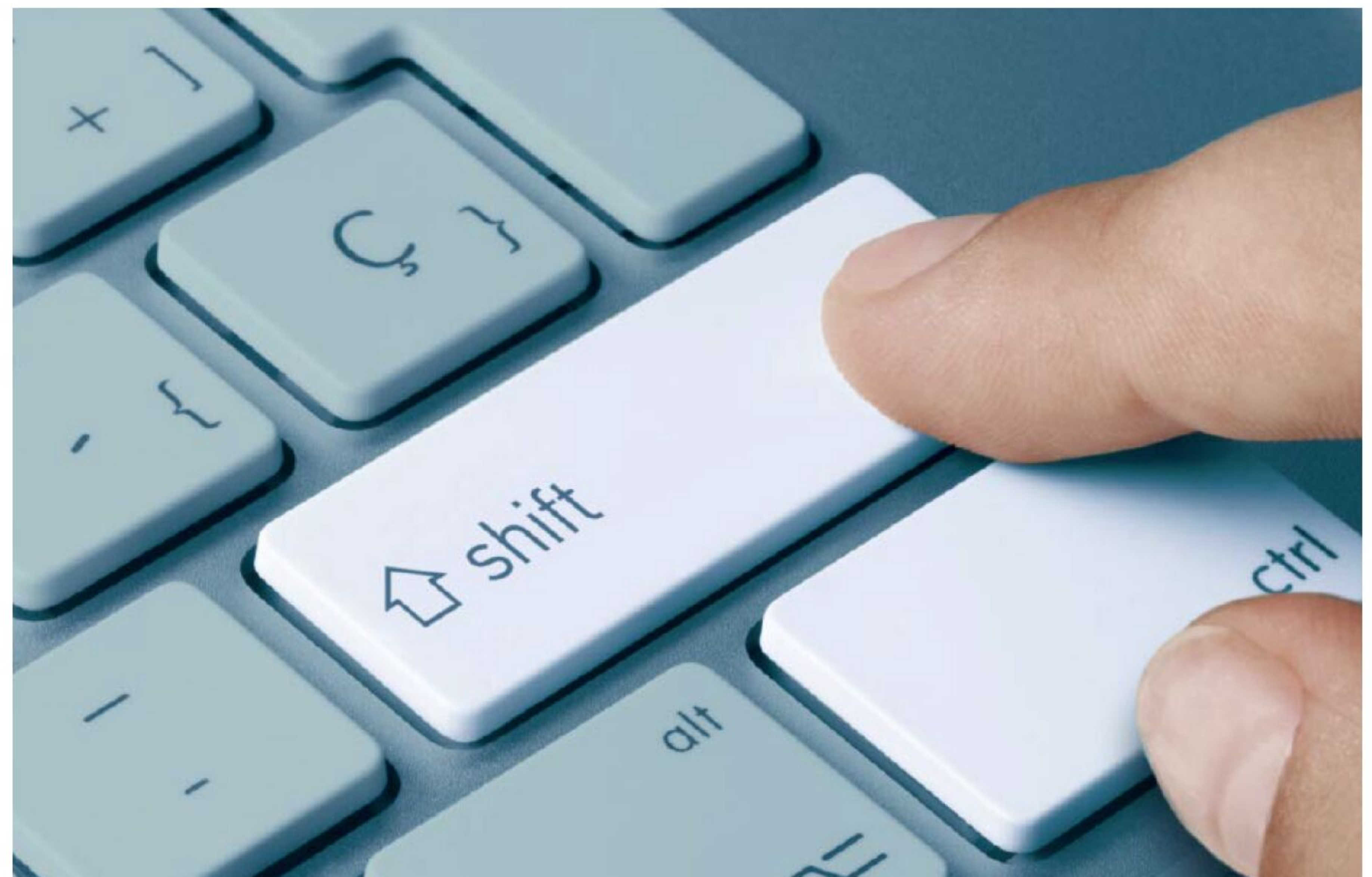


Immer das richtige Programm starten

Ob PDF, Foto oder Musik – Windows öffnet viele Dateien mit dem falschen Programm. Das lässt sich leicht ändern: Mit wenigen Klicks, cleveren Tools und praktischen Tastenkürzeln starten Sie künftig immer genau die Software, die Sie wollen – überall, blitzschnell und jederzeit.

VON STEFFEN ZELFELDER

Wenig nervt so sehr wie falsch verknüpfte Dateien: Sie doppelklicken auf ein Foto, und statt des Bildbetrachters startet ein träges Grafikmonster. Oder Sie wollen schnell etwas im PDF nachlesen, landen aber im Browser statt im Lieblingsviewer. Dabei lässt sich Windows mit wenigen Handgriffen so einstellen, dass jede Datei direkt im gewünschten Programm öffnet – automatisch, sauber und sofort. In diesem Artikel zeigen wir, wie Sie Dateizuord-



© Mit Material von momius - AdobeStock

nungen richtig festlegen, Verknüpfungen nutzen, Kontextmenüs aufräumen und sogar Tastenkombinationen für den Blitzstart beliebiger Programme erstellen. Wer einmal erlebt hat, wie schnell Programme per Shortcut, Hotkey oder mit einem maßgeschneiderten Kontextmenü starten, fragt sich, warum er sich je durchs Startmenü geklickt hat.

„Öffnen mit“ – das richtige Standardprogramm festlegen

Wenn sich eine Datei im falschen Programm öffnet, können Sie das mit dem klassischen Rechtsklick-Trick beheben. Klicken Sie eine Datei mit der rechten Maustaste an und wählen Sie im Menü „Öffnen mit → Andere App auswählen“. Jetzt sehen Sie eine Liste verfügbarer Anwendungen, die sich mit einem Klick auf „Weitere Apps“ erweitern lässt. Wählen Sie das gewünschte Programm aus und vergessen Sie nicht, ein Häkchen bei „Immer diese App zum Öffnen verwenden“ zu setzen. Bestätigen

Sie Ihre Wahl mit einem Klick auf „OK“ – fertig. Windows merkt sich die Zuordnung und öffnet künftig alle Dateien dieses Typs mit dem gewählten Programm.

Wer lieber zentral arbeitet, kann Dateizuordnungen auch systemweit verwalten. Öffnen Sie „Einstellungen → Apps → Standard-Apps“. Je nachdem, ob Sie Windows 10 oder 11 nutzen, sieht die App-Verwaltung etwas unterschiedlich aus. Unter Windows 10 können Sie Standardprogramme für Mails, Karten oder Musik direkt über einen Klick auf die entsprechende Kachel festlegen. Am unteren Ende der Liste finden Sie die Funktionen „Standard-Apps nach Dateityp auswählen“ oder „Standardeinstellungen nach App festlegen“. Damit können Sie wahlweise Dateitypen mit Apps verknüpfen oder Apps mit Dateitypen.

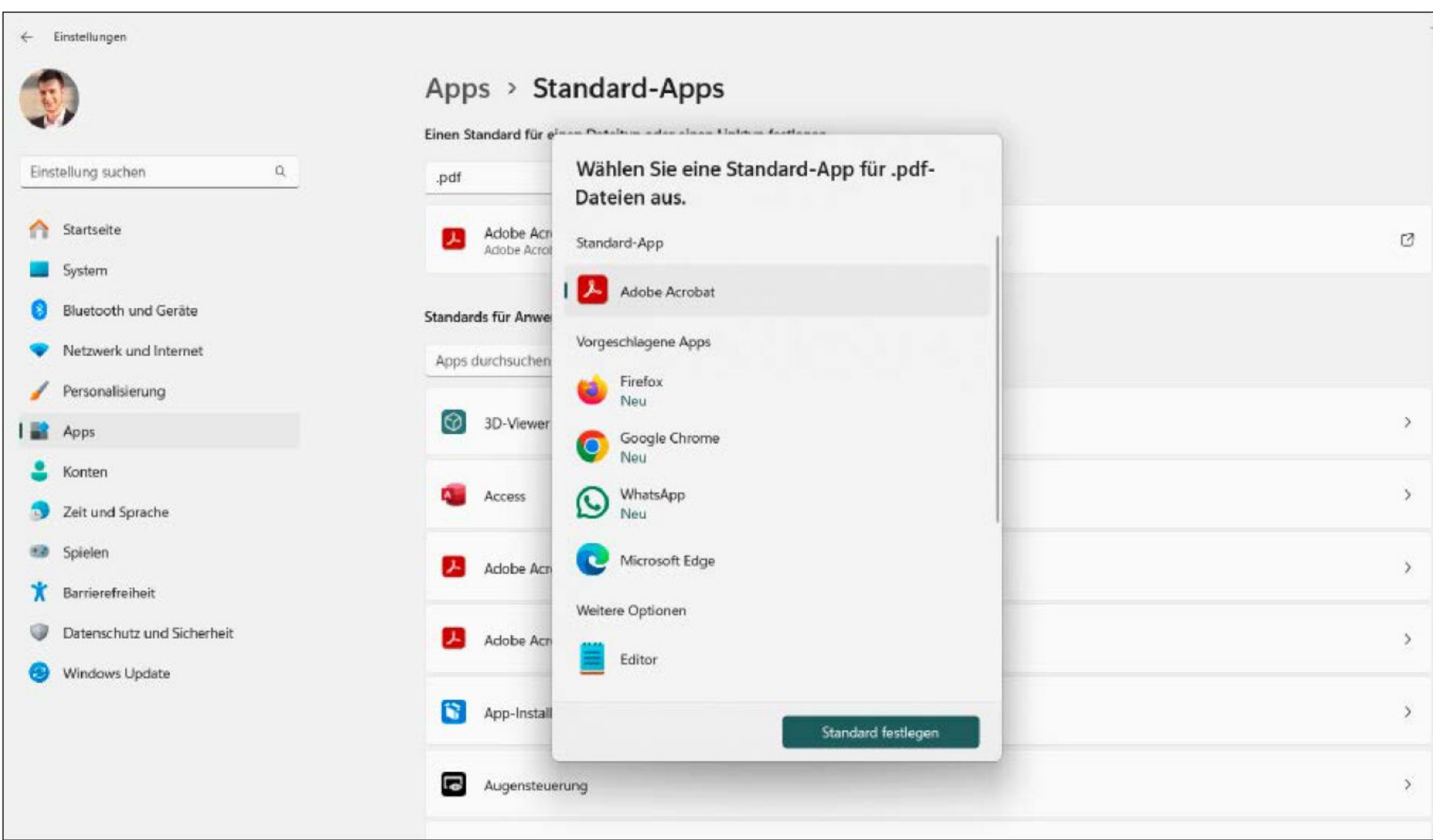
Windows 11 regelt beides im gleichen Funktionsfenster (siehe Bild rechts). Unter „Einen Standard für einen Dateityp oder einen Linktyp festlegen“ können Sie eine Dateiendung eingeben (etwa *mp3*

„Per Shortcut, Hotkey oder maßgeschneidertes Kontextmenü starten Sie Programme deutlich schneller als über das Startmenü von Windows.“

oder pdf) und die Auswahl mit Enter bestätigen. Windows 11 sucht sofort die aktuelle Standard-App heraus. Diese Zuordnung lässt sich mit einem Klick auf das Programm direkt unter der Suchzeile anpassen. Sind Sie unsicher, welches Programm aktuell mit einem bestimmten Dateityp verknüpft ist, scrollen Sie im Fenster ganz nach unten zu „Standardwerte nach Dateityp auswählen“. Dort sehen Sie alle Endungen von jpg bis zip inklusive der zugeordneten Programme. Um alle Verknüpfungen zurückzusetzen, klicken Sie im vorherigen Fenster (Standard-Apps) ganz unten auf „Alle Standard-Apps zurücksetzen“.

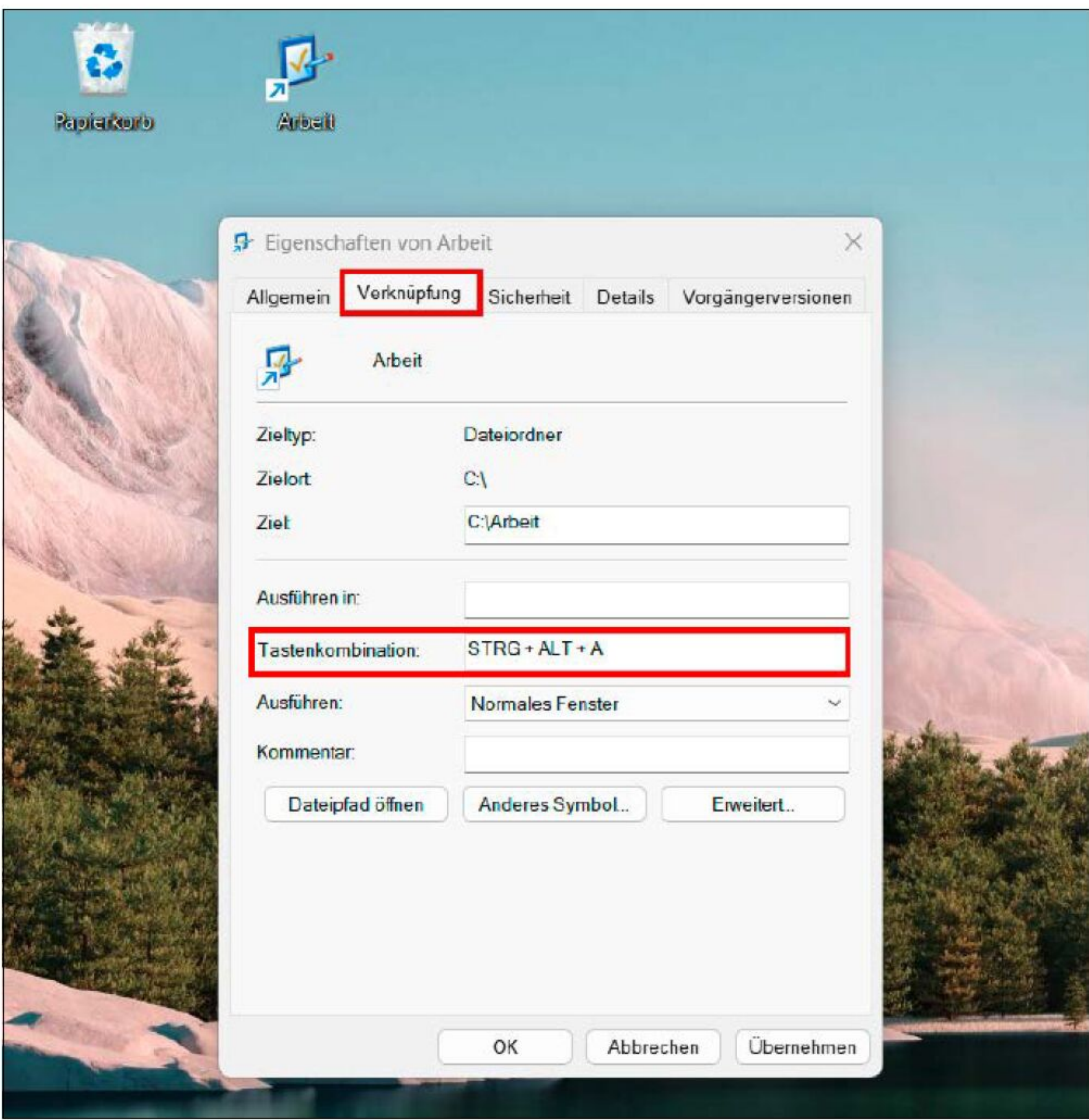
Programme und Dateien per Verknüpfung und Hotkey öffnen

Oft genügt ein Doppelklick – per Tastenkombination geht es aber noch schneller. Mit eigenen Verknüpfungen und Hotkeys öffnen Sie Lieblingsprogramme, Dokumente oder Ordner direkt von der Tastatur aus, auch, wenn Sie gerade ein Youtube-Video schauen oder mitten im Spiel sind. Das klappt mit jeder beliebigen Verknüpfung: Klicken Sie mit der rechten Maustaste auf den Desktop, und wählen Sie „Neu → Verknüpfung“. Geben Sie dann den Pfad zur gewünschten EXE-Datei oder zu einem Dokument ein, beispielsweise C:\Programme\Firefox\firefox.exe. Per „Durchsuchen...“ können Sie Dateien auch via Menü auswählen. Klicken Sie auf „Weiter“, vergeben Sie einen Namen, etwa „Firefox“, und beenden Sie mit „Fertig stellen“. Wählen Sie nun Ihre neue Verknüpfung per Rechtsklick aus, und klicken Sie auf „Eigenschaften“. Im Tab „Verknüpfung“ finden Sie die Zeile „Tastenkombination“: Klicken Sie darauf und geben Sie den gewünschten Shortcut ein, etwa wie im Bild „Strg + Alt + A“ für einen Arbeitsordner. Klicken Sie abschließend auf „OK“. Ab sofort öffnen sich das Programm oder Dokument



Die Zuordnung von Dateitypen sieht unter Windows 10 und 11 unterschiedlich aus. Im Bild sehen Sie Windows 11, bei dem die Verwaltung etwas intuitiver und übersichtlicher gelöst ist.

Eine Verknüpfung können Sie unter Windows jederzeit mit einer einfachen Tastenkombination aufrufen. So starten Sie Programme oder öffnen Dokumente und Ordner per Hotkey von jedem Ort aus – schnell und praktisch.



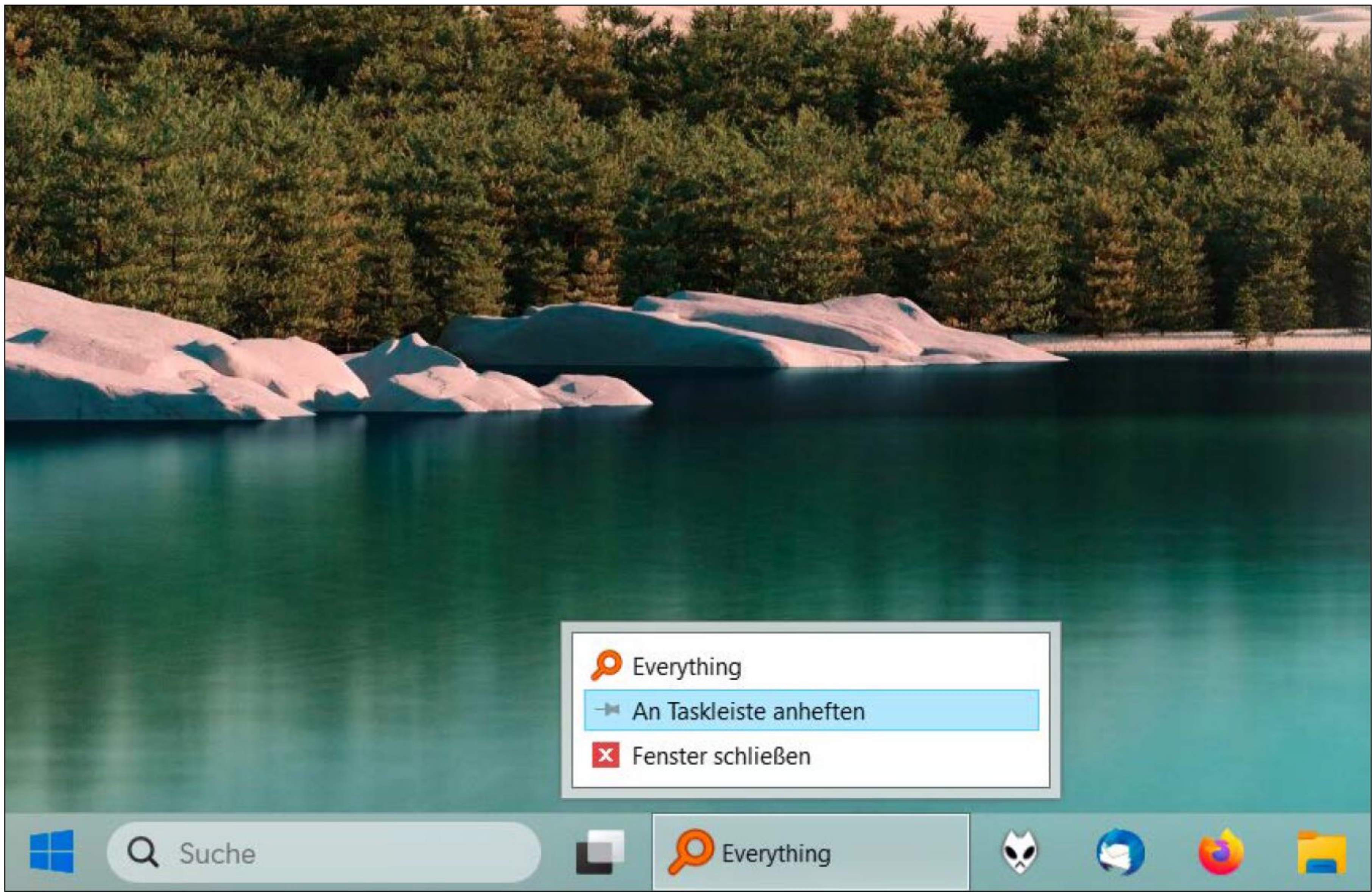
mit der gewählten Tastenkombi, egal wo Sie sich gerade im System befinden. Diese Hotkeys funktionieren universell, auch wenn Sie in einem anderen Fenster

ZUGRIFF AUF PROGRAMME, DATEIEN UND WEBSEITEN ANPASSEN

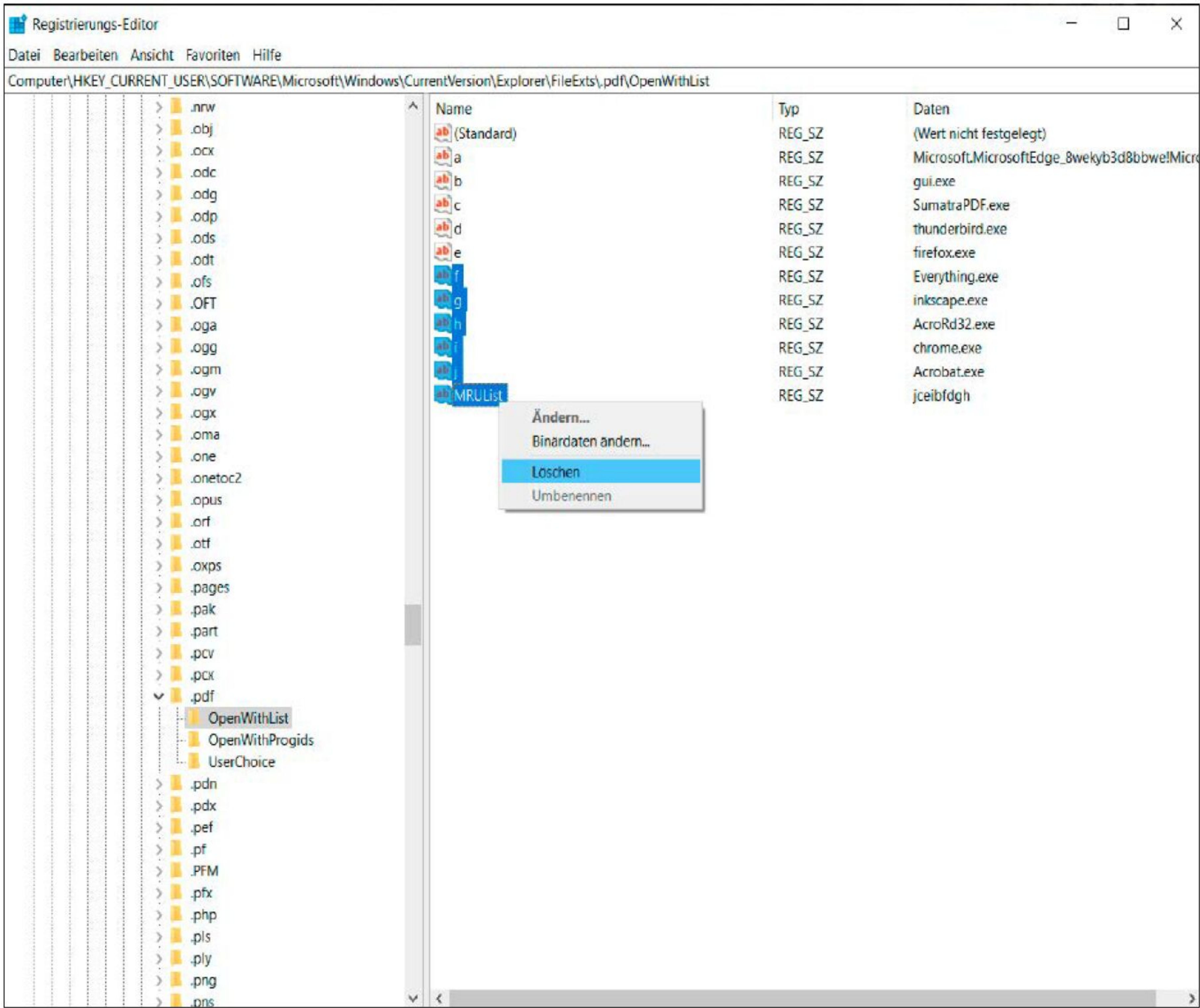


Name	Beschreibung	URL	Auf	Sprache	Preis
Explorer Patcher	Macht das klassische Windows-10-Startmenü und die alte Taskleiste wieder verfügbar	https://github.com/valinet/explorerpatcher/releases	Heft-DVD	Englisch	Kostenlos
Open With View	Zeigt „Öffnen mit“-Einträge und kann sie per Klick deaktivieren	www.nirsoft.net/utis/open_with_view.html	Heft-DVD	Englisch	Kostenlos
Start All Back	Bringt klassische Windows-Optik zurück und ist dabei sehr ressourcenfreundlich	www.startallback.com	Heft-DVD	Deutsch	Ca. 5 Euro
WiseCleaner Wise Hotkey*	Startet Programme per Tastenkürzel; eingeschränkte Gratis-Version kostenlos erhältlich	www.wisecleaner.eu/wise-hotkey.html	Heft-DVD	Englisch	Ca. 8 Euro pro Jahr*

* Kostenlose, zeitlich unbegrenzte Vollversion auf Heft-DVD



Windows 11 zeigt sich beim Anpassen der Taskleiste zwar weniger flexibel als sein Vorgänger. Wichtige Programme lassen sich aber auch hier mit wenigen Klicks dauerhaft verankern und anschließend mit nur einem Klick starten.



Wer das „Öffnen mit“-Menü aufräumen und Einträge löschen oder hinzufügen möchte, kann das direkt in der Registry erledigen. Einfacher und sicherer übernimmt dies jedoch das Tool Open With View. Für beide Methoden empfiehlt sich ein Registry-Backup.

arbeiten oder gerade keine Maus zur Hand haben. Ideal also, um Browser, Editor, Mailprogramm oder den Datei-Explorer blitzschnell zu öffnen. Ein Tipp: Wählen Sie Kombinationen, die nicht von anderen Programmen belegt sind, etwa Strg + Alt + E (Explo-

rer) oder Strg + Alt + T (Texteditor). Wer es besonders aufgeräumt mag, kann die Verknüpfungen anschließend in einen eigenen Ordner (etwa „Hotkeys“) verschieben oder an die Taskleiste anheften – die Tastenkombinationen funktionieren trotzdem weiter.

Schnellzugriff in der Taskleiste von Windows 10 und 11

Die Taskleiste ist der schnellste Zugriffsort für wichtige Programme, funktioniert aber unter Windows 10 und 11 etwas unterschiedlich. Unter Windows 10 genügen ein Rechtsklick auf ein Programm oder eine App-Verknüpfung und der Befehl „An Taskleiste anheften“. Anschließend ist die Verknüpfung dauerhaft in der Taskleiste sichtbar und kann mit einem Klick gestartet werden – auch nach einem Neustart. Solche Programme lassen sich auch per Drag & Drop verschieben oder gruppieren. Unter Windows 11 hat Microsoft die Leiste modernisiert, leider auf Kosten der Funktionalität. Icons können nur noch zentriert angezeigt werden, und der Schnellstartbereich ist nicht mehr so flexibel. Trotzdem lohnt sich das Anheften: Öffnen Sie ein Programm, klicken Sie dessen Symbol in der Taskleiste mit der rechten Maustaste an und wählen Sie „An Taskleiste anheften“. Über „Einstellungen → Personalisierung → Taskleiste“ steuern Sie, welche Systemelemente (Suche, aktive Apps, Chat etc.) angezeigt werden sollen. So schaffen Sie bei Bedarf mehr Platz für eigene Programme. Wer sich die alte Freiheit von Windows 10 zurückwünscht, kann mit Tools wie **Start All Back** oder **Explorer Patcher** (beide auf Heft-DVD) nachhelfen. Beide erlauben es, die Taskleiste wieder nach oben zu verschieben, Abstände zwischen Icons zu verändern oder das klassische Windows-10-Verhalten inklusive Schnellstartleiste und anpassbarer Symbolgrößen zurückzubringen.

Kontextmenü „Öffnen mit“ per Registry aufräumen oder erweitern

Wenn Sie regelmäßig verschiedene Programme für denselben Dateityp verwenden, wächst das Menü „Öffnen mit“ schnell zu einer unübersichtlichen Liste heran. Alte, deinstallierte Programme bleiben oft darin hängen, neue fehlen manchmal ganz. Wer hier aufräumen will oder manuell Einträge hinzufügen möchte, kann das direkt in der Registry erledigen. Bevor Sie Änderungen an der Registry vornehmen, sollten Sie sie aber sichern. Drücken Sie dazu die Windows-Taste + R, geben Sie *regedit* ein und drücken Sie „Enter“. Wählen Sie im geöffneten Fenster anschließend „Datei → Exportieren“. So lässt sich im Notfall alles per „Datei → Importieren“ wiederherstellen.

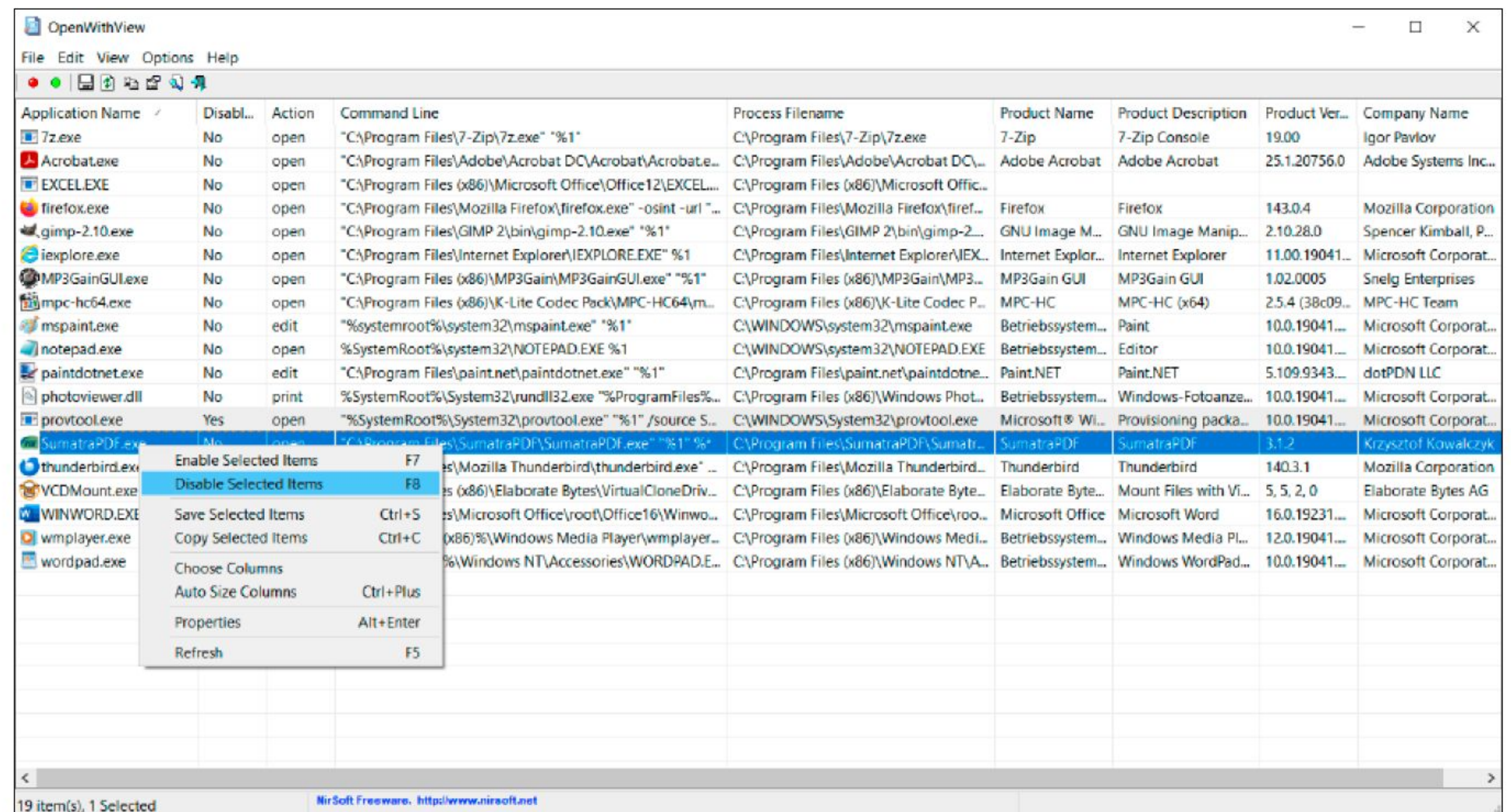
Um überflüssige Einträge aus dem „Öffnen mit“-Menü zu entfernen, öffnen Sie den Registry-Editor wie oben beschrieben (regedit). Navigieren Sie zu HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts und suchen Sie dort nach dem gewünschten Dateityp. Löschen Sie innerhalb des Unterschlüssels „OpenWithList“ oder „OpenWithProgids“ die Einträge, die nicht mehr benötigt werden. Schließen Sie danach den Editor, die Änderungen greifen sofort. Wenn ein gewünschtes Programm nicht in der „Öffnen mit“-Liste erscheint, können Sie dies ebenfalls mit einem Eintrag ändern. Unter dem gleichen Pfad (FileExts\[Dateiendung]\OpenWithList) legen Sie nach einem Rechtsklick und „Neu → Zeichenfolge“ einen neuen Zeichenfolgenwert an: Wählen Sie einen Buchstaben als Namen, der noch nicht in der Liste steht. Mit einem Doppelklick auf die neue Zeichenfolge geben Sie unter „Wert“ den (exakten) Programmnamen ein, etwa „Acrobat.exe“. Ein Neustart des Explorers reicht, schon taucht das Programm künftig im Menü auf. Bei häufiger Nutzung lohnt sich dieser Eingriff aber nur bedingt – einfacher und sicherer geht es mit dem Tool **Open With View** von Nirsoft (auf Heft-DVD), das diesen Bereich grafisch darstellt und editierbar macht. Doch dazu mehr im nächsten Abschnitt.

Kontextmenü komfortabel bearbeiten mit Open With View

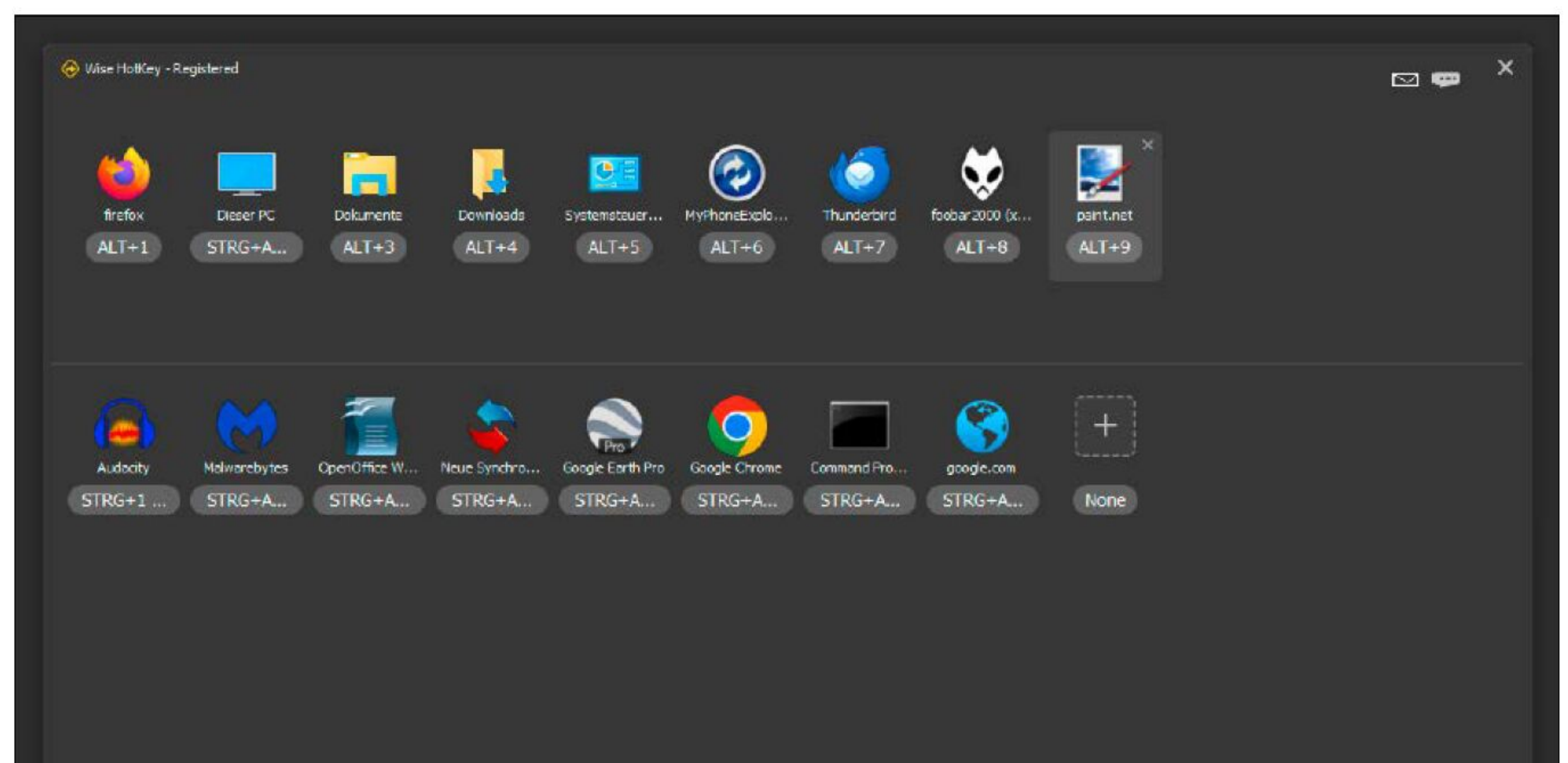
Wer keine Lust auf Registry-Arbeit hat, kann das Kontextmenü mit dem kostenlosen Tool Open With View deutlich einfacher verwalten. Das Programm listet die „Öffnen mit“-Einträge tabellarisch auf – inklusive Pfad, Beschreibung und Status. Überflüssige Programme lassen sich hier mit einem Klick deaktivieren, ohne sie gleich löschen zu müssen.

Nach dem Entpacken und Starten der EXE-Datei zeigt das Tool sofort die registrierten Programme samt Dateizuordnungen an. Mit einem Rechtsklick auf einen Eintrag können Sie den Befehl „Disable Selected Items“ ausführen, um das entsprechende Programm im Kontextmenü auszublenden. Rückgängig machen Sie den Schritt per „Enable Selected Items“.

Der Vorteil des Tools: Sie riskieren keine fehlerhaften Registry-Einträge und können eine einfache grafische Oberfläche nutzen.



Statt mühsam an der Registry herumzubasteln, reicht bei Open With View ein Klick, und das Tool zeigt „Öffnen mit“-Einträge übersichtlich an. Auf diese Weise lässt sich das Kontextmenü gezielt aufräumen und anpassen.



Mit Wisecleaner Wise Hotkey starten Sie Programme, Webseiten und Ordner per Tastenkürzel. Das geht blitzschnell und ohne Umwege über das Startmenü oder Herumklicken in der Taskleiste – ein Komfort, an den man sich schnell gewöhnt.

Zudem lassen sich gleich mehrere Programme markieren. Das ist ideal, um veraltete oder doppelte Einträge in einem Rutsch zu entfernen. Open With View arbeitet nur auf Benutzerebene, verändert also keine systemweiten Zuordnungen. Es zeigt jedoch nur klassische Desktop-Programme an. Moderne Apps wie Chrome, Edge oder Fotos bleiben teils unsichtbar, weil sie ihre Zuordnungen über neuere Windows-Mechanismen verwalten.

Lieblingsprogramme blitzschnell starten mit Wise Hotkey

Wer viele Programme parallel nutzt, kommt mit Windows-Bordmitteln irgendwann an Grenzen. **Wisecleaner Wise Hotkey** (Vollversion auf Heft-DVD) ist dann eine komfortable Lösung: Das Tool erwei-

tert Ihr System um frei belegbare Tastenkombinationen für Programme, Ordner und Webseiten. Die Bedienung ist dabei intuitiv und auch für Einsteiger leicht verständlich: Klicken Sie im Programm auf ein Plus-Symbol und wählen Sie das gewünschte Programm, einen Ordner oder eine URL aus. Mit einem Doppelklick auf die Kombination lassen sich die Hotkeys ändern, auch Tastenfolgen wie Ctrl + Alt + W sind möglich. Wise Hotkey zeigt Ihnen alle vergebenen Tastenkürzel auf einen Blick, kann zwischen geöffneten Fenstern wechseln und läuft dabei stabil im Hintergrund. Die Software startet automatisch mit Windows, verbraucht kaum Ressourcen und wird so zur Schaltzentrale für produktives Arbeiten, besonders wenn die Taskleiste schon voll ist. ■

Von Microsoft gelöscht

Immer wieder überarbeitet Microsoft einzelne Windows-Tools oder löscht sie gar komplett aus dem Betriebssystem. Wir zeigen, welche Tools verschwinden, wo Sie Ersatz dafür finden und wie Sie Ihre Daten retten.

VON ROLAND FREIST

Microsoft hat in den letzten Jahren begonnen, Windows von Grund auf zu renovieren. Davor schleppte das Betriebssystem einige Altlasten mit sich herum, die teilweise bereits in den 16-Bit-Versionen Windows 3.0 und 3.1 enthalten waren und seither nur einige kosmetische Änderungen erfahren hatten. Dazu gehörten die beiden Textprogramme **Editor** und **Wordpad**, aber auch das Malprogramm **Paint**. Während Notepad und Paint gründlich überarbeitet wurden, ist Wordpad aus Windows mittlerweile verschwunden.

Aber auch neuere Apps und Systemelemente sind vor den Aufräumarbeiten nicht sicher. So hat Microsoft die in Windows enthaltenen Programme **Mail**, **Kalender** und **Kontakte** in den vergangenen Monaten nach und nach aus dem Betriebssystem entfernt und durch das neue Outlook ersetzt. Parallel dazu existiert aber auch noch das Outlook aus Microsoft 365. Ob die neue Version bereits einen vollwertigen Ersatz darstellt und wann sie den Vorgänger verdrängen wird, ist

derzeit eine der spannendsten Fragen rund um Microsofts Office-Strategie.

Mail & Co. gegen das neue Outlook

Das neue Outlook ersetzt die kostenlos in Windows enthaltenen, aber wenig genutzten Apps **Mail**, **Kalender** und **Kontakte**. Das Programm wird automatisch mit dem Betriebssystem installiert. Während Sie anfangs die mittlerweile als „Outlook (new)“ bezeichnete Software noch parallel mit den drei Apps benutzen konnten, führt seit Anfang 2025 der Versuch, etwa den Kalender zu öffnen, zum Start des neuen Outlook. Gleichzeitig hat Microsoft die Apps aus dem Microsoft Store entfernt, sodass sie sich nicht neu installieren lassen.

Da das neue Outlook Daten wie Mails, die nicht bei einem Mailsdienst von Microsoft gehostet werden, nicht automatisch übernimmt, werden die alten Apps eventuell noch benötigt. Sie sind in Windows auch nach wie vor enthalten, das neue Outlook blockiert lediglich den Start. Dagegen lässt sich allerdings etwas machen: Mit einem Workaround können Sie Outlook deinstallieren und gleichzeitig verhindern, dass es automatisch neu installiert wird. Dazu benötigen Sie die Powershell von Windows.

Alte Mail-App wiederherstellen

Tippen Sie *powershell* ins Eingabefeld der Taskleiste, klicken Sie im folgenden Fenster auf der rechten Seite auf „Als Administrator ausführen“ und anschließend auf „Ja“. Geben Sie nun den Befehl

```
Get-AppxPackage -AllUsers | where
{$_.Name -like "*outlook*"} |
Remove-AppxPackage -AllUsers
```

ein und drücken Sie Enter. Sie bekommen keine Rückmeldung, was im Hintergrund passiert. Sobald ein neuer Prompt mit „PS C:\WINDOWS\system32>“ erscheint, können Sie das Fenster schließen. Das neue Outlook ist jetzt deinstalliert.

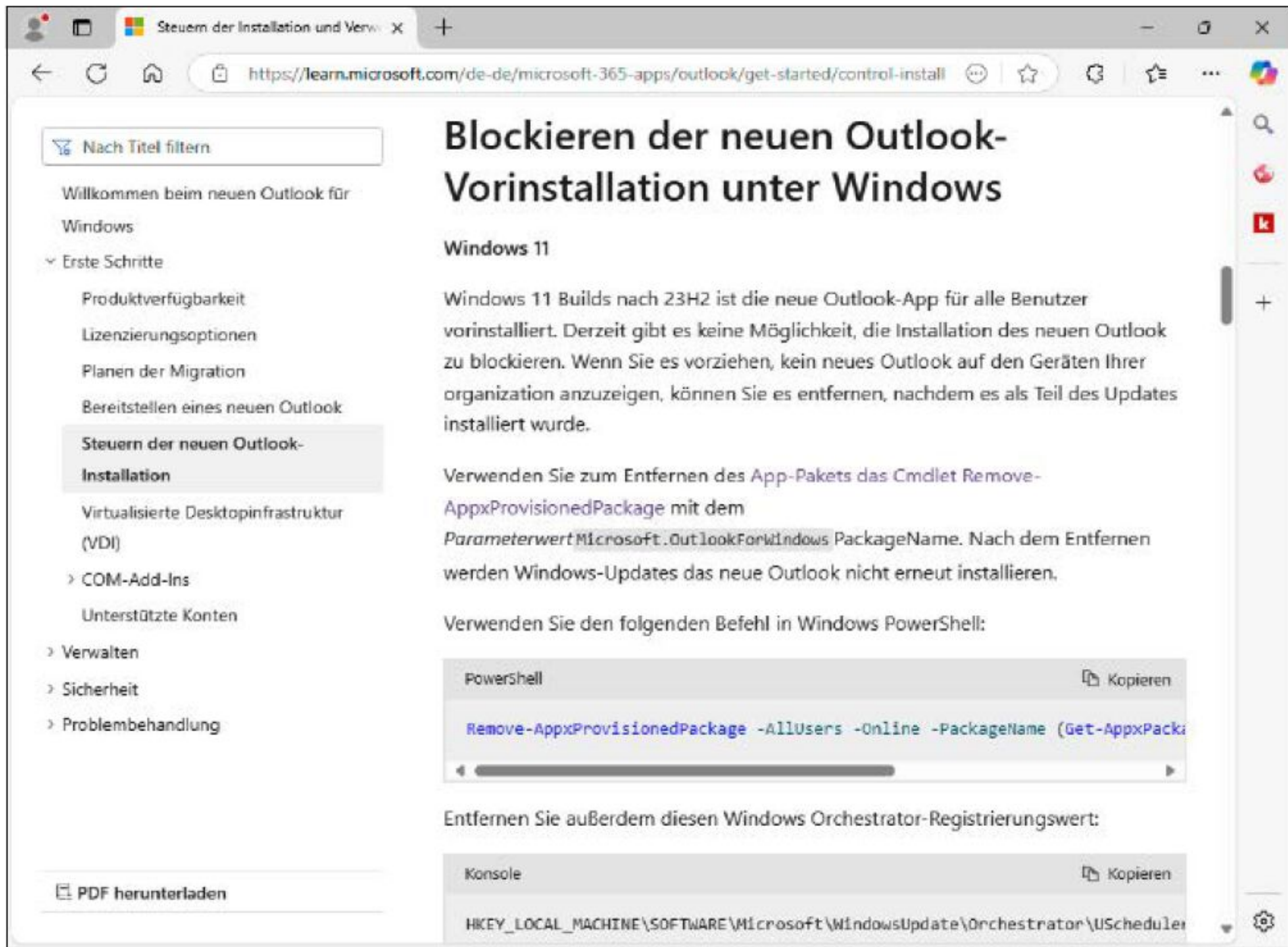
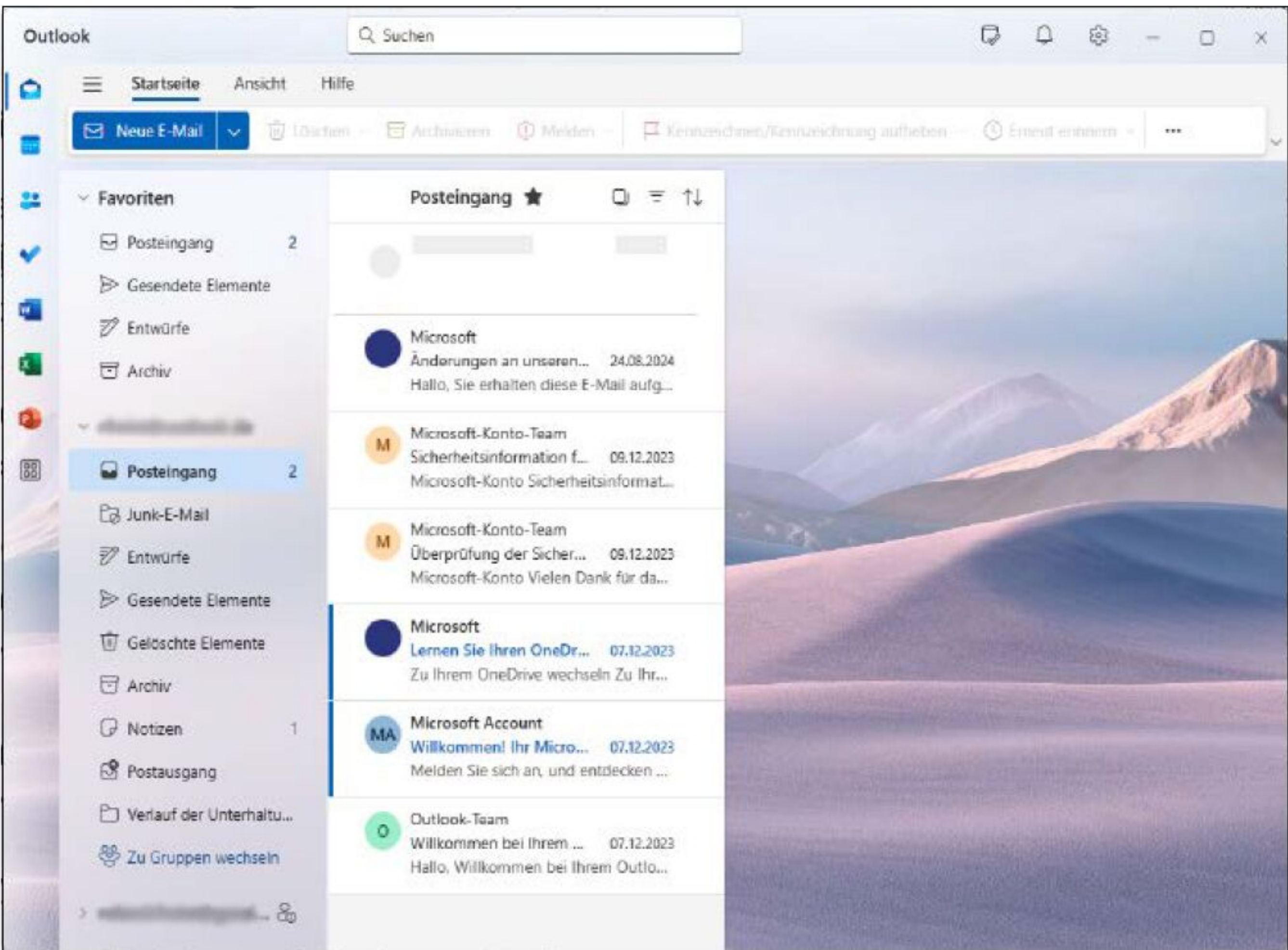
Um zu verhindern, dass Windows das neue Outlook sofort wieder einrichtet, täuschen Sie eine bereits laufende Installation vor. Öffnen Sie dazu über das Startmenü den „Microsoft Store“ und suchen Sie dort nach „Outlook für Windows“. Klicken Sie den Treffer an und gehen Sie auf „Herunterladen“. Die Store-App bereitet nun den Download vor. Sobald im Button der Hinweis „Wird installiert“ erscheint, klicken Sie sofort auf das Pausezeichen. Im Button steht nun „Angehalten“.

Schließen Sie jetzt den Microsoft Store. Danach können Sie Mail und Kalender wieder



© Spectral-Design - AdobeStock

„So sichern Sie Ihre Daten aus Mail, Kalender & Co., bevor Microsoft sie blockiert.“



Das neue Outlook hat bereits die Apps Mail, Kalender und Kontakte ersetzt und soll mittelfristig auch das klassische Outlook aus Microsoft 365 verdrängen.

Im Internet hat Microsoft eine Anleitung veröffentlicht, wie die Abonnenten der Business-Versionen von Microsoft 365 die Installation des neuen Outlook verhindern.

starten. In beiden Programmen erscheint nun ein englischsprachiger Hinweis, dass Windows Mail und Calendar nicht mehr unterstützt werden. Dazu gibt es zwei Buttons. Gehen Sie auf „Export Data“, erscheint ein Explorer-Fenster, das im Unterordner „Mail“ die Ordnerstruktur Ihres Postfachs nachbildet. Wenn Sie auf „Open Outlook“ klicken, öffnet sich wieder die alte Mail- beziehungsweise Kalender-App. Eventuell müssen Sie das Postfach bei Ihrem Provider über „Konten → Konto hinzufügen“ erneut einrichten.

Falls Sie Outlook (new) später einmal doch installieren wollen, öffnen Sie wieder den Microsoft Store und klicken links unten auf „Downloads“. Im nächsten Fenster klicken Sie dann beim Eintrag „Outlook für Windows“ auf der rechten Seite auf den Button mit dem Wolkensymbol.

Outlook (classic) mit Gnadenfrist

Das neue Outlook wurde konzipiert, um die alten Mail-, Kalender- und Kontakte-Apps

zu ersetzen. Es soll aber auch das alte, klassische Outlook aus dem Office-Paket Microsoft 365 auf den Rechnern der Anwender verdrängen. Seit Anfang Januar 2025 taucht bei den Abonnenten der Business-Versionen von Microsoft 365 anstatt der alten Version das neue Outlook auf. Allerdings hat Microsoft auch Anleitungen veröffentlicht, wie der Administrator diese Änderung rückgängig machen beziehungsweise Neuinstallationen so konfigurieren kann, dass wieder das klassische Outlook erscheint.

Bei Privatkunden soll der Wechsel im Herbst 2026 erfolgen. Microsoft will für die klassische Version nach heutigem Stand allerdings noch bis zum Jahr 2029 Support leisten.

Wordpad und Editor ersetzen

Wordpad war lange Jahre so etwas wie der kleine Bruder von Word. Der in Windows enthaltene Texteditor besaß allerdings deutlich weniger Funktionen und hatte teilweise Schwierigkeiten mit langen Doku-

menten. Vermutlich wird kaum ein Anwender das Programm vermissen. Falls doch, siehe den Text im Kasten auf Seite 32.

Ansonsten bieten sich gleich mehrere Alternativen an. Wer ein Microsoft-Konto besitzt, kann im Browser auf Microsoft 365 Copilot zugreifen, das ehemalige Office Online. Die darin enthaltene Version von Word steht der in Microsoft 365 kaum nach. Bei Google gibt es mit Google Docs ebenfalls eine umfangreiche kostenlose Textverarbeitung.

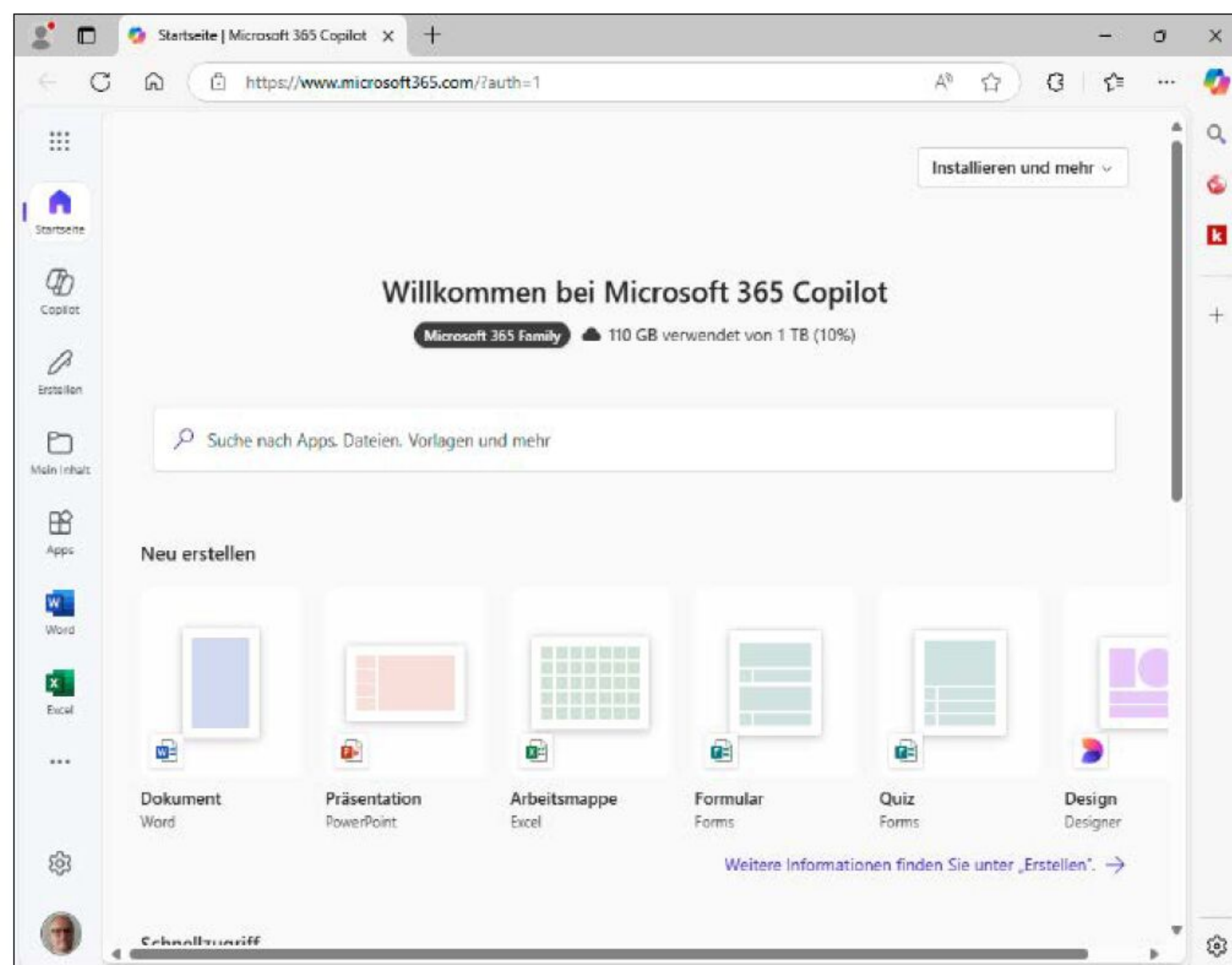
Wenn Sie Ihre Texte nicht Microsoft oder Google übergeben möchten, können Sie auf lokal installierte Programme ausweichen. **Libre Office** ist ein professionelles Office-Paket aus der Open-Source-Szene und bringt mit Write einen leistungsfähigen Texteditor mit. Wenn Sie eher eine kleine und leichte Alternative suchen, sollten Sie sich **Abiword** ansehen.

Microsoft ist der Meinung, dass das Gespann aus dem kostenlosen Editor in Windows und Word ausreichend Alternativen

IM ÜBERBLICK: WINDOWS-TOOLS



Name	Beschreibung	Auf	Internet	Sprache	Preis
Abiword	Textverarbeitung	Heft-DVD	www.pcwelt.de/article/1143393	Deutsch	Kostenlos
Anvir Task Manager Free	Systemprogramm	Heft-DVD	www.anvir.com	Englisch	Kostenlos
Google Chrome	Browser	Heft-DVD	www.pcwelt.de/article/2577178	Deutsch	Kostenlos
Libre Office	Office-Paket	Heft-DVD	www.pcwelt.de/article/1140010	Deutsch	Kostenlos
Mitec Task Manager Deluxe	Systemprogramm	Heft-DVD	www.mitec.cz/tmx.html	Englisch	30 Euro
Paint.net	Bildbearbeitung	Heft-DVD	www.pcwelt.de/article/1135563	Deutsch	Kostenlos
Verschwundene Windows-Tools					
Aurora-Screensaver, Editor, Kurznotizen, Paint, Rechner, Systemkonfiguration, Task-Manager, Wordpad	Alte Versionen und verschwundene Tools	–	https://win7games.com	Deutsch	Kostenlos



Das ehemalige Online-Office heißt nun Microsoft 365 Copilot. Es ist nach wie vor kostenlos, bietet aber weniger als das Office-Paket Microsoft 365.



Abiword ist eine kostenlose Textverarbeitung, die alle Funktionen für das Schreiben und die Gestaltung privater und geschäftlicher Korrespondenz enthält.

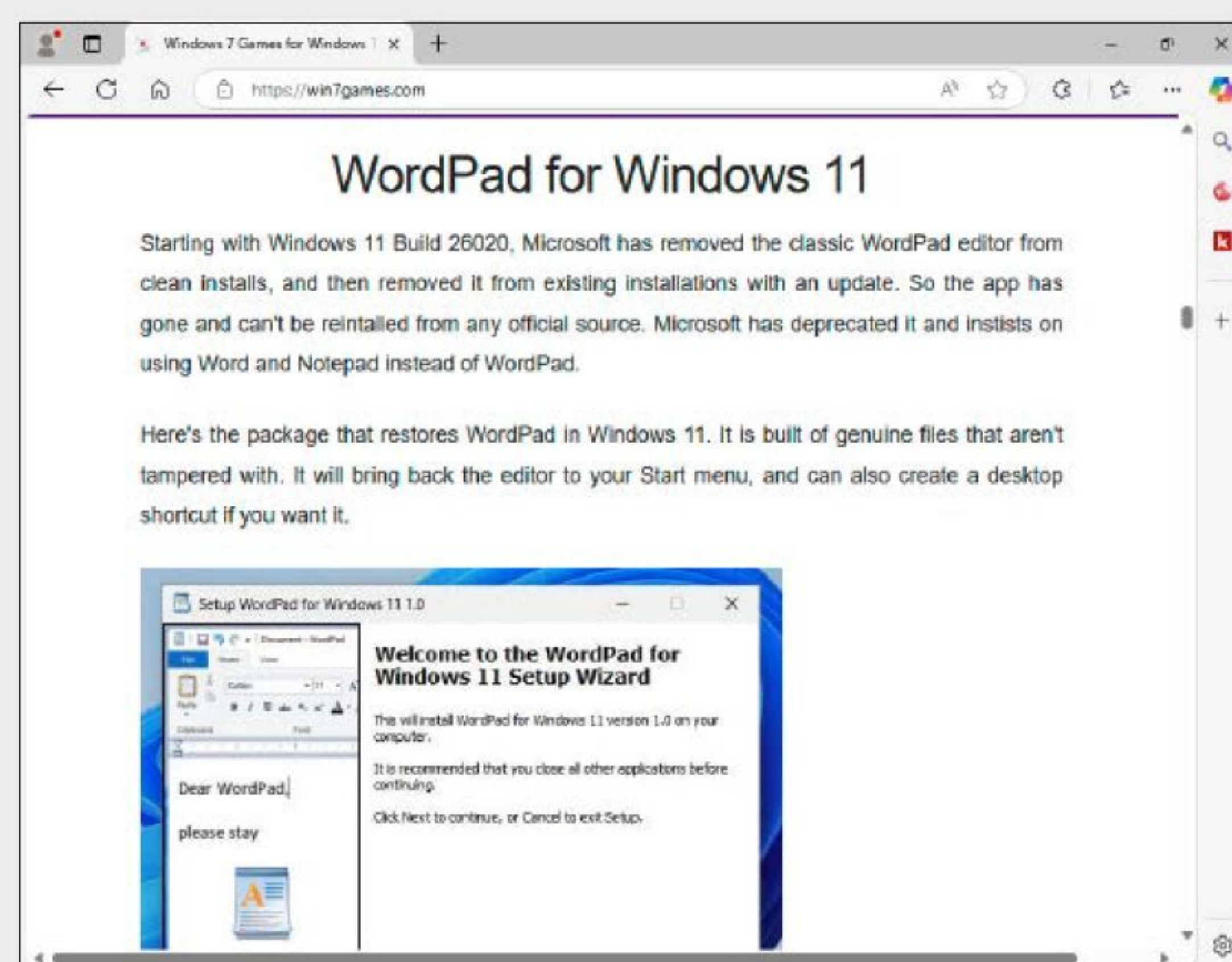
bietet, um Wordpad schnell vergessen zu machen. Die Firma hat daher den **Editor** von Windows, der in der englischen Version Notepad heißt, um einige Funktionen erweitert. Ursprünglich war der Editor eine auf das Minimum beschränkte Textverarbeitung ohne jeglichen Komfort. Vor drei

Jahren spendierte Microsoft dem Programm jedoch einen Zeilenumbruch, eine Rechtschreibprüfung und eine Autokorrektur. Genau wie Wordpad lässt sich die alte Version aus dem Internet herunterladen und installieren. Sie läuft dann parallel zum neuen Editor.

VERSCHWUNDENE PROGRAMME NEU INSTALLIEREN

Microsoft nimmt bei Updates und neuen Windows-Versionen immer mal wieder althergebrachte Programme aus dem Betriebssystem. Teilweise sind sie einfach veraltet, teilweise geschieht dies aber auch, weil sich die Strategie der Firma geändert hat. Fast immer gibt es Fans, die den gewohnten Tools nachtrauern. Ihnen bietet die Website Windows 7 Games (<https://win7games.com>) eine Möglichkeit, diese Programme wieder neu zu installieren.

Sie finden auf der Site neben den noch in Windows 7 enthaltenen Spielen wie **Solitaire** oder **Minesweeper** auch die alten Versionen der Anwendungen **Rechner**, **Wordpad**, **Editor**, **Kurznotizen**, **Task-Manager**, **Systemkonfiguration** und **Paint** sowie den **Aurora-Screensaver**. Alle sind mit einem eigenen Installationsprogramm versehen und werden größtenteils auch in allen verfügbaren Sprachen zum Download angeboten. Windows 7 Games liefert zudem bebilderte Anleitungen für die Einrichtung der Software.



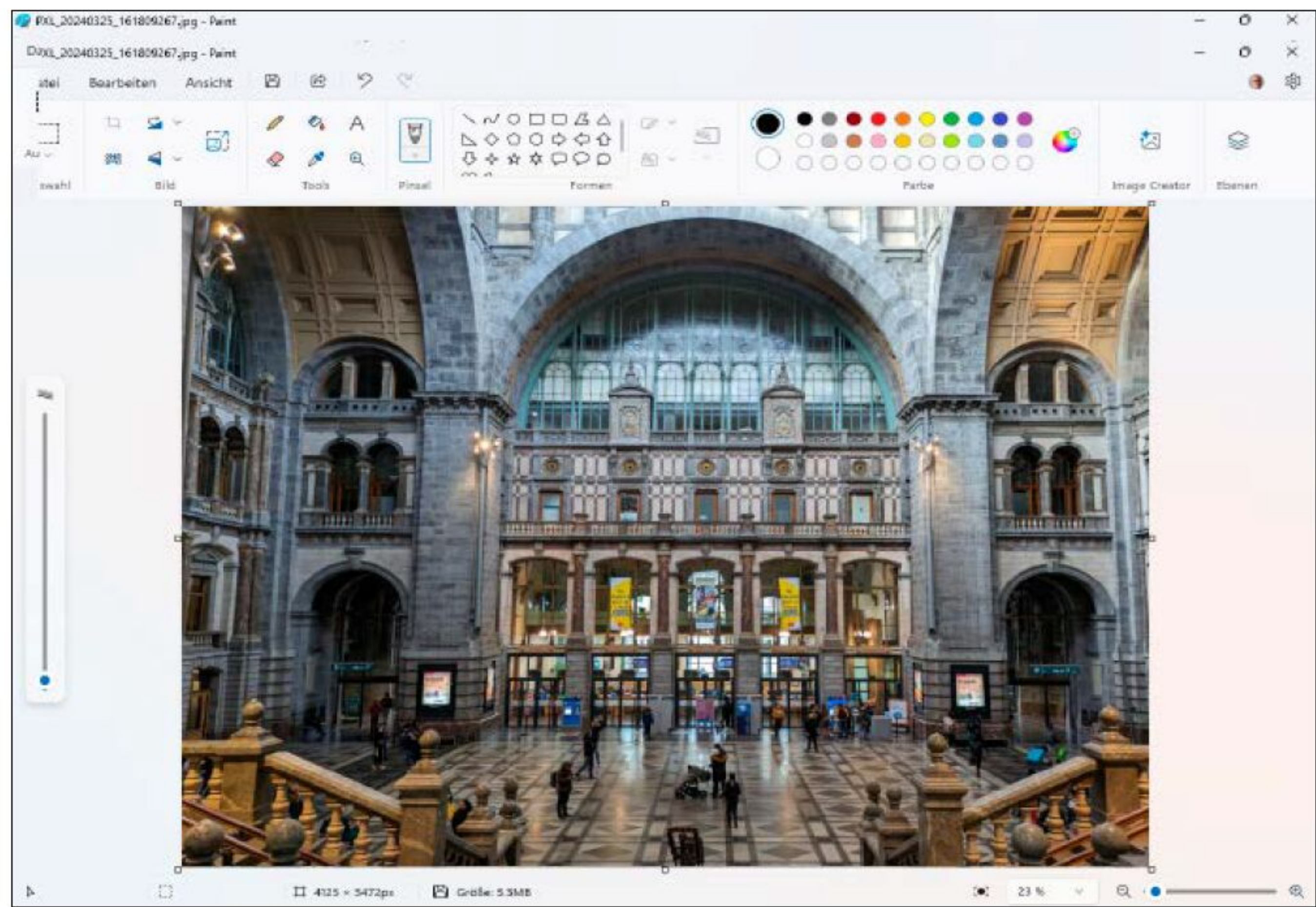
Auf der Website Windows 7 Games finden Sie unter anderem eine Version von Wordpad, die sich unter Windows 11 installieren lässt und die originale Bedienoberfläche bietet.

Cortana, IE und S-Modus

Cortana war ein virtueller Assistent, der Fragen von Windows-Benutzern mithilfe von Bing-Abfragen beantwortete und auf Wunsch auch Terminerinnerungen entgegennahm. Seit 2019 begann Microsoft, die Funktion nach und nach aus Windows herauszunehmen, 2023 kündigte die Firma an, dass Cortana durch den KI-Chatbot Copilot ersetzt werden würde.

Der Internet Explorer (IE) fristet bereits seit Jahren nur noch ein Schattendasein. Die letzten Reste des ehemals am weitesten verbreiteten Browsers der Welt waren nur noch aus Kompatibilitätsgründen in Windows enthalten. Mit Edge entwickelte Microsoft einen komplett neuen Browser auf Basis des Open-Source-Projekts Chromium, auf dem auch **Google Chrome** aufbaut. Edge verfügt noch über einen IE-Modus, um die Kompatibilität zu älteren Browser-Anwendungen zu gewährleisten.

Windows 10 im S-Modus ist eine Betriebssystem-Variante, die als Anwendungen lediglich Apps aus dem Microsoft Store akzeptiert. Microsoft hatte sie entwickelt, da sich die Notebooks mit Googles Chrome OS in den USA sehr gut verkauften. Diese Rechner verfügen lediglich über eine kleine SSD, von der sie das Betriebssystem laden. Die Anwendungen beziehen sie nahezu ausschließlich aus dem Internet. Die Microsoft-Variante dieses Konzepts fand jedoch kaum Käufer. Während der S-Modus zuvor für Windows in der Home-, Pro- und Enterprise-Version verfügbar war, gibt es ihn jetzt nur noch für Windows 11 Home Edition.



Mit Paint bringt Windows eine einfache Bildbearbeitung mit, die jedoch mit vergleichbaren Tools nicht mithalten kann.

Paint 3D, Skype, Onenote

Wenn Sie von Windows 10 auf 11 umgestiegen sind, vermissen Sie eventuell Paint 3D, Skype und Onenote für Windows 10. In Windows 10 waren die drei Programme noch enthalten, aus Windows 11 hat Microsoft sie herausgenommen. Falls Sie jedoch Windows 11 über 10 installieren, bleiben die Tools erhalten. Außerdem sind alle drei nach wie vor über den Microsoft Store erhältlich.

Paint 3D war zusammen mit dem ebenfalls in Windows 10 integrierten 3D-Viewer eine Art Test, ob die Windows-Anwender 3D-Programme annehmen und benutzen würden. Das ist offenbar nicht der Fall, daher wurden die Tools aus Windows gestrichen. Das Ende von **Skype** war lange absehbar. Microsoft konzentriert seine Ressourcen seit Längerem auf die Weiterentwicklung von Teams, das den Funktionsumfang von Skype deutlich übertrifft und stärker auf die Bedürfnisse von Unternehmenskunden ausgerichtet ist.

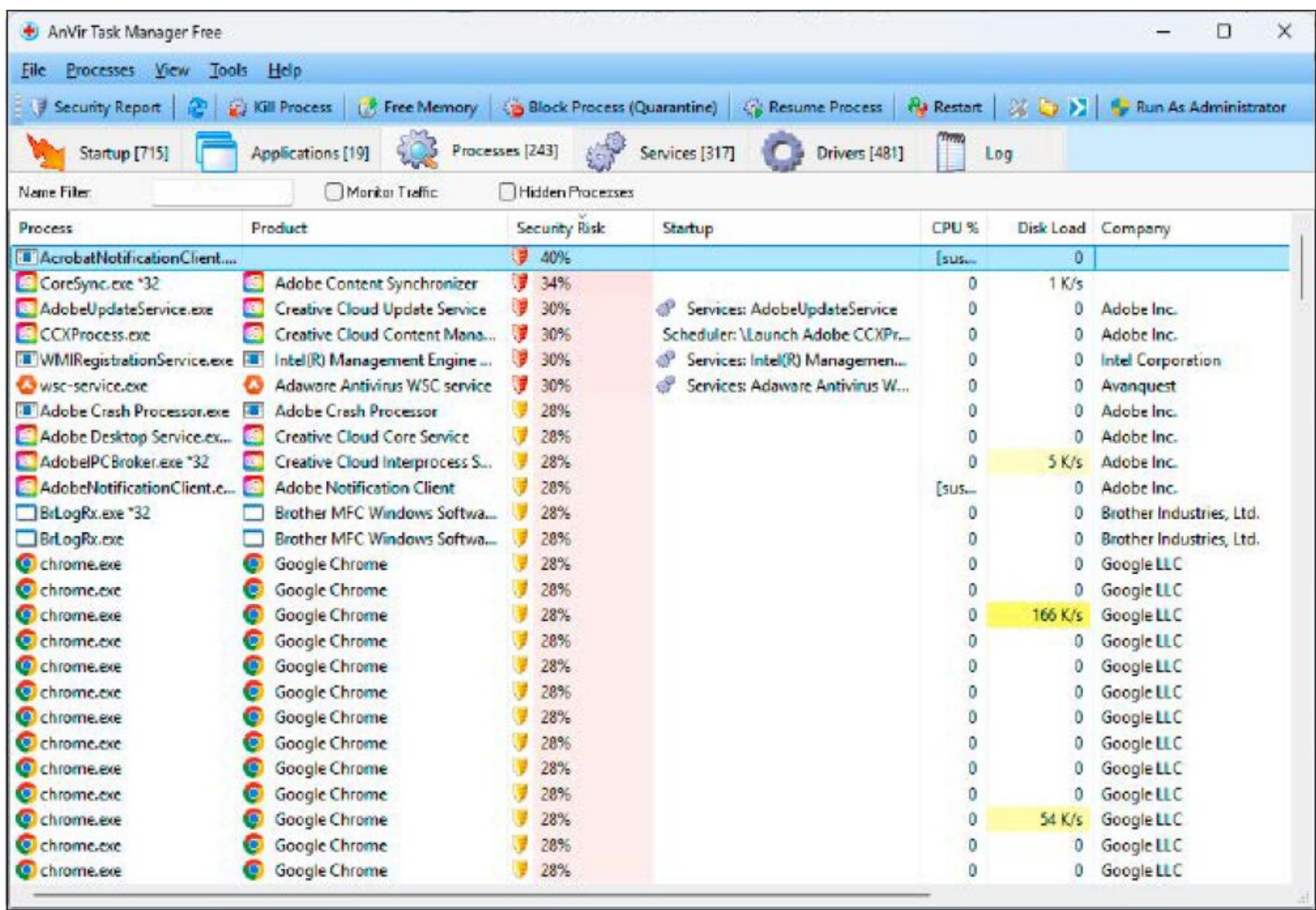
Bei **Onenote** gibt es bereits seit Jahren ein Durcheinander mit konkurrierenden Versionen. Das klassische Onenote ist eine Desktopanwendung und in Microsoft 365 enthalten. Onenote für Windows 10 war hingegen der Versuch, das Programm auch der großen Masse der Windows-Benutzer schmackhaft zu machen. Das Tool bekam eine UWP-Oberfläche (Universal Windows Platform, die Bedienoberfläche der Windows-eigenen Apps) und wurde in Windows 10 integriert. Die parallele Bereitstellung von zwei Onenote-Versionen führte jedoch bei den Anwendern zu Verwirrung, die letztgenannte Variante ist daher in Windows 11 nicht mehr enthalten.

Paint wird intelligent

Die Anwendung Paint wurde früher leicht abschätzig als „Malprogramm“ bezeichnet, so als eigne sich die Bildbearbeitung lediglich für kindliche Malversuche mit der Maus. Tatsächlich waren die Möglichkeiten der Software sehr bescheiden. Doch mittlerweile hat sich das geändert.

So beherrscht das Tool seit einiger Zeit die Arbeit auf mehreren Ebenen, ein Feature, das für eine professionelle Bildbearbeitung unverzichtbar ist. Zum Zweiten hat Microsoft im vergangenen Jahr die KI-Funktionen Cocreator und Image Creator neu in Paint integriert. In beiden Fällen können Sie eine Textbeschreibung eingeben, und Paint erzeugt daraus ein entsprechendes Bild. Cocreator kann neben Text auch Benutzerskizzen verarbeiten und beherrscht mehrere Stilvarianten wie Ölgemälde oder Fotorealismus. Die Funktion arbeitet lokal auf dem PC, setzt allerdings einen Copilot-Plus-Rechner voraus. Image Creator kann lediglich Texte verarbeiten, lässt keine Stilauswahl zu und vollzieht seine Berechnungen in der Cloud. Es handelt sich letztlich also um eine abgespeckte Variante von Cocreator.

Die nächste Stufe bei der Bildbearbeitung ist dann eine Software wie **Paint.net**. Das Programm wurde als Studentenprojekt an der Washington State University mit dem Ziel entwickelt, eine leistungsfähigere Alternative zu Paint auf den Markt zu bringen. Es bietet eine umfangreiche Auswahl an Werkzeugen für die Fotoretusche sowie zahlreiche Effektfiler und beherrscht alle wichtigen Bilddateiformate. Die Bedienung des Tools ist einfach, KI-Funktionen sucht man allerdings vergebens.



Der AnVir Task Manager Free liefert detaillierte Informationen über die laufenden Prozesse und Anwendungen und gibt jeweils Einschätzungen zu ihrer Sicherheit.

Task-Manager und Msconfig.exe

Der **Task-Manager** hat in den vergangenen Jahren gleich zweimal sein Gesicht geändert. Bis hin zu Windows 7 handelte es sich um ein kleines, übersichtliches Tool, das nicht viele Ressourcen benötigte und entsprechend schnell war. Mit Windows 8 kam eine neue Version, die vom Systemkonfigurationsprogramm Msconfig.exe die Übersicht zu den automatisch gestarteten Anwendungen übernommen hatte. Außerdem waren die Anzeigen zu den laufenden Prozessen und der Auslastung von CPU, Arbeitsspeicher, Datenträgern, Netzwerk und Grafikprozessor erheblich detaillierter und aussagekräftiger.

Mit Windows 11 22H2 änderte Microsoft das Design des Task-Managers ein weiteres Mal. Die Tab-Leiste wurde durch eine Seitenleiste im Stil der „Einstellungen“ von Windows ersetzt. Der Funktionsumfang blieb jedoch gleich.

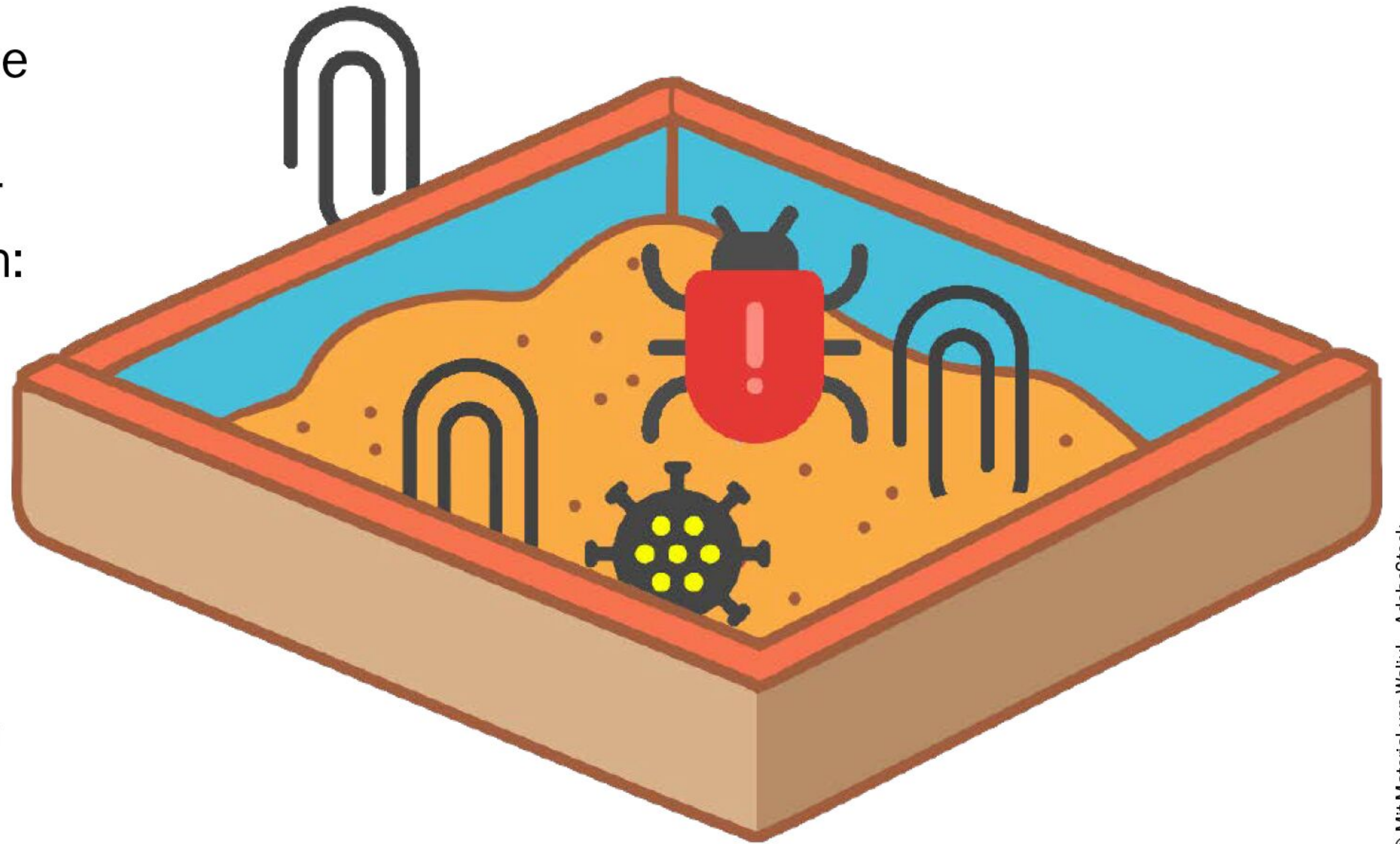
Der aktuelle Task-Manager ist deutlich besser als seine Vorgänger. Für die Version, die bis hin zu Windows 7 im Einsatz war, spricht lediglich der geringere Ressourcenbedarf. Sie können diese Ausgabe über Windows 7 Games (siehe Kasten) herunterladen, installieren und damit den neuen Task-Manager ersetzen, empfehlenswert ist es nicht.

Für den Fall, dass Sie nach einer Alternative suchen, sollten Sie sich das kostenlose Programm **Anvir Task Manager Free** ansehen oder den kostenpflichtigen **Task Manager Deluxe** von Mitec.

Mit der neuen Task-Manager-Version in Windows 8 verschwand der Überblick über die Autostart-Programme aus Msconfig.exe. Sonst gibt es keine Änderungen. ■

Alles sicher öffnen

Öffnen oder löschen? Diese Frage sollten Sie sich bei unbekannten Dateien oder Programmen immer stellen: Ein E-Mail-Anhang scheint verdächtig, könnte aber wichtige Infos enthalten. Eine neue Software klingt interessant, könnte aber Malware einschleusen. Mit speziellen Tools öffnen Sie sie ohne Risiko.



© Mit Material von Wallui - AdobeStock

VON THOMAS RAU

Jede Datei und jedes Programm hinterlassen Spuren in Ihrem System: Sie greifen auf andere Dateien zu, nutzen Windows-Ressourcen, machen Einträge in der Registry und installieren möglicherweise weitere Software. Im besten Fall vermüllen Sie sich damit nur Ihr Windows, wenn die Deinstallations-Routine der Software nicht alle verbundenen Dateien und Registry-Einträge löscht. Im schlimmsten Fall versucht eine Malware Ihr System, oder eine Ransomware verschlüsselt Ihre Dateien.

Wenn Sie neue Programme ausprobieren oder unbekannte Dateien öffnen wollen, sollte das am besten in einer besonders sicheren Umgebung passieren, die vom laufenden System getrennt ist: Genau das bietet eine Sandbox. Wenn Sie ein Programm in einer Sandbox öffnen, funktioniert es wie erwartet, kann aber keine dau-

erhaften Änderungen am System vornehmen oder auf Ressourcen außerhalb seiner Umgebung zugreifen – die Sandbox verhindert das, leitet die Zugriffe um und löscht alle Aktivitäten des Programms und es selbst, wenn Sie sie schließen.

Mit einer Sandbox können Sie daher mit geringerem Risiko neue Software ausprobieren oder Programme aus zweifelhaften Quellen installieren, auf möglicherweise unsicheren Webseiten surfen und Ihr System sauber halten.

Wir stellen Ihnen verschiedene Möglichkeiten vor, wie Sie eine passende Sandbox für Programme und Dateien unter Windows einrichten und nutzen: Das reicht von Windows-Bordmitteln über virtuelle Systeme bis zu Browsern sowie Programmen mit eigener Sandbox-Funktion. Besonders ausführlich beschreiben wir die Software **Sandboxie-Plus** (auf DVD) – für die meisten Anwender die einfachste und praktischste Lösung.

Sandbox für den Browser: Bordmittel von Chrome & Co.

Wahrscheinlich nutzen Sie schon eine Sandbox: Denn aktuelle Browser wie **Chrome** und **Firefox** setzen diese Schutztechnik ein. Sie verlassen sich dabei auf Sicherheitsmechanismen von Windows: Das hat den Vorteil, dass sie einen hohen Schutz

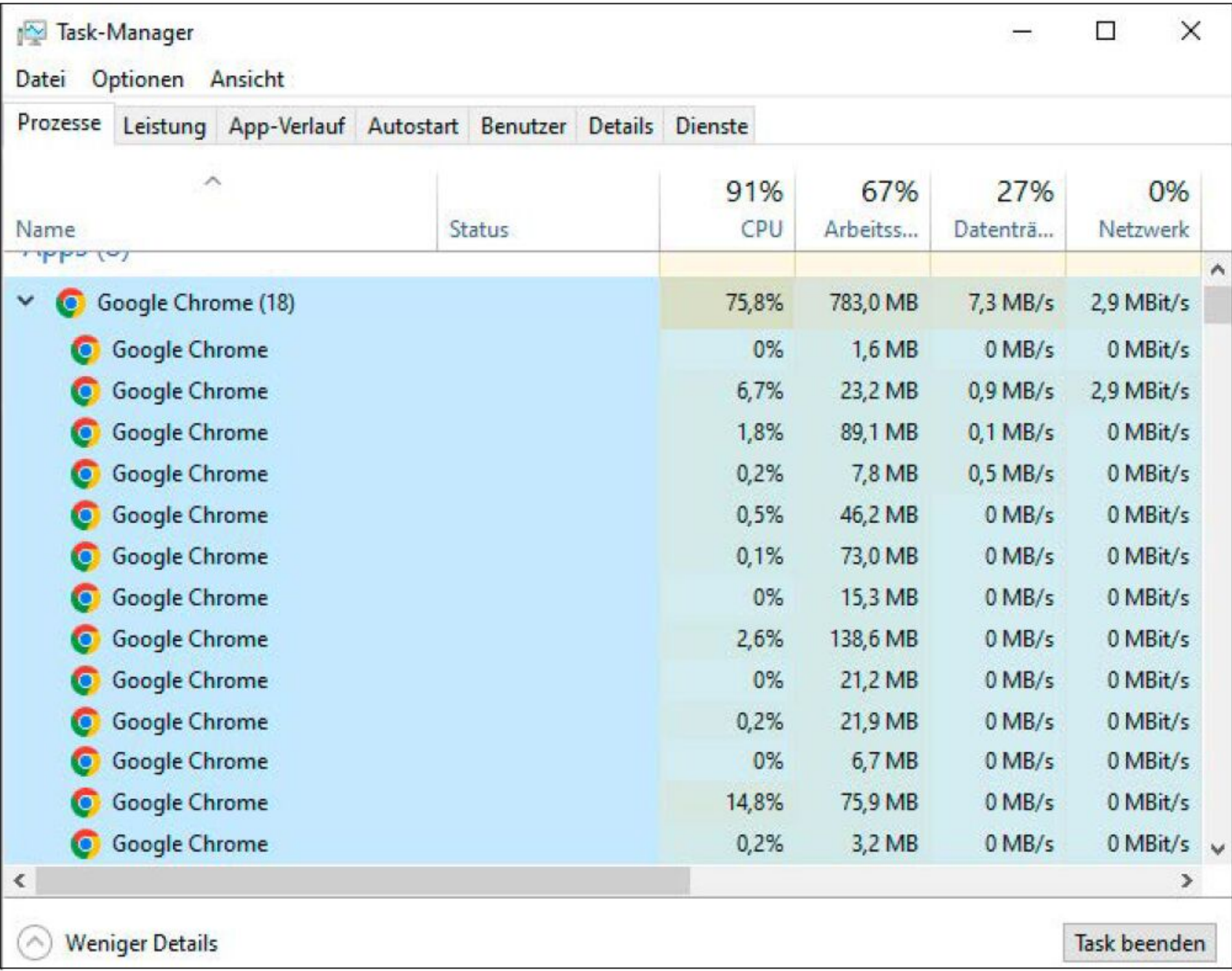
gewährleisten können, ohne viele Ressourcen in Anspruch nehmen zu müssen, was zum Beispiel dazu führen könnte, dass sich Webseiten nur langsam öffnen.

Jeder Browser-Reiter wird dafür in einer eigenen Sandbox geöffnet. So verhindern Chrome & Co., dass Programme auf einer Webseite automatisch heruntergeladen werden oder schädliche Scripts ablaufen. Zudem schützt dieses Verfahren vor Angriffen, die über eine Webseite ausgeführt werden, ohne dass ein Antivirenprogramm Alarm schlägt (Zero-Day-Exploits).

Jeder Reiter des Browsers läuft als isolierter Prozess und hat keinen Zugriff auf andere Reiter und das System. Zudem startet er mit sehr reduzierten Rechten – daher müssen Sie zum Beispiel üblicherweise den Zugriff einer Webseite auf die Rechner-Kamera freigeben. Außerdem soll die Trennung der einzelnen Reiter dazu führen, dass der Absturz einer Webseite nicht den ganzen Browser lahmlegt, sondern nur den entsprechenden Reiter.

Wie und ob die Browser-Sandbox arbeitet, lässt sich im Task-Manager von Windows beobachten: Unter „Prozesse“ sehen Sie, dass unter dem Eintrag „Google Chrome“ zahlreiche weitere Prozesse laufen – das sind die getrennten Sandboxes der einzelnen Reiter. Weitere Details erfahren Sie,

„Mit Sandboxie-Plus lassen sich riskante Tools gefahrlos ausprobieren.“



The screenshot shows the Windows Task Manager window with the 'Prozesse' tab selected. It lists 18 Google Chrome processes. The columns shown are Name, Status, CPU usage (91%), Arbeitsspeicher (67%), Datentransfer (27%), and Netzwerk (0%). The first process is highlighted in blue.

Name	Status	91% CPU	67% Arbeitsspeicher	27% Datentransfer	0% Netzwerk
Google Chrome (18)		75,8%	783,0 MB	7,3 MB/s	2,9 MBit/s
Google Chrome		0%	1,6 MB	0 MB/s	0 MBit/s
Google Chrome		6,7%	23,2 MB	0,9 MB/s	2,9 MBit/s
Google Chrome		1,8%	89,1 MB	0,1 MB/s	0 MBit/s
Google Chrome		0,2%	7,8 MB	0,5 MB/s	0 MBit/s
Google Chrome		0,5%	46,2 MB	0 MB/s	0 MBit/s
Google Chrome		0,1%	73,0 MB	0 MB/s	0 MBit/s
Google Chrome		0%	15,3 MB	0 MB/s	0 MBit/s
Google Chrome		2,6%	138,6 MB	0 MB/s	0 MBit/s
Google Chrome		0%	21,2 MB	0 MB/s	0 MBit/s
Google Chrome		0,2%	21,9 MB	0 MB/s	0 MBit/s
Google Chrome		0%	6,7 MB	0 MB/s	0 MBit/s
Google Chrome		14,8%	75,9 MB	0 MB/s	0 MBit/s
Google Chrome		0,2%	3,2 MB	0 MB/s	0 MBit/s

Chrome öffnet wie die meisten Browser jeden Reiter in einem eigenen isolierten Prozess, zu sehen im Task-Manager. Alle Webseiten sind gegeneinander abgesichert.

wenn Sie in die Adresszeile des Browsers den Befehl `chrome://sandbox/` eingeben: Die Reiter heißen hier „Renderer“ – das ist die Funktion, die Webseiten darstellt. Jeder sollte außerdem in der Spalte „Sandbox“ auftauchen und in der nächsten Spalte mit dem Vermerk „Lockdown“. Das bedeutet ebenso wie der Eintrag „Untrusted“ rechts davon, dass dieser Prozess sehr wenige Zugriffsrechte auf das System hat. Trotzdem sollten Sie unbedingt stets den Browser aktualisieren, da Hacker häufig versuchen, über andere Sicherheitslücken die Sandbox auszuhebeln, um Scripts und Programmen auf einer Webseite mehr Zugriffsrechte zu verschaffen.

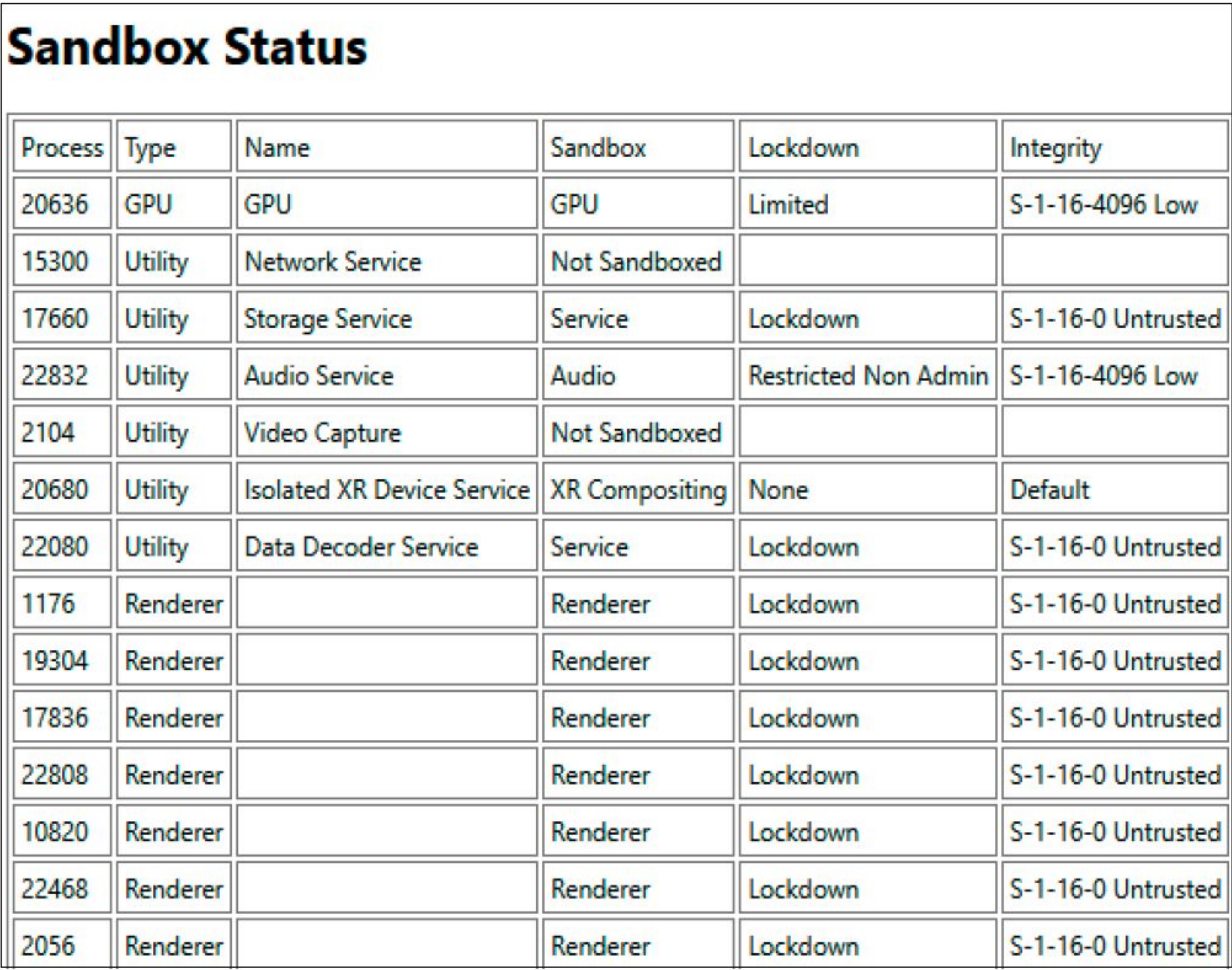
Diese Programme haben eine eingebaute Sandbox

Auch Windows setzt für bestimmte Programme eine Sandbox ein: Apps aus dem Microsoft Store – die sogenannten UWP-Apps (Universal Windows Platform) – laufen in einem isolierten Prozess mit reduzierten Rechten. Dadurch lassen sie sich rückstandslos deinstallieren. In vielen Fällen müssen Sie ihnen außerdem den Zugriff auf Dateien oder auf Hardware wie Kamera oder Mikrofon erlauben. Allerdings nutzen nur wenige Anwender UWP-Apps. Die häufiger installierten Standardprogramme – die sogenannten Desktop-Apps – laufen ohne Sandbox und Rechtebeschränkung. Außerdem geben Sie auch vielen UWP-Apps bereits bei der Installation bestimmte Rechte. Welche das sind, prüfen Sie vor der Installation auf der App-Seite im

Microsoft Store unter dem Eintrag „Diese App kann“ sowie nach der Installation in den Windows-Einstellungen unter „Datenschutz → App-Berechtigungen“. Dort können Sie ihnen Rechte wieder entziehen – was allerdings häufig zur Folge hat, dass die App nicht mehr korrekt funktioniert. Windows 11 unterstützt ab Version 24H2 auch eine Sandbox-Funktion für normale Programme – die Win32-App Isolation. Die müssen die Hersteller aber in ihre Software einbauen, damit der Schutz wirkt. Für PDF-Dokumente bietet **Acrobat Reader** eine sichere Sandbox-Funktion: Wenn Sie ein PDF als Anhang einer E-Mail oder aus einer unsicheren Quelle erhalten, können Sie so verhindern, dass im Dokument enthaltener Code ausgeführt wird oder Sie beim Klick auf einen Link im PDF auf eine manipulierte Webseite gelangen. Um die PDF-Sandbox zu nutzen, gehen Sie im Reader-Menü auf „Einstellungen → Sicherheit (erweitert)“ und aktivieren die Option „Geschützten Modus beim Start aktivieren“. Zusätzlichen Schutz bietet die „Geschützte Ansicht“ darunter, bei der Sie wählen können, ob sie für alle PDFs oder nur für solche aus unsicheren Quellen gelten soll. Damit öffnet der Reader das PDF im Lesemodus, es lässt sich dann nicht ausfüllen und meist auch nicht speichern und drucken.

So nutzen Sie das kostenlose Spezial-Tool Sandboxie-Plus

Das kleine Open-Source-Tool Sandboxie-Plus (<https://sandboxie-plus.com>) eignet

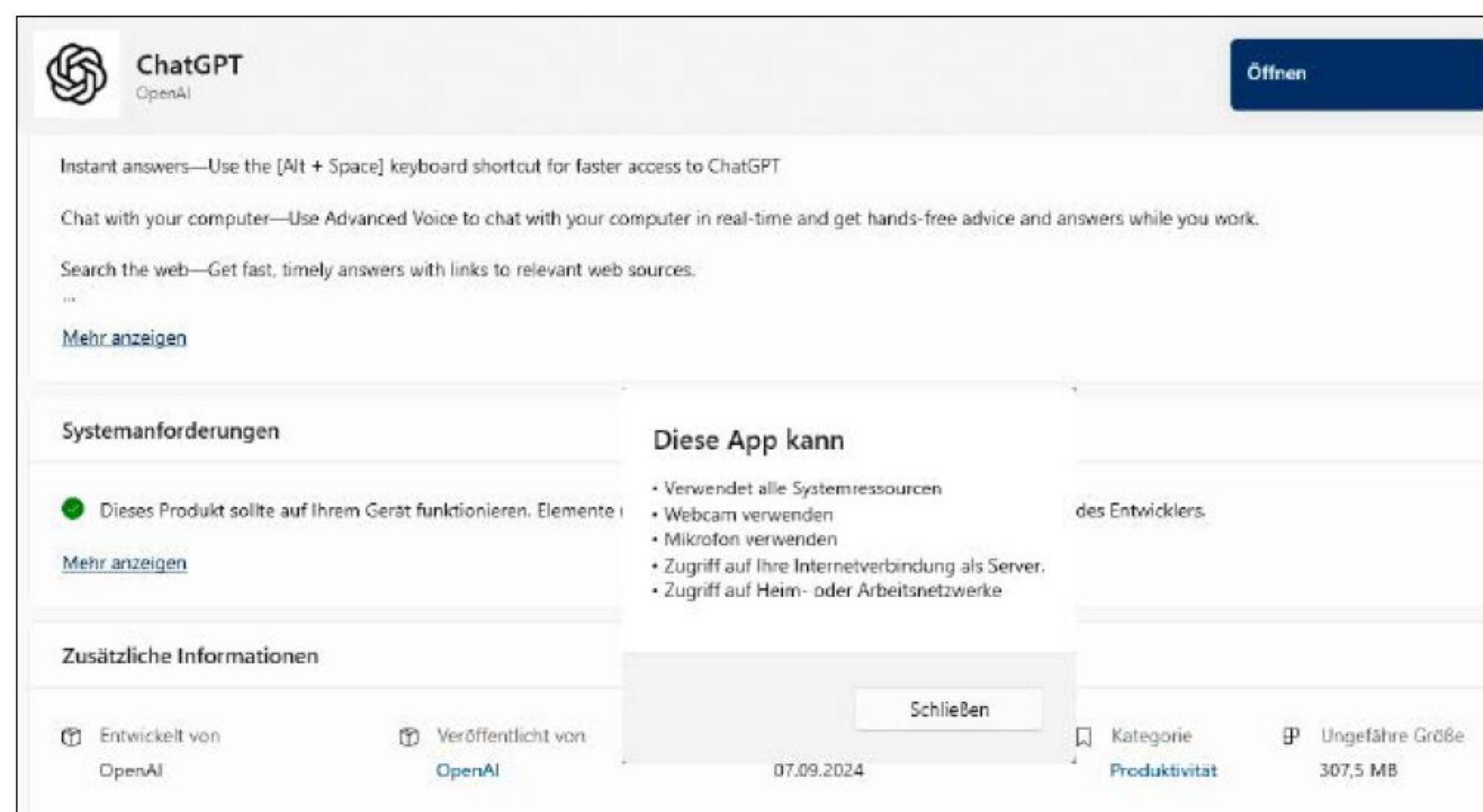


The screenshot shows the 'Sandbox Status' window. It contains a table with columns: Process, Type, Name, Sandbox, Lockdown, and Integrity. The table lists various system processes and their sandboxing status.

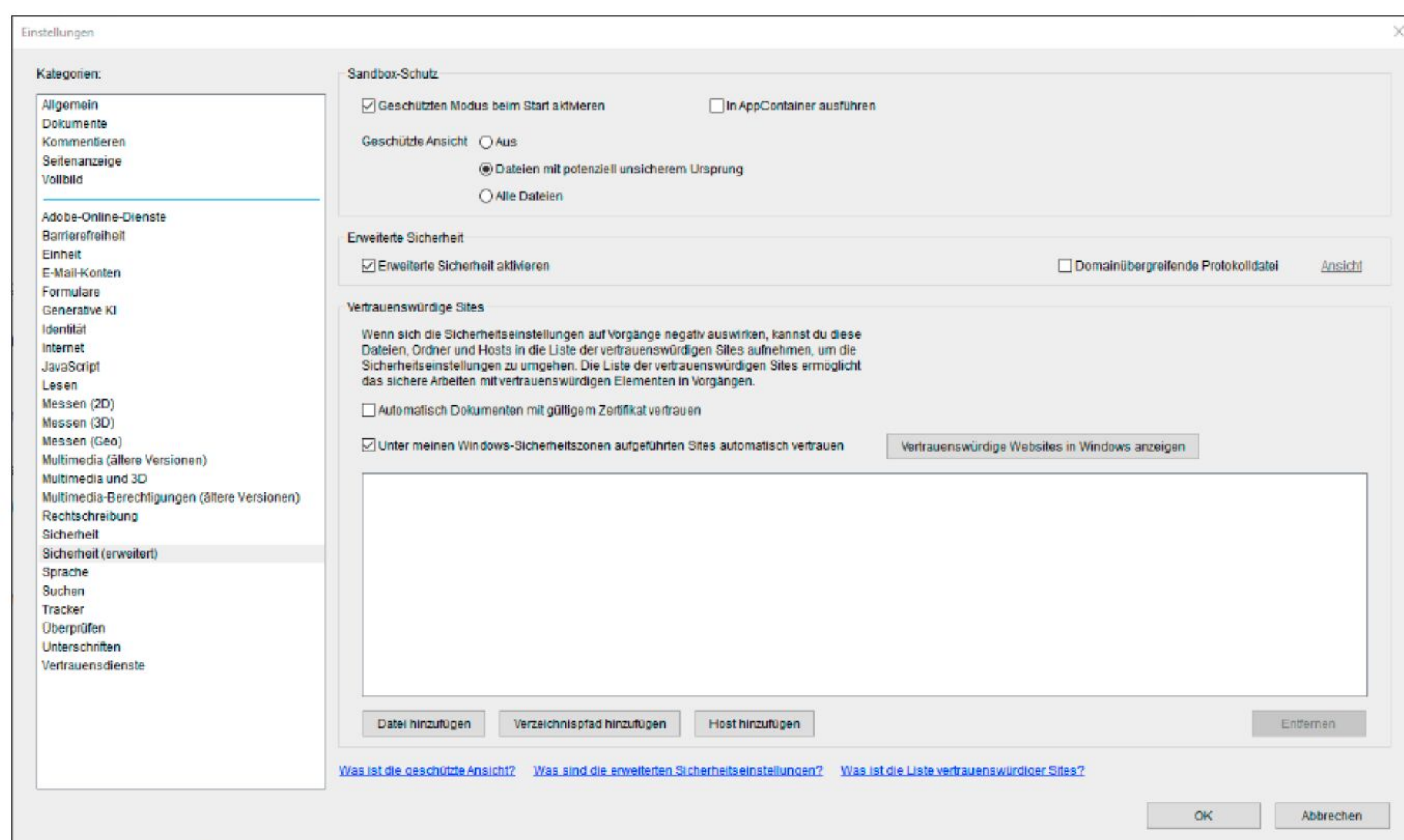
Process	Type	Name	Sandbox	Lockdown	Integrity
20636	GPU	GPU	GPU	Limited	S-1-16-4096 Low
15300	Utility	Network Service	Not Sandboxed		
17660	Utility	Storage Service	Service	Lockdown	S-1-16-0 Untrusted
22832	Utility	Audio Service	Audio	Restricted Non Admin	S-1-16-4096 Low
2104	Utility	Video Capture	Not Sandboxed		
20680	Utility	Isolated XR Device Service	XR Compositing	None	Default
22080	Utility	Data Decoder Service	Service	Lockdown	S-1-16-0 Untrusted
1176	Renderer		Renderer	Lockdown	S-1-16-0 Untrusted
19304	Renderer		Renderer	Lockdown	S-1-16-0 Untrusted
17836	Renderer		Renderer	Lockdown	S-1-16-0 Untrusted
22808	Renderer		Renderer	Lockdown	S-1-16-0 Untrusted
10820	Renderer		Renderer	Lockdown	S-1-16-0 Untrusted
22468	Renderer		Renderer	Lockdown	S-1-16-0 Untrusted
2056	Renderer		Renderer	Lockdown	S-1-16-0 Untrusted

Einen detaillierten Überblick über die Sandbox-Funktion von Chrome erhalten Sie nach der Eingabe des passenden Befehls in die Adresszeile.

sich optimal, um alle verdächtigen Dateien und Programme isoliert auszuführen. Sie installieren es wie gewohnt unter Windows und können dann die gewünschten Inhalte direkt in einem Sandbox-Container starten. Der komplette Funktionsumfang von Sandboxie-Plus kostet 40 Euro pro Jahr: Sie können den Programmierer direkt per Paypal bezahlen oder Sie kaufen sich auf der Webseite ein Supporter-Zertifikat. Für den Einsatz am Heimrechner genügen aber die kostenlosen Grundfunktionen, die wir im Folgenden vorstellen. Sandboxie-Plus gibt es in Versionen für das Standard-Windows und für ARM-Windows. Außerdem lässt sich das Tool auch als mobile App auf einem USB-Stick installieren. Nach der Installation begrüßt Sie ein Einrichtungsassistent: Dort wählen Sie zunächst für die kostenlosen Funktionen die Option „Persönlich, für nicht-kommerziellen Gebrauch“. Im nächsten Fenster können Sie sich ein sogenanntes Evaluationszertifikat besorgen, indem Sie auf den roten, unterstrichenen Text klicken: Damit lässt sich die Software zehn Tage mit allen Funktionen testen. Ansonsten klicken Sie auf „Weiter“. Bei der Nutzeroberfläche können Sie zwischen einem Experten- und einem Anfängermodus wählen sowie einen hellen oder dunklen Modus für die Darstellung. Am besten übernehmen Sie die vorgegebenen Einstellungen und klicken erneut auf „Weiter“. Die Einrichtung der Software beenden Sie im letzten Fenster mit einem Klick auf „Abschließen“. Auch im folgenden Fenster für die „Globalen Einstel-



Programme aus dem Microsoft Store laufen in einer isolierten Umgebung: Allerdings fordern sie oft schon bei der Installation zahlreiche Rechte, die diesen Schutz durchlöchern.



Einige Programme wie hier der Acrobat Reader bieten erweiterte Sicherheitseinstellungen, mit denen Sie Dateien in einer geschützten Umgebung öffnen, ohne dass diese Zugriff aufs System haben.

lungen“ müssen Sie nichts anpassen und klicken auf „OK“.

Risikante Programme in Sandboxie-Plus ausführen und testen

Sandboxie-Plus startet mit einer zweigeteilten Oberfläche: Oben sehen Sie den Eintrag für eine „DefaultBox“. In dieser können Sie verdächtige Programme starten. Im unteren Fenster protokolliert das Tool alle Aktionen und Einstellungen. Die Benutzeroberfläche lässt sich auch aufrufen, indem Sie mit der rechten Maustaste auf das Toolsymbol im Systray klicken und „Anzeigen / Verbergen“ auswählen. Um eine Software sicher in einer Sandbox zu starten, klicken Sie auf „Sandbox → In Sandbox ausführen“. Bestätigen Sie die Einstellungen im nächsten Fenster mit „OK“. Anschließend erscheint ein weiteres Fenster: Dort geben Sie den Namen der Software ein, die Sandboxie-Plus starten soll, und bestätigen mit „OK“. Kennen Sie den genauen Namen nicht oder findet das Tool

kein Programm, das zu Ihrer Eingabe passt, können Sie über „Suchen“ die Software direkt mit dem Explorer aufrufen.

Diese Startverfahren empfehlen sich bei Programmen, die Sie installiert haben, aber ein weiteres Mal in der sicheren Umgebung starten wollen – zum Beispiel bei Ihrem Webbrowser: Wenn Sie ihn in der Sandbox erneut aufrufen, können Sie damit ohne Risiko verdächtige Webseiten besuchen. Das Programm startet anschließend: Die entsprechende EXE-Datei erscheint im oberen Fenster von Sandboxie-Plus. An zwei Merkmalen erkennen Sie, dass eine Software in der Sandbox läuft: Ihr Name im Programmfenster beginnt und endet mit einem Rautensymbol – wenn Sie zum Beispiel den Chrome-Browser in der Sandbox öffnen und die Maus auf sein Symbol in der Taskleiste ziehen, steht dort [#] Neuer Tab – Google Chrome [#]. Bewegen Sie die Maus an den oberen Rand des Programmfensters, erscheint ein gelber Rahmen. Außerdem gibt es in Sandboxie-Plus unter

„Sandbox → Ist das Fenster in einer Sandbox?“ einen sogenannten Fensterfinder: Klicken Sie dort auf den Kreis im kleinen Programmfenster links, halten Sie die linke Maustaste gedrückt und lassen Sie ihn im Fenster des Programms los, dessen Status Sie prüfen wollen: Im Fensterfinder erscheint dann die Antwort auf die Frage.

Außerdem trägt sich Sandboxie-Plus ins Kontextmenü des Windows-Explorers ein: Sie können dann das gewünschte Programm mit einem Rechtsklick und dem Befehl „Starte Sandgeboxt“ aufrufen. So lässt sich zum Beispiel Software, die Sie gerade heruntergeladen haben, in der Sandbox installieren, indem Sie die entsprechende EXE- oder Installations-Datei mit Sandboxie-Plus starten.

Es ist empfehlenswert, jedes Programm und jede Datei in einer eigenen Sandbox auszuführen: Beim Start über Sandboxie-Plus oder das Kontextmenü wählen Sie dafür im nächsten Fenster den Eintrag „In einer neuen Sandbox ausführen“ und anschließend „Standard Sandbox“. Außerdem können Sie hier jeder Sandbox einen aussagekräftigen Namen geben.

Wichtige Programme lassen sich besonders schnell in Sandboxie-Plus starten, zum Beispiel Ihr Browser, das E-Mail-Programm oder der Windows-Explorer: Klicken Sie rechts oben im Tool-Fenster auf eine vorhandene Sandbox. Anschließend wählen Sie „Starten → Standard-Programme“ und dort die gewünschte Software aus.

Verdächtige Dateien in Sandboxie-Plus öffnen und prüfen

Wie Programme, lassen sich auch einzelne Dateien in einer isolierten Sandbox aufrufen. Sandboxie-Plus startet dazu das Standardprogramm für diese Datei – zum Beispiel Word bei einer DOCX-Datei.

Stürzt das Programm dabei ab, ändern Sie eine Einstellung in Sandboxie-Plus: Öffnen Sie die Datei wie beschrieben in einer neuen Sandbox. Im Fenster, in dem Sie „Standard Sandbox“ als Boxtyp auswählen, setzen Sie einen Haken vor die Option „Konfiguriere erweiterte Optionen“ rechts unten. Nach einem Klick auf „Weiter“ wählen Sie bei „Virtualisierungsschema“ die „Version 1“, klicken mehrmals auf „Weiter“ und beenden mit „Abschließen“.

Wichtig: Ein Programm, das Sie in der Sandbox starten, kann Dateien außerhalb der Sandbox nur lesen und nicht verändern.

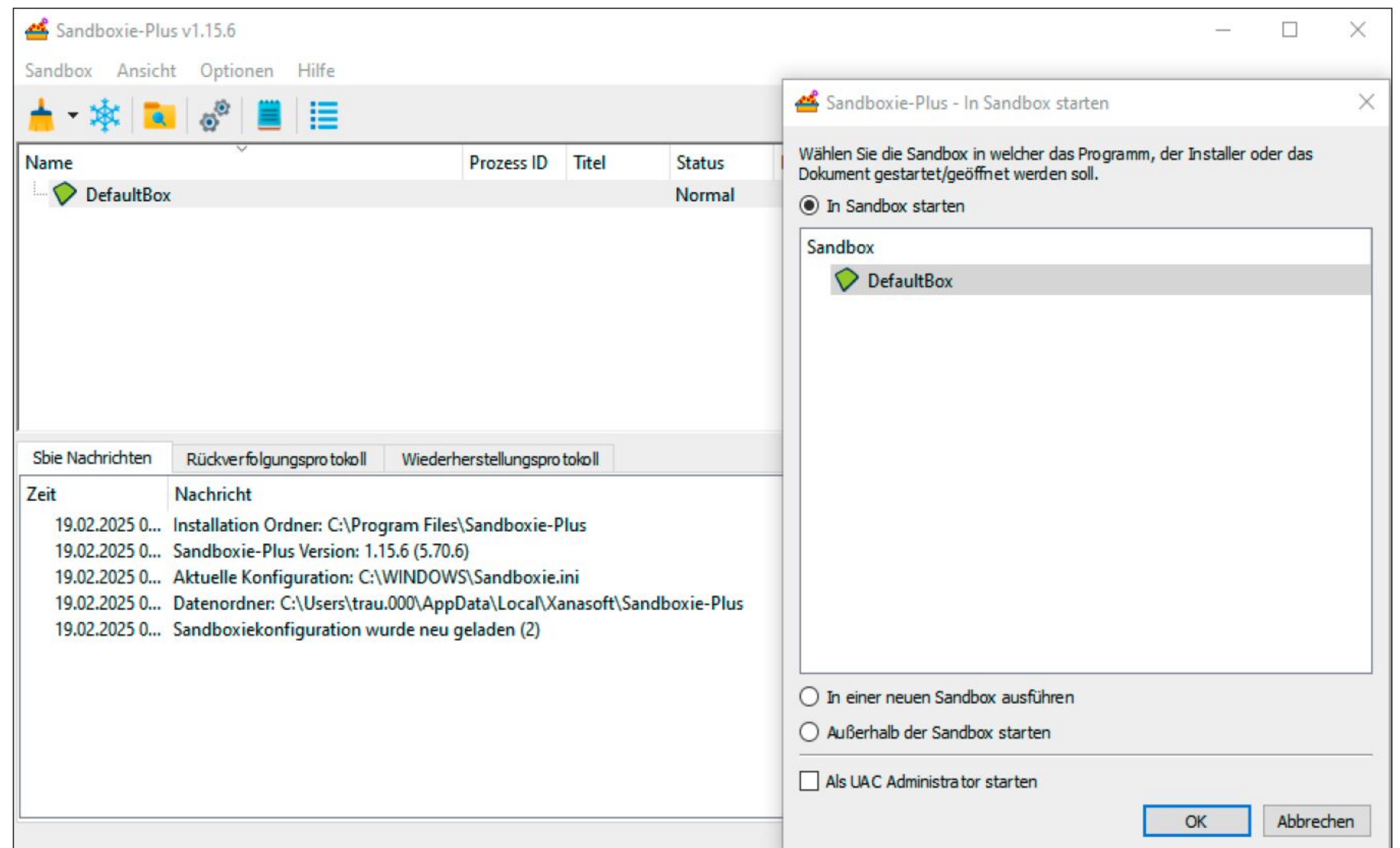
Öffnen Sie eine Datei innerhalb der sandboxten Software, lässt sie sich ändern, was aber keine Auswirkungen auf die Originaldatei hat: Wenn Sie zum Beispiel Outlook in der Sandbox starten und dort eine E-Mail löschen, ist diese nach wie vor vorhanden, wenn Sie Outlook normal öffnen. Auf diese Weise lassen sich E-Mails mit verdächtigen Anhängen untersuchen: Sie öffnen Ihr Mailprogramm in der Sandbox und öffnen den Anhang. Erscheint er Ihnen verdächtig oder kommt er von einem unerwarteten Absender, löschen Sie die Sandbox und anschließend diese Mail im normalen E-Mail-Programm, ohne sie zu öffnen oder den Anhang anzuschauen.

Sandboxie-Plus isoliert Programme und Dateien, indem es für sie eigene Verzeichnisse erstellt: Diese liegen im Programmverzeichnis „C:\Sandbox\Benutzername“, wo es für jede Sandbox einen eigenen Ordner gibt. Dort hinterlegt das Tool auch Änderungen in der Registry, die das isolierte Programm vornimmt. Auf diese Weise bleiben keine Spuren davon im System, wenn Sie die entsprechende Sandbox löschen. Das erledigen Sie, indem Sie im oberen Fenster von Sandboxie-Plus einen Rechtsklick auf die gewünschte Sandbox ausführen und aus dem Kontextmenü „Sandbox entfernen“ wählen. Wollen Sie die Sandbox behalten, aber die dort laufenden Programme beenden, wählen Sie im Kontextmenü den Befehl „Alle Prozesse beenden“.

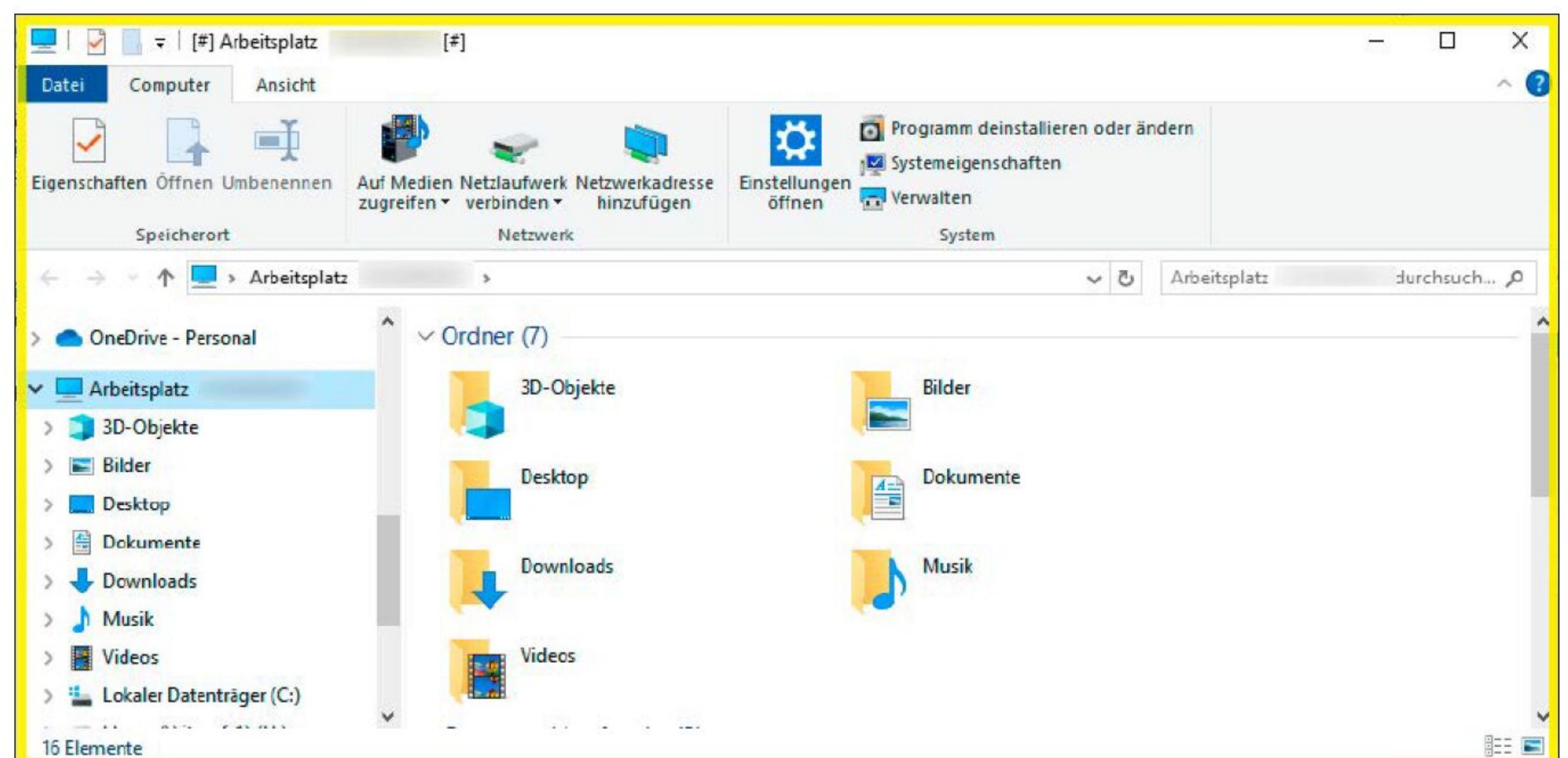
Alternative: Virtuellen PC statt Sandbox nutzen

Um riskante Programme zu starten oder verdächtige Dateien zu öffnen, eignet sich auch ein virtueller PC (VPC). Windows bringt dafür die **Windows Sandbox** mit. Sie ist ein VPC auf Basis der Virtualisierungssoftware Hyper-V von Microsoft, aber nur in Windows Pro enthalten.

Zudem müssen Sie sie zunächst installieren: Das machen Sie über die Systemsteuerung und „Windows-Features aktivieren oder deaktivieren“. Markieren Sie dort den Eintrag „Windows Sandbox“ und starten Sie den Rechner neu. Anschließend finden Sie das Programm als „Windows Sandbox“ in der Auswahl der installierten Apps. Nach dem Start öffnet sich ein weiterer Windows-Desktop als Benutzeroberfläche des virtuellen PCs: Diesen bedienen Sie wie Ihr normales System – so lassen sich Programme in der Windows Sandbox installieren



Mit Sandboxie-Plus lassen sich Programme in einer isolierten Umgebung starten: Sie können dann nicht aufs System zugreifen und lassen sich rückstandslos entfernen.

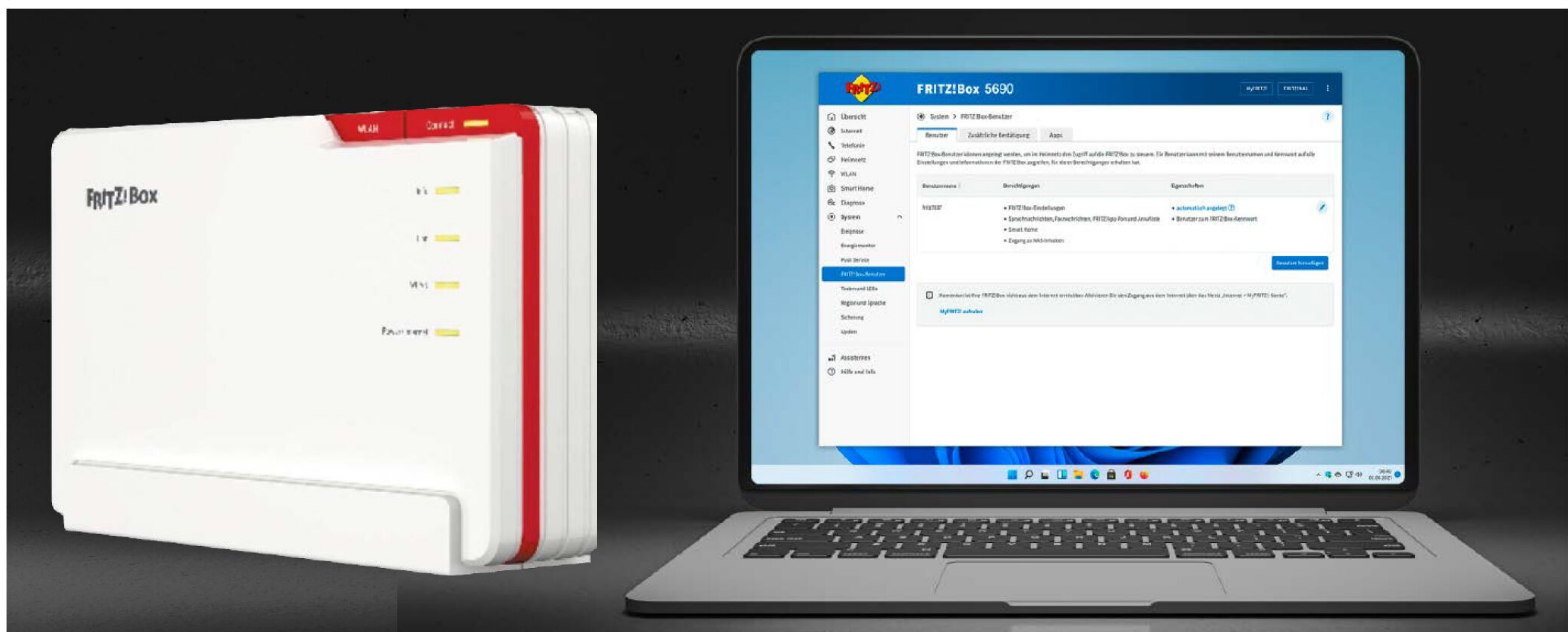


Ob eine Software wirklich in der Sandbox arbeitet, erkennen Sie bei Sandboxie-Plus am gelben Rahmen ums Programmfenster und an den Hashtags vor und hinter dem Programmnamen ganz oben.

und ausprobieren. Verdächtige Dateien können Sie per Copy & Paste vom Hauptsystem ins virtuelle Windows übertragen. Seit dem Windows-11-Update 22H2 unterstützt der VPC auch einen Neustart, bei dem seine Daten und Anwendungen erhalten bleiben. Das gilt aber nur, wenn Sie ausschließlich die Sandbox neu starten: Wenn Sie das VPC-Fenster schließen oder das Hauptsystem neu starten, werden die Inhalte der Sandbox gelöscht.

Falls Sie Windows Home nutzen, können Sie für einen VPC kostenlose Virtualisierungsprogramme wie **Virtualbox** (auf DVD, www.virtualbox.org) einsetzen. Allerdings braucht der virtuelle Rechner ein Betriebssystem – soll es Windows sein, benötigen Sie dafür eine zusätzliche Lizenz. Ein VPC ist gegenüber dem Haupt-System zwar

weitgehend abgeschottet und eine sichere Testumgebung. Im Vergleich zu Sandboxie-Plus ist er aber überdimensioniert, wenn Sie nur gelegentlich unbekannte Programme ausprobieren oder verdächtige E-Mail-Anhänge öffnen möchten: Sie müssen im VPC ein eigenes Betriebssystem installieren, das entsprechend hohe Anforderungen an die Hardware Ihres Rechners stellt. Das gilt zum einen für die CPU-Leistung, aber vor allem für den Arbeitsspeicher: Mindestens 4 GB RAM sollten Sie ausschließlich für das virtuelle System bereitstellen, mehr Arbeitsspeicher erhöht den Bedienkomfort des VPC erheblich. Auch für einen raschen Datei-Check ist es nicht optimal: Den VPC müssen Sie wie ein normales System starten und warten, bis das virtuelle Windows einsatzbereit ist. ■



© Mit Material von Who is Danny – AdobeStock, AVM

Sicher zugreifen auf Fritzbox & Co.

Bei einem WLAN-Router wie der Fritzbox lässt sich viel einstellen, um Tempo und Sicherheit im Heimnetz zu verbessern. Das Wichtigste ist aber, dass nur Sie das dürfen: Denn wenn der Zugang zum Router nicht ausreichend geschützt ist, können Hacker die Kontrolle übernehmen. Das verhindern Sie mit diesen Tipps.

VON MICHAEL SEEMANN

Wer Ordnung im Heimnetz schaffen und halten will, sollte regelmäßig das Webmenü seines Internetrouters aufrufen. Wenn aber auch andere Personen darauf Zugriff haben, entsteht meist Chaos im Netzwerk: Denn im Routermenü lassen sich beliebige Änderungen vornehmen und damit bestimmte Einstellungen gezielt manipulieren. Das reicht vom Versuch des Nachwuchses, die eingeschränkte Internetzeit zu erweitern, indem das entsprechende Profil in der

Fritzbox-Kindersicherung angepasst wird, bis zu schwerwiegenden Angriffen, bei denen Hacker zum Beispiel den DNS-Server im Router ändern, um Ihren Internetzugriff auf Phishing-Seiten umzuleiten.

Daher sollten Sie als Grundlage für die Sicherheit im Heimnetz unbedingt dafür sorgen, den Zugang zum Routermenü ausreichend zu schützen – mit unseren Tipps geht das leichter als gedacht.

Was Sie sofort tun sollten: Ändern Sie das voreingestellte Kennwort

Bei fast allen aktuellen Heimnetzroutern ist der Zugang zum Webmenü ab Werk mit einem individuellen Passwort gesichert: Bei einer Fritzbox zum Beispiel steht das Kennwort in den mitgelieferten Unterlagen und auf einem Schild auf der Unterseite des Routers. Ändern Sie deshalb sofort das voreingestellte Passwort – denn ansonsten kann jeder, der am Router vorbeikommt, sich das Kennwort notieren und damit das Webmenü aufrufen.

Bei einer Fritzbox ändern Sie das Werkswort, indem Sie im Menü in der rechten oberen Ecke auf die drei Punkte klicken und dann die Option „Kennwort ändern“ wählen. Geben Sie ein neues, starkes Kennwort ein, notieren Sie es auf einem Zettel oder in einer Passwortsafe und bestätigen Sie mit „Übernehmen“.

Menü nur über eine verschlüsselte Verbindung aufrufen

Als nächsten Schritt zum besseren Zugangsschutz sollten Sie die Verbindung sichern, über die Sie das Menü aufrufen. Nutzen Sie dafür auch im lokalen Netzwerk das SSL-verschlüsselte HTTPS-Protokoll statt einer HTTP-Verbindung, die alle Daten unverschlüsselt zwischen der Fritzbox und dem Client, über dessen Browser Sie ins Routermenü gelangen, überträgt. Sie melden sich dann über die Webadresse <https://192.168.178.1> am Webmenü Ihrer Fritzbox an, nicht mehr über <http://fritz.box> oder über <http://192.168.178.1>. Eventuell

„Schützen Sie das Fritzbox-Menü besonders gut, um die Kontrolle über Ihr Heimnetz zu behalten.“

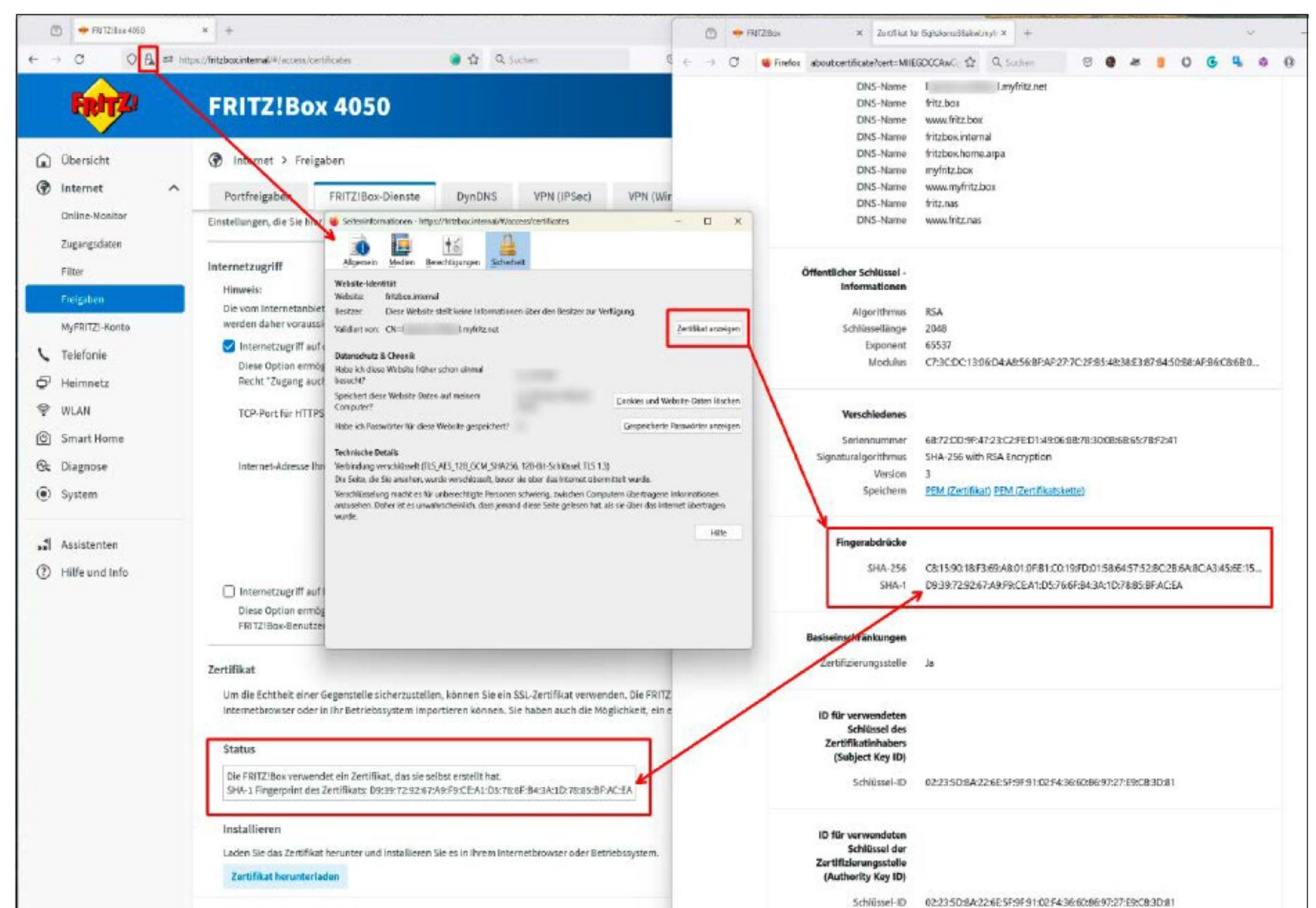
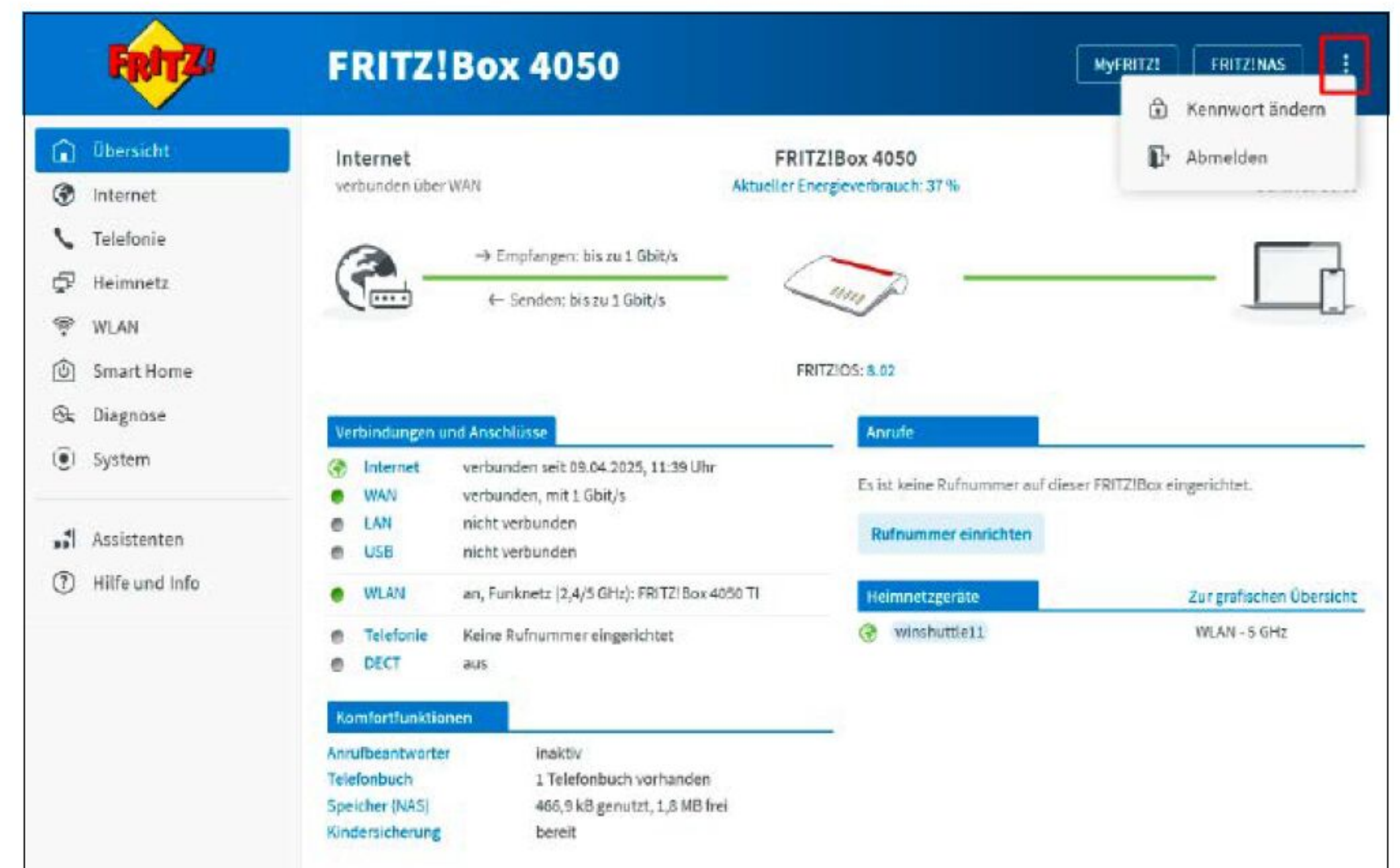
erscheint nun ein Warnhinweis des Browsers, der ein ungültiges Sicherheitszertifikat moniert. Das können Sie übergehen, indem Sie im Firefox-Browser auf die Schaltflächen „Erweitert → Risiko akzeptieren und fortfahren“ klicken. Der Chrome-Browser hingegen warnt Sie mit der Anzeige „Dies ist keine sichere Webseite“. Gehen Sie hier auf die Links „Erweitert → Weiter zu 192.168.178.1(unsicher)“. Damit haben Sie im Browser eine Ausnahme für das von Fritz (früher AVM) erstellte Sicherheitszertifikat hinzugefügt, und die Warnmeldung erscheint beim nächsten HTTPS-Zugriff nicht mehr. Wichtig ist dabei, dass Sie sicherstellen, dass tatsächlich Sie es sind, der sich gerade von einem vertrauenswürdigen Gerät mit der Fritzbox verbindet.

Ob das laut Browser „nicht vertrauenswürdige“ Zertifikat für die HTTPS-Verbindung mit der Fritzbox wirklich von Ihrem Router stammt – und damit für Sie doch vertrauenswürdig ist –, prüfen Sie über seinen Fingerabdruck im Router und im Browser. Bei einer Fritzbox finden Sie den Fingerabdruck des Zertifikats im Menü unter „Internet → Freigaben → Fritzbox-Dienste“ im umrandeten Kasten rechts neben „SHA-1 Fingerabdruck des Zertifikats“. Öffnen Sie das Fritzbox-Menü in einem zweiten Browserfenster, um es mit dem im Browser gespeicherten Fingerabdruck zu vergleichen. Klicken Sie dazu bei Firefox oben links in der Adressleiste auf das kleine Symbol mit dem Schloss und wählen „Verbindung nicht sicher → Weitere Informationen“. Im nun geöffneten Fenster „Seiteninformationen“ gehen Sie auf die erste Schaltfläche „Zertifikat anzeigen“ – es öffnet sich ein großes Browserfenster mit der Überschrift „Zertifikat“. Scrollen Sie nach unten bis zu „Fingerabdrücke“ und vergleichen Sie den SHA-1 mit dem in der Fritzbox. Sind beide identisch, nutzt Ihr Browser für die HTTPS-Verbindung zur Fritzbox tatsächlich deren SSL-Zertifikat – alles ist in Ordnung.

So erreichen Sie Ihren Router sicher im Heimnetz

Aus Sicherheitsgründen sollten Sie das Fritzbox-Menü nicht mehr über *fritz.box* aufrufen. Nutzen Sie stattdessen die lokale IP-Adresse Ihrer Fritzbox. Läuft auf dem Router bereits das aktuelle Fritz-OS 8, können Sie auch die lokale Domain *https://fritzbox.internal* verwenden. Die installierte Firmwareversion der Fritzbox sehen Sie in

Rechts oben im Fritzbox-Menü rufen Sie die Einstellung zur Änderung des voreingestellten Kennworts auf. Das sollten Sie unbedingt tun, auch wenn eine Fritzbox bereits ab Werk ein personalisiertes Passwort besitzt.



Damit eine sichere HTTPS-Verbindung zum Fritzbox-Menü funktioniert, sollten Sie prüfen, ob der Fingerabdruck des Zertifikats im Router mit dem des Browsers übereinstimmt.

der „Übersicht“ des Webmenüs unter dem Routersymbol.

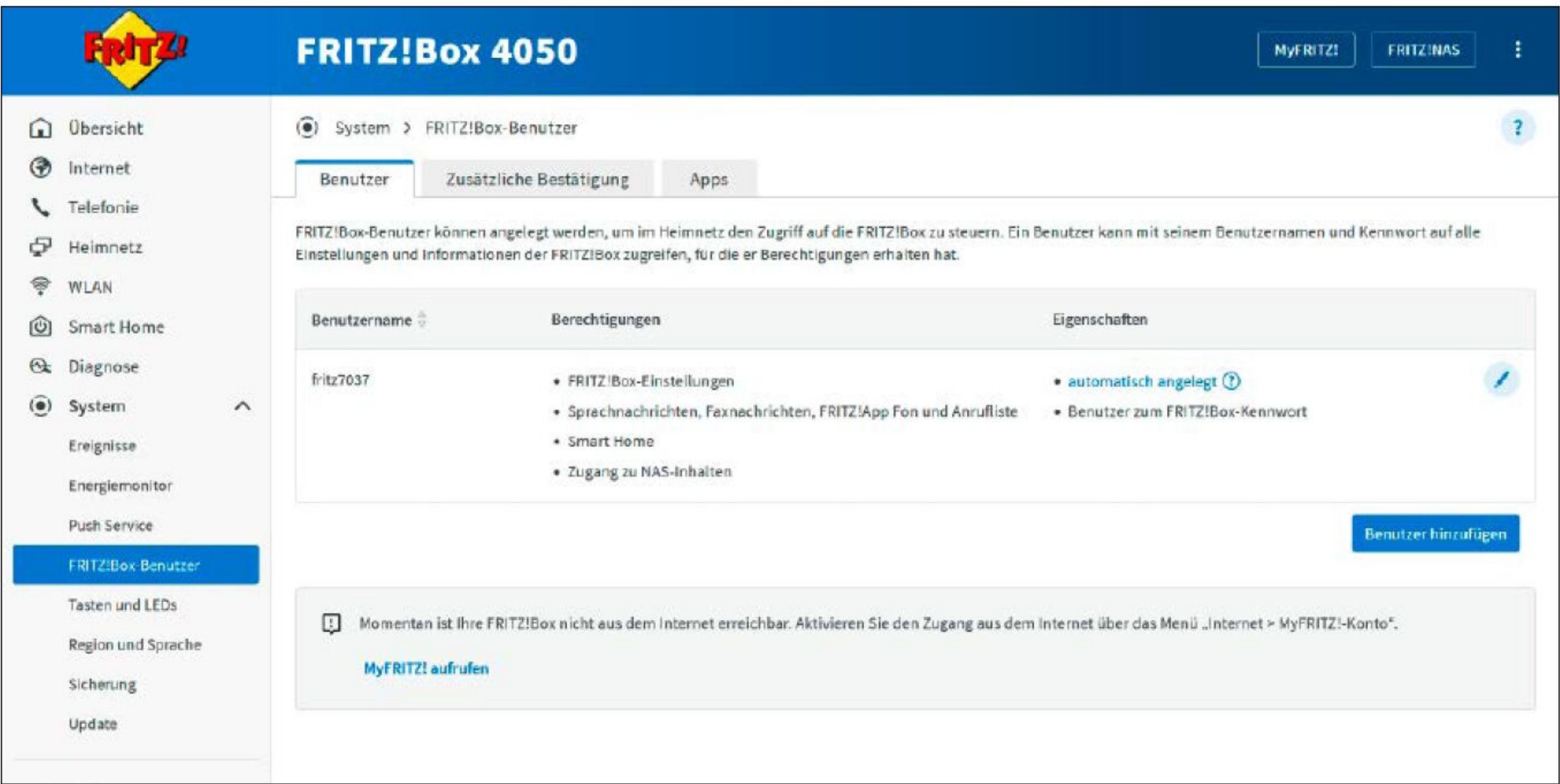
Beim ersten Aufruf des Menüs über diese neue Webadresse müssen Sie eventuell erneut eine Zertifikats-Ausnahme im Browser hinzufügen – auch dann, wenn Sie sich vom selben Client mit demselben Browser anmelden.

Legen Sie ein zusätzliches Benutzerkonto für den Menüzugriff an

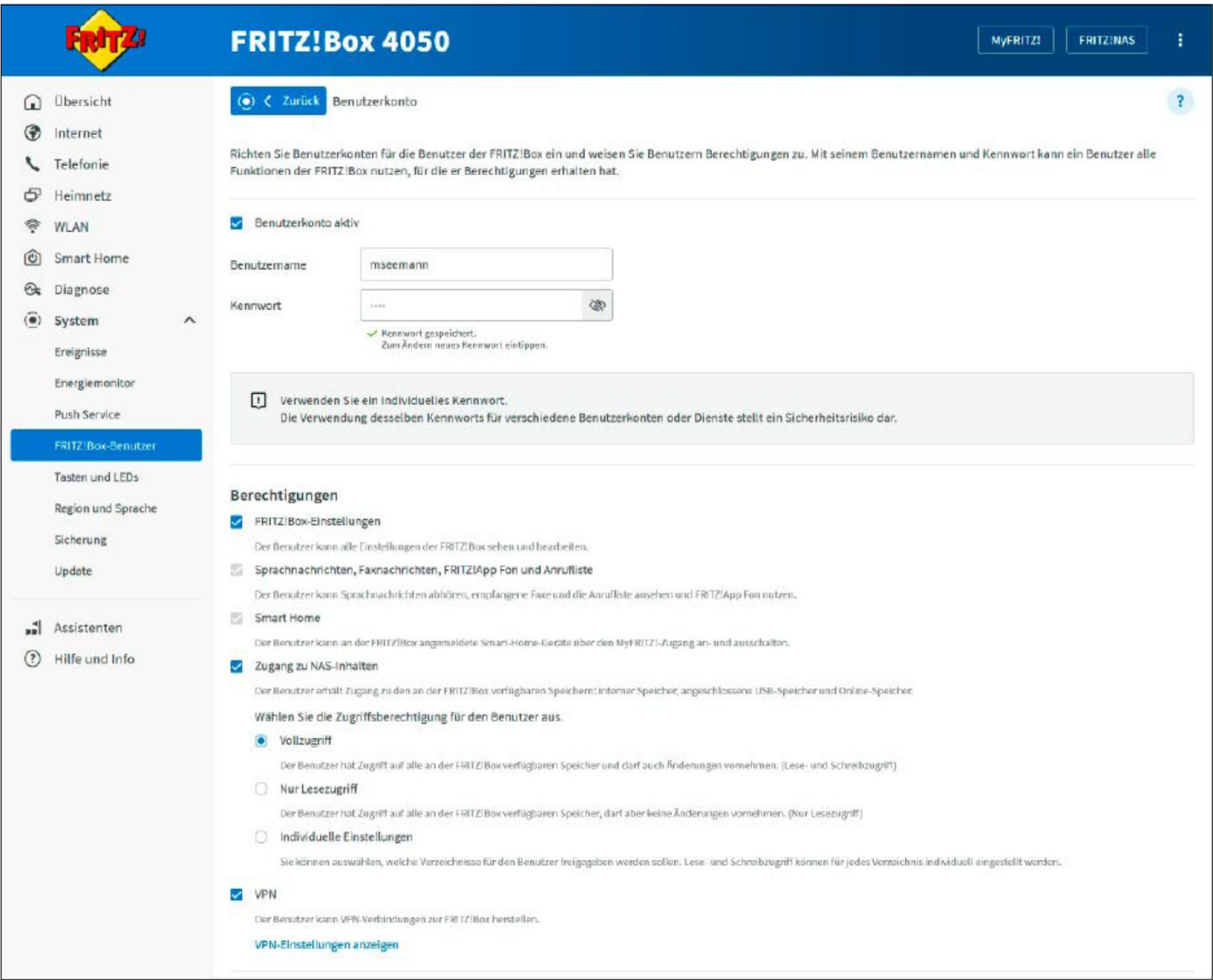
Ab Werk benötigen Sie nur das Kennwort, um sich im Fritzbox-Menü anzumelden. Einen besseren Schutz erzielen Sie, wenn Sie stattdessen die Kombination aus Benutzername und Kennwort nutzen. Nur so kommen Sie auch ins Fritzbox-Menü, wenn Sie außerhalb des lokalen Netzwerks übers Internet darauf zugreifen wollen.

Die Anmeldung per Benutzerkonto aktivieren Sie im Routermenü unter „System → Fritzbox-Benutzer → Benutzer“. Dort steht bereits ein Benutzername: Es ist der von Fritz ab Werk angelegte Fritzbox-Standardbenutzer, dessen Name mit „fritz“ beginnt und mit vier Ziffern endet – beispielsweise „fritz7037“. Solange nur das Konto dieses Fritzbox-Benutzers im Router hinterlegt ist, genügt das Kennwort bei der Anmeldung am Webmenü.

Das ändern Sie, indem Sie auf „Benutzer hinzufügen“ klicken: Legen Sie nun einen neuen Benutzer mit neuem Benutzernamen und neuem Kennwort an. Achten Sie darauf, dass Sie ein starkes Kennwort verwenden – ob das zutrifft, verrät Ihnen die Fritzbox mit dem Balken unterhalb des Eingabefeldes. Wichtig: Verwenden Sie unbe-



Ab Werk ist in einer Fritzbox bereits ein Standardbenutzer angelegt, wie hier fritz7037. Solange keine Benutzer hinzukommen, genügt daher das Kennwort, um sich am Routermenü anzumelden.



Damit die Fritzbox neben dem Kennwort auch einen Benutzernamen für die Anmeldung fordert, legen Sie einen weiteren Benutzer mit starkem Kennwort und allen Berechtigungen außer dem „Zugang aus dem Internet“ an.

dingt ein anderes Kennwort als das des Fritzbox-Standardbenutzers. Unter „Berechtigungen“ können Sie angeben, ob dieser Benutzer Einstellungen im Fritzbox-Menü vornehmen darf oder ob er nur auf die Kommunikation zugreifen oder das Smart Home bedienen darf. Auch NAS- und VPN-Zugriff lassen sich hier regeln. Wir empfehlen, dass Sie für den Fritzbox-Zugriff von zu Hause ein Benutzerkonto mit starkem Passwort anlegen, das mit allen Berechtigungen außer „Zugang aus dem Internet“ ausgestattet ist. Nach dem Anle-

gen des neuen Benutzerkontos mit „Übernehmen“ müssen Sie noch eine Taste an Ihrer Fritzbox zur Bestätigung drücken.

Sicherheitsfalle umgehen: Schalten Sie die Benutzerauswahl ab

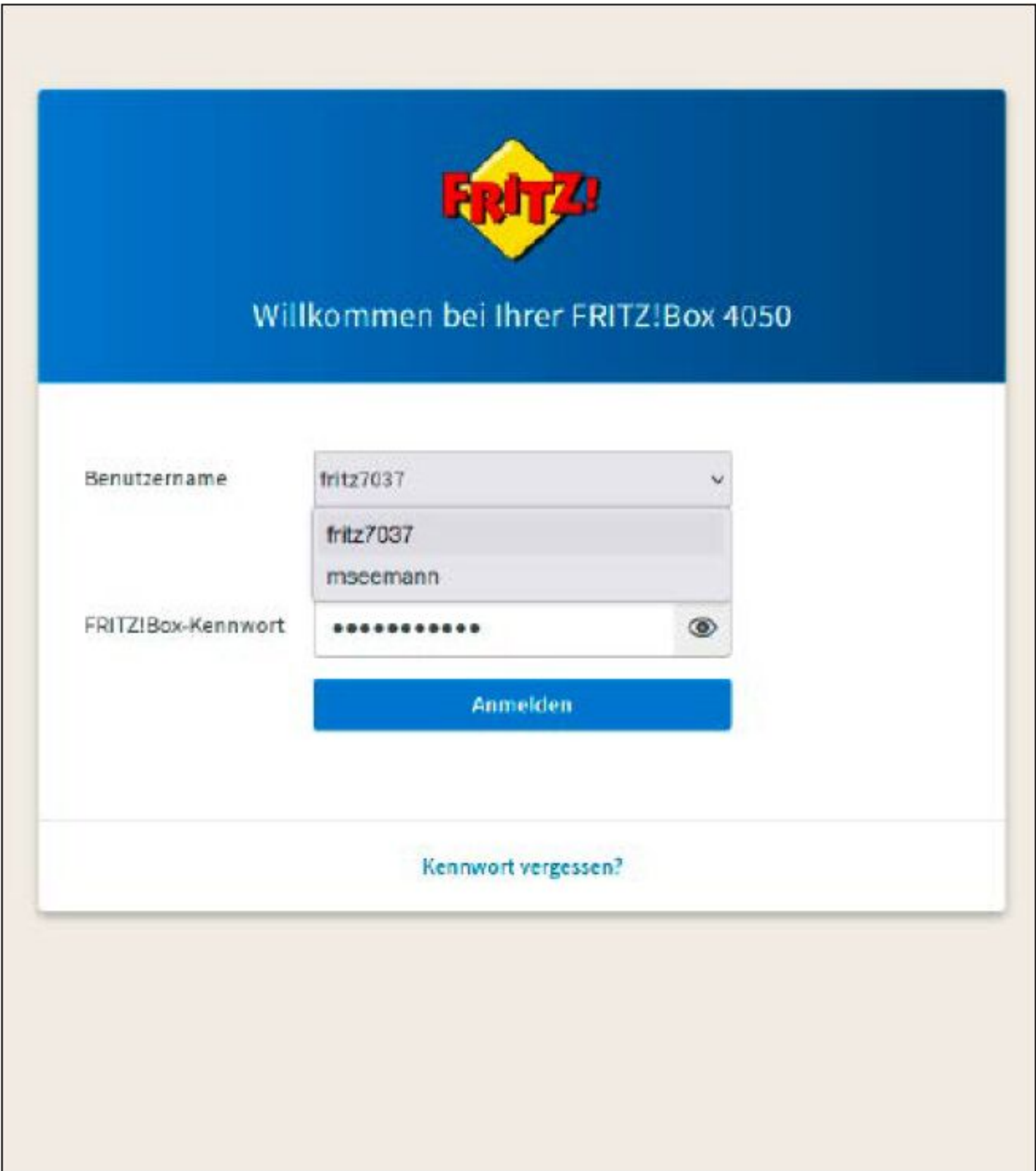
Haben Sie das zusätzliche Benutzerkonto eingerichtet, melden Sie sich rechts oben über die drei Punkte mit „Abmelden“ vom Fritzbox-Menü ab. Nun landen Sie wieder im Anmeldefenster „Willkommen bei Ihrer Fritzbox...“. Direkt unter der Eingabemaske für das Kennwort sehen Sie nun den Hin-

weis, dass Sie „sich auch mit Ihrem Benutzernamen und Kennwort anmelden“ können. Klicken Sie darauf und nutzen Sie zur Anmeldung das gerade angelegte Benutzerkonto. Allerdings lauert noch eine Sicherheitsfalle im Anmeldefenster: Im Drop-down-Menü stehen nach wie vor die Benutzernamen aller aktiven Benutzerkonten – der Sicherheitsgewinn durch die zusätzliche Abfrage des Benutzernamens ist dann natürlich nutzlos.

Um das zu ändern, gehen Sie im Menü zu „System → Fritzbox-Benutzer → Benutzer“ und schieben unten den grünen Regler neben „Liste der Benutzernamen bei Anmeldung anzeigen“ nach links auf die Stellung „inaktiv“. Nun zeigt die Fritzbox die Benutzernamen im „Willkommen“-Fenster nicht mehr an – sie müssen ab jetzt wie das Kennwort eingetippt werden. Natürlich kostet diese Art der Anmeldung mehr Zeit und ist nicht so komfortabel wie die Anmeldung mit vorgegebenen Benutzernamen. Aber der Sicherheitsgewinn ist enorm: Denn ein möglicher Angreifer muss nun neben dem Passwort auch den dazugehörigen Benutzernamen kennen, um ins Fritzbox-Menü zu kommen.

Fernzugriff: Wie Sie von überall aus Ihren Router erreichen

Auch wenn Sie nicht zu Hause sind, können Sie das Routermenü aufrufen, um den Status im Heimnetz zu prüfen. Da diese Verbindung anfälliger für Angriffe ist als der Kontakt zur Fritzbox im lokalen Netzwerk, müssen Sie dafür zusätzliche Sicherheitsvorkehrungen treffen. Eine Fritzbox müssen Sie für den Fernzugriff zunächst beim Fritz-Dienst My Fritz anmelden. Das müssen Sie erledigen, wenn Sie sich im Heimnetz befinden. Gehen Sie im Menü auf „Internet → MyFritz-Konto“ und tragen dort eine gültige E-Mail-Adresse ein. An diese Adresse schickt die Fritzbox eine Nachricht mit dem Absender „noreply@myfritz.net“. Klicken Sie auf den darin befindlichen Link und registrieren Sie sich bei My Fritz Net mit derselben Mailadresse und einem neuen Zugangspasswort. Durch die Anmeldung bei My Fritz bekommt Ihre Fritzbox einen festen DDNS-Domainnamen zugewiesen: Damit erreichen Sie den Router garantiert vom Internet aus, selbst wenn er täglich seine öffentliche IP-Adresse ändert.

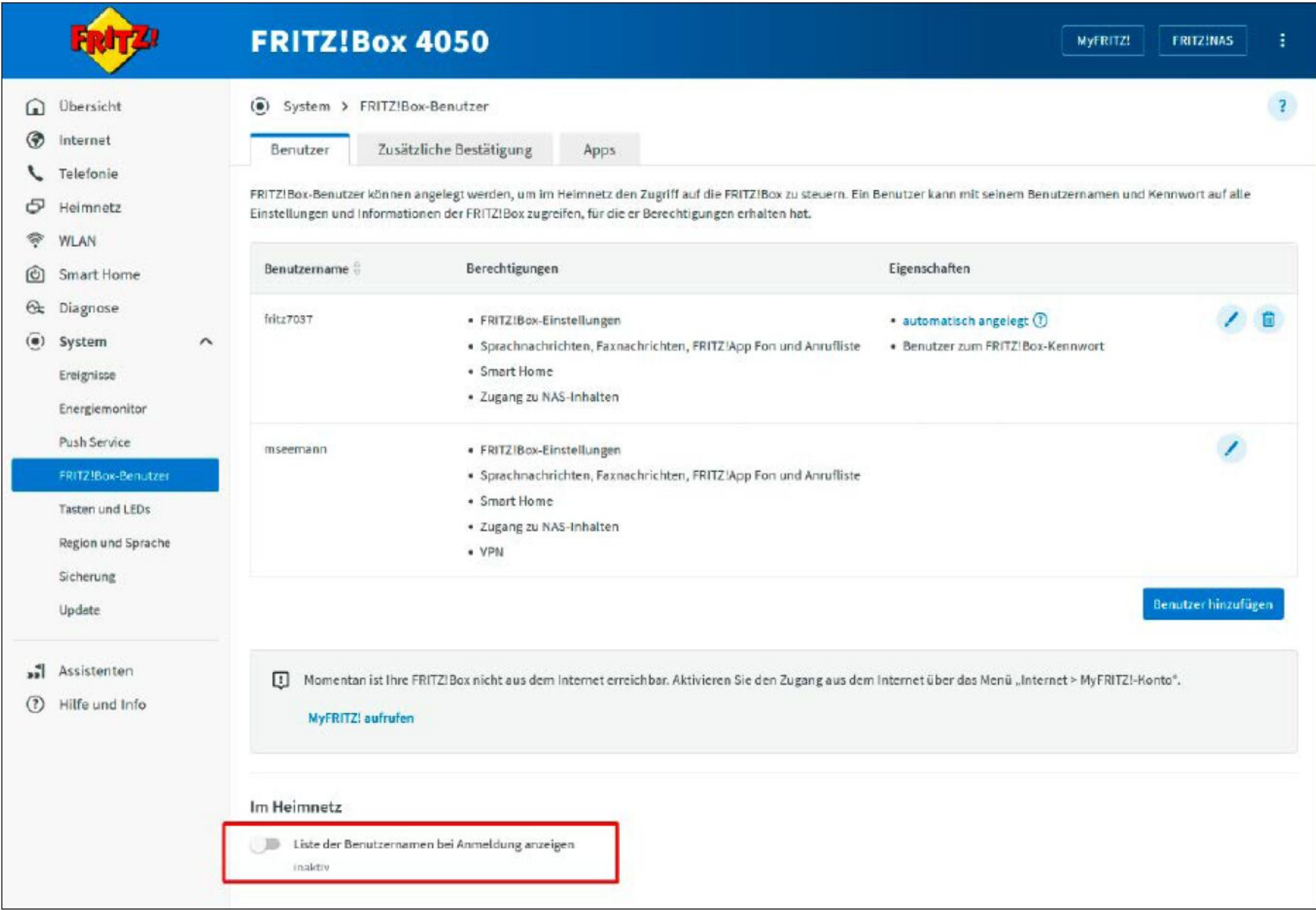


Die Fritzbox zeigt im Anmeldefenster alle aktiven Benutzernamen an, wie hier zu sehen. Das ist komfortabel, schwächt aber die Sicherheit: Schalten Sie diese Funktion daher im Routermenü ab (Bild rechts).

Gehen Sie anschließend wieder ins Routermenü zu „Internet → MyFritz-Konto“. Der grüne Punkt zeigt, dass die Fritzbox mit dem My-Fritz-Dienst verbunden ist. Im Bereich unter „MyFritz-Internetzugriff“ wird Ihnen die My-Fritz-Adresse Ihrer Fritzbox angezeigt. Der erste Teil besteht aus einer Reihe von Kleinbuchstaben und Ziffern, der zweite aus *myfritz.net*. Damit Sie die Fritzbox unter dieser Adresse aus dem Internet erreichen, klicken Sie auf das blau hinterlegte „MyFritz-Internetzugriff einrichten“. Das Menü meldet nun, dass der „Internetzugriff auf die Fritzbox über HTTPS aktiviert“ ist. Außerdem erscheint rechts neben „My-Fritz-Internetzugang“ die vollständige Webadresse mit vorangestelltem „https://“ und einer fünfstelligen Portnummer nach dem Doppelpunkt. Mit dieser Adresse inklusive Portnummer können Sie Ihre Fritzbox auch an einem Internetzugang außerhalb Ihres Heimnetzes ansteuern, sodass Ihnen die Anmeldeseite „Willkommen bei Ihrer Fritzbox...“ angezeigt wird. Damit Sie die komplizierte Webadresse der Fritzbox stets verfügbar haben, speichern Sie sie am besten als Browser-Lesezeichen.

Legen Sie für den Fernzugriff einen speziellen Benutzer an

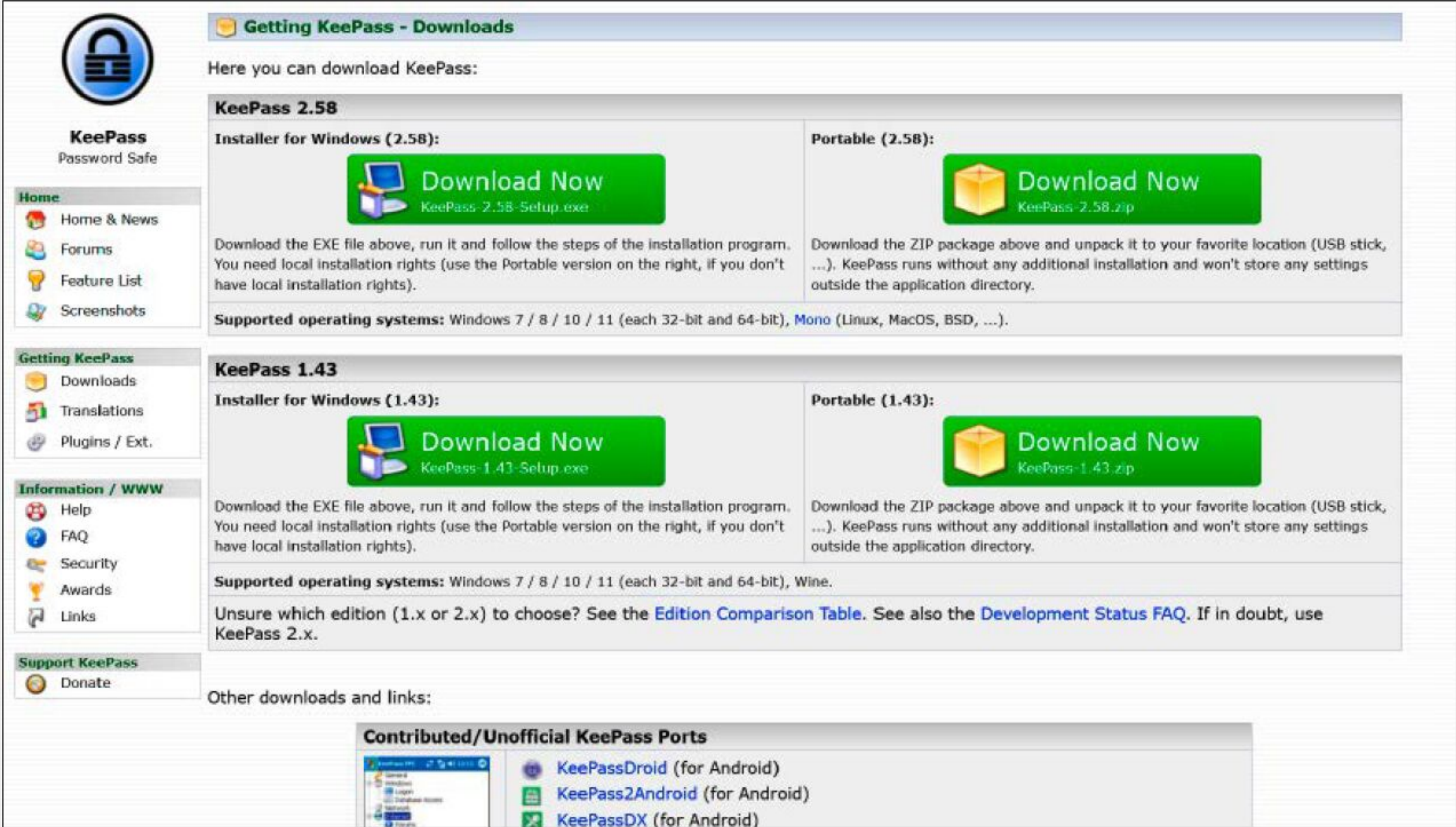
Das Benutzerkonto, mit dem Sie aus dem Internet auf das Routermenü zugreifen, muss für den Fernzugriff berechtigt sein. Dieses Konto sollten Sie besonders umfassend schützen, denn die Fritzbox öffnet über den fünfstelligen Port einen Webser-



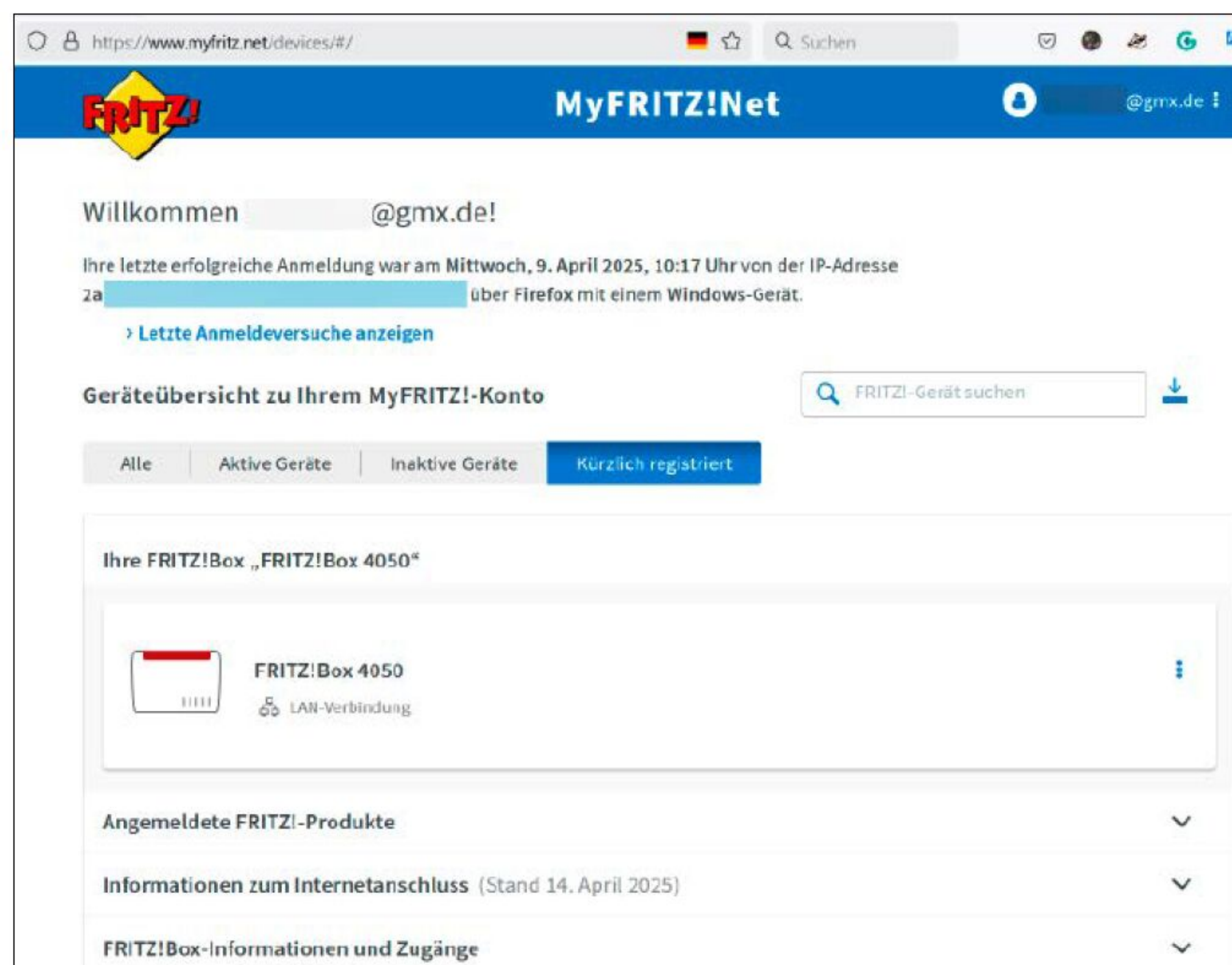
WANN IST EIN KENNWORT SICHER?

*****_

Je stärker das Kennwort für den Fritzbox-Zugang, umso besser ist Ihr Router geschützt. Das Passwort für den Zugang aus dem lokalen Netzwerk sollte mindestens zehnstellig sein und neben Groß- und Kleinbuchstaben auch Ziffern enthalten. Verwenden Sie keine Namen, keine Wörter aus dem Wörterbuch und keine Geburtsdaten. Notieren Sie sich das neue Kennwort und deponieren Sie die Notiz an einem geschützten Ort – ein Zettel unter dem Router oder unter Ihrer PC-Tastatur ist keine sichere Stelle. Alternativ verwenden Sie einen Passwortsafe, um das Kennwort zu speichern. Für den Fernzugriff aus dem Internet richten Sie für das separate Benutzerkonto ein mindestens zwölfstelliges Kennwort ein, das zusätzlich mindestens ein Sonderzeichen enthalten sollte. Die Fritzbox versteht folgende Sonderzeichen für Kennwörter: _ - ! „ # \$ % & , () * + , . / : ; < = > ? @ [\] ^ ` { | } ~ Folgende Zeichen dürfen Sie dagegen in Fritzbox-Kennwörtern nicht verwenden: ä, ö, ü, ß, €, \$, ´



Am sichersten merken Sie sich Passwörter wie für das Routermenü oder den Fernzugriff, indem Sie sie in einem Passwortsafe wie dem Open-Source-Tool KeePass 2.58 speichern.



Damit Sie sich auch aus dem Internet an der Fritzbox zu Hause anmelden können, müssen Sie den Router in Ihrem My-Fritz-Konto registrieren – das Modell erscheint dann unter www.myfritz.net.

Schützen Sie das Routermenü vor Brute-Force-Attacken

Die Anmeldung zum Menü schützt die Fritzbox durch einen zusätzlichen Sicherheitsmechanismus.

Sind die Anmeldedaten wie Benutzername und Kennwort nicht korrekt, wird der Anmeldebildschirm für eine kurze Zeitdauer gesperrt.

Mit jeder fehlerhaften Eingabe verdoppelt sich diese Wartezeit. Damit erschwert der Router sogenannte Brute-Force-Attacken, bei denen Angreifer das Internet nach zugänglichen Webservern durchsuchen und an diesen dann automatisiert viele Passwortkombinationen hintereinander ausprobieren, bis sie die passende Kombination gefunden haben.

So meldet Ihnen der Router jeden Zugriffsversuch

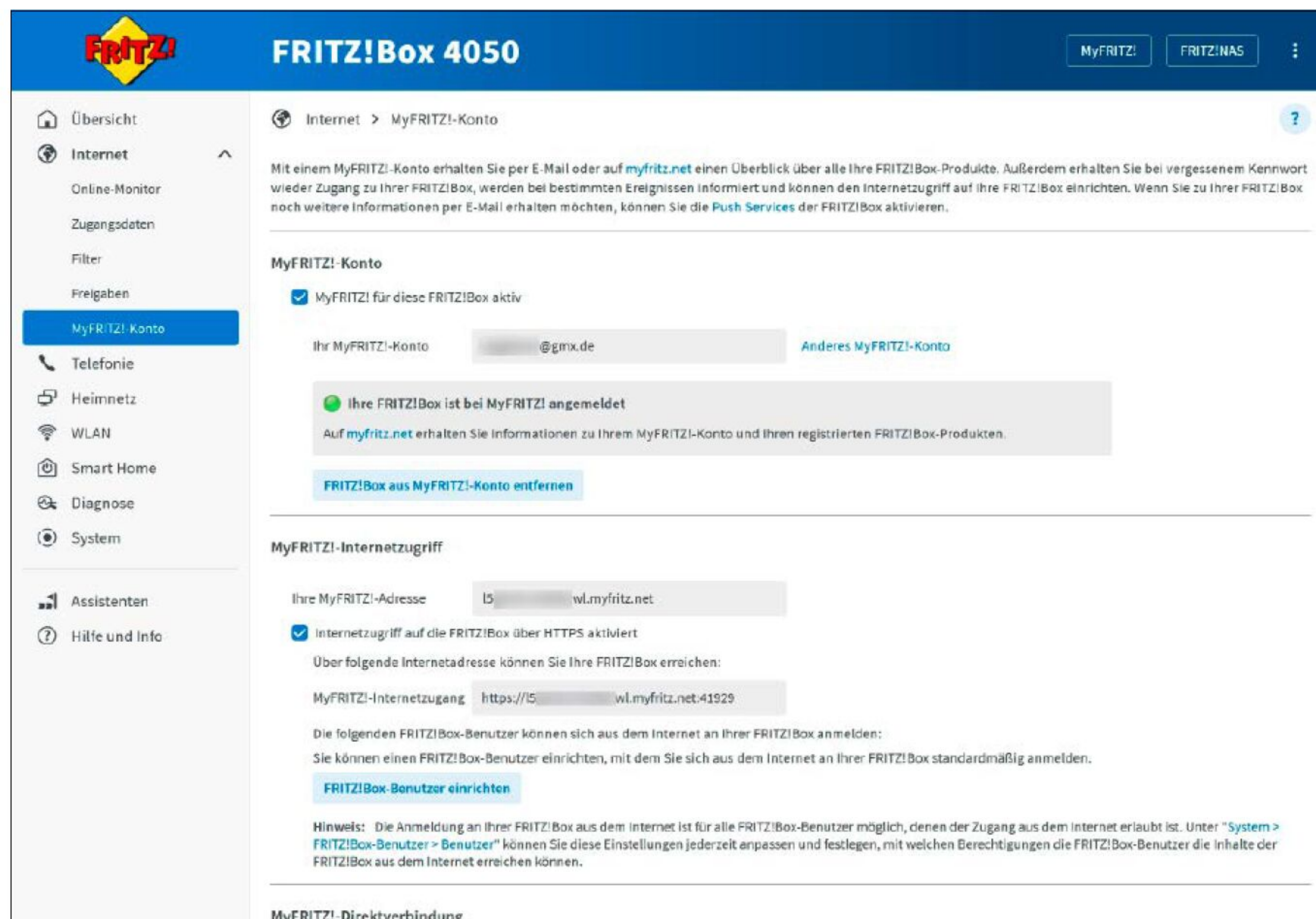
Außerdem kann Ihnen der Router bei jeder Anmeldung automatisch eine E-Mail senden: So können Sie sofort handeln, falls sich jemand anderer mit Ihrer Fritzbox verbindet.

Die entsprechende Einstellung finden Sie im Webmenü von My Fritz Net, wo Sie sich mit Ihrer E-Mail-Adresse registriert haben. Öffnen Sie dafür <https://www.myfritz.net> und melden Sie sich an Ihrem My-Fritz-Konto an mit der E-Mail-Adresse, die Sie für die Anmeldung beim My-Fritz-Dienst benutzt haben, sowie dem entsprechenden My-Fritz-Passwort. Gehen Sie auf „Anmelden“ und klicken Sie im folgenden Fenster mit der Geräteübersicht oben rechts auf Ihre Mailadresse.

Wählen Sie dann die Option „Einstellungen von MyFritzNet“ und anschließend „E-Mail-Benachrichtigungen“. Hier sollten alle Optionen bereits automatisch aktiviert sein. Die beiden ersten sorgen dafür, dass Sie bei jedem erfolgreichen Fernzugriff auf Ihre Fritzbox eine Benachrichtigung an Ihre Mailadresse erhalten. Öffnen Sie erneut rechts oben per Klick auf die Mailadresse das Kontextmenü und gehen Sie dieses Mal auf „Kontoeinstellungen“. Hier sehen Sie unter „Anmeldungen“ alle kürzlich erfolgten Anmeldeversuche am My-Fritz-Konto.

Zwei-Faktor-Authentifizierung für My Fritz nutzen

Mit einem starken Passwort sorgen Sie für einen grundlegenden Schutz des Routermenüs. Zusätzliche Sicherheit bringt eine



Am grünen Punkt erkennen Sie, dass sich diese Fritzbox über My Fritz aus dem Internet erreichen lässt, wenn Sie ihre Webadresse im Browser eingeben. Sie steht bei „MyFRITZ!-Internetzugang“.

ver-Zugang in Richtung Internet, über den nicht nur Sie, sondern auch andere Internetteilnehmer auf das „Willkommen“-Menü Ihrer Fritzbox gelangen können.

Deshalb weisen Sie die Berechtigung „Zugang aus dem Internet“ am besten nur einem speziellen Benutzerkonto zu: Nutzen Sie dafür ein sehr starkes Kennwort und einen besonderen Benutzernamen – keinesfalls den eigenen Namen oder „admin“. Das neue Benutzerkonto für den Internetzugriff legen Sie im Routermenü „Internet → MyFritz-Konto“ an. Gehen Sie auf das blau hinterlegte „FritzBox-Benutzer einrichten“ und anschließend auf „Neuer Benutzer“. Wählen Sie einen mindestens zehnstelligen

Benutzernamen und ein mindestens zwölfstelliges Kennwort für dieses Benutzerkonto. Es sollte ein Kennwort sein, das Sie für kein anderes Onlinekonto nutzen. Notieren Sie die Zugangsdaten des neuen Fernzugriff-Benutzers, übernehmen Sie die Kontoeinstellung und drücken Sie zur Bestätigung der Übernahme eine der Tasten an Ihrer Fritzbox. Das neue Benutzerkonto wird Ihnen unter „MyFritz-Internetzugriff“ mit einem kleinen Wolkensymbol angezeigt. Wechseln Sie danach in das Menü „System → Fritzbox-Benutzer → Benutzer“. Bei den Berechtigungen sollten Sie nur „Zugang aus dem Internet“ und „FritzBox-Einstellungen“ aktivieren.

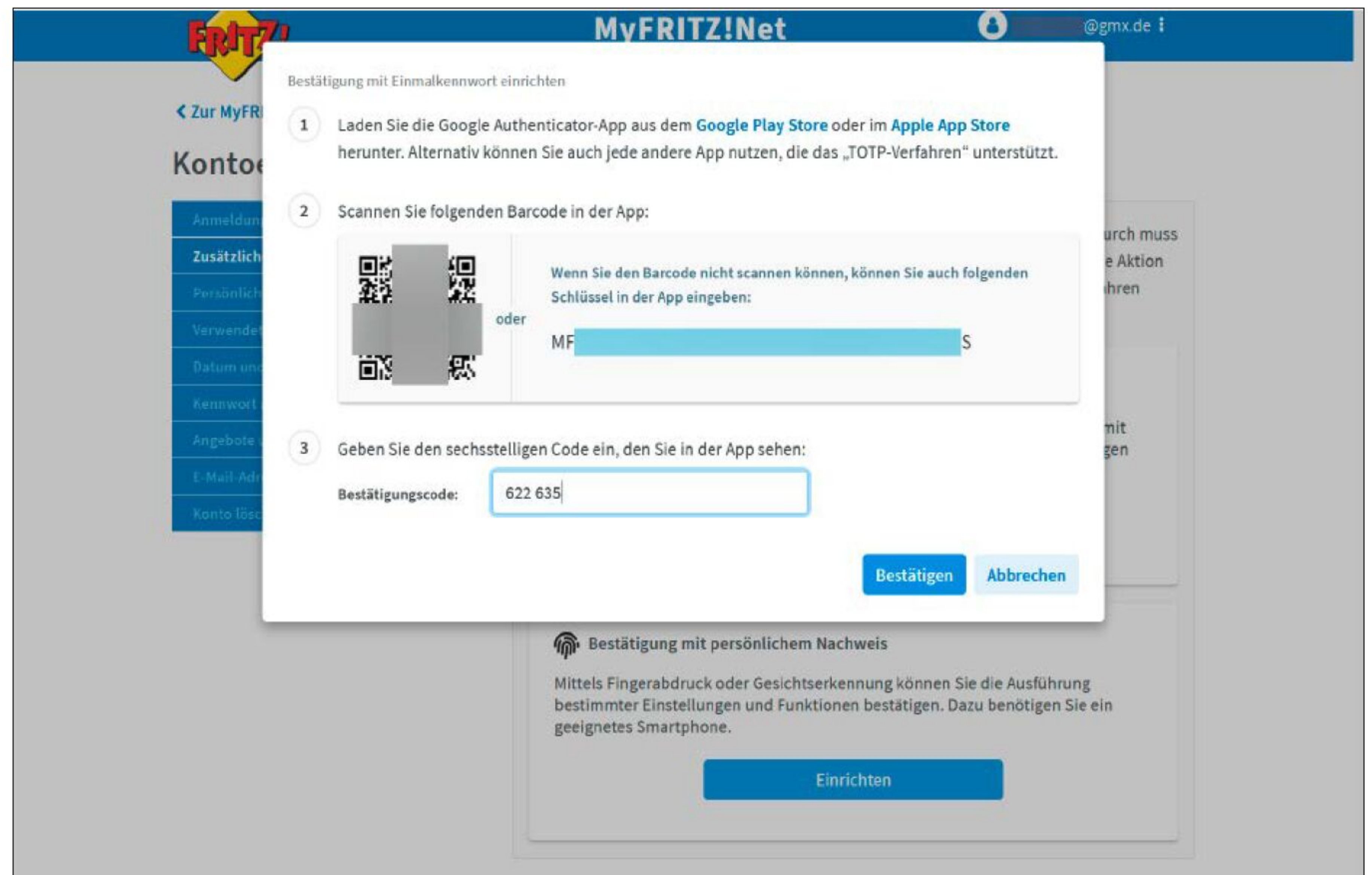
Zwei-Faktor-Authentifizierung (2FA) bei der Anmeldung. Die benötigen Sie zudem, wenn Sie per Fernzugriff im Fritzbox-Menü sicherheitskritische Einstellungen ändern wollen. Denn die Fritzbox fordert dafür normalerweise eine Bestätigung durch Drücken eines Knopfs am Gehäuse. Diesen Vorgang können Sie durch 2FA ersetzen, wenn Sie nicht zu Hause sind.

Sie brauchen dafür ein Smartphone mit einer Authenticator-App – zum Beispiel die Open-Source-Lösung **2FA Authenticator (2FAS)**, die für iOS und Android erhältlich ist. Nach dem Start der App klicken Sie sich durch die Kurzeinführung, bis die Schaltfläche „Neuen Dienst koppeln“ erscheint.

Nun öffnen Sie das My-Fritz-Menü, klicken rechts oben auf Ihre Mailadresse und wählen die Option „Kontoeinstellungen → Zusätzlicher Schutz“. Klicken Sie im Bereich rechts unter „Bestätigung mit Einmalkennwort“ auf die „Einrichten“-Taste. Im folgenden Fenster erscheint unter Punkt 2 ein QR-Code. Diesen scannen Sie mit der Authenticator-App am Smartphone – eventuell müssen Sie zuvor der App einmal erlauben, dass sie die Smartphone-Kamera nutzen darf. Nach dem Scan zeigt Ihnen die App eine sechsstellige Authentifizierungsnummer an. Diese tragen Sie unter Punkt 3 im My-Fritz-Menü ein und gehen auf „Bestätigen“. Der angezeigte Code ist nur 30 Sekunden gültig und wird dann durch einen neuen ersetzt. Sie dürfen daher beim Eintragen des aktuellen Codes nicht trödeln. Im folgenden Fenster steht ein Wiederherstellungsschlüssel: Sie benötigen ihn, falls Sie Ihr Smartphone verlieren sollten. Speichern Sie den Schlüssel unbedingt ab, drucken Sie ihn zusätzlich aus und verwahren Sie die Sicherungen an einem geschützten Ort. Setzen Sie danach den Haken vor „Ich habe den Schlüssel gesichert“ und schließen Sie das Fenster mit „Fertig“.

Jetzt haben Sie den Fernzugriff durch 2FA zusätzlich geschützt: My Fritz Net fordert nun nach Eingabe der Zugangsdaten eine „Bestätigung mit Einmalkennwort“, das die Authenticator-App anzeigt.

Damit Sie 2FA statt eines Knopfdrucks nutzen können, um sicherheitskritische Einstellungen im Fritzbox-Menü zu bestätigen, gehen Sie zum Benutzerkonto mit der Berechtigung für den Fernzugriff unter „System → Fritzbox-Benutzer → Benutzer“. Der weitere Vorgang entspricht der 2FA-Einrichtung für My Fritz. ■



Zusätzlich zu einem starken Kennwort können Sie eine Zwei-Faktor-Authentifizierung nutzen, um den Fernzugriff auf die Fritzbox besser abzusichern. Dazu benötigen Sie eine Authenticator-App auf dem Smartphone.

WARUM SIE FRITZ.BOX NICHT MEHR VERWENDEN SOLLTEN

Der einfachste Weg zum Fritzbox-Menü führt über die Eingabe der Domainadresse

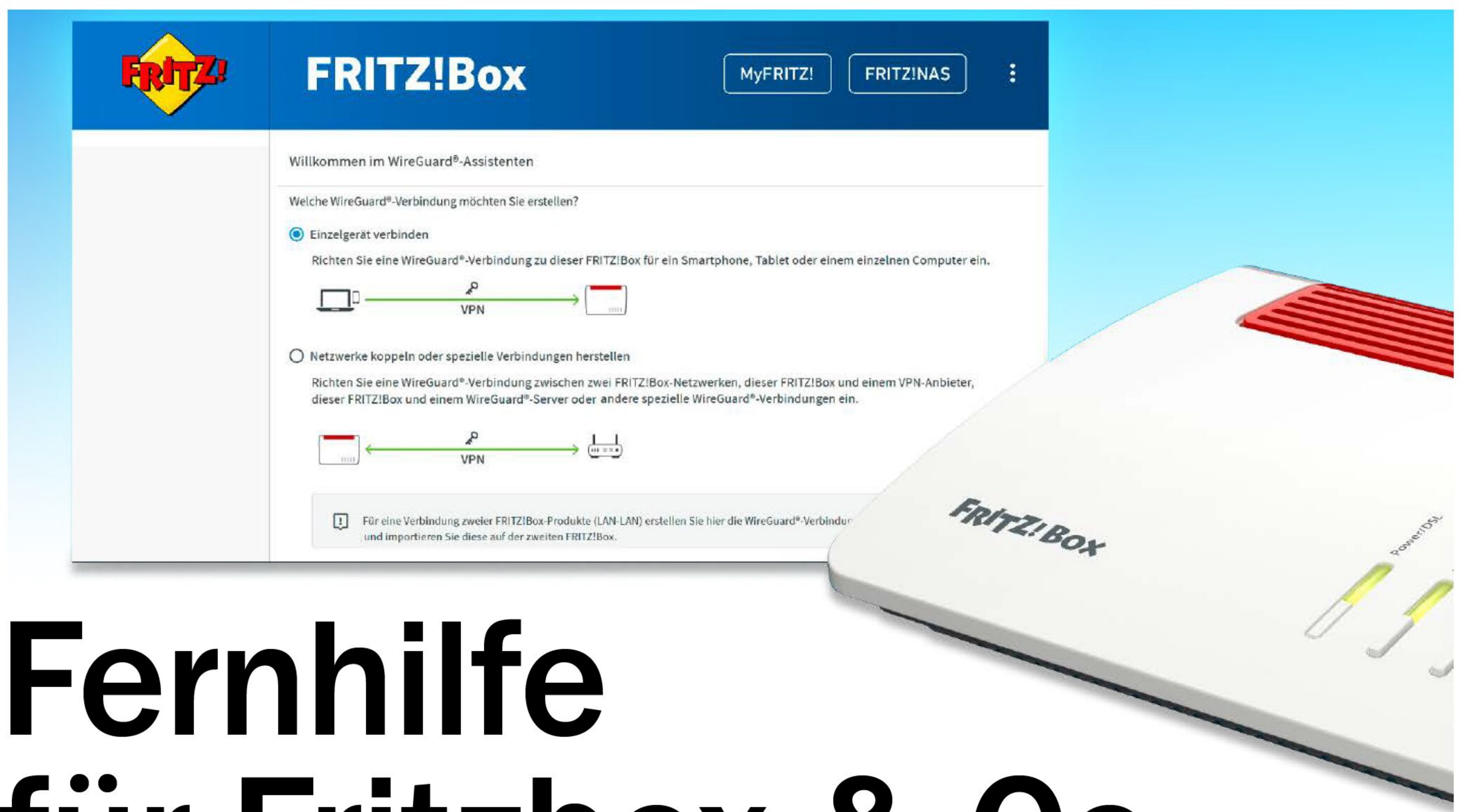
fritz.box im Browser. Besonders sicher ist das allerdings nicht: Denn im Gegensatz zur lokalen IPv4-Adresse des Routers **192.168.178.1** funktioniert diese Adresse theoretisch auch im Internet, weil **.box** inzwischen als Top-Level Domain (TLD) registriert und daher von öffentlichen DNS-Servern aufgelöst werden kann. Das hat im Fall von **fritz.box** bereits zu Sicherheitsproblemen geführt.

Allerdings gibt es Domains, die ausschließlich in lokalen Netzwerken genutzt werden dürfen: Lokale Domains wie **.internal** oder **.home.arpa** sind von der Weiterleitung durch das globale Domain Name System ausgeschlossen – sie können daher nicht als Domain registriert und eventuell missbraucht werden.

Ab Fritz-OS 8 dürfen auch Fritzbox-Router diese lokalen Domainnamen nutzen: Wenn Sie **fritzbox.internal** oder **fritzbox.home.arpa** im Browser eines Heimnetzgerätes aufrufen, kommen Sie zur Anmeldeseite des Routermenüs. Diese lokalen DNS-Adressen stellen sicher, dass Ihre Anfrage nicht auf eine öffentliche IP-Adresse außerhalb des lokalen Netzwerks weitergeleitet wird. Wer sichergehen möchte, sollte deshalb für den Zugriff auf die Fritzbox aus dem Heimnetz immer eine dieser beiden Adressen wählen – und nicht mehr **fritz.box**.

Das Internetgremium IANA legt fest, dass sich bestimmte Domains wie **home.arpa** nur in lokalen Netzwerken (residential home networks) nutzen lassen.

.ARPA Zone Management	
Domain Names	The .arpa domain is the "Address and Routing Parameter Area" domain and is designated to be used exclusively for Internet-infrastructure purposes. We administer the domain in cooperation with the Internet technical community through the guidance of the Internet Architecture Board. For the management guidelines and operational requirements of the .arpa domain, see RFC 3172. The .arpa domain currently includes the following second-level domains:
Overview	
Root Zone Management	
IANA Registry	
ARPA Registry	
IDN Practices Repository	
Root Key Signing Key (DNSSEC)	
Reserved Domains	
DOMAIN	USAGE / REFERENCE
6tisch.arpa	For IPv6 over the Time-Slotted Channel Hopping mode of IEEE 802.15.4 RFC 9031
arpa	Reserved exclusively to support operationally-critical infrastructural identifier spaces as advised by the Internet Architecture Board RFC 3172
as112.arpa	For sinking DNS traffic for reverse IP address lookups and other applications RFC 7535
e164.arpa	For mapping E.164 numbers to Internet URIs RFC 6116
nap-noob.arpa	For the Nimble Out-Of-Band authentication method of the Extensible Authentication Protocol framework RFC 9140
home.arpa	For non-unique use in residential home networks RFC 8375
in-addr-servers.arpa	For hosting authoritative name servers for the in-addr.arpa domain RFC 5855



Fernhilfe für Fritzbox & Co.

Den eigenen Internetrouter haben Sie im Griff. Deshalb bitten Familie und Freunde Sie häufig bei Netzwerkproblemen um Unterstützung. Doch Sie können nicht immer vor Ort sein, und Anweisungen per Telefon oder Whatsapp helfen oft nicht weiter. Besser lösen Sie Probleme mit Fritzbox & Co. in anderen Heimnetzen per Fernzugriff.

VON MICHAEL SEEMANN

Das Internet geht nicht. Das WLAN ist weg. Als erfahrener Heim-Netzwerker haben Sie diese Sätze sicher schon oft gehört. Zu Hause sind diese Probleme mit wenigen Mausklicks schnell gelöst. Doch Familienmitgliedern und Freunden in größerer Entfernung bei diesen Problemen zu helfen, ist aufwendiger.

Mit den passenden Tricks müssen Sie für diesen privaten Support die eigenen vier Wände nicht verlassen: Lässt sich ein Fernzugriff auf den auswärtigen Router

einrichten, können Sie helfen, als würden Sie selbst vor der Fritzbox stehen.

Wir zeigen, mit welchen Verfahren sich Internetrouter erreichen lassen, die woanders stehen. Zudem geben wir Ihnen Tipps, die unabhängig vom konkreten Routermodell sind, und mit denen Sie Probleme mit beliebigen Netzwerkgeräten lösen können.

Router einstellen, bevor die ersten Probleme auftauchen

Am einfachsten lässt sich ein akutes Netzwerkproblem aus der Ferne lösen, wenn ein passender Fernzugriff bereits eingerichtet ist. Das sollten Sie den Hilfesuchenden unbedingt vorab erläutern. Denn Familie und Freunden per Telefon oder Videocall zu erklären, wie sie einen funktionierenden Fernzugriff am Router einrichten, wird in der Regel immer scheitern. Sie sollten daher vorab dorthin fahren, um über einen Rechner im lokalen Netzwerk die entsprechenden Einstellungen vorzunehmen.

Wichtig ist dabei, dass Sie den betroffenen Personen erklären, wie der Eingriff erfolgt und inwiefern dabei die Privatsphäre betroffen sein könnte. Zeigen Sie Möglichkeiten auf, wie der Hilfesuchende den aktuellen Fernzugriff nachvollziehen kann oder wie er möglicherweise auch verhindern kann, dass beispielsweise ein heimlicher Fernzugriff erfolgt.

Externe Hilfe: Drei Verfahren für den Fernzugriff auf einen Router

Grundsätzlich gibt es drei unterschiedliche Verfahren, um auf einen Router an einem anderen Ort zuzugreifen: Sie können zum Beispiel das Menü des Routers übers Internet aufrufen, indem Sie einen Port in dessen Firewall öffnen. Üblicherweise würde ein Router diesen Zugriff blockieren, da er nicht als Antwort auf eine Anfrage aus dem eigenen Heimnetz erfolgt. Mithilfe des geöffneten Ports funktioniert es aber, sofern Sie die aktuelle öffentliche IP-Adresse des Routers, die Nummer des

„Auch wenn Sie nicht vor Ort sind, können Sie Freunden bei Netzwerkproblemen schnell helfen.“

geöffneten Ports und die Zugangsdaten zum Menü des Routers kennen. Die meisten Routerhersteller bieten für diese Art des Zugriffs eigene Webdienste an – bei Fritz (früher AVM) gibt es etwa MyFritz. Eine weitere Option ist der Fernzugriff per VPN-Tunnel. Dazu muss der Router als VPN-Server arbeiten können. In dieser Funktion sollte er die beiden IP-Protokolle IPv4 und IPv6 sowie häufig genutzte VPN-Protokolle wie Wireguard oder Open VPN unterstützen. Für beide Protokolle gibt es kostenlose Software für Windows oder Mac-OS, die Sie auf Ihrem Rechner installieren, um damit die VPN-Verbindung zum Router aufzubauen. Fritzbox-Router, auf denen mindestens die Firmware Fritz-OS 7.50 installiert ist, nutzen Wireguard für eine VPN-Verbindung.

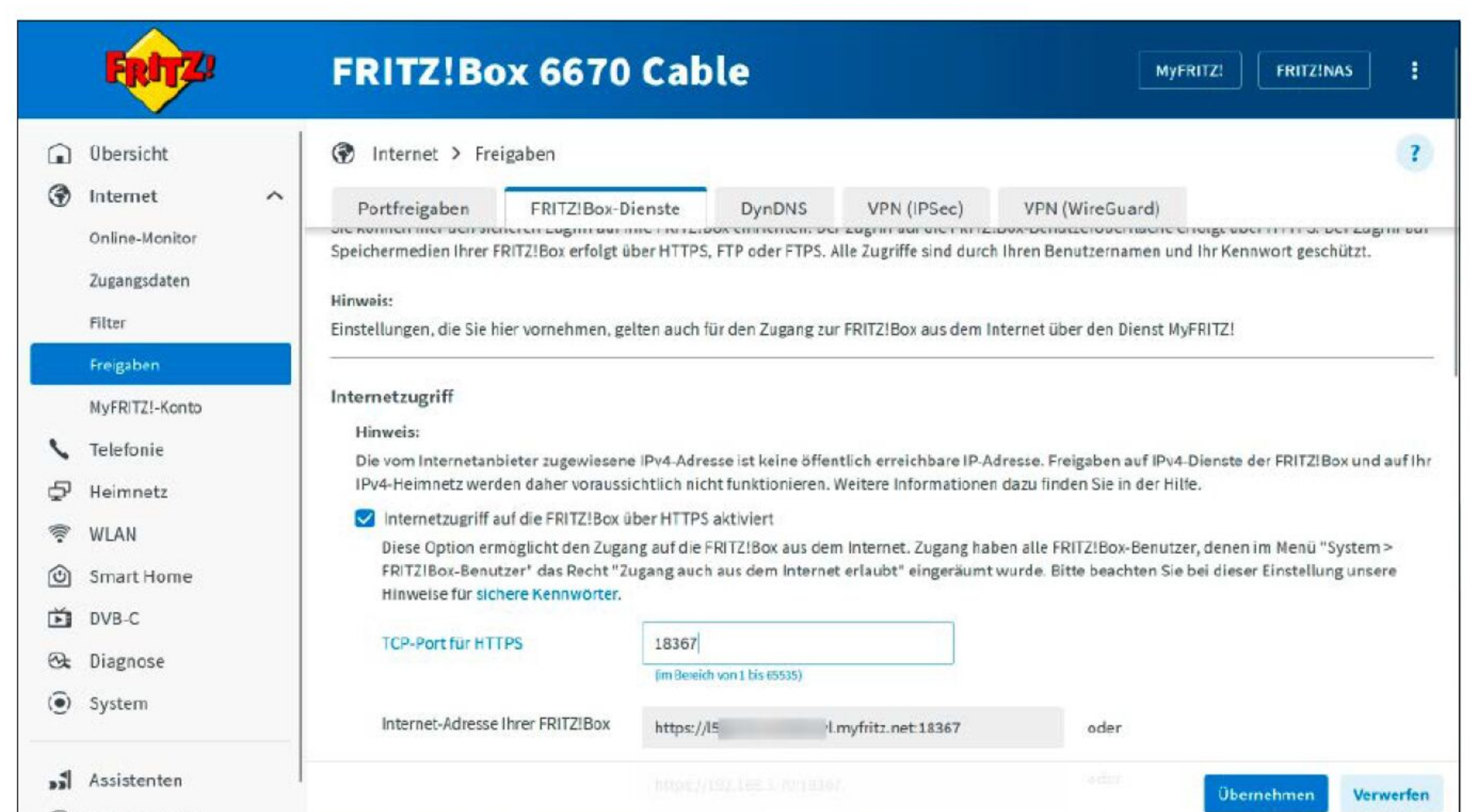
Die dritte Möglichkeit ist der Zugriff über einen Umweg: Sie greifen nicht direkt auf den Router, sondern auf einen Rechner zu, der mit ihm verbunden ist. So sind Sie im entfernten Heimnetz und lösen Internet- und WLAN-Probleme, wie Sie es zu Hause tun. Dazu benötigen Sie eine Fernzugriffssoftware wie **Teamviewer**: Sie muss auf beiden Rechnern aktiviert sein, damit sich vom eigenen PC aus der andere steuern lässt. Das funktioniert auch bei einem besonders kniffligen Problem: Wenn beim Hilfesuchenden ein Smartphone und ein PC mit zwei Netzwerkschnittstellen vorhanden sind, können Sie über Teamviewer selbst dann auf den entfernten Router zugreifen, wenn er nicht mit dem Internet verbunden ist.

Wichtig: Wenn Sie bei der Fritzbox bestimmte Einstellungen ändern, verlangt der Router eine zusätzliche Bestätigung, dass er diese Aktion ausführen soll – üblicherweise das Drücken einer Taste am Gehäuse. Das können Sie beim Fernzugriff auf einen Fritzbox-Router nicht selbst machen. Halten Sie deshalb auch stets telefonischen Kontakt zum Hilfesuchenden, damit dieser bei Bedarf die entsprechende Taste drückt.

Fernzugriff auf Router über einen geöffneten Port

Folgende Voraussetzungen muss der Router erfüllen, damit Sie aus der Ferne auf sein Menü zugreifen können: Sie müssen zunächst seine aktuelle, öffentliche IP-Adresse kennen. Da diese häufig wechselt, nutzen Sie einen sogenannten DynDNS-

Jede falsche Kennworteingabe im Log-in einer Fritzbox führt zu einer Verzögerung, was Brute-Force-Attacken von Angreifern erheblich erschwert.



Damit der Fernzugriff auf das Webmenü der Fritzbox funktioniert, muss ein HTTPS-Port freigeschaltet werden.

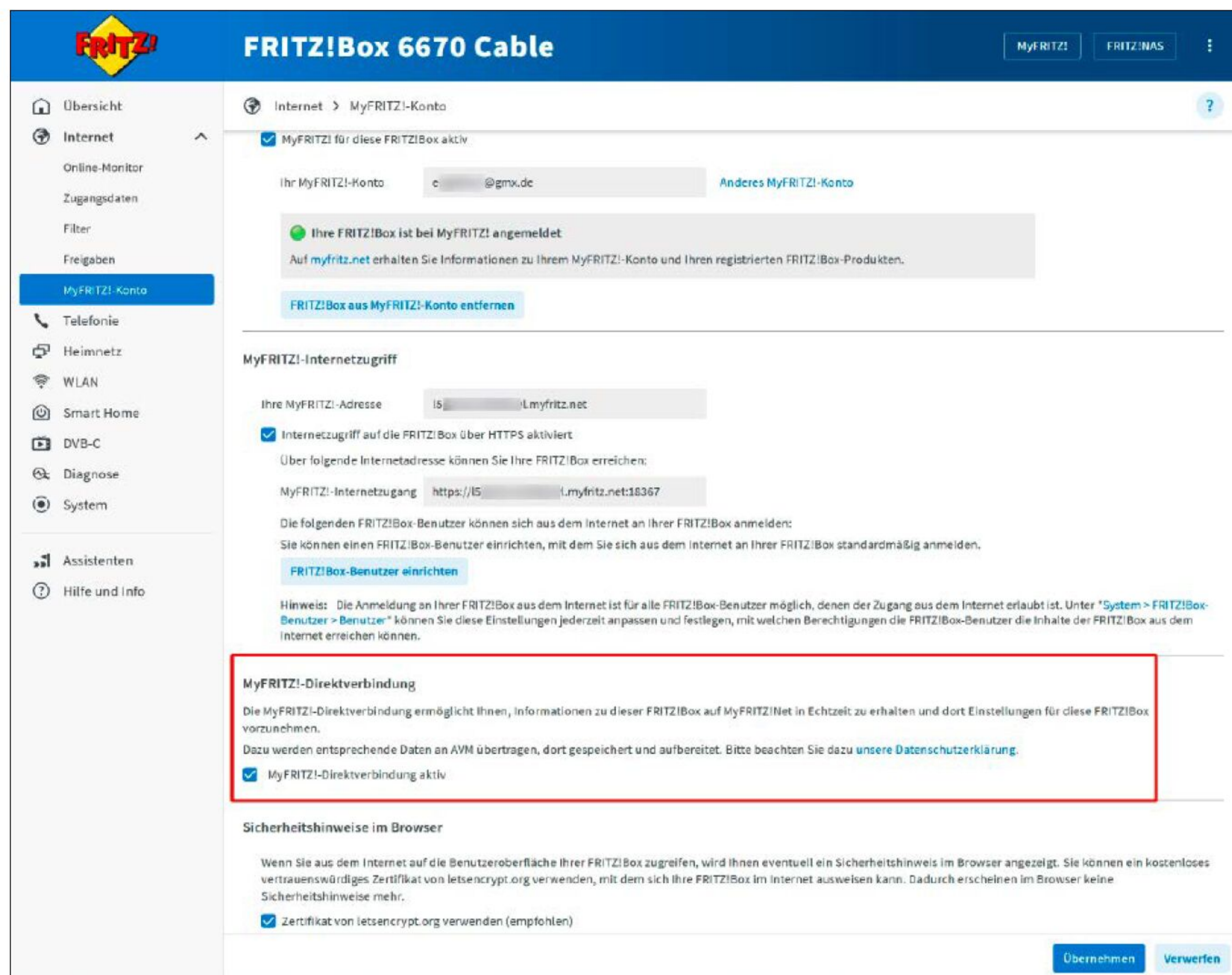
Dienst: Damit lässt sich der Router immer über eine festgelegte Webadresse erreichen, die der Dienst mit der jeweils gültigen IP verknüpft.

Zudem muss der Router den Zugriff auf sein Menü durch einen Rechner außerhalb des lokalen Netzwerks erlauben. Dafür öffnet er einen Port in der Router-Firewall. Um diesen entfernten Zugriff abzusichern, sollten Sie dafür keinen Standardport wie Port 80 oder 443 nutzen. Wählen Sie auch nicht die von vielen Routerherstellern alternativ genutzten Zugriffsport, etwa 8080 oder 8443: Alle sind häufig das Ziel automatisierter Portscans von Angreifern, die das Internet nach IP-Adressen mit offenen Ports absuchen. Ob sich der externe

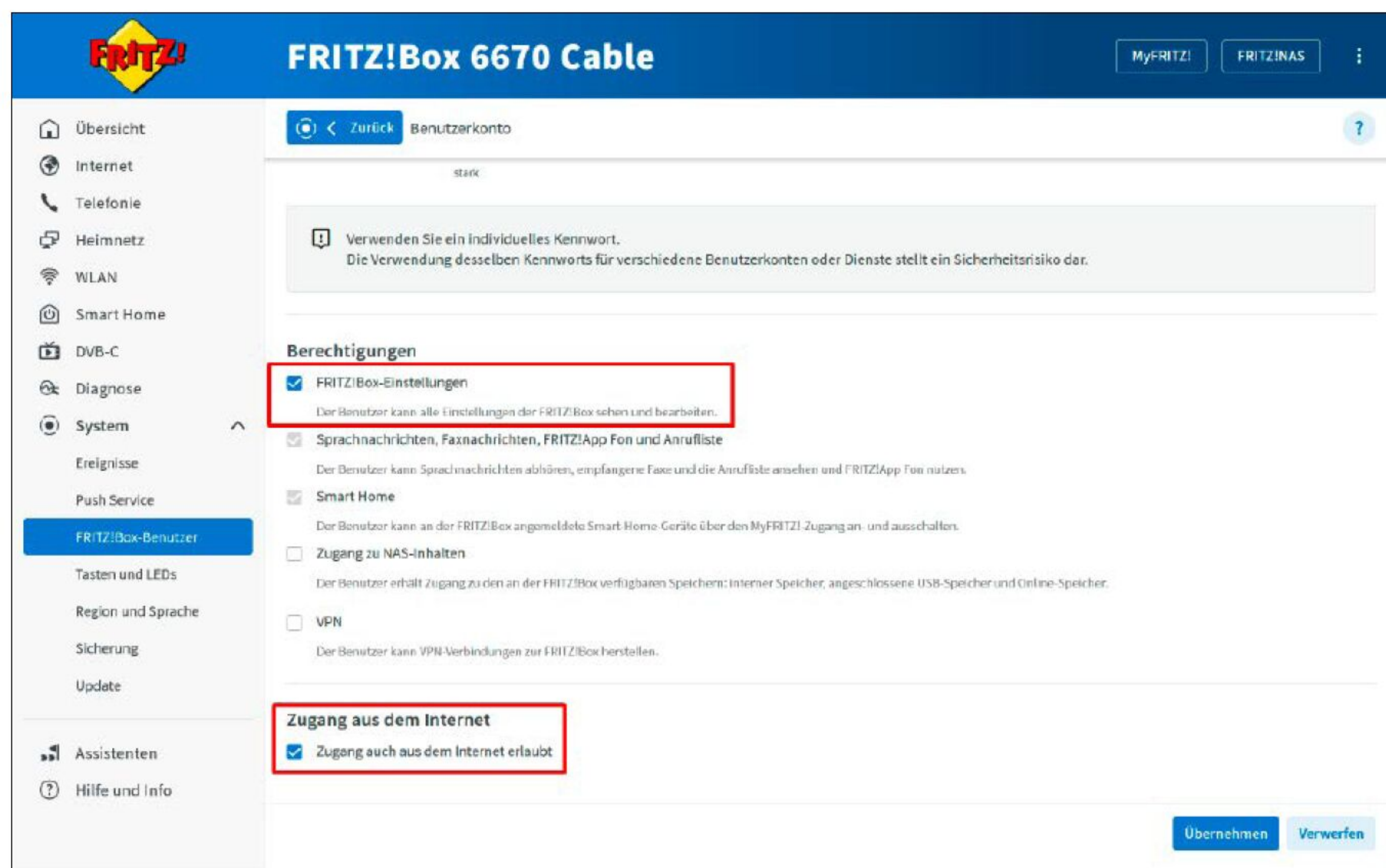
Zugriffsport im Routermenü ändern lässt, hängt vom Gerät ab – bei Fritzbox-Router ist dies möglich.

Außerdem sollte der Fernzugriff über das verschlüsselte HTTPS-Protokoll erfolgen. Hilfreich ist auch, wenn der Router den Zugriff auf das Menü erschwert oder sperrt, wenn ein falsches Kennwort eingegeben wurde – so lassen sich Brute-Force-Attacken verhindern, bei denen der Angreifer in kurzer Zeit verschiedene Zugangskennwörter ausprobiert. Eine weitere Sicherheitsfunktion: Der Router lässt den Fernzugriff nur über ein dafür eingerichtetes Benutzerkonto zu.

Eine Fritzbox erfüllt all diese Voraussetzungen, sodass Sie damit einen sicheren



Wenn Sie die MyFritz-Direktverbindung aktivieren, können Sie diese Fritzbox komfortabel über die Geräteübersicht des MyFritz.net-Kontos verwalten.



Diese Berechtigungen benötigen Sie für das Fernzugriffs-Benutzerkonto auf das Fritzbox-Webmenü.

Fernzugriff für die externe Wartung anlegen können.

So kommen Sie bei einem entfernten Router ins Menü

Um einen Fernzugriff auf einen externen Router einzurichten, melden Sie diesen als Erstes bei einem DynDNS-Dienst an. Bei einer Fritzbox erledigen Sie das über ein MyFritz-Konto: Gehen Sie im Menü der Fritzbox des Hilfesuchenden zu „Internet →

MyFritz-Konto“ und melden Sie sich über eine E-Mail-Adresse für den Fritz-Dienst an. Da Sie die Fernwartung dieses Routers übernehmen sollen, nutzen Sie dafür am besten Ihre eigene Mailadresse.

Haben Sie bereits für die eigene Fritzbox ein MyFritz-Konto angelegt, können Sie die externe Fritzbox ebenfalls dort registrieren, damit Sie sie bei Problemen über den gewohnten MyFritz-Zugang erreichen können.

Nach der erfolgreichen Registrierung bei MyFritz gehen Sie ins Menü zu „Internet → Freigaben → Fritzbox-Dienste“. Versehen Sie dort die Option „Internetzugriff auf die Fritzbox über HTTPS aktiviert“ mit einem Haken. Der Router vergibt nun einen individuellen, fünfstelligen Port für den Fernzugriff und zeigt Ihnen die vollständige Webadresse, über die die externe Fritzbox ab jetzt erreichbar ist. Klicken Sie auf „Übernehmen“.

Anschließend gehen Sie im Menü zu „Internet → MyFritz-Konto“. Hier sollte inzwischen die Meldung „Ihre Fritzbox ist bei MyFritz angemeldet“ erscheinen. Scrollen Sie zum Abschnitt „MyFritz-Direktverbindung“ und setzen Sie einen Haken vor „MyFritz-Direktverbindung aktiv“. Damit können Sie diese Fritzbox später direkt über die MyFritz.net-Oberfläche ansteuern und erhalten vorab wichtige Status-Infos zu diesem Router.

Empfehlenswert ist es, die Option „Zertifikat von letsencrypt verwenden“ zu aktivieren. Damit vermeiden Sie eine Warnmeldung des Browsers, wenn Sie zum ersten Mal aus der Ferne per HTTPS auf diese Fritzbox zugreifen. Speichern Sie alle Einstellungen mit „Übernehmen“.

Spezielles Benutzerkonto für den Fernzugriff anlegen

Anschließend legen Sie unter „System → Fritzbox-Benutzer → Benutzer“ einen neuen Benutzer für den Fernzugriff an. Dazu klicken Sie auf „Benutzer hinzufügen“ und vergeben neben einem Benutzernamen ein starkes Kennwort mit mindestens zwölf Stellen, das neben Klein- und Großbuchstaben auch Ziffern enthalten sollte. Notieren Sie sich beides auf einem Zettel oder verwenden Sie einen Passwortsafe.

Aktivieren Sie nun für dieses Benutzerkonto die Berechtigungen „Fritzbox-Einstellungen“ und „Fernzugriff auch aus dem Internet erlaubt“. Sobald der neue Benutzer mit „Übernehmen“ angelegt ist, können Sie von überall aus dem Internet via Browser direkt auf das Webmenü dieser Fritzbox zugreifen. Rufen Sie die vollständige Fernzugriffsadresse im Browser Ihres Notebooks auf und speichern Sie diese als Lesezeichen. Alternativ lässt sich die Ziel-Fritzbox über die MyFritz.net-Oberfläche aufrufen. Dazu melden Sie sich unter www.myfritz.net am Konto an, unter dem Sie die Fritzbox zuvor registriert haben. Das Gerät erscheint in

der Geräteübersicht und sollte mit „Direktverbindung zu MyFritzNet“ gekennzeichnet sein. Wenn Sie den Mauszeiger auf den Namen der Fritzbox bewegen, wird Ihnen der MyFritz-Link samt Portnummer angezeigt. Ein Klick darauf stellt die Verbindung zum Menü dieses Routers her. Anschließend geben Sie die Zugangsdaten des zuvor angelegten Fernzugriffs-Benutzers ein – und schon befinden Sie sich im Webmenü des Zielrouters.

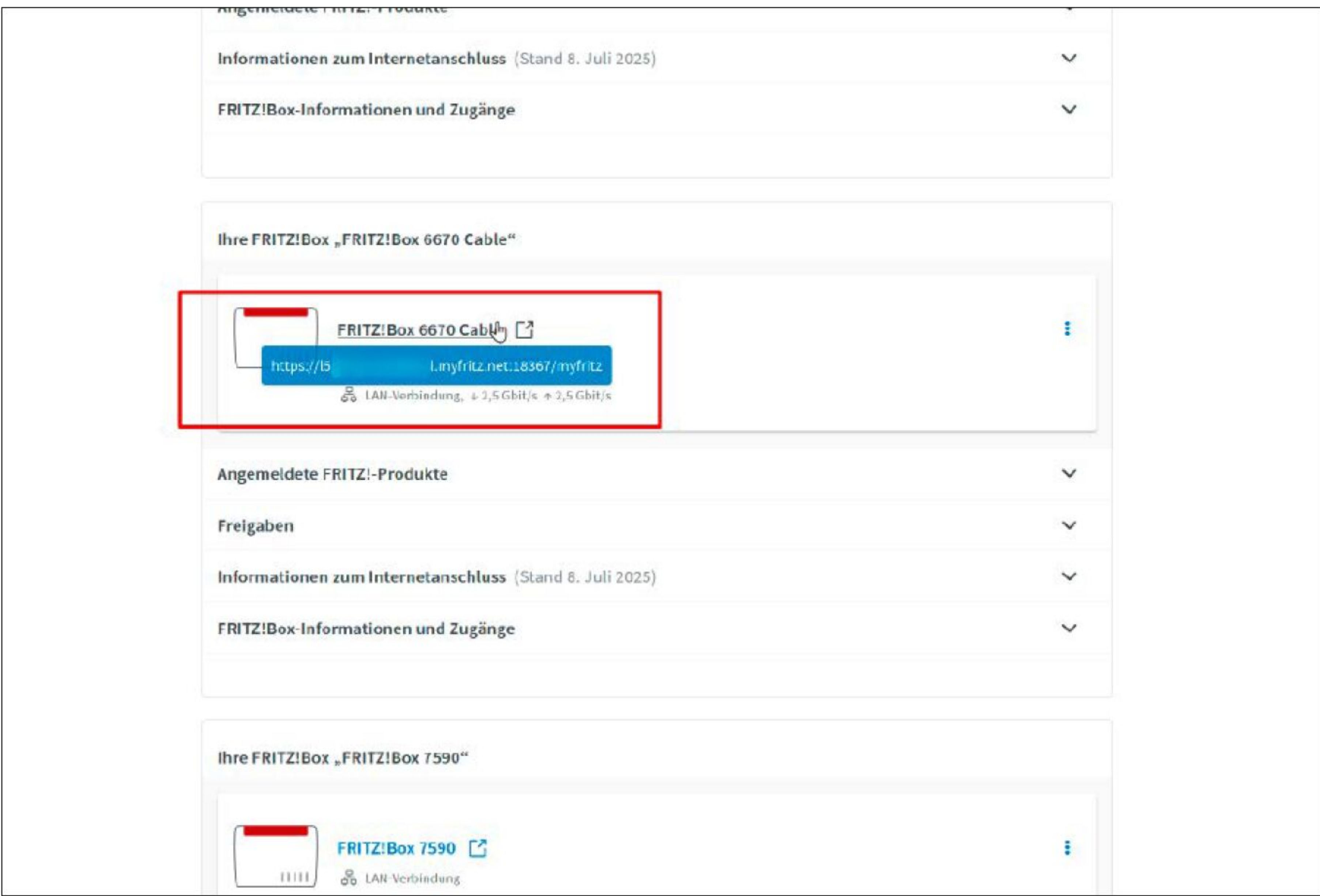
Für zusätzliches Vertrauen beim Besitzer der externen Fritzbox zeigen Sie ihm am besten, wie er das neu angelegte Benutzerkonto nach dem Eingriff deaktivieren kann. Das funktioniert unter „System → Fritzbox-Benutzer → Benutzer“, indem nach einem Klick auf das Bearbeiten-Symbol (Stift) des Benutzerkontos der Haken vor „Benutzerkonto aktiv“ entfernt und auf „Übernehmen“ geklickt wird. Das Konto erscheint nun als inaktiv, und es ist kein Fernzugriff mehr möglich. Bei einer erneuten Bitte um Problemlösung muss das entsprechende Konto aber wieder aktiviert werden.

Verschlüsselte Verbindung: Sicherer Fernzugriff per VPN

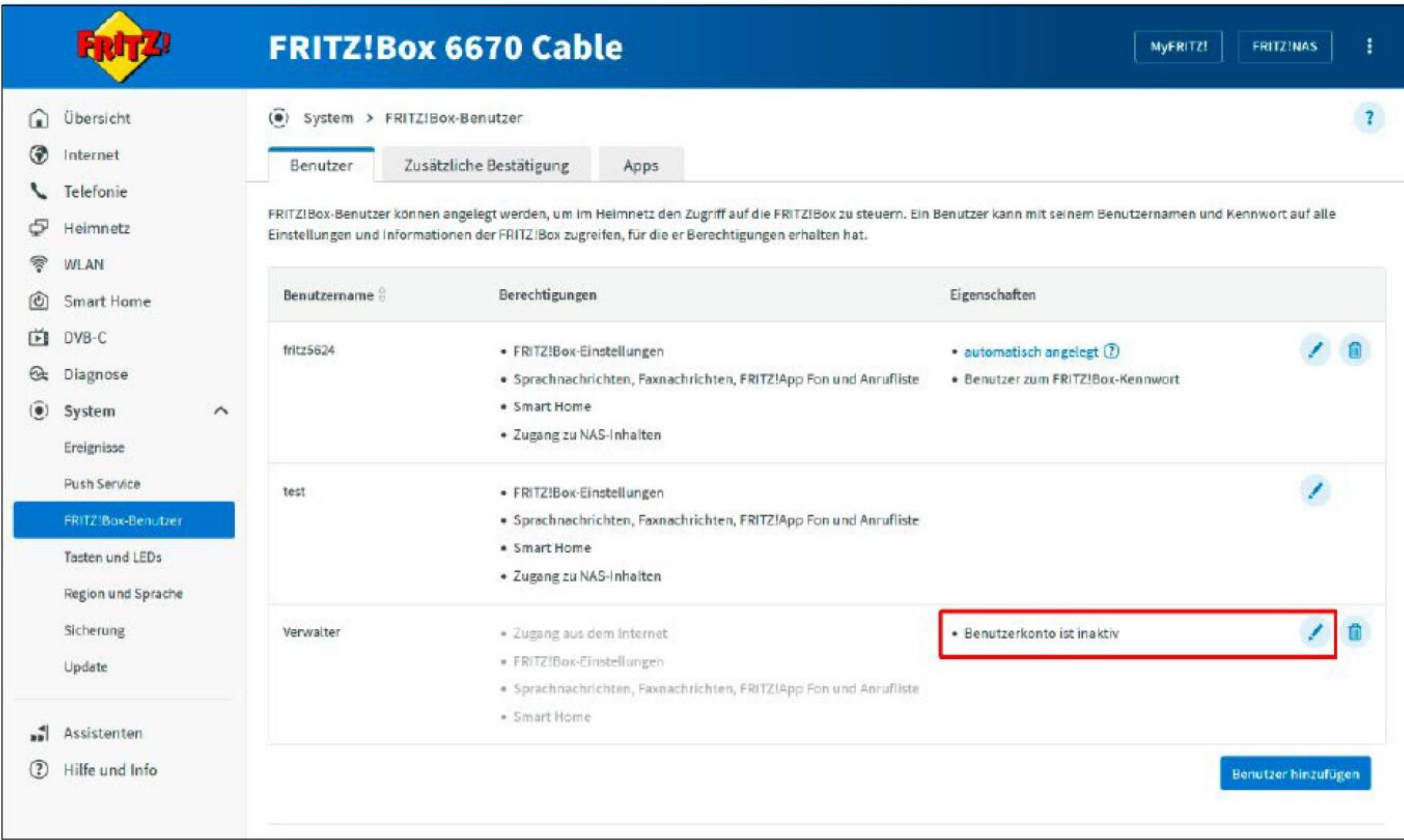
Über eine VPN-Verbindung zu einem Router erreichen Sie nicht nur dessen Menü, sondern alle mit ihm verbundenen Geräte im entfernten Netzwerk. So können Sie Familie und Freunden auch bei Problemen mit Notebook, NAS, Internetkamera und anderen Netzwerkgeräten helfen.

Den VPN-Zugang sollten Sie ebenfalls direkt vor Ort im lokalen Netzwerk des Routers anlegen, den Sie später per VPN erreichen wollen. Nutzen Sie für die erste Konfiguration am besten das Notebook, mit dem Sie später aus der Ferne über VPN zugreifen möchten.

Um das VPN einzurichten, muss eine Fritzbox bei einem MyFritz-Konto angemeldet sein wie oben beschrieben. Anschließend können Sie im Menü der Fritzbox unter „Internet → Freigaben → VPN (WireGuard)“ mit „Verbindung hinzufügen“ eine Wireguard-VPN-Verbindung einrichten. Wählen Sie hierfür „Einzelgerät verbinden“, tragen Sie den Namen Ihres VPN-Clients ein, und laden Sie sich schließlich die VPN-Einstellungen in der Datei „wg.config.conf“ auf Ihr Notebook. Danach installieren Sie die kostenlose **Wireguard**-Software von www.wireguard.com auf dem Notebook und importieren dort die Datei „wg.config.conf“



In der Geräteübersicht im MyFritz-Konto finden Sie die Webadresse der Fritzbox, die Sie mit diesem Fritz-Dienst verbunden haben: Damit erhalten Sie direkten Zugriff auf das Webmenü des Routers.



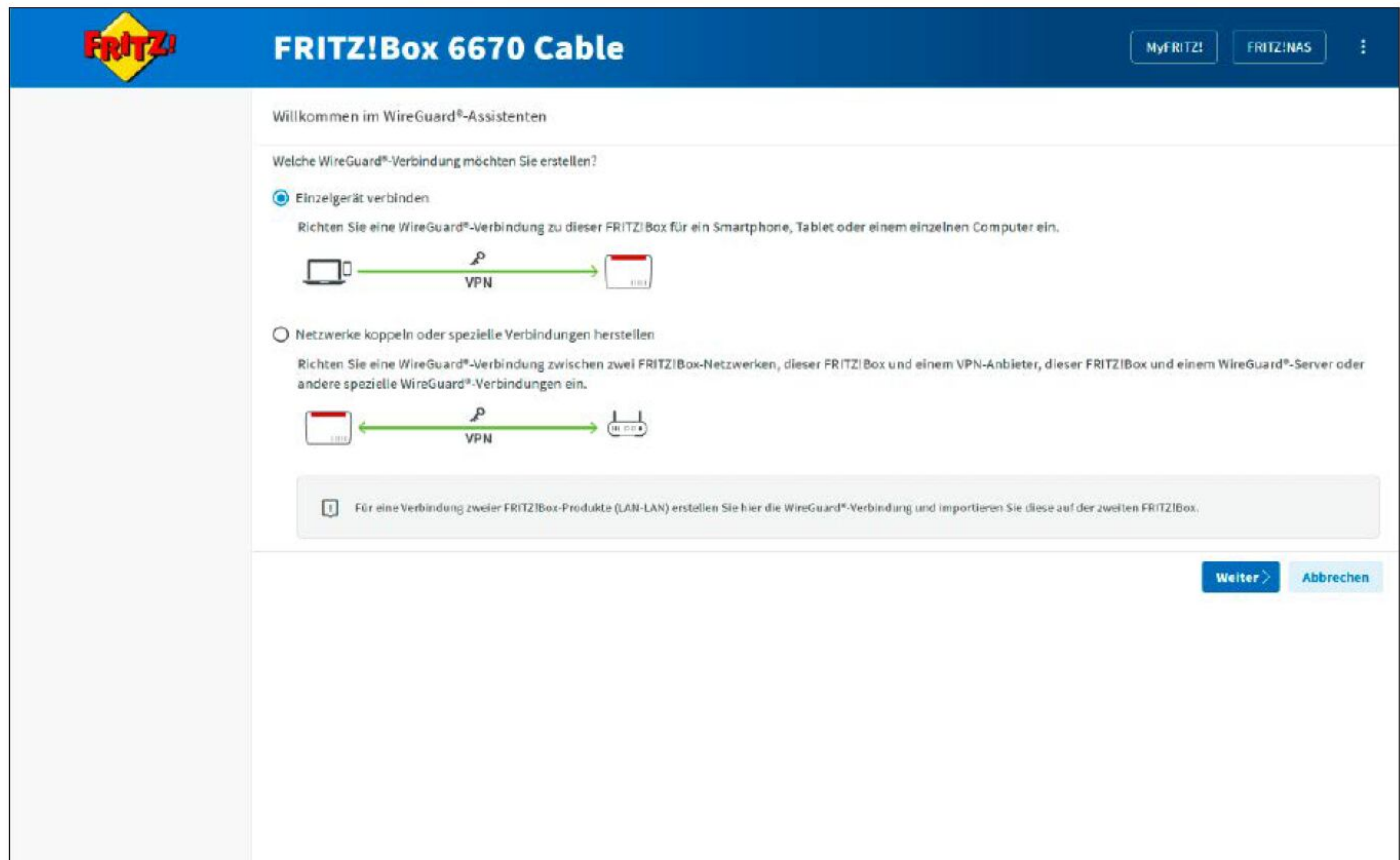
Bei Sorgen um die Privatsphäre kann der Hilfesuchende das Benutzerkonto für den Fernzugriff abschalten. Es muss allerdings wieder aktiviert werden, wenn er erneut externe Unterstützung bei Netzwerkproblemen braucht.

mit „Tunnel hinzufügen“. Der Nachteil des VPN-Fernzugriffs ist, dass Sie für jedes Gerät, mit dem Sie auf den externen Router zugreifen wollen, eine eigene VPN-Verbindung einrichten müssen. Der Hilfesuchende kann im Menü „Übersicht“ seiner Fritzbox unter „Verbindungen und Anschlüsse“ immer sehen, ob ein eingerichteter „Fernzugang“ gerade verwendet wird – er ist dann mit einem grünen Punkt markiert. Auch ein VPN-Fernzugang lässt sich vorübergehend deaktivieren, wenn er nicht gebraucht wird oder nicht heimlich ge-

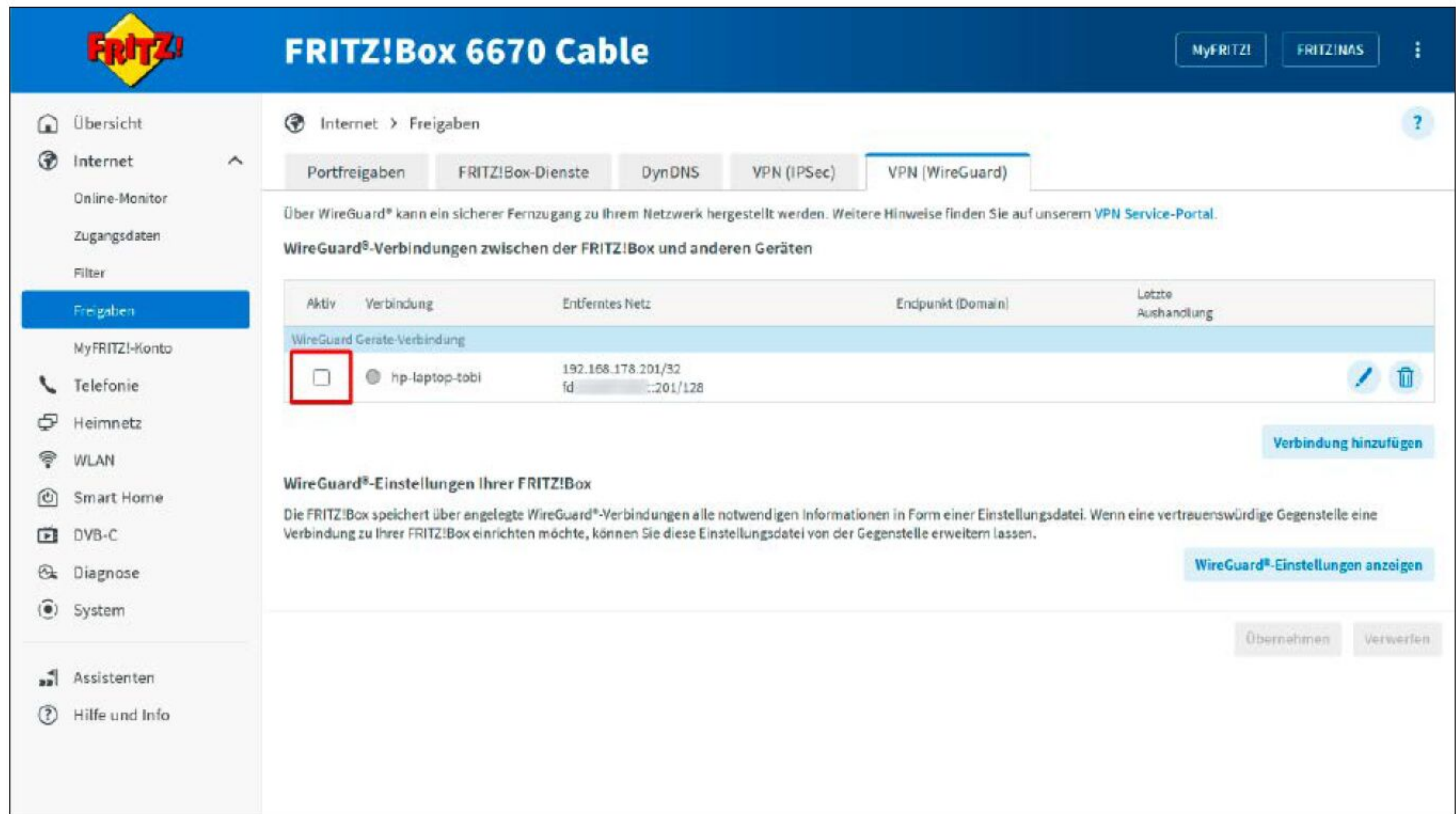
nutzt werden soll: Dazu wird unter „Internet → Freigaben → VPN (WireGuard)“ das Häkchen vor der entsprechenden „WireGuard Geräte-Verbindung“ entfernt und mit „Übernehmen“ gespeichert. Nun verschwindet der Eintrag „Fernzugang“ aus dem „Übersicht“-Menü der Fritzbox.

Cleverer Umweg: So erreichen Sie den Router per Teamviewer

Als Alternative zum direkten Zugriff auf den Router bietet sich bei Heimnetzproblemen der Zugriff auf einen Rechner an, der mit dem Router verbunden ist. Wenn



Eine VPN-Verbindung per Wireguard können Sie in der Fritzbox sehr schnell einrichten. Dafür muss der Router allerdings zuvor beim DynDNS-Dienst MyFritz von Fritz angemeldet worden sein.



Statt eine eingerichtete VPN-Verbindung zu löschen, nachdem ein Problem behoben wurde, lässt sie sich im Menü der Fritzbox ausschalten, solange keine Hilfe mehr benötigt wird.

Sie diesen fernsteuern, können Sie bequem den Router und andere Netzwerkgeräte erreichen und einstellen. Der Vorteil für den Hilfesuchenden: Er kann an seinem PC direkt mitverfolgen, was Sie gerade im Heimnetz machen, und die Verbindung auch jederzeit unterbrechen. Ein empfehlenswertes Tool für dieses Verfahren ist das für private Nutzung kostenlose Teamviewer (www.teamviewer.com/de). Sie finden den Download auf der Webseite unter „Lösungen → Nach Rollen → Privater Gebrauch“ und „Jetzt herunterladen“. Im folgenden Fenster können Sie die Windows-Version herunterladen. Für den Fernzugriff müssen Sie noch ein kostenloses Konto bei Teamviewer einrichten. Auch die Person,

der Sie Hilfe leisten wollen, muss Teamviewer auf einem Rechner installieren. Nach Installation und Start des Tools erscheint ein zweigeteiltes Programmfenster: Der rechte, weiß hinterlegte Bereich ist für den Hilfesuchenden gedacht. Für Sie ist zunächst nur der linke, dunkelblau hinterlegte Bereich interessant, der Sie auffordert, sich bei Teamviewer anzumelden – dafür verwenden Sie die Zugangsdaten des zuvor angelegten Kontos. Dabei erhalten Sie eventuell eine Bestätigungsanfrage per Mail, mit der Sie Ihr aktuelles Gerät als vertrauenswürdigen Teamviewer-Client bestätigen sollen. Um eine Fernverbindung zum externen PC herzustellen, gehen Sie im Hauptfenster

des Tools unter „Aktionen“ auf die Option „Session erstellen“. Im Fenster „Session-Name“ gehen Sie auf „Einladung senden“ und geben dort unter „E-Mail des End-Users“ die E-Mail-Adresse des Hilfesuchenden ein. Klicken Sie auf „Einladen und starten“. Der Hilfesuchende erhält eine Benachrichtigung per Mail mit einem Link zur Sitzungsteilnahme. In seinem Teamviewer-Fenster erscheint dann zunächst eine Verifizierungsanfrage. Per Klick auf „Benutzer verifizieren“ erhält der Hilfesuchende die Infos des Hilfeleistenden wie E-Mail-Adresse und Name und kann anschließend den „Zugriff erlauben“. Anschließend sehen Sie im Teamviewer-Fenster auf Ihrem Notebook den Desktop des entfernten Rechners. Der Hilfesuchende kann währenddessen Ihre Handlungen auf seinem Rechner verfolgen. Ein großer Vorteil dieses Verfahrens: Es funktioniert unabhängig vom Router, der im externen Netzwerk steht, weil Sie ihn wie in einem lokalen Netzwerk über das Browsermenü bedienen – Einstellungen für Ports oder VPN sind deshalb nicht notwendig.

Das können Sie tun, wenn der andere Router offline ist

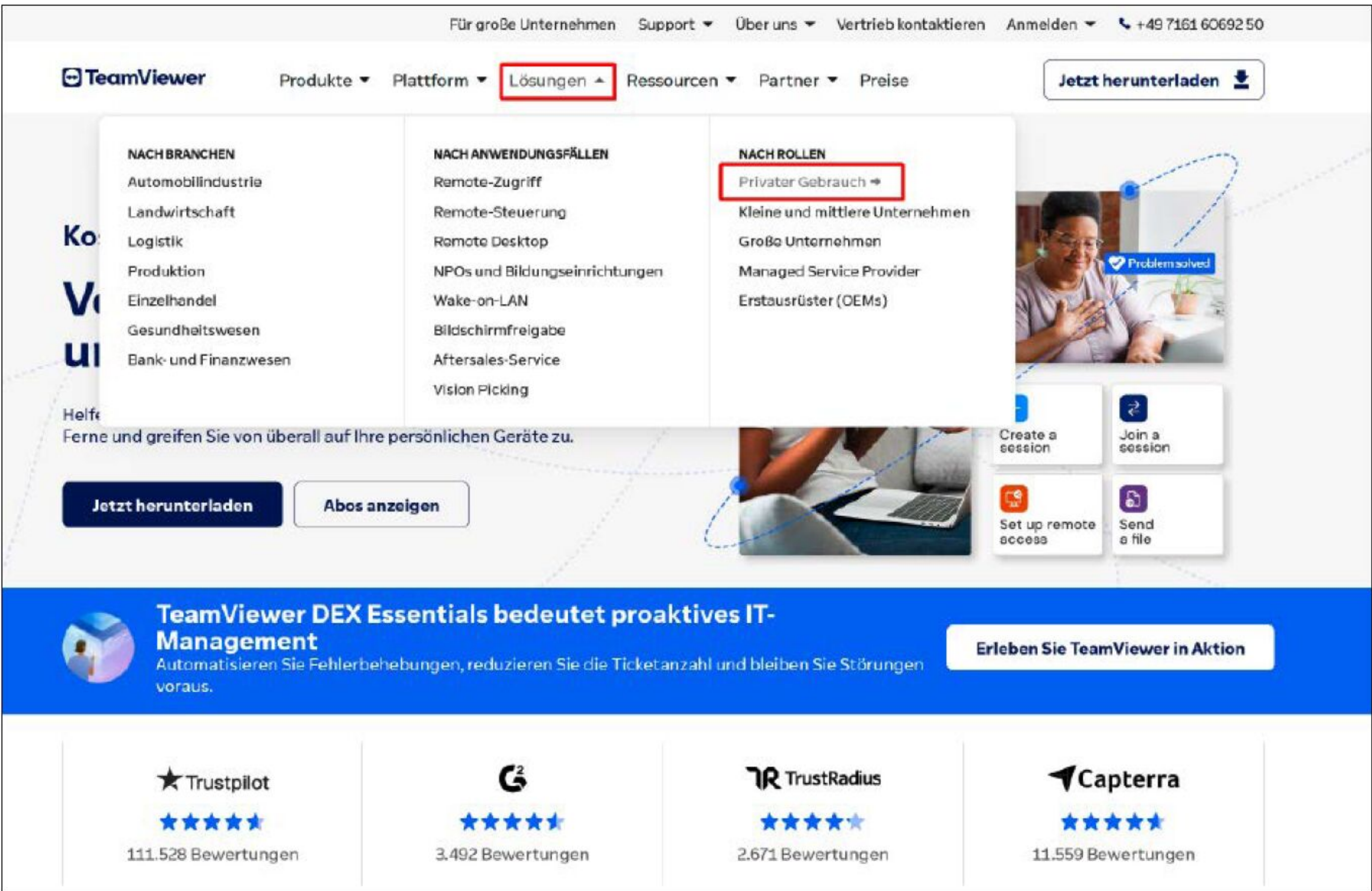
Falls der externe Router nicht mit dem Internet verbunden ist, funktioniert keine der vorgestellten Methoden zum Fernzugriff. Da der Router offline ist, lässt er sich nicht über einen geöffneten Port oder eine VPN-Verbindung erreichen. Auch der Weg über Teamviewer wird nicht funktionieren, da infolge des Routerausfalls auch der dafür notwendige Rechner im entfernten Netzwerk keine Internetverbindung herstellen kann. In diesem Fall lässt sich eine Verbindung zum Router per Mobilfunk herstellen. Dazu nutzt der Hilfesuchende sein Smartphone als WLAN-Hotspot, um seinen Rechner darüber online zu bringen. Der Rechner muss aber über einen weiteren Netzwerkadapter wie eine Ethernet-Schnittstelle verfügen, über den er mit dem Router verbunden werden kann. Treffen diese Voraussetzungen zu, muss der Hilfesuchende sein Smartphone in den WLAN-Hotspot-Modus schalten. Das Smartphone ist dann per Mobilfunk mit dem Internet verbunden und stellt diesen Zugang per WLAN anderen Geräten bereit. Ein Rechner des Hilfesuchenden

muss sich mit dem WLAN-Hotspot des Smartphones verbinden, indem die passende SSID ausgewählt und das entsprechende Kennwort eingegeben wird. Jetzt ist der Rechner online – Sie können nun per Teamviewer wie beschrieben die Einladung zu einer Session übermitteln und anschließend eine direkte Verbindung zwischen Ihrem und dem externen Rechner herstellen.

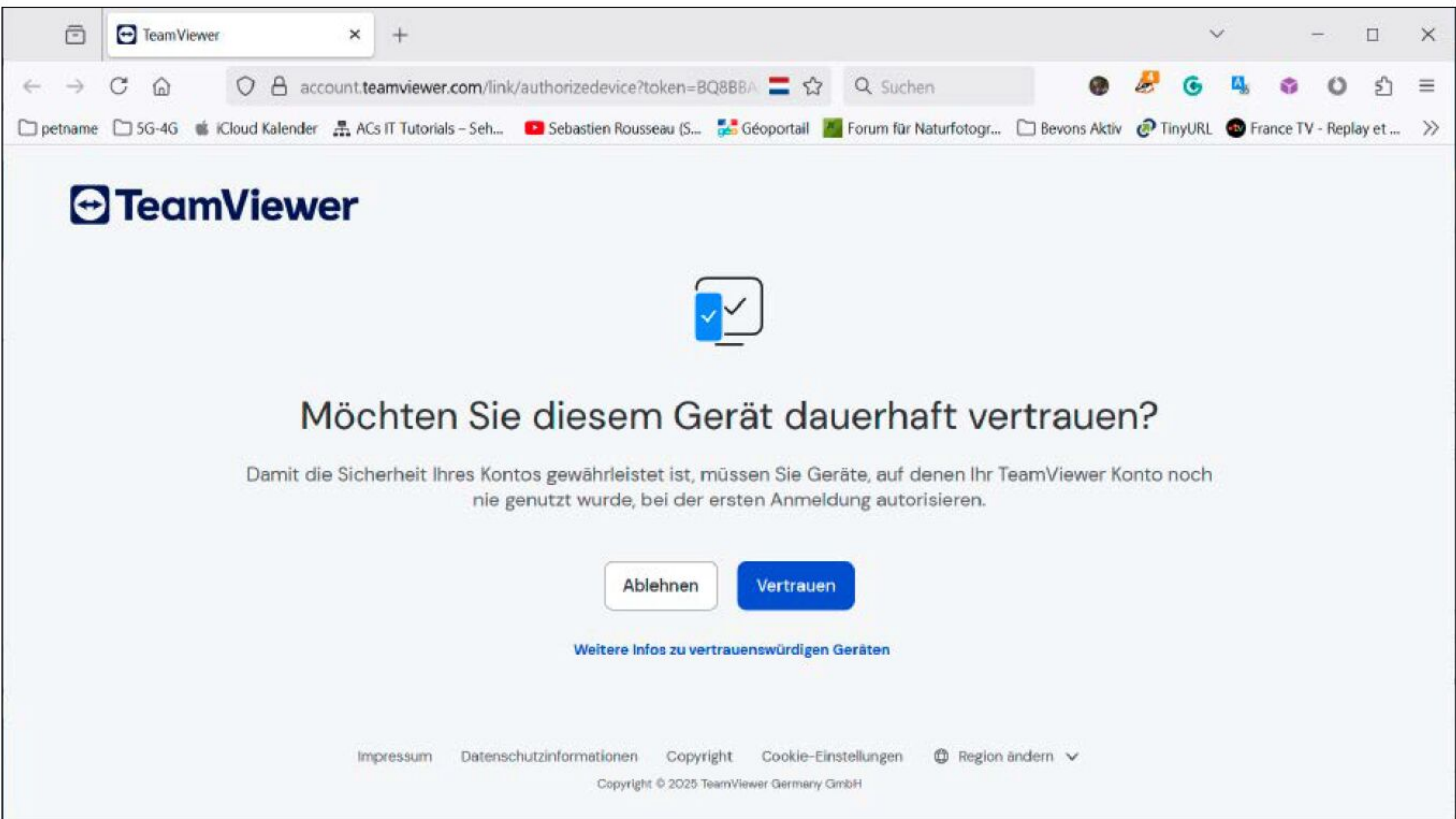
Steht die Teamviewer-Verbindung, muss der Hilfesuchende seinen PC per Ethernet-Kabel mit einem freien LAN-Port seines Routers verbinden. Damit ist eine durchgehende Verbindung von Ihrem PC bis zum externen Router hergestellt: Sie können jetzt das Menü des Routers aufrufen und mit der Problemlösung beginnen. Grundsätzlich lässt sich bei vielen Smartphones die mobile Internetverbindung auch per USB-Kabel an einen Rechner weiterreichen. Dann könnte sich der Rechner wie gewohnt per WLAN mit dem Router im Heimnetz verbinden. Unserer Erfahrung nach arbeitet dieses sogenannte USB-Tethering aber nicht zuverlässig, da die Verbindung häufig abbricht. Daher ist es keine optimale Lösung für externe Hilfe bei Netzwerkproblemen.

Schnelle Hilfe übers Internet bei Netzwerkproblemen

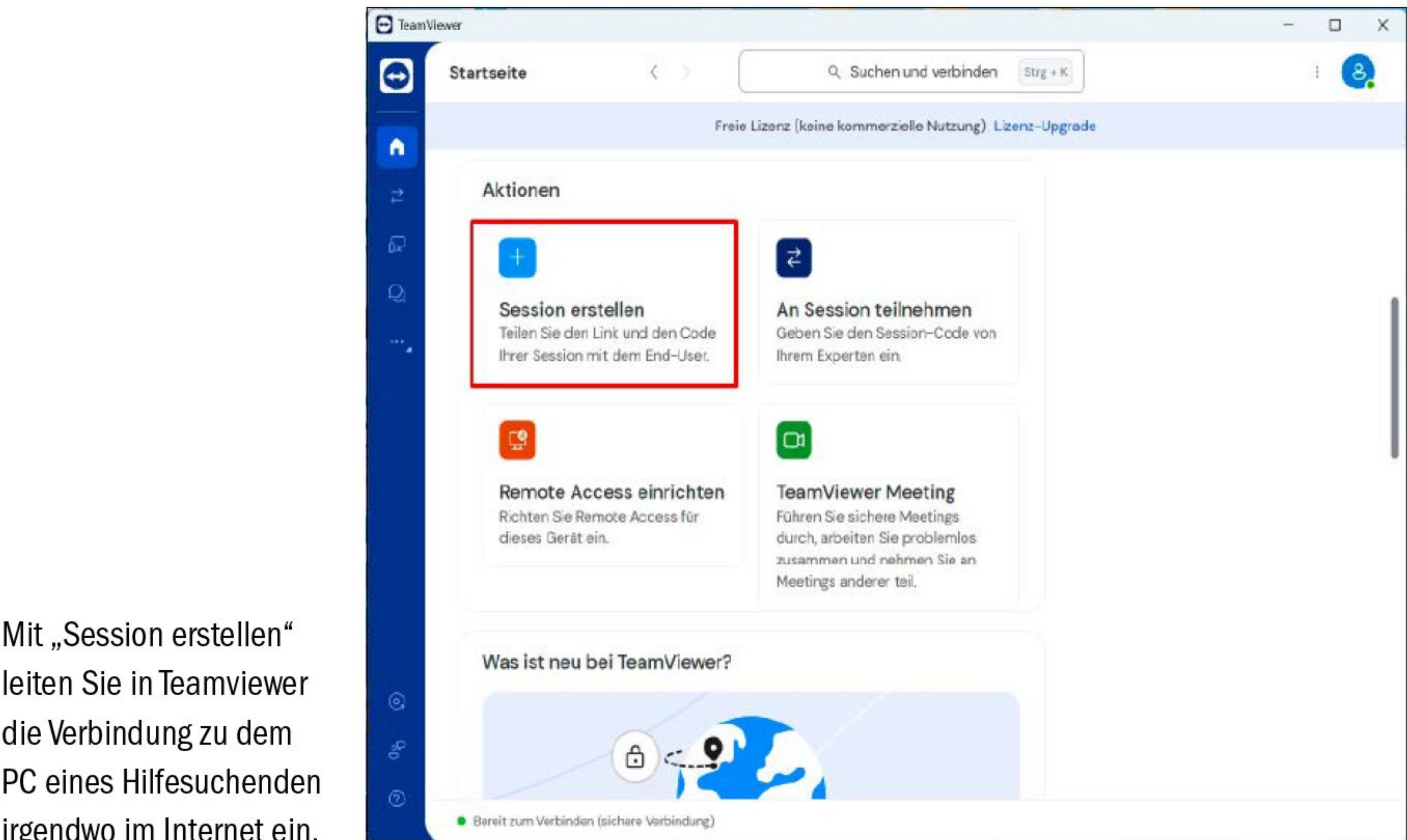
Alle Fernzugriffsmethoden sind sehr sicher, wenn Sie die für den Web-/VPN-Zugriff beschriebenen Sicherheitsvorkehrungen beachten – und wenn es sich beim Zielrouter um eine Fritzbox handelt. Welche die Beste ist, hängt vor allem davon ab, welches Problem gelöst werden muss: Geht es um eine instabile Internet- oder WLAN-Verbindung, genügt meist der Fernzugriff auf das Routermenü, über den sich die passenden Einstellungen ändern lassen. Erstreckt sich das Problem auch auf andere Netzwerkgeräte, ist der Zugriff per VPN ratsam. Beide Zugriffsmethoden sind schnell, Sie müssen sie aber vorab am Zielrouter einrichten. Ohne umfassende Vorarbeit funktioniert der Zugriff per Teamviewer – sofern der Hilfesuchende das Tool auf seinem Rechner installieren und einrichten kann. Außerdem muss der externe Rechner eingeschaltet sein – und die Fernsteuerung des eigenen PCs kann das Gefühl für die eigene Privatsphäre empfindlicher stören als der direkte Zugriff auf den Router. ■



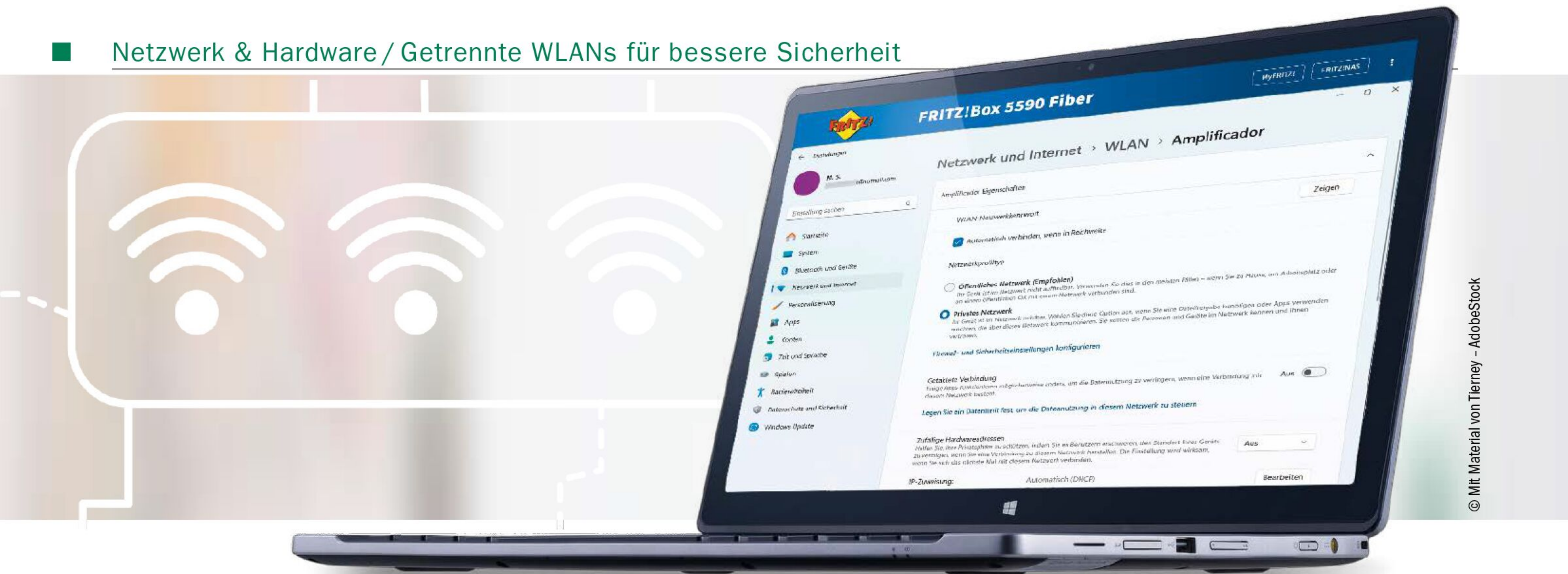
Hier können Sie die für die Privatnutzung kostenlose Teamviewer-Software herunterladen.



Vor der Nutzung verlangt Teamviewer zahlreiche Sicherheitsbestätigungen: Das ist bei einem konkreten Problemfall nervig, geht aus Sicherheitsgründen bei einem Fernzugriffstool aber absolut in Ordnung.



Mit „Session erstellen“ leiten Sie in Teamviewer die Verbindung zu dem PC eines Hilfesuchenden irgendwo im Internet ein.



© Mit Material von Tierney - AdobeStock

Getrennte WLANs für bessere Sicherheit

Aktuelle Router können mehrere WLAN-Netze aufbauen. Damit lässt sich zum Beispiel das Tempo bei der Datenübertragung verbessern. Aber vor allem stärken Sie damit den Schutz des Heimnetzes: Indem Sie Clients in verschiedenen, voneinander getrennten Netzen unterbringen, verhindern Sie, dass eine Sicherheitslücke bei einem Gerät alle anderen gefährdet. Wir zeigen, wie das bei Fritzbox & Co. funktioniert.

VON MICHAEL SEEMANN

Wahrscheinlich nutzen Sie bereits getrennte WLANs – wenn auch nicht unbedingt aus Sicherheitsgründen: Denn eine Standardfunktion in den meisten Heimnetzroutern aller Hersteller ist der WLAN-Gastzugang. Und dieses Gastnetz ist strikt vom privaten WLAN-Heimnetz getrennt, sodass Geräte, die dort angemeldet sind, zwar online gehen können, aber keinen Zugriff auf Ihr WLAN haben, wo sich das NAS mit Ihrer Fotosammlung oder der PC mit privaten Unterlagen befinden. Auch das Menü des Routers ist per Gastzugang nicht erreichbar.

„Bei der WLAN-Trennung können andere Router mehr als die Fritzbox.“

Wenn Sie den WLAN-Gastzugang aktivieren, können Sie Freunden und Bekannten einen kostenlosen Internetzugang bereitstellen, der sich zudem mit separaten Anmeldedaten versehen lässt. So müssen Sie nicht das Kennwort für das eigene WLAN weitergeben.

Doch auch, wenn Sie keinen Besuch haben, lohnt es sich, WLANs zu Hause zu trennen: Denn neben PC, Notebook, Smartphone oder Drucker sind inzwischen oft auch Smart-Home-Geräte, Saugroboter, Kühlschränke, Photovoltaikanlagen oder Wetterstationen im Netzwerk aktiv. Viele dieser Geräte steuern Sie nicht direkt über das lokale Netzwerk, sondern über einen Clouddienst des Herstellers. Das ist einerseits vorteilhaft, weil Sie sie dadurch auch erreichen, wenn Sie unterwegs sind: Sie nehmen dann Einstellungen per App am Smartphone vor.

Andererseits genießen viele dieser Geräte nicht den besten Ruf, wenn es um Sicherheit geht: Häufig stopfen die Hersteller Sicher-

heitslücken spät oder überhaupt nicht. Ohne ein Firmwareupdate, das den Schutz wiederherstellt, können Angreifer problemlos diese Geräte übernehmen und für eine Attacke auf das gesamte Heimnetz nutzen. Deshalb sollten Sie vor allem solche Geräte in einem separaten, vom Heimnetz getrennten Netzwerk unterbringen und sie wie WLAN-Gäste behandeln. Je nach Routermodell lässt sich auch für diesen Zweck das Besuchernetz nutzen. Manche Router erlauben auch, mehr als nur zwei voneinander getrennte Gastnetzwerke einzurichten, oder ermöglichen es sogar, so viele Teilnetze anzulegen, wie Sie benötigen – sogar für Geräte, die nur über einen LAN-Anschluss verfügen. Wir zeigen, wie das bei der Fritzbox funktioniert und welche Alternativen es gibt.

Fritzbox-Gastzugang: So erhöhen Sie seine Sicherheit

In allen Fritzbox- Routern lässt sich ein WLAN-Gastnetz aktivieren. Gehen Sie dazu

im Routermenü zu „WLAN → Gastzugang“. Wenn sich Clients in diesem Netz anmelden, können sie Geräte, die mit dem Haupt-WLAN verbunden sind, nicht mehr erreichen. Dementsprechend sollten Sie für das Gastnetz andere WLAN-Zugangsdaten vergeben. Sie können den Gastzugang aber auch als öffentlichen WLAN-Hotspot ohne Passwortabfrage betreiben, für den Sie keine Zugangsdaten weitergeben müssen. Dann empfiehlt es sich, im Fritzbox-Menü unter „Weitere Einstellungen“ die Funktion „Internetanwendungen beschränken“ auszuwählen, sodass Gäste nur surfen und mailen können.

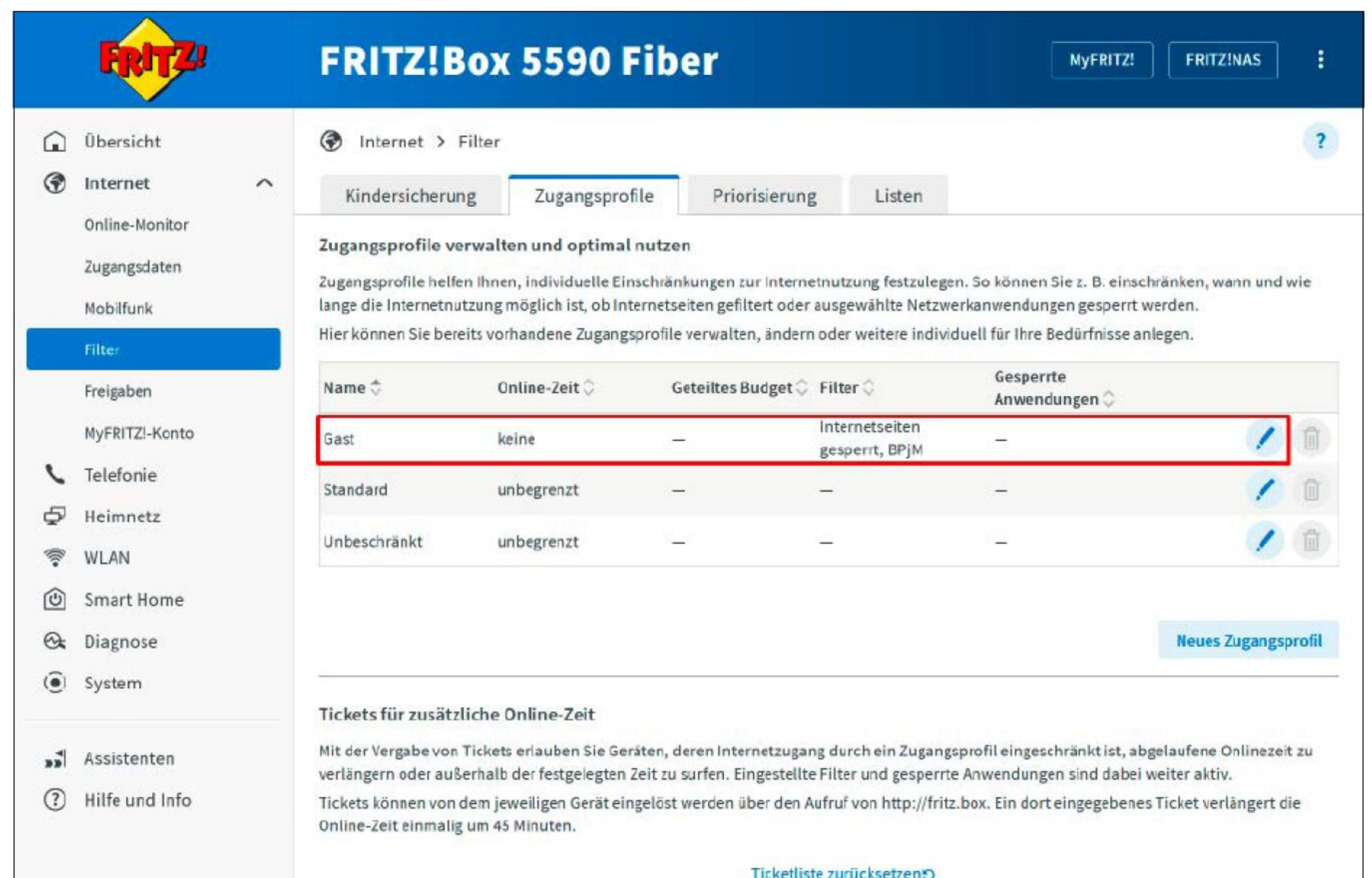
Alle Geräte im Gastnetz nutzen das entsprechende Fritzbox-Profil „Gast“. Es lässt sich unter „Internet → Filter → Zugangsprofile“ anpassen und mit weiteren Filtern und Einschränkungen versehen.

Sie können zum Beispiel anhand eines wöchentlichen Zeitplaners komfortabel festlegen, für welchen Zeitraum die Internetnutzung im Gastzugang erlaubt ist. Wenn Sie das BPjM-Modul aktivieren, sperren Sie viele jugendgefährdende Webinhalte, die die dort angemeldeten Geräte nicht mehr aufrufen können.

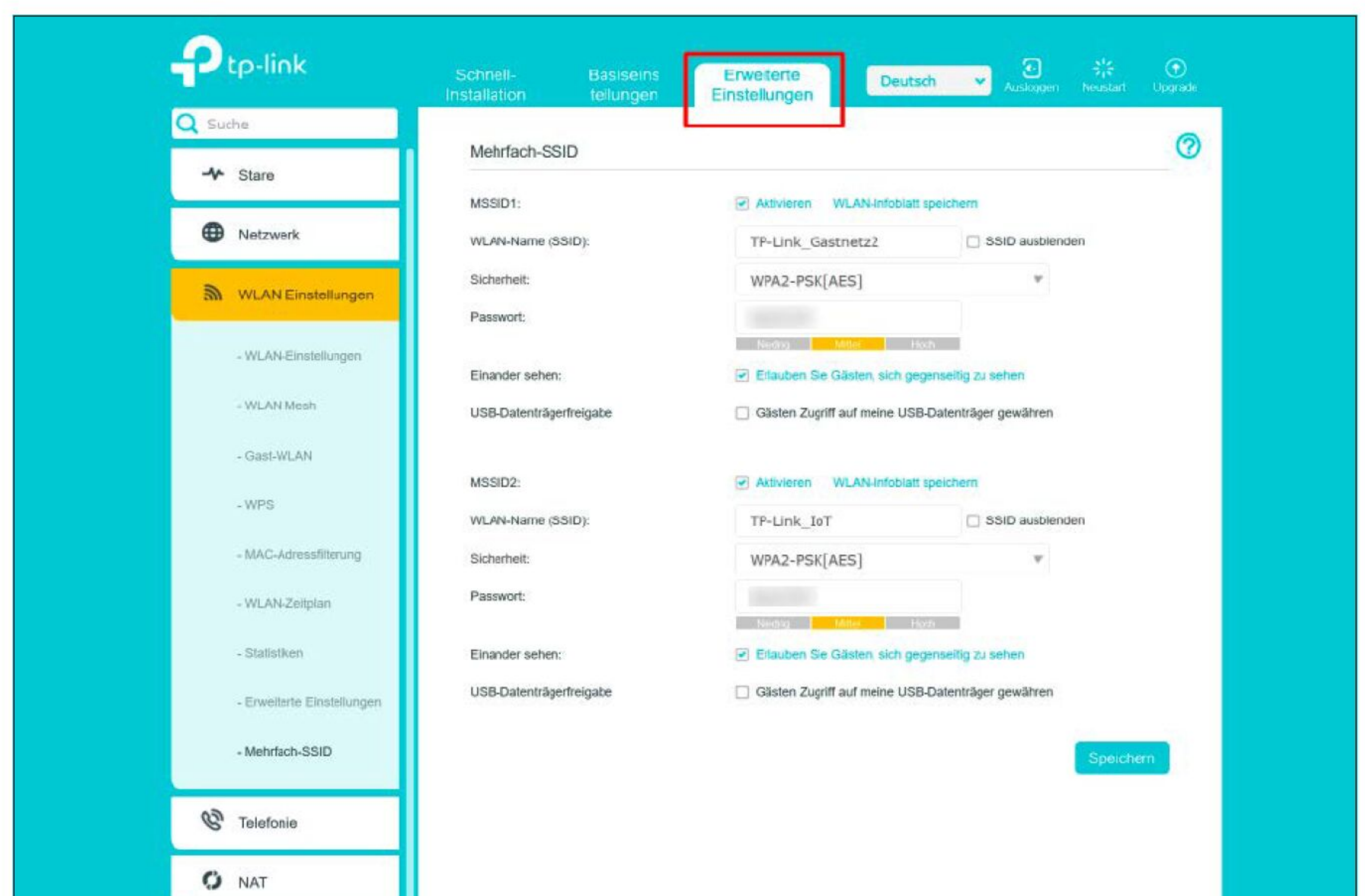
In den meisten Fritzbox-Modellen lassen sich zudem LAN-Geräte in den Gastzugang integrieren. Dazu setzen Sie unter „Heimnetz → Netzwerk → Netzwerkeinstellungen“ einen Haken vor „Gastzugang für LAN 4 aktiv“. Ein am LAN-Port 4 der Fritzbox angeschlossenes Gerät befindet sich dann im Gastnetz. Wenn Sie einen Switch anschließen, lassen sich auch mehrere LAN-Geräte so einbinden.

Fritzbox: Beschränkung der Bandbreite im Gastzugang

Damit Geräte im Gastnetz nicht den Onlinezugang Ihrer eigenen Geräte ausbremsen, können Sie die Bandbreite des Internetzugangs für Gäste beschränken. Dazu reservieren Sie einen bestimmten Anteil der verfügbaren Bandbreite für das Hauptnetz. Diese Einstellung findet sich unter „Internet → Filter → Priorisierung“ im Bereich „Geschwindigkeit im Heimnetz“. Wenn Sie hier die Option „Bandbreite für das Heimnetz reservieren“ aktivieren, können Sie mit der Auswahl „feste Reservierung von Bandbreite für das Heimnetz“ die „für das Heimnetz reservierte Bandbreite“ als Prozentwert einstellen. Der WLAN-Gastzugang einer Fritzbox entspricht immer den unter „WLAN → Funkka-



Geräten im Gast-WLAN weist die Fritzbox das Profil „Gast“ zu. Über das Stift-Symbol rufen Sie dessen Einstellungen auf, wo Sie zusätzliche Filter aktivieren können, um die Sicherheit zu verbessern.



Bei einem Router von TP-Link lassen sich mit der Option „Mehrfach-SSIDs“ zusätzliche getrennte WLANs einrichten. Deren SSIDs und Passwörter konfigurieren Sie im Menü „Erweiterte Einstellungen“.

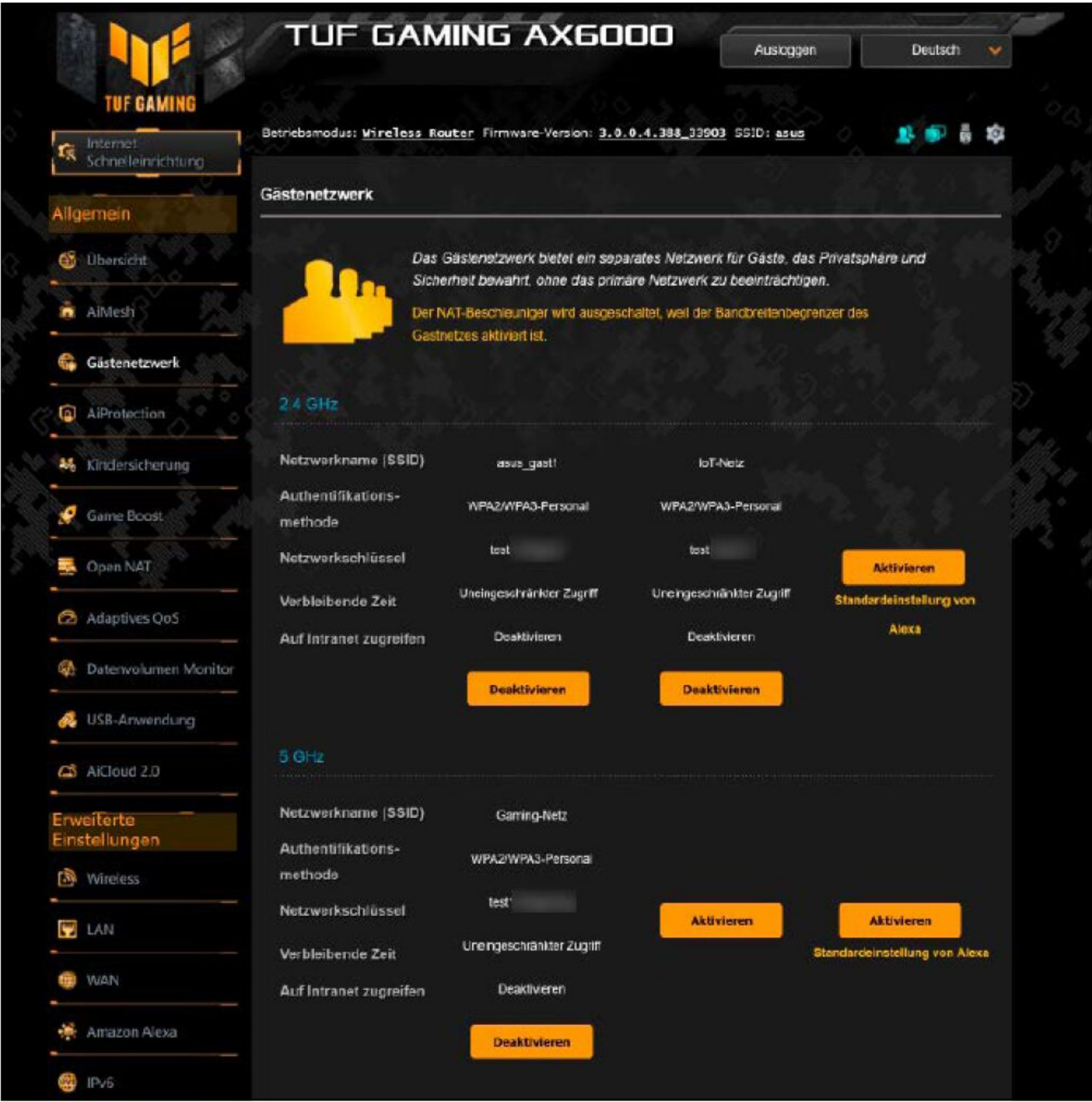
nal“ eingestellten WLAN-Frequenzbändern: Sind beide Frequenzen einer Dualband-Fritzbox aktiviert, ist auch der WLAN-Gastzugang darüber erreichbar. Haben Sie bei der Fritzbox nur das 2,4-GHz-WLAN aktiviert, so können auch Geräte im Gast-WLAN nur diese Frequenz nutzen.

Bei einer Fritzbox gibt es nur einen einzigen Gastzugang. Deshalb lässt sich Ihr WLAN nur in zwei getrennte Netzwerke aufteilen. Wer neben einem Gastnetz noch weitere separate Netzwerke für Smart-Home-Geräte, zusätzliche cloudbasierte Systeme oder

den Untermieter benötigt, muss den Router eines anderen Herstellers nutzen.

Router von TP-Link: Gastzugang für jedes Funkmodul

Mehr Möglichkeiten bieten zum Beispiel Router von TP-Link. Dazu müssen Sie die Grundeinstellungen anpassen. Ab Werk ist bei einem TP-Link-Router wie dem VX231v „Band-Steering“ aktiviert: Die WLAN-Netze der beiden Frequenzen verfügen über dieselben Zugangsdaten, sodass der Router die verbundenen Geräte optimal darauf



Einige Asus-Router wie der TUF Gaming AX6000 bieten bis zu sechs zusätzliche WLAN-Netze an: Hier sind drei bereits angelegt – zwei über 2,4 GHz und eines über die Frequenz 5 GHz.

Frequenz und vom Heimnetz-WLAN getrennt – das ergibt drei voneinander getrennte Teilnetzwerke.

Die beiden Gast-WLANs teilen sich dann aber WLAN-Passwort und Verschlüsselung, was die Trennung wenig effektiv macht. Zudem kann das abgeschaltete Band-Steering im Haupt-WLAN die Übertragungsraten im Heimnetz reduzieren.

TP-Link: Netzwerktrennung per Mehrfach-SSIDs

Doch die Router von TP-Link bieten eine sinnvolle Alternative: Sie können das Band-Steering im Haupt-WLAN aktiviert lassen und stattdessen die Funktion „Basiseinstellungen → WLAN → Mehrfach-SSID“ nutzen. Mit Mehrfach-SSIDs lassen sich bis zu zwei zusätzliche, vom restlichen Heimnetz getrennte WLANs erstellen, die über beide WLAN-Frequenzen erreichbar sind. Wenn Sie außerdem das Gast-WLAN aktivieren, besitzen Sie insgesamt vier getrennte Teilnetzwerke.

Für jedes zusätzliche Teilnetzwerk lässt sich einstellen, ob sich die Clients gegenseitig sehen („Client-Isolierung“) und ob sie auf den Speicher des Router-NAS zugreifen dürfen. Dies nehmen Sie im Menü unter „Erweiterte Einstellungen → WLAN-Einstel-

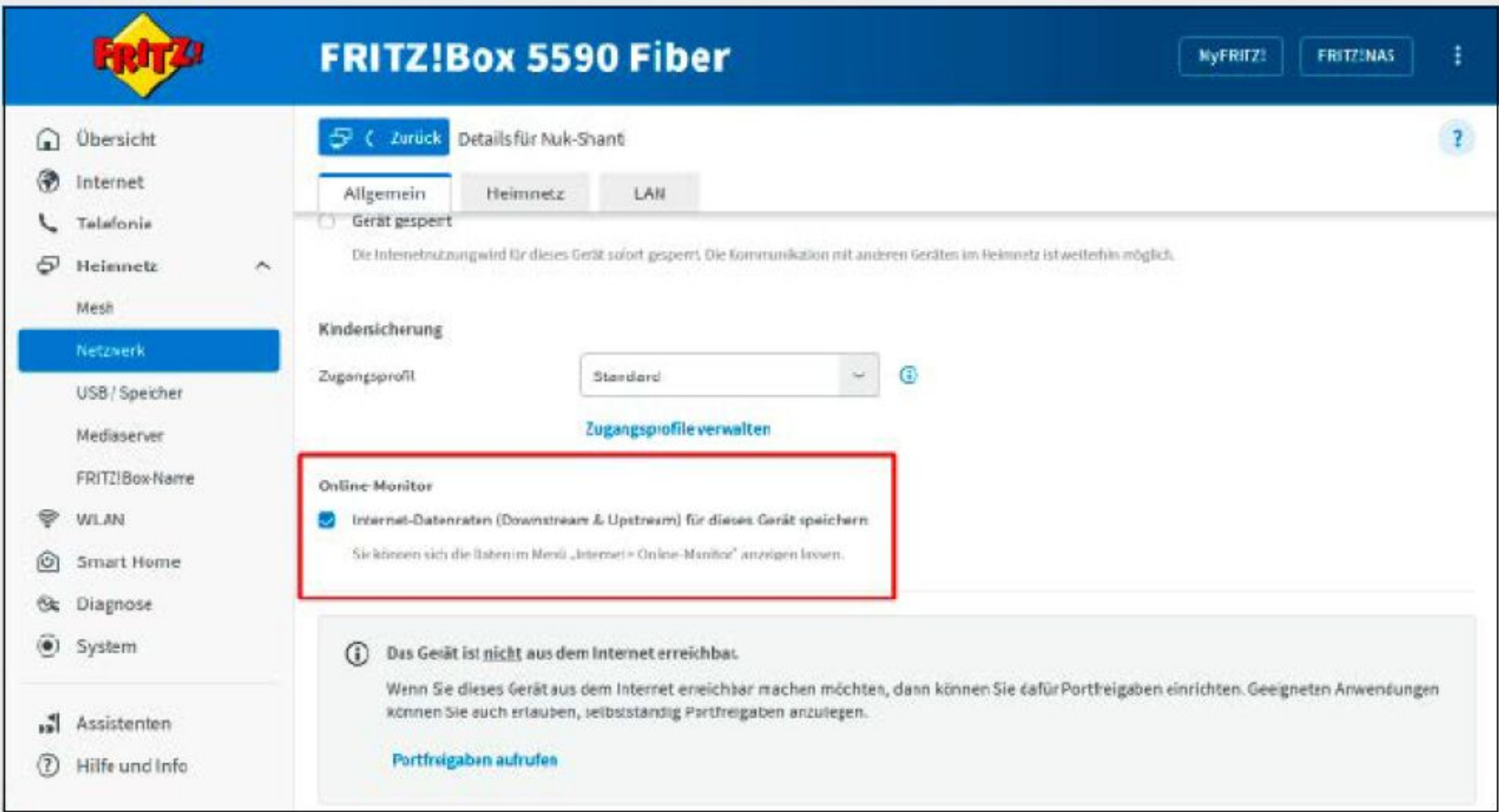
verteilen kann. Ein aktiviertes Gast-WLAN ist dann ebenfalls über beide Funkbänder erreichbar, was wie bei einer Fritzbox zwei getrennte Netzwerke ergibt. Sie können das Band-Steering unter „Basiseinstellungen → WLAN → WLAN-Einstellungen“ aber abschalten: Dann erhalten die

WLAN-Netze über das 2,4- und das 5-GHz-Band jeweils eine separate SSID. Anschließend lässt sich in den Routereinstellungen ebenfalls für jedes Funkband ein eigenes Gast-WLAN erstellen: Jedes der beiden Gastnetze besitzt dann eine eigene SSID und ist vom Gast-WLAN auf der anderen

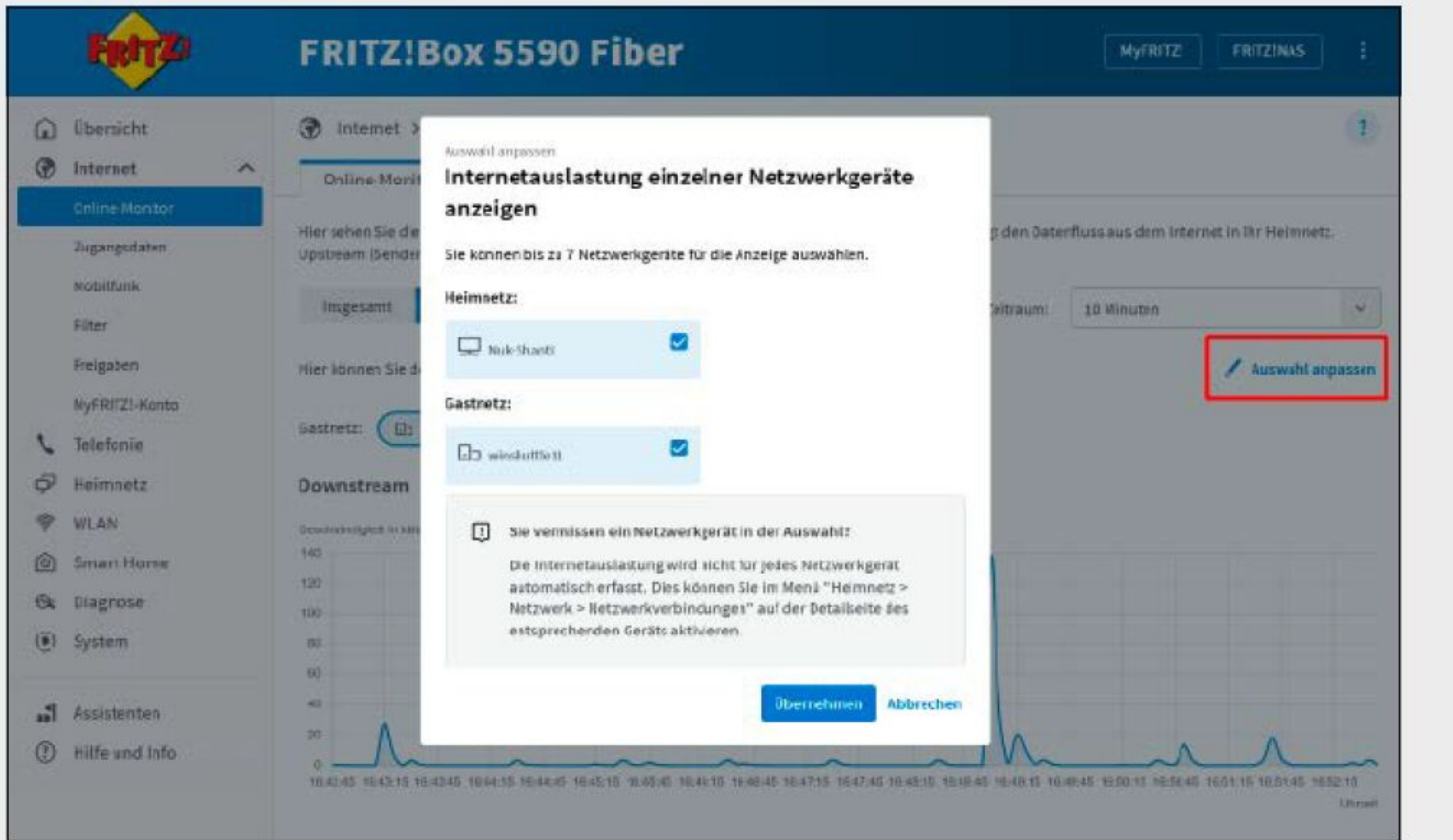
FRITZBOX: VERBESSERTE BANDBREITENKONTROLLE MIT FRITZ-OS 8

Ab Fritz-OS-Version 8 lässt sich unter „Internet → Online-Monitor → Online-Monitor“ anzeigen, wie viel Bandbreite einzelne Geräte belegen. Dazu müssen Sie die anzuzeigenden Geräte unter „Heimnetz → Netzwerk → Netzwerkverbindungen“ aktivieren, indem Sie in den Detailsinstellungen (rundes Stift-Symbol) des Geräts unter „Allgemein“ ein Häkchen vor „Internet-Datenraten (Downstream & Upstream) für dieses Gerät

speichern“ setzen und diese Einstellung „Übernehmen“. Auf diese Weise sehen Sie die Bandbreitennutzung von bis zu sieben Einzelgeräten im Online-Monitor. Die jeweiligen Geräte wählen Sie unter „Einzelne Geräte“ über den Link „Auswahl anpassen“ aus.



Das neue Fritz-OS zeigt Ihnen die Geräte im Heimnetz, die am meisten Bandbreite belegen: Um ihre Datenrate im Online-Monitor der Fritzbox anzuzeigen, aktivieren Sie diese Funktion in den Einstellungen Ihrer Netzwerkverbindung.



Anschließend markieren Sie die Geräte, deren Down- und Upstream-Rate Sie beobachten wollen. Sie tauchen dann mit unterschiedlichen Farblinien im Online-Monitor des Fritzbox-Menüs auf. Dazu klicken Sie auf die Schaltfläche „Einzelne Geräte“. Bis zu sieben Geräte lassen sich anzeigen.

lungen → Mehrfach-SSIDs“ vor. Ähnliches gilt für die erweiterten Einstellungen des Gast-WLANs, die Sie unter „Erweiterte Einstellungen → WLAN-Einstellungen → Gast-WLAN“ finden.

Asus-Router: Gäste-WLANs nach Frequenz trennen

Noch mehr Möglichkeiten zur WLAN-Trennung bieten viele Asus-Router, etwa der TUF-AX6000: Sie können im Menü unter „Allgemein → Gästenetzwerk“ bis zu sechs separate Gast-WLANs einrichten. Diese werden auf die beiden WLAN-Funkbänder des Routers aufgeteilt: drei Gast-WLANs im 2,4-GHz-Band und drei im 5-GHz-Band. Auf diese Weise lassen sich beispielsweise weiter entfernte Smart-Home-Clients über ein eigenes 2,4-GHz-Netz mit guter Reichweite, aber geringer Durchsatzrate einbinden, während nähere Streamingclients wie Fernseher, Konsolen und Tablets in einem schnelleren 5-GHz-Netzwerk unterkommen.

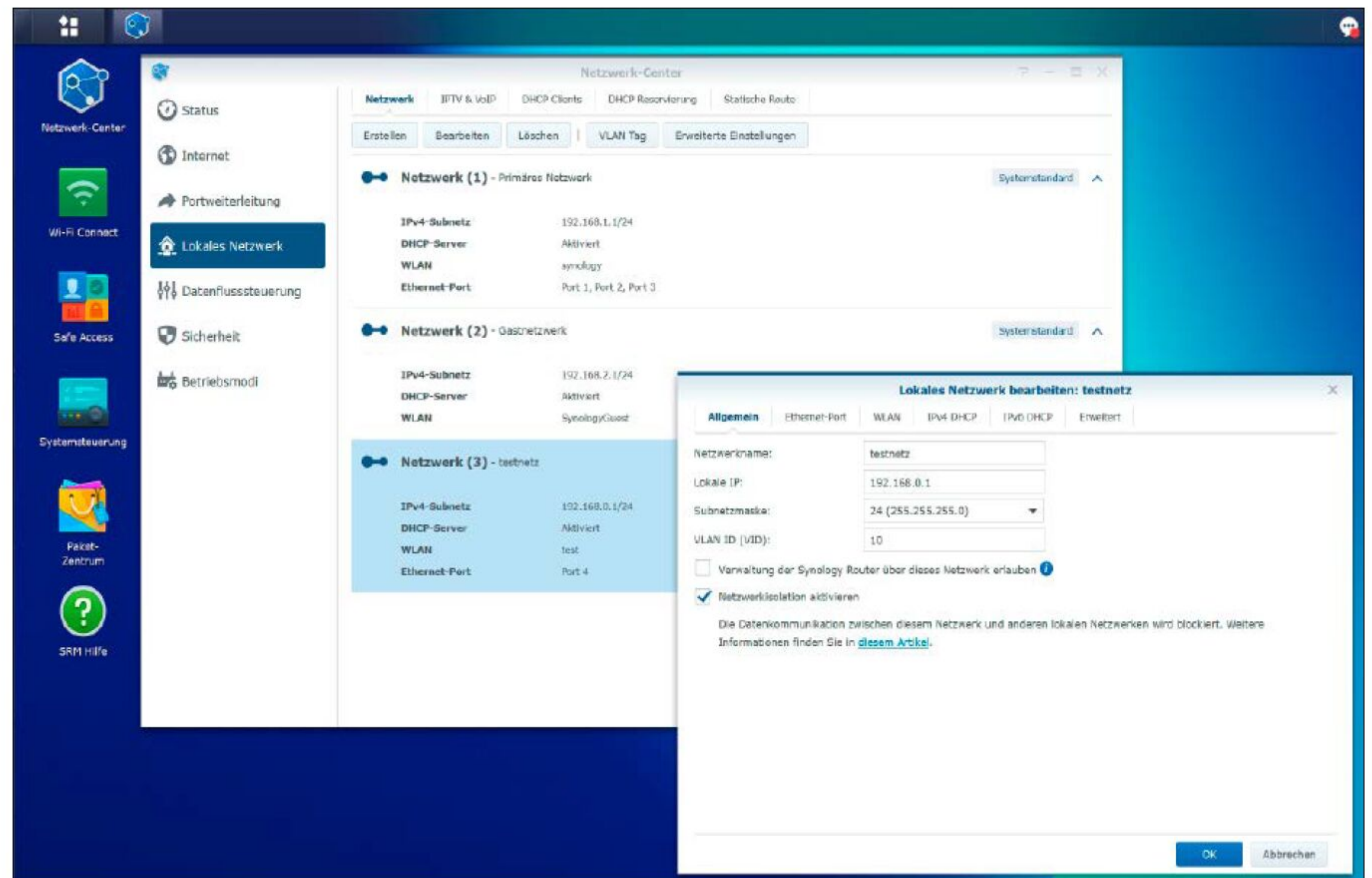
Das Heimnetz als siebtes Teil-WLAN ist weiterhin über beide Funkfrequenzen erreichbar und kann seine Clients optimal auf beide WLAN-Bänder verteilen – diese Band-Steering-Funktion heißt bei Asus „Smart Connect“.

Sie können für jedes aktive Gästenetzwerk zudem getrennte Zugangsdaten oder Clientzugriffszeiten angeben sowie einen MAC-Filter aktivieren. Außerdem lässt sich die maximale Up- und Download-Bandbreite für jedes Gästenetzwerk per QoS-Funktion begrenzen.

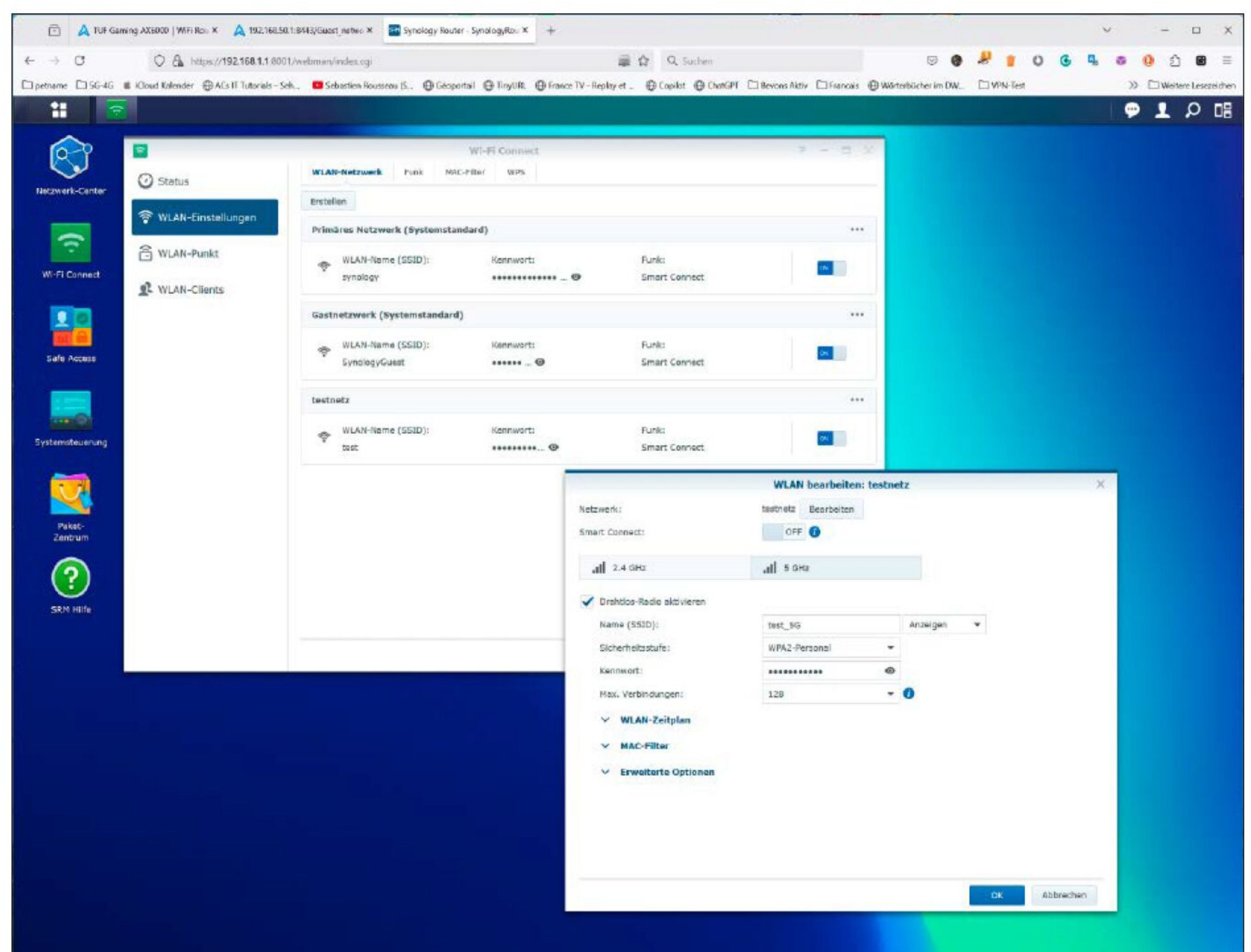
Bei Bedarf geben Sie einem Gästenetzwerk auch den Zugriff auf das normale Heimnetz („Intranet“) frei: Damit erhalten alle Clients dieses Gästenetzes eine Netzwerk-IP-Adresse des Hauptnetzes und dieselben Zugriffsrechte wie ein im Hauptnetz angemeldeter Client. Das kann sinnvoll sein, wenn Sie Gästen vorübergehend einen Vollzugriff auf Ihr Heimnetz gewähren wollen, ohne die Zugangsdaten Ihres Haupt-WLANs preisgeben zu müssen.

Synology: Netzwerke trennen mit Einstellungen auf Profi-Niveau

Die meisten Funktionen für WLAN-Trennung bieten die Routermodelle von Synology. Die entsprechenden Einstellungen im Webmenü des Routers finden sich unter „Netzwerk-Center → Lokales Netzwerk → Netzwerk“. Hier lassen sich beliebige Subnetzwerke mit eigener WLAN-SSID erstellen



Die meisten Möglichkeiten zur WLAN-Trennung bieten Router von Synology: Den einzelnen Netzen können Sie sogar bestimmte LAN-Ports zuordnen, sodass sich dort auch Ethernet-Geräte einbinden lassen.



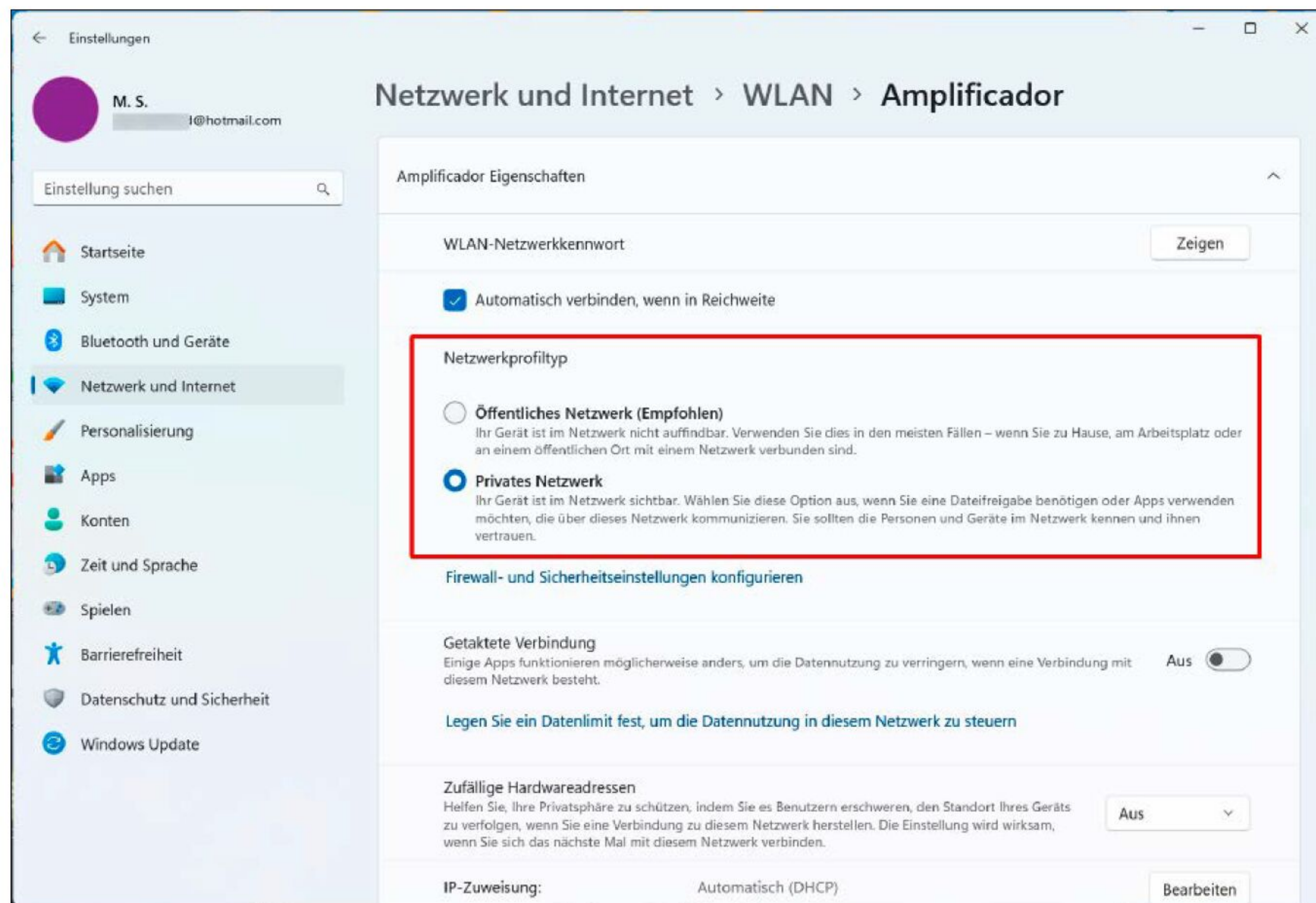
Bei Synology können Sie außerdem die Einstellungen für jedes Subnetz separat und unabhängig vom Haupt-WLAN einstellen, zum Beispiel die verwendete Frequenz, SSIDs und Passwörter.

len, denen sich sogar einzelne LAN-Ports des Routers zuweisen lassen.

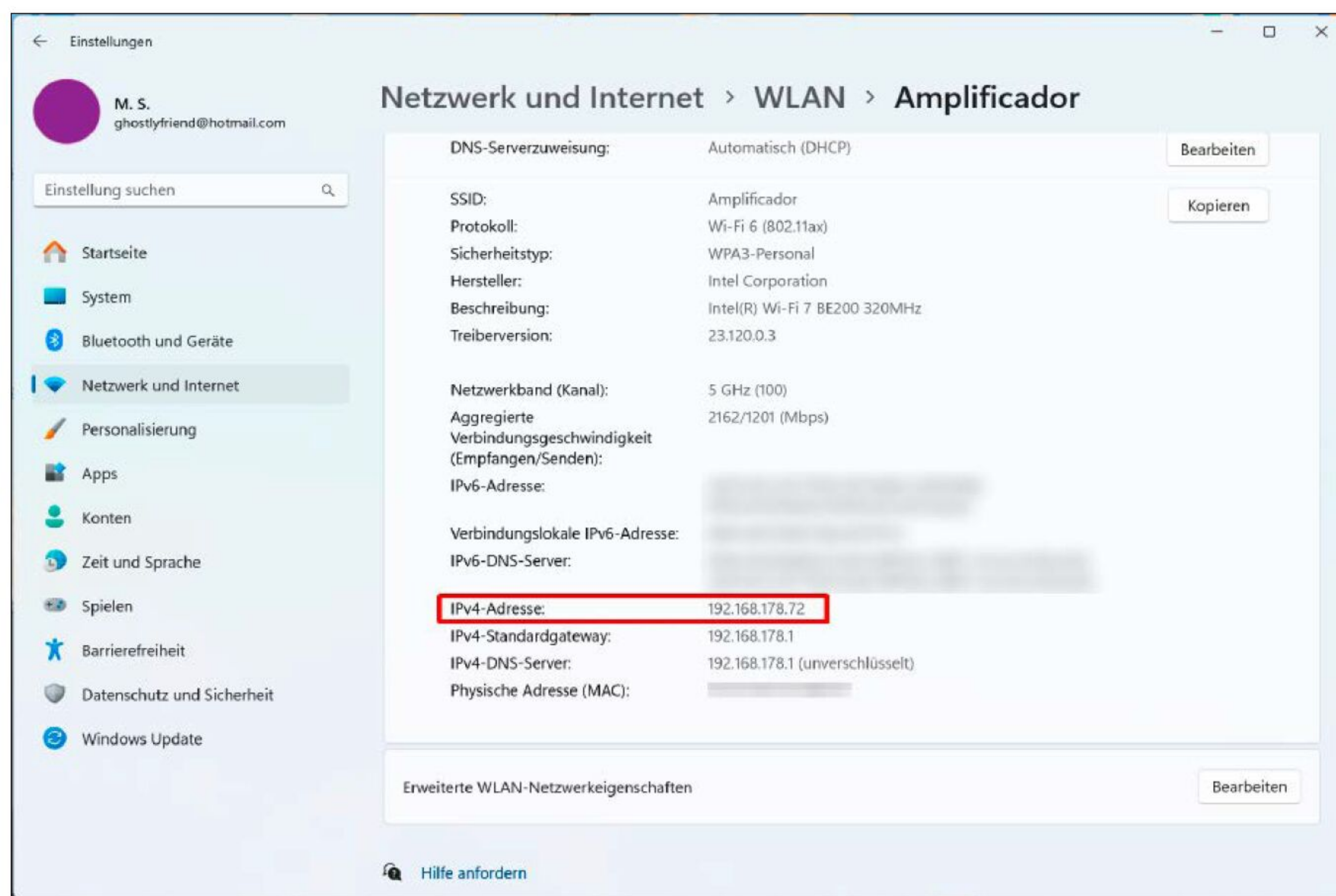
Die einzelnen Subnetzwerke sind durch die Netzwerkisolation strikt getrennt. Allerdings können Sie bei Bedarf den Zugriff eines Geräts aus Subnetz A auf ein anderes Gerät im Subnetz B erlauben: Der Router deaktiviert dann die Netzwerkisolation der betroffenen Subnetze und ersetzt sie durch drei Einträge in der Routerfirewall. Mit die-

ser Netzwerksegmentierung können Sie zum Beispiel ein Homeoffice-Netzwerk vom Heimnetz trennen und trotzdem einzelnen Clients den Zugriff in andere Subnetze erlauben – zum Beispiel dem Büro-PC den Zugriff auf das Heimnetz-NAS.

Darüber hinaus lässt sich bei einem Synology-Router für jedes Teilnetz einstellen, über welche Funkbänder es arbeiten soll – etwa nur über 2,4 GHz, nur über 5 GHz



Mit einem Netzwerkskan prüfen Sie, ob die einzelnen WLAN-Netze, die Ihr Router bereitstellt, tatsächlich voneinander getrennt sind und kein Datenpaket die Netzgrenzen überschreiten kann. Auf dem Windows-Rechner, den Sie für den Scan nutzen, müssen Sie zuvor das Netzwerkprofil „Privates Netzwerk“ einschalten.



Vor dem Scan notieren Sie sich die aktuelle IPv4-Adresse Ihres PCs: Von ihr sind in diesem Fall die ersten drei Zahlen wichtig – im vorliegenden Beispiel müssen Sie also auf 192.168.178. achten.

oder über beide Frequenzen. Das funktioniert unabhängig davon, über welche Frequenzbänder das Haupt-WLAN funkt. Bei Routern von Fritz (früher AVM), TP-Link oder Asus ist das nicht möglich.

So finden Sie heraus, ob die WLANs getrennt sind

Mit den vorgestellten Optionen können Sie getrennte WLANs einrichten. Für die Sicherheit ist aber entscheidend, dass der Daten-

verkehr zwischen diesen Netzen tatsächlich unterbunden wird. Dies prüfen Sie am besten mit einem Netzwerkskanner, wie dem kostenlosen **Angry IP Scanner 3.9.1** (Download unter <https://angryip.org>).

Installieren Sie sich das Tool auf einem Rechner, den Sie mit dem Haupt-WLAN verbinden. Führen Sie anschließend einen Rechtsklick auf die Windows-Start-Taste aus und öffnen Sie im Kontextmenü die Option „Netzwerkverbindungen“. Klicken

Sie im folgenden Fenster oben rechts neben dem großen WLAN-Symbol auf die Schaltfläche „Eigenschaften“.

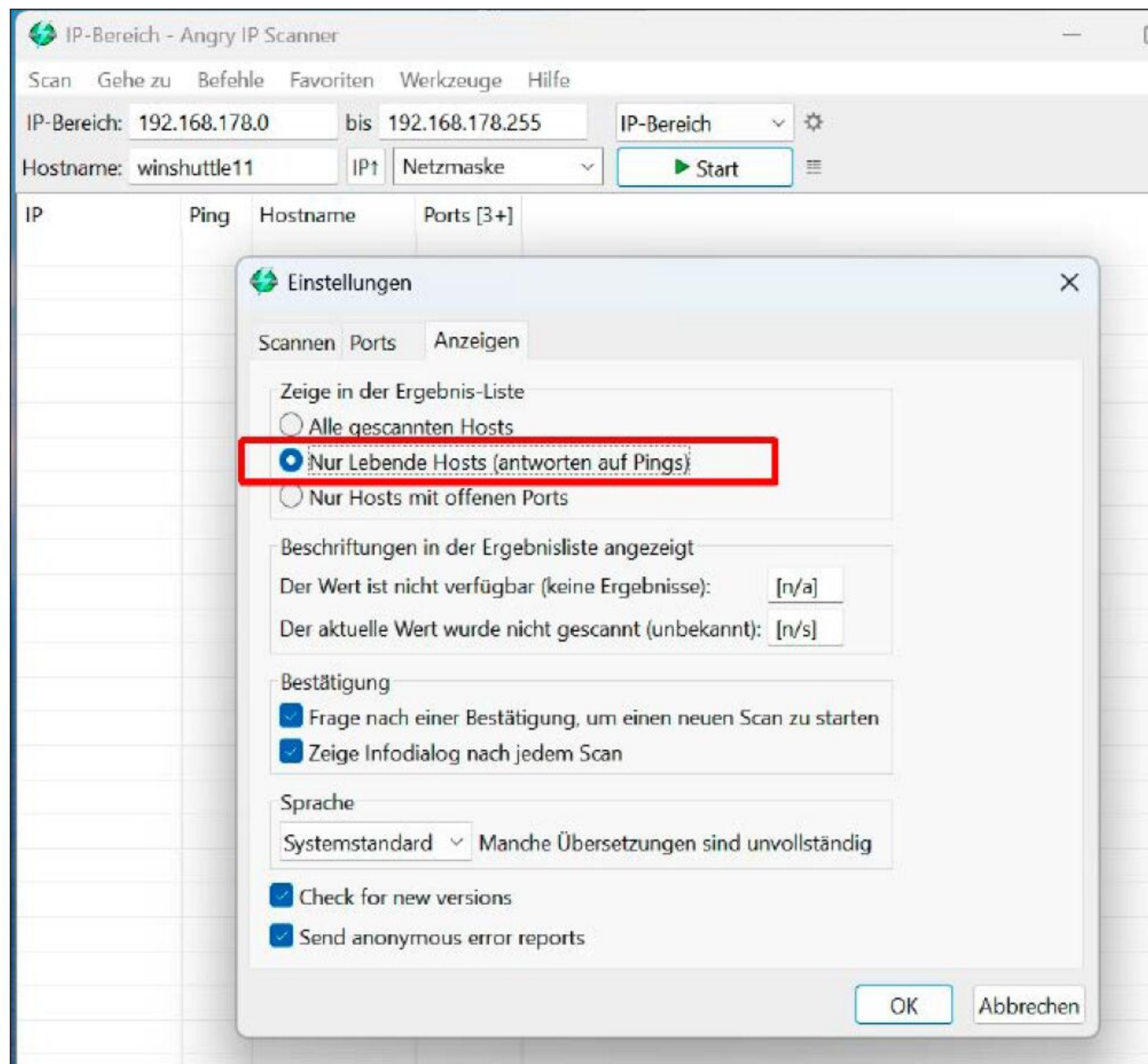
Im folgenden „Eigenschaften“-Fenster muss für Ihre WLAN-Verbindung der „Netzwerkprofiltyp“ auf „Privates Netzwerk“ gestellt sein: Damit stellen Sie sicher, dass das Netzwerktool sinnvolle Scanergebnisse liefert und nicht von der Windows-Firewall behindert wird. Scrollen Sie in diesem Fenster weiter nach unten und notieren Sie die „IPv4-Adresse“ Ihres Notebooks. Interessant sind hier die drei ersten Zahlen, beispielsweise „192.168.178.<x>“, „192.168.1.<x>“ oder „192.168.50.<x>“. Sie geben im Heimnetz in der Regel den Netzwerkbereich eines lokalen Netzwerkes oder Subnetzes an. Die vierte Zahl (<x>) der IPv4-Adresse interessiert zunächst nicht.

Starten Sie nun den Angry IP Scanner und prüfen Sie, ob im Toolmenü in den beiden Eingabefeldern der Zeile „IP-Bereich“ die jeweils ersten drei Zahlen mit den ersten drei Zahlen Ihrer IPv4-Adresse aus den Windows-WLAN-Einstellungen übereinstimmen. Falls nicht, passen Sie die ersten drei Zahlen im linken Eingabefenster entsprechend an, die vierte Zahl („0“) dagegen nicht. Die Werte für die dritte und vierte Zahl werden dann automatisch ins zweite Eingabefenster übertragen. Dort müssen Sie noch die vierte Zahl „0“ durch „255“ ersetzen, nur dann prüft der Angry IP Scanner den gesamten Netzwerkbereich.

Gehen Sie anschließend im Toolmenü auf „Werkzeuge → Einstellungen → Anzeigen“ und setzen Sie die Auswahl unter „Zeige in der Ergebnis-Liste“ auf „Nur Lebende Hosts (antworten auf Ping)“. Das macht das Scanergebnis übersichtlicher, da Angry IP Scanner dann nur die tatsächlich im Netzwerk vorhandenen und eingeschalteten Netzwerkclients zeigt. Bestätigen Sie diese Einstellung mit „OK“. Der Angry IP Scanner prüft nun standardmäßig alle entdeckten Netzwerkgeräte auf die Standard-Webserver-Ports 80, 443 und 8080.

Führen Sie im Anschluss daran einen Netzwerkskan durch, indem Sie auf die Schaltfläche „Start“ klicken.

Nach einigen Sekunden zeigt das Tool mit „Scan vollständig“ ein Ergebnis: Dort sollten alle im Heimnetz aktiven Clients auftauchen. Neben dem Router und Ihrem Client-PC handelt es sich um alle Geräte, die derzeit über das Haupt-WLAN oder über einen



Das Netzwerktool Angry IP Scanner stellen Sie für den Test am besten so ein, dass es in der Ergebnisliste nur aktive Netzwerkclients anzeigt. Damit erhalten Sie einen besseren Überblick über die Geräte im Heimnetz.

LAN-Port mit dem Router verbunden sind, zum Beispiel Smartphone, NAS und Netzwerkdrucker. Geräte, die sich in einem getrennten WLAN befinden – zum Beispiel einem bereits aktivierten Besucher-WLAN – dürfen nicht in dieser „Heimnetz“-Ergebnisliste auftauchen.

Wenn Sie unter „Werkzeuge → Einstellungen → Ports“ im Eingabefeld der Portauswahl noch die Ports 139 und 445 per Komma getrennt hinzufügen und mit „OK“ bestätigen, prüft Angry IP Scanner alle entdeckten Geräte auch auf vorhandene Netzwerkfreigaben.

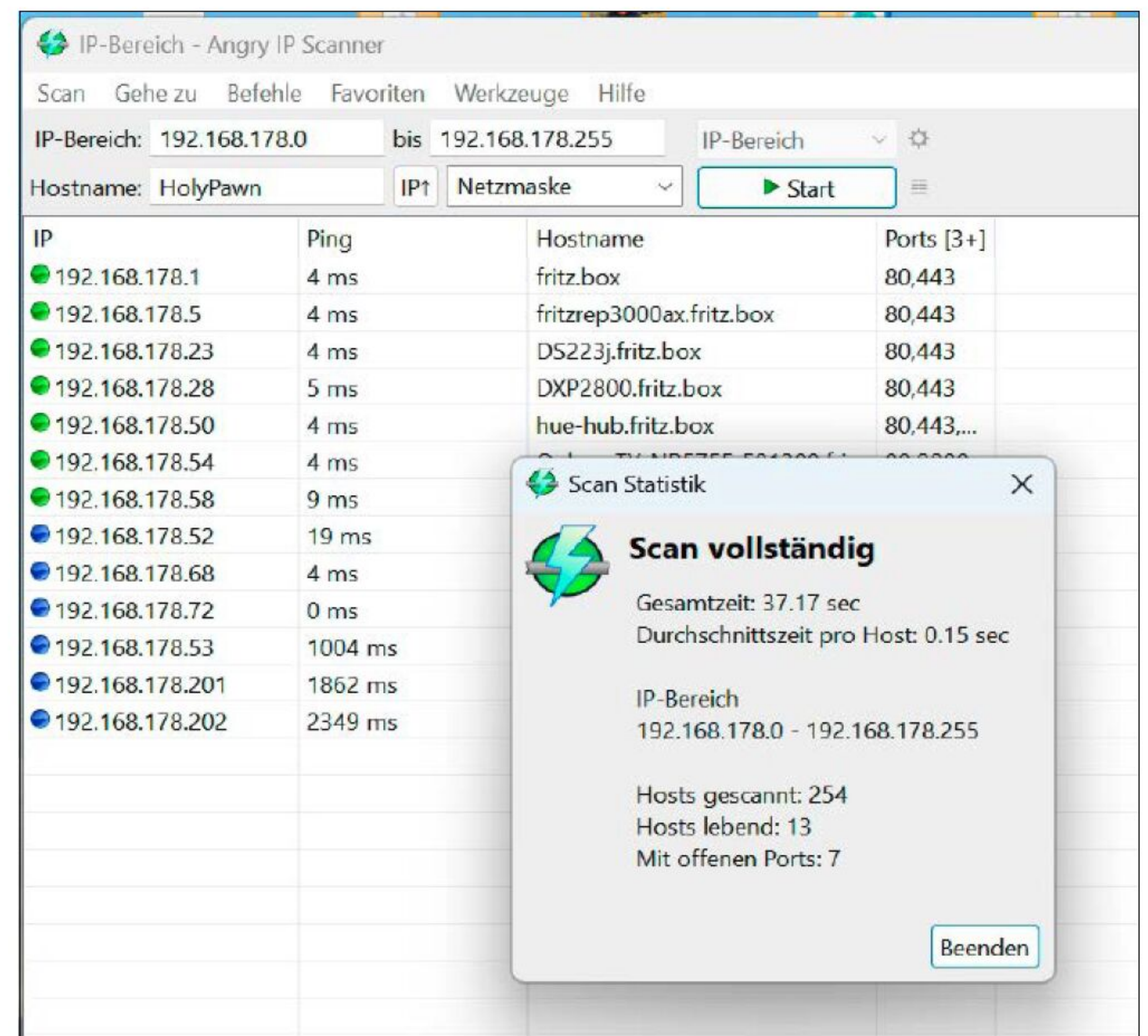
Nun machen Sie die Gegenprobe und verbinden Ihr Notebook mit dem Gäste-WLAN des Routers. Beenden Sie Angry IP Scanner und starten Sie das Tool neu. Nun gehen Sie erneut in die WLAN-Netzwerkeinstellungen des Rechners, stellen den Netzwerkprofiltyp auf „Privates Netzwerk“ und sehen sich die ersten drei Zahlen Ihrer „IPv4-Adresse“ im Gäste-WLAN an. Die dritte Zahl der IPv4-Adresse im Gastnetz sollte sich von der dritten Zahl des Heimnetzes unterscheiden.

Bei einer Fritzbox lautet die Gastzugangsadresse beispielsweise „192.168.189.x“. Ein Client, der in diesem Netzwerkbereich angemeldet ist, kann keine Verbindung zum Hauptnetz herstellen, da sich dieses im Adressbereich „192.168.178.x“ befindet. Starten Sie nun einen Scan mit Angry IP

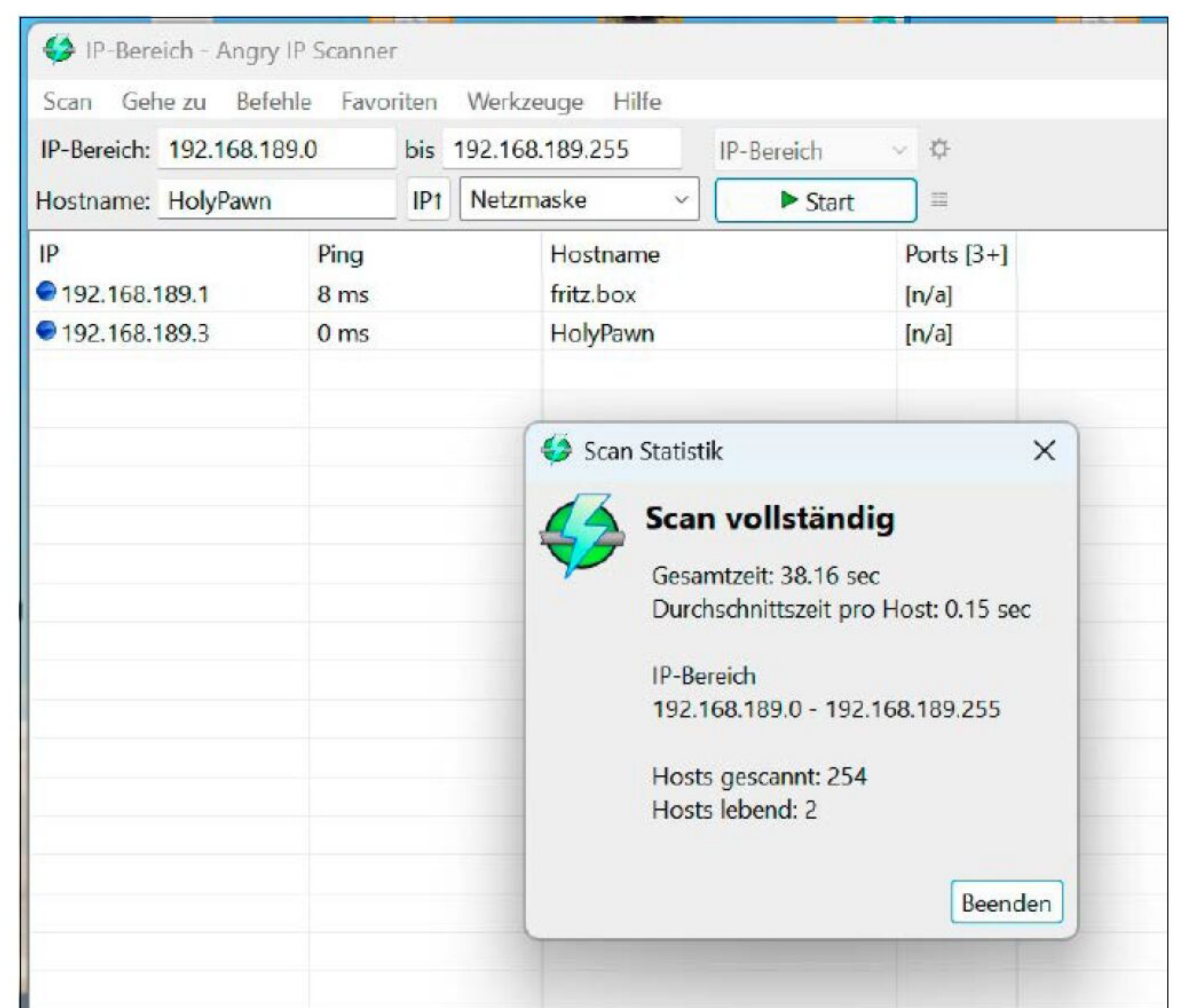
Der Gegentest im Gäste-WLAN sollte anschließend wie im Bild nur den Router und Clients im Gäste-WLAN anzeigen. Die Geräte aus dem ersten Test im Hauptnetz dürfen nicht mehr auftauchen.

Scanner im Gast-WLAN. In der Ergebnisliste sollten nur der Router, Ihr Notebook und weitere mit dem Gast-WLAN verbundene Clients erscheinen. Zeigt die Ergebnisliste hingegen auch Clients aus dem normalen Heimnetz, sind Heimnetz und Gast-WLAN nicht getrennt: Die unterschiedlichen Funknetze bringen dann keinen Sicherheitsgewinn.

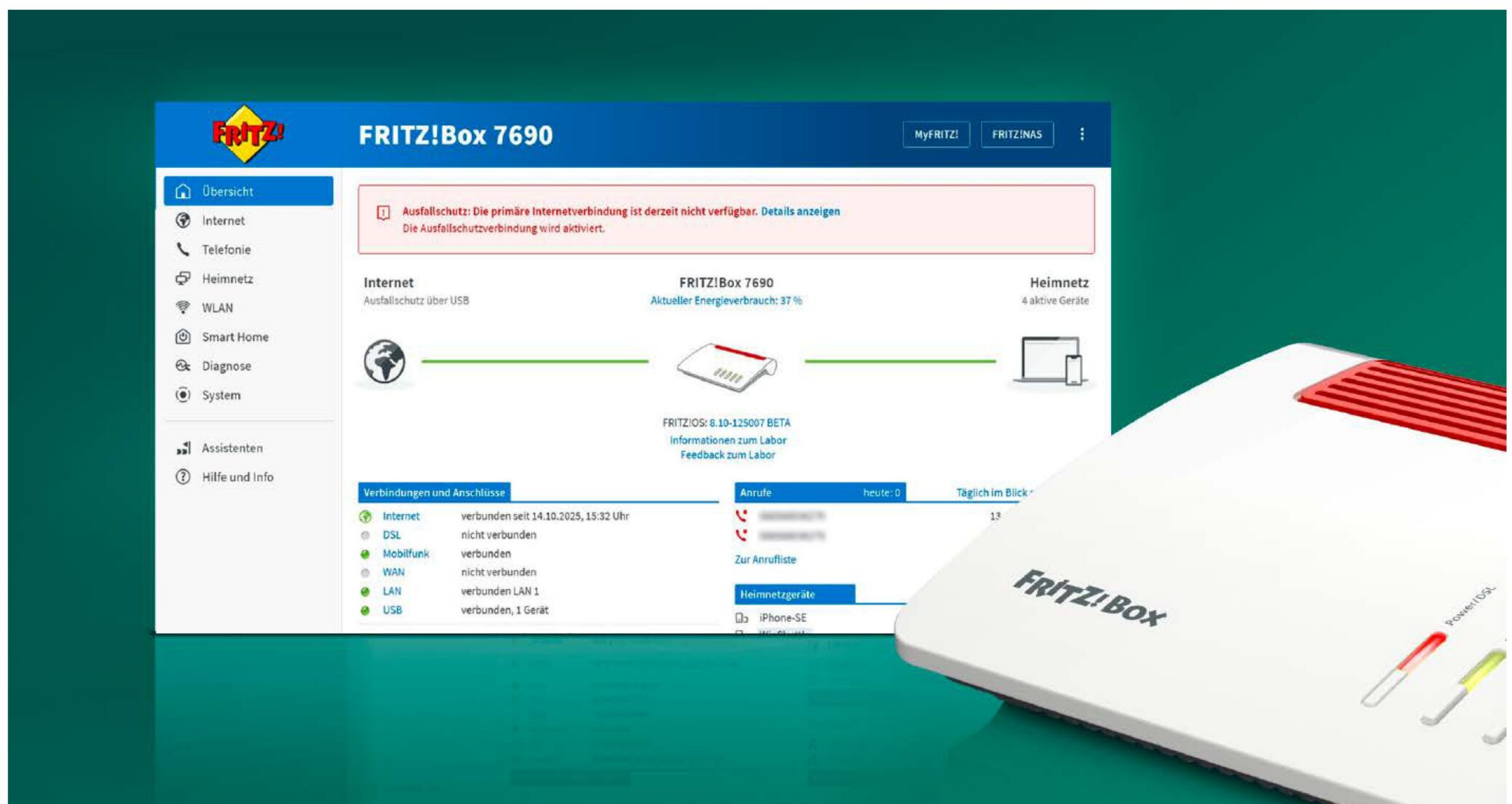
Verlassen Sie sich daher nicht auf die Einstellungen des Routermenüs: Bei vielen Modellen machen sie nicht sofort ersichtlich, ob beispielsweise eine Mehrfach-SSID-



Ist Ihr Rechner mit dem Haupt-WLAN des Routers verbunden, sollte ein Test mit Angry IP Scanner nur Clients anzeigen, die sich ebenfalls in diesem Netz befinden – aber nicht die Clients im Gäste-WLAN.



Funktion nur verschiedene WLAN-Zugänge ins selbe Netzwerk erlaubt oder ob jede dieser mehrfachen SSIDs ein eigenes Teilnetzwerk aufspannt. Erst der Test mit Angry IP Scanner gibt darüber Aufschluss. Zudem lässt sich mit dem Netzwerkscanner testen, ob die Clientisolierung zwischen Geräten im selben Netz funktioniert: Bei aktiver Clientisolierung im Router oder in einem Teilnetz sollte bei mehreren angemeldeten Clients kein weiteres Gerät im Scanergebnis erscheinen außer dem, auf dem Sie das Tool ausführen. ■



© Mit Material von Fritz.com

Online bleiben, wenn das Internet ausfällt

Wenn der Internetzugang nicht mehr funktioniert, sind Sie und Ihr Heimnetz lahmgelegt. Doch mit den passenden Routereinstellungen gehen Sie schnell über andere Wege wieder online. Vor allem eine Fritzbox bietet mit der neuen Firmware einen umfassenden Ausfallschutz. Wir zeigen, wie Sie ihn am besten einsetzen.

VON MICHAEL SEEMANN

Dass das Internet funktioniert, ist inzwischen für die meisten Menschen so wichtig wie die Stromversorgung. Während es noch verschmerzbar sein mag, mal einen Abend

„Mit dem neuen Fritz-OS bekommt die Fritzbox einen erweiterten Internet-Ausfallschutz.“

ohne Netflix & Co. zu verbringen, haben bei einem Online-Blackout Arbeiter im Home-office ein genauso ernsthaftes Problem wie Anwender, die auf Onlinedienste oder VPN-Verbindungen in andere Netzwerke angewiesen sind.

Die Internetverbindung kann jederzeit und ohne Vorwarnung unterbrochen werden: Oft sind dafür Kanal- oder andere Tiefbauarbeiten in der Nachbarschaft verantwortlich, bei denen ein Bagger versehentlich Kabel durchtrennt. Auch wenn ein Verteilerknoten des Netzbetreibers ausfällt oder er seine Netzinfrastruktur umstrukturiert, kann es passieren, dass der Onlinezugang für längere Zeit – sogar für Tage – zum Er-

liegen kommt oder immer wieder unterbrochen wird.

Ein einzelnes Gerät wie ein Notebook können Sie in dieser Notlage schnell über die Tethering- oder Hotspot-Funktion des Smartphones per Mobilfunkverbindung wieder online bringen. Doch das komplette Heimnetz sollten Sie nicht auf diesem Weg mit dem Internet verbinden, da das Smartphone kein vollwertiger Router ist. Das ist auch gar nicht erforderlich, denn mittlerweile bieten einige Heimnetzrouter einen komfortablen Internet-Ausfallschutz: Damit haben Sie eine Art Notfall-„Backup“ für die eigene Internetverbindung – das ist üblicherweise ein zusätzlicher Onlinezu-

gang, der idealerweise automatisch ein-springt, falls der primäre Internetzugang wie VDSL, Kabel oder Glasfaser einmal ausfallen sollte.

Der große Vorteil: In diesem Fall bleiben die Funktionen des Routers und die Verbindungen aller Heimnetz-Clients mit dem Router erhalten. Zudem funktioniert das Umschalten auf den Ersatz-Internetzugang automatisch – genauso wie das Zurückschalten auf den Hauptanschluss, sobald dieser wieder verfügbar ist.

Besonders einfach geht das bei einer Fritzbox: Mit der neuen Firmware-Version Fritz-OS 8.20 bekommen diese Router einen erweiterten Ausfallschutz für die Internetverbindung, der Sie davor bewahren soll, länger offline gehen zu müssen.

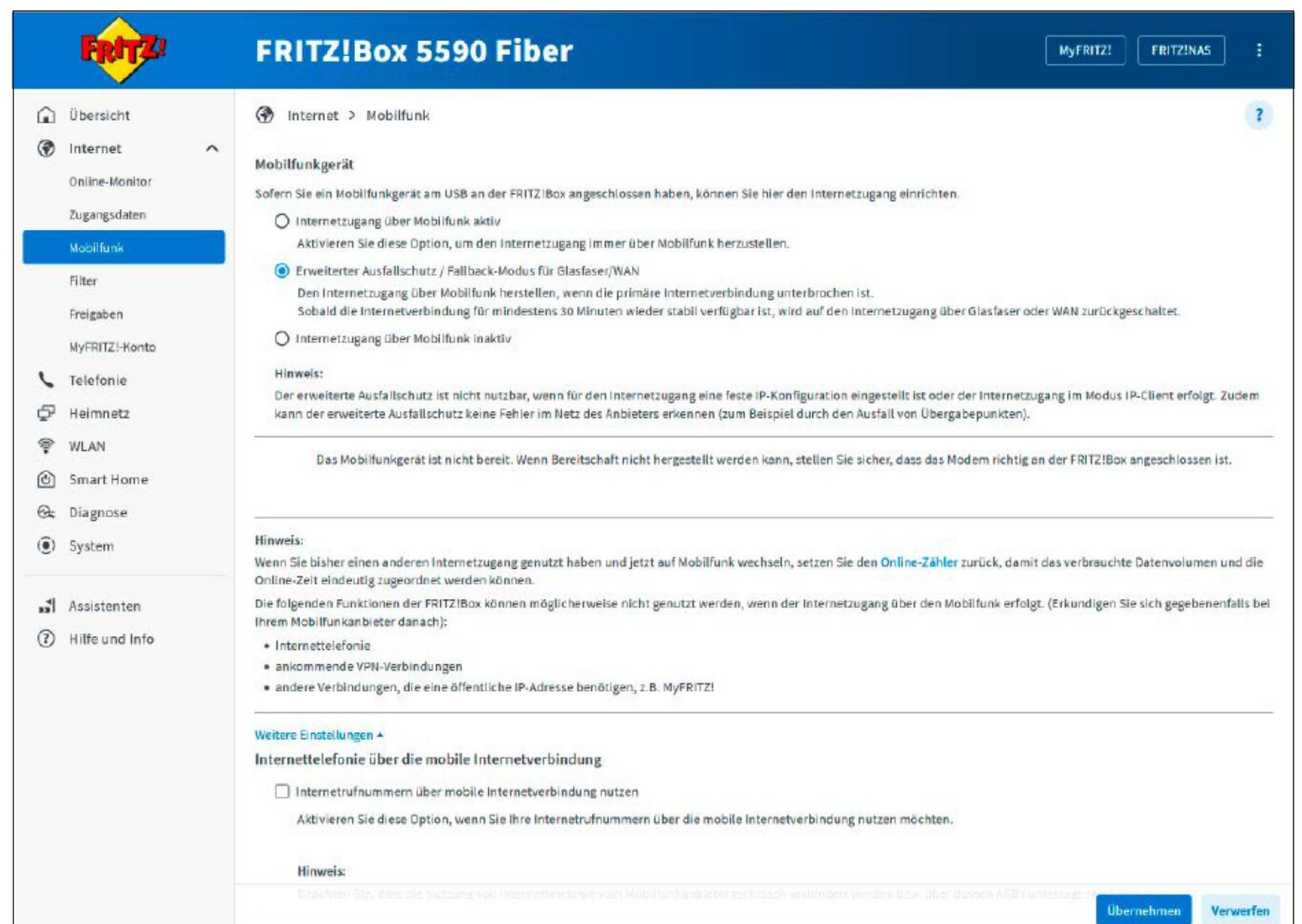
Fritz-Failsafe: Der erweiterte Ausfallschutz für die Fritzbox

Üblicherweise nutzt ein Router als Ausfallschutz eine Mobilfunkverbindung, da nur in wenigen Haushalten ein zusätzlicher Onlinezugang per Festnetz verfügbar ist. Mobilfunk gibt es dagegen (fast) überall – allerdings oft nicht mit derselben Übertragungsleistung.

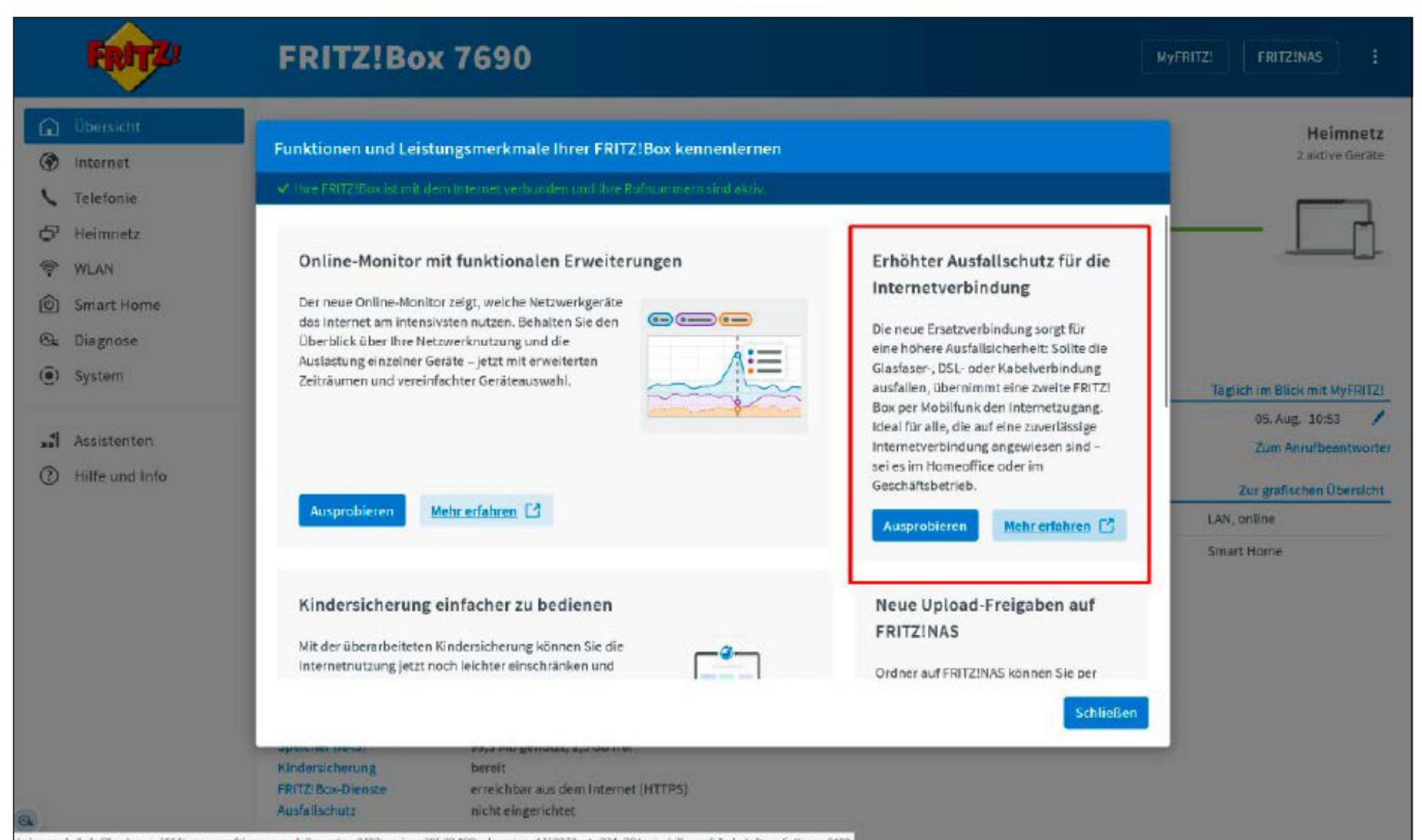
Auch in vielen Fritzbox-Routern finden Sie schon seit einigen Jahren einen rudimentären Internet-Ausfallschutz, mit dem sich ein ausgefallener Internet-Hauptzugang per Mobilfunk überbrücken lässt. Dazu stecken Sie einen Mobilfunk-Stick in den USB-Port des Routers oder verbinden ihn mit einem Android-Smartphone im USB-Tethering-Modus. Die Fritzbox spricht dann das entsprechende Gerät direkt als Modem an. Mit einem iPhone funktioniert dies an der Fritzbox allerdings nicht.

Mit Fritz-OS-Version 8.20 bekommen alle aktuellen Fritzbox-Modelle einen neuen, deutlich erweiterten Ausfallschutz. Ob es die neue Firmware für Ihre Fritzbox schon gibt, prüfen Sie im Routermenü unter „System → Update → FRITZ!OS-Version → Neues FRITZ!OS suchen“. Sollte das noch nicht der Fall sein, können Sie den Ausfallschutz auch mithilfe der Betaversion Fritz-OS 8.10 testen, die Sie für bestimmte Modelle unter fritz.com/pages/fritz-labor finden. Den neuen Ausfallschutz nennt der Hersteller markant Fritz-Failsafe.

Direkt nach dem Update auf Fritz-OS 8.20 (oder die Labor-Version 8.10) weist Sie das Webmenü der Fritzbox auf den neuen Ausfallschutz hin. Er findet sich im Menü unter



Auch ohne Fritz-OS 8.20 ließe sich mit einer Fritzbox ein Ausfallschutz fürs Internet nutzen: Sie aktivieren ihn über den Punkt „Mobilfunk“ und müssen dafür ein Mobilfunkgerät am USB-Port anschließen.



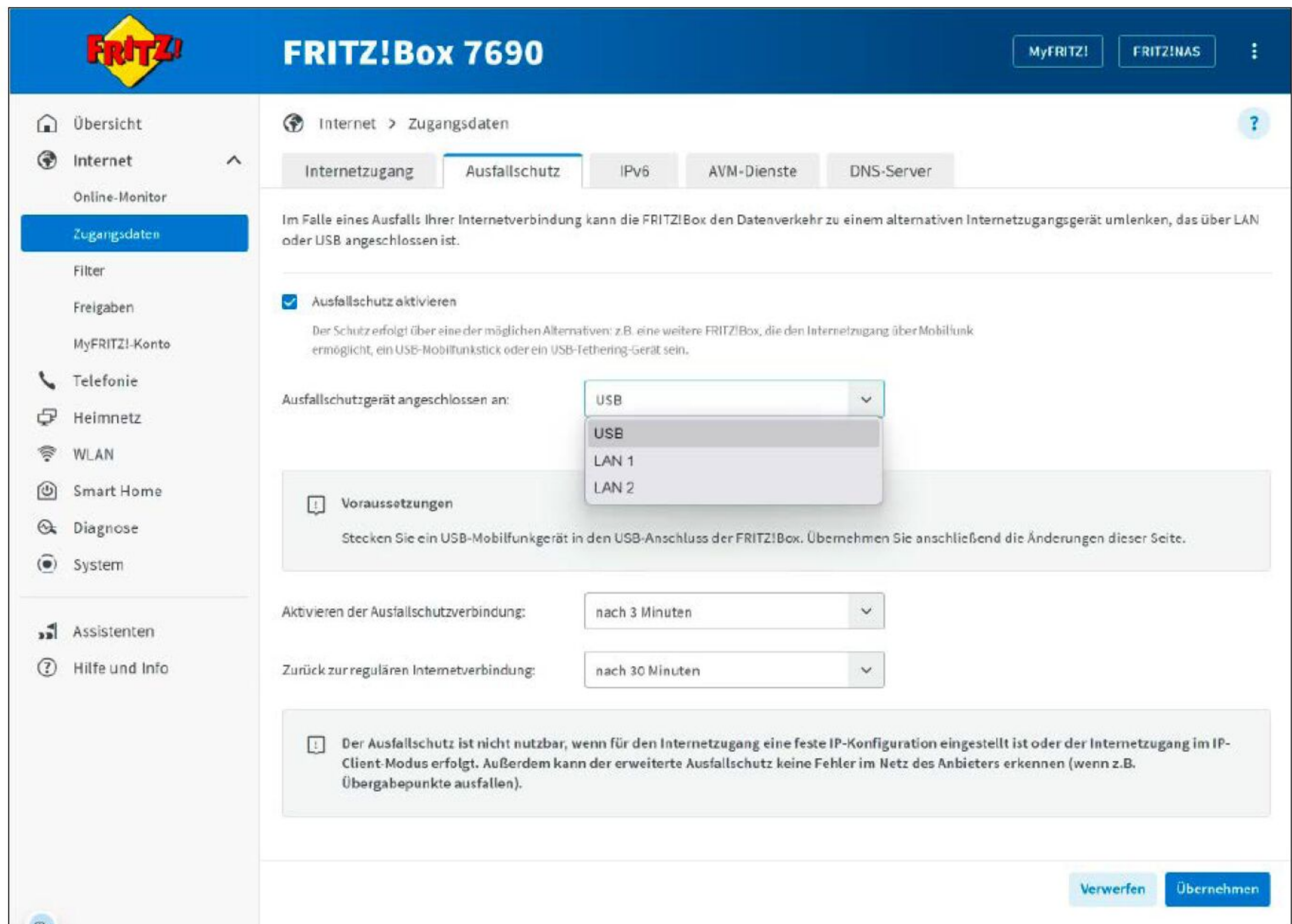
Gleich nach der Installation des neuen Fritz-OS macht Sie die Fritzbox auf den verbesserten Ausfallschutz aufmerksam. Über die entsprechende Schaltfläche können Sie ihn sofort einrichten.

„Internet → Zugangsdaten → Ausfallschutz“. Der hilfsweise Internetzugang lässt sich auf zwei Arten herstellen – entweder über einen USB- oder einen LAN-Port des Routers. Fritz-Failsafe schalten Sie ein, indem Sie einen Haken vor die Option „Ausfallschutz aktivieren“ setzen. Danach sehen Sie einige erweiterte Einstellungen: Im ersten Dropdown-Menü neben „Ausfallschutz angeschlossen an:“ wählen Sie aus, über welchen Anschluss der Ersatzzugang laufen soll. Bei einer Fritzbox 7690 stehen zum Beispiel die Optionen „USB“, „LAN 1“ und

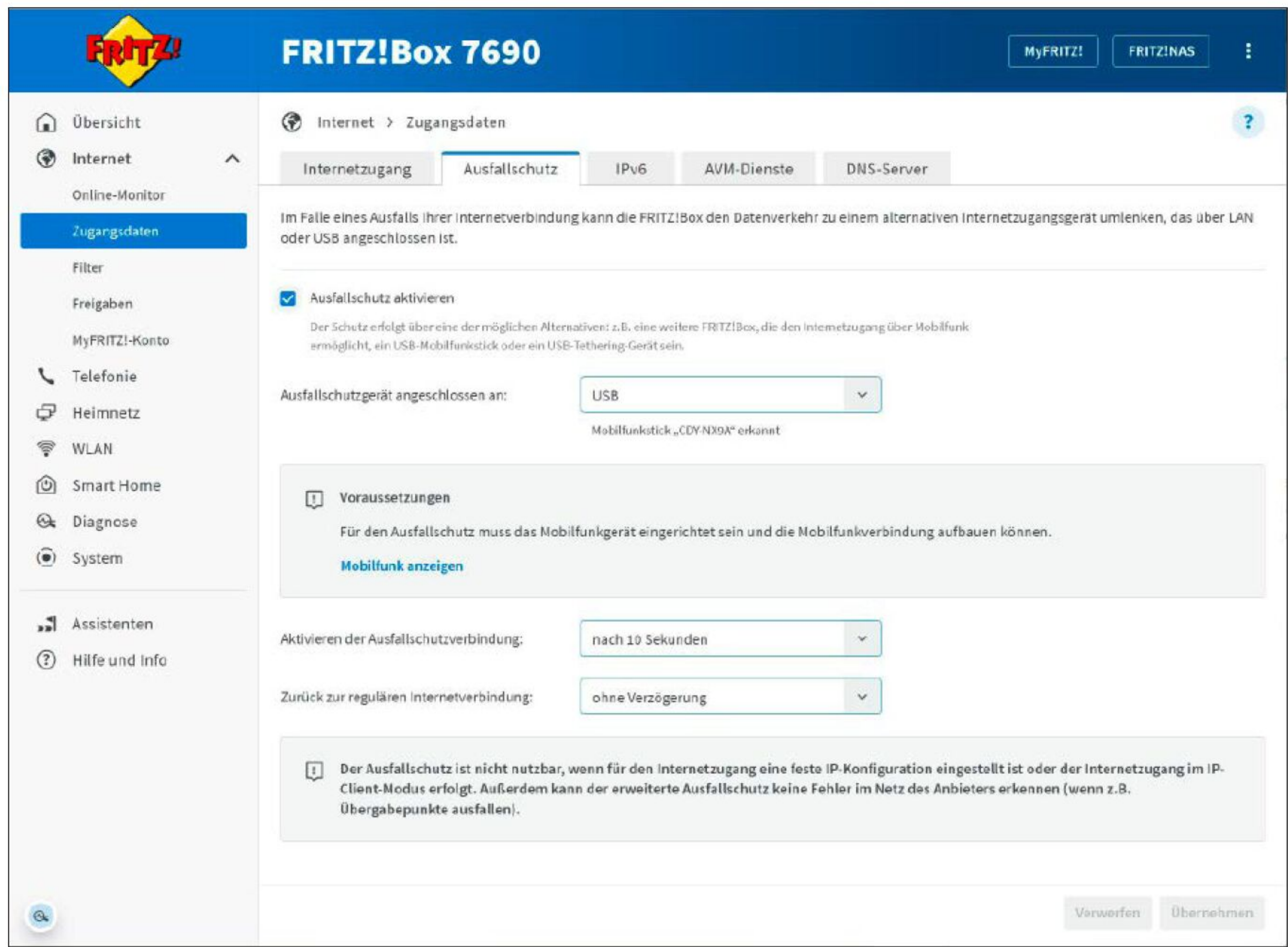
„LAN 2“ zur Verfügung, der LAN-3-Port bleibt für den LAN-Gastzugang reserviert. Je nach Ausstattung Ihrer Fritzbox haben Sie zusätzliche Anschlussoptionen – meist einen weiteren USB- und LAN-Port. Der LAN-Port, der für den Gastzugang vorgesehen ist, lässt sich aber in keinem Fall für den Ausfallschutz nutzen.

Ausfallschutz per Smartphone im Tethering-Modus

Fritz-Failsafe funktioniert mit einem Smartphone, das Sie per USB-Kabel an die Fritz-



Je nach Ausstattung Ihrer Fritzbox haben Sie unterschiedliche Möglichkeiten, ein Gerät für den Ausfallschutz anzuschließen. Bei einer Fritzbox 7690 stehen dafür ein USB-Anschluss und zwei LAN-Ports bereit.



Wechsel-Einstellungen: Für einen ersten Test verkürzen wir die Zeit auf zehn Sekunden, bis der Ausfallschutz anspringt. Wenn die reguläre Internetverbindung wieder aktiv ist, soll sie die Fritzbox sofort nutzen.

box anschließen. Setzen Sie dazu im Fritzbox-Menü unter „Internet → Zugangsdaten → Ausfallschutz“ die Auswahl im ersten Drop-down-Menü auf „USB“, direkt darunter erscheint dann die Meldung „Kein USB-Mobilfunkgerät erkannt“. Verbinden Sie nun Ihr Android-Smartphone per USB-Kabel mit der Fritzbox und aktivieren Sie auf dem Smartphone den USB-Tethering-Mo-

dus. Sie finden ihn üblicherweise in den „Einstellungen“ bei „Netzwerk & Internet“. Suchen Sie nach einer Option wie „Hotspot und Tethering“ oder „Persönlicher Hotspot“, wo Sie den Schalter bei „USB-Tethering“ umstellen. Wechseln Sie zurück zum Fritzbox-Menü und gehen Sie zu „Internet → Zugangsdaten → Ausfallschutz“. Setzen Sie im zweiten

Drop-down-Menü die voreingestellte Ausfallzeit neben „Aktivieren der Ausfallschutzverbindung:“ auf zehn Sekunden. Nach dieser Zeit schaltet die Fritzbox auf den USB-Smartphone-Ausfallschutz um, wenn der Hauptzugang nicht mehr verfügbar ist. Die Einstellung bei „Zurück zur normalen Verbindung:“ können Sie für einen ersten Test auf „Ohne Verzögerung“ umstellen, damit die Fritzbox direkt zurück auf die Hauptverbindung wechselt, wenn diese wieder aktiv ist. Bestätigen Sie Ihre Einstellungsänderungen mit „Übernehmen“. Spätestens jetzt sollte die Fritzbox das angeschlossene Smartphone unter der Auswahl „USB“ erkannt haben.

Damit Sie sich auf Fritz-Failsafe verlassen können, sollten Sie sofort testen, ob es funktioniert: Trennen Sie dazu die Festnetz-Internetverbindung der Fritzbox, indem Sie das WAN-, DSL-, TV- oder Glasfaser-Kabel vorsichtig aus dem Router herausziehen. Nach etwa zehn Sekunden sollte Ihr Heimnetz wieder online sein – und zwar über die Ausfallschutzverbindung des Smartphones am USB-Anschluss.

Eine Bestätigung erhalten Sie im Fritzbox-Menü im Punkt „Übersicht“: Hier erscheint oben in einem roten Kasten der Hinweis, dass der Ausfallschutz aktiv ist und die primäre Internetverbindung wie „WAN“ oder „DSL“ derzeit „nicht verbunden“ ist. Dafür ist die Verbindung „Mobilfunk“ aktiv und weist einen grünen Punkt auf – ebenso wie die USB-Verbindung zwischen Smartphone und Fritzbox.

Diese Probleme verursacht der Ausfallschutz per Mobilfunk

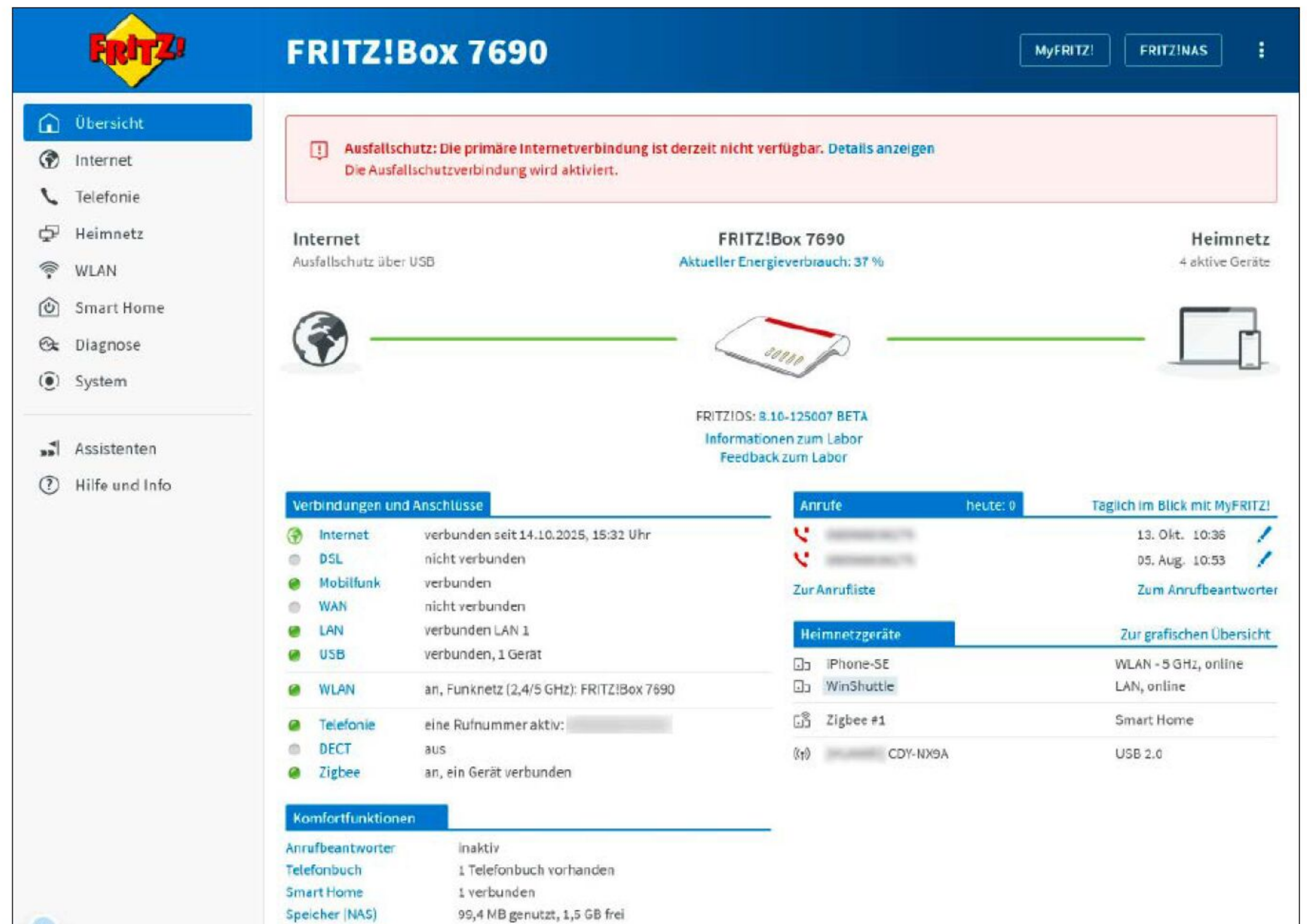
Wenn Sie wie beschrieben vorgehen, sollten Ihre Heimnetzgeräte nun wieder mit dem Internet verbunden sein. Allerdings können bei Fritz-Failsafe per Mobilfunk einige Fritzbox-Funktionen trotz des ersatzweisen Onlinezugangs nicht mehr verfügbar sein – zum Beispiel Telefonie und VPN. Üblicherweise umfasst ein Internettarif Onlinezugang und Telefonanschluss von einem Provider. Deshalb können Sie üblicherweise nur dann telefonieren, wenn die Verbindung über den dazugehörigen Internetanschluss erfolgt. Andernfalls gelten die Telefonie-Zugangsdaten nicht mehr, die Sie vom Provider bekommen und in der Fritzbox eingetragen haben – der Provider will damit die sogenannte nomadische Nutzung der Zugangsdaten unterbinden. Beim Aus-

fallschutz läuft die Onlineverbindung aber über Mobilfunk, weswegen das Telefonieren in diesem Fall meistens nicht mehr funktioniert.

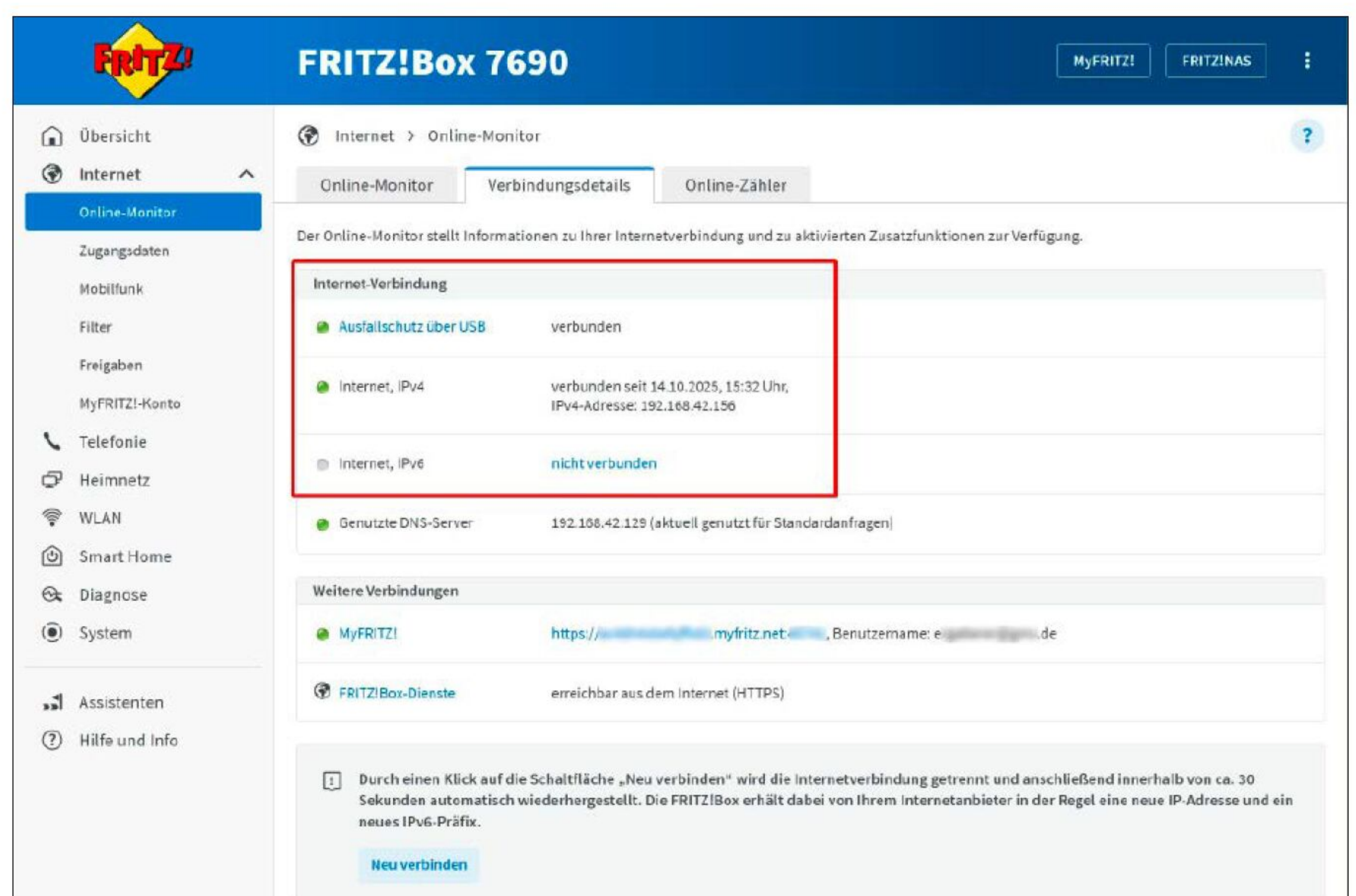
Nutzen Sie dagegen in diesem Fall die Zugangsdaten eines anderen Telefonieproviders, sollte die Festnetztelefonie auch während des Ausfallschutzes kein Problem machen. Bei unseren Tests mit einer SIP-Verbindung über Sipgate ließen sich Telefongespräche führen und Sprachnachrichten auf dem Anrufbeantworter der Fritzbox empfangen, während Fritz-Failsafe aktiv war.

Auch ein VPN-Zugang kann durch Fritz-Failsafe ausgehebelt werden: Nutzen Sie Ihre Fritzbox als VPN-Server, um von auswärts auf Ihr Heimnetz zuzugreifen, scheitert der VPN-Zugang an der öffentlichen IP-Adresse. Bei einem normalen Internetzugang ist die Fritzbox über eine eindeutige öffentliche IP-Adresse direkt erreichbar. Greift aber der Ausfallschutz per Mobilfunkverbindung, ist die IP-Adresse nicht mehr eindeutig: Viele Mobilfunkprovider teilen nämlich eine IPv4-Adresse über ein sogenanntes Carrier Grade NAT (CGNAT) mehreren Endgeräten zu. Dieses Problem können Sie im Fritzbox-Menü unter „Internet → Online-Monitor → Verbindungsdetails“ nachvollziehen: Bei aktivem „Ausfallschutz über USB“ erhält die Fritzbox unter „Internet, IPv4“ meist eine private (CGNAT-)IPv4-Adresse. Unter dieser ist sie nicht mehr aus dem Internet erreichbar, was den Fernzugriff über VPN unmöglich macht. Selbst der Fernzugriff auf das Webmenü der Fritzbox über HTTPS und das IPv6-Protokoll ist oft nicht möglich, wenn der Mobilfunkanbieter keine IPv6-Adresse bereitstellt – was auch bei uns der Fall war. Doch selbst wenn der Mobilfunkprovider IPv6 bereitstellen sollte, kann das die VPN-Clientsoftware überfordern, sofern der Client nicht auch IPv6 angebunden ist.

Wer auch während des Ausfallschutzes auf eine funktionierende VPN-Verbindung ins Heimnetz angewiesen ist, sollte auf eine cloudbasierte Lösung ausweichen wie **Teamviewer** (www.teamviewer.com) oder **Any-Desk** (<https://anydesk.com>). Sie installieren das entsprechende Tool auf einem Heimnetzgerät wie einem PC oder einem NAS, das eine Verbindung mit dem Cloudserver des Anbieters herstellt. Auch auf dem Gerät für den Fernzugriff installieren Sie das Tool, um über den Cloudserver Ihr Heimnetz zu erreichen.



Wenn die Hauptverbindung ausgefallen ist, weist Sie die Fritzbox mit einem roten Kasten auf der Übersichtsseite darauf hin. Zudem sehen Sie, über welchen Anschluss am Router der Ausfallschutz erfolgt.



Ist der Ausfallschutz aktiv, kann es Probleme beim Telefonieren oder bei VPN-Verbindungen geben. Denn von einem Mobilfunkprovider bekommt die Fritzbox dann meist nur eine private CGNAT-IPv4-Adresse (192.168.xxx.xxx) und ist damit nicht mehr aus dem Internet erreichbar.

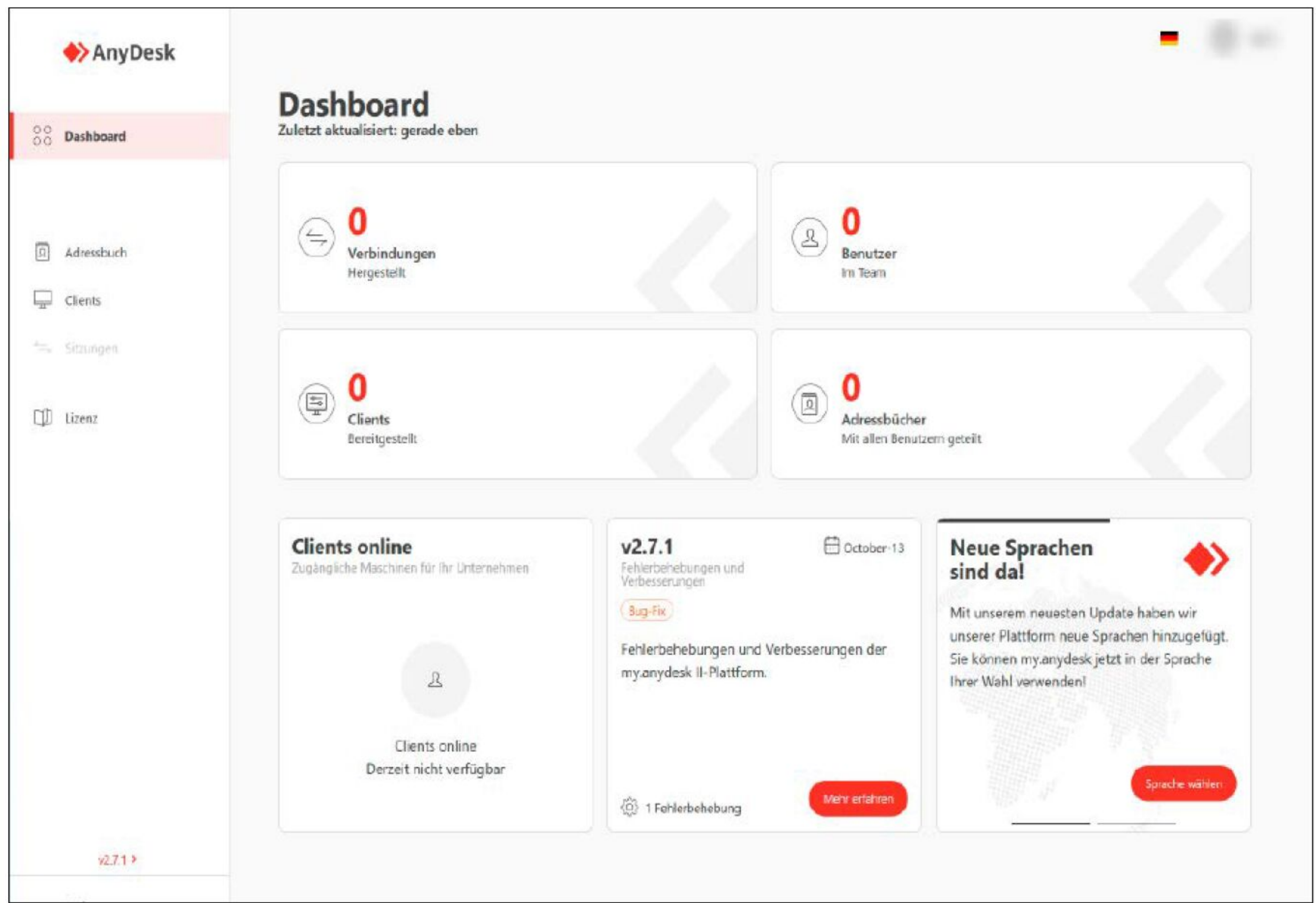
Für beide Anwendungen gibt es kostenlose Privatanwender-Tarife mit gewissen Einschränkungen, deren Leistungsumfang für die Anwendung im privaten Umfeld jedoch ausreichen sollte.

Ausfallschutz per Kabel über eine LAN-Verbindung

Als Alternative zum Smartphone können Sie einen (Mobilfunk-)Router verwenden,

der der Fritzbox vorgeschaltet ist. Es genügt nicht, einfach ein externes Modem an den LAN-Port anzuschließen.

Die LAN-IP-Adressbereiche der beiden Router müssen unterschiedlich sein: Wenn es sich beim Ausfallschutzrouter ebenfalls um eine Fritzbox handelt, müssen Sie deren lokale IP-Adresse von der voreingestellten 192.168.178.1 auf eine abweichende IP-Adresse umstellen, beispielsweise auf



Wenn die VPN-Verbindung zur Fritzbox bei einer Ausfallschutzverbindung nicht mehr funktioniert, können Sie als Alternative ein Fernzugriffstool wie Any-Desk oder Teamviewer nutzen, um Ihr Heimnetz zu erreichen.

192.168.158.1 oder 192.168.198.1. Das erledigen Sie im Menü der Ausfallschutz-Fritzbox unter „Heimnetz → Netzwerk → Netzwerkeinstellungen“ am unteren Rand des Menüs per Klick auf „weitere Einstel-

lungen“. Dort scrollen Sie nach unten bis „IP-Adressen“ und klicken auf die blaue Schaltfläche „IPv4-Einstellungen“. Ändern Sie im folgenden Fenster direkt unterhalb des roten „Achtung“-Kastens die dritte Zahl

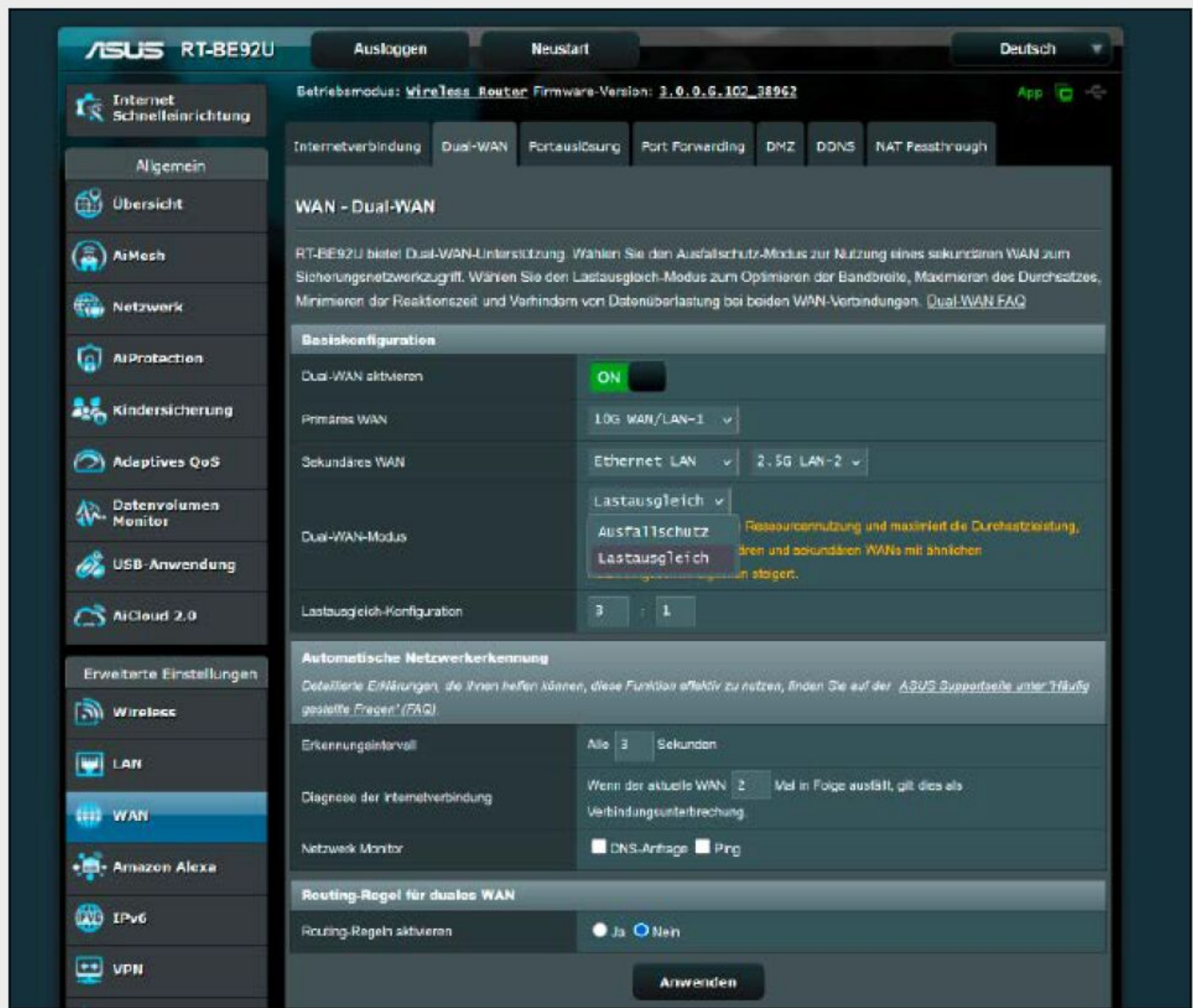
der dort eingestellten vierteiligen IPv4-Adresse von „178“ auf beispielsweise „198“. Die beiden ersten Zahlen (192.168) und die vierte Zahl „1“ der IPv4-Adresse bleiben unverändert – ebenso die Subnetzmaske. Alle anderen Zahlenwerte auf dieser Seite, wie zum Beispiel die unter „DHCP-Server“ oder unter „Lokaler DNS-Server“, passt der Router dann automatisch an. Bestätigen Sie mit „Übernehmen“ und drücken Sie zur weiteren Bestätigung eine Taste am Routergehäuse. Im Anschluss zeigt Ihnen die Fritzbox noch einmal die neue IPv4-Adresse: Die sollten Sie sich notieren, denn darüber gelangen Sie von jetzt an ins Webmenü des Ausfallschutzrouters. Wenn Sie einen anderen Router für den Ausfallschutz nutzen, müssen Sie nichts ändern, da deren LAN-IP-Adressen immer von denen einer Fritzbox abweichen.

Auch wenn Sie eine weitere Fritzbox für den Ausfallschutz verwenden, lassen sich die beiden Router nicht per Mesh verbinden. Denn Ihr Fritzbox-Hauptrouter und der Ausfallschutzrouter arbeiten hintereinandergeschaltet in einer sogenannten Routerkaskade – jedes Gerät als eigenständiger Router. In einem Fritzbox-Mesh gibt es dagegen nur einen eindeutigen Mesh-Master als Router, während alle anderen Fritzboxen sich im IP-Client- oder Repeater-Modus befinden und ihre IP-Adresse vom Mesh-Master erhalten.

AUSFALLSCHUTZ BEI ANDEREN ROUTERN

Neben der Fritzbox bieten auch Router anderer Hersteller bestimmte Einstellungen für einen zweiten, zusätzlichen Internetzugang. Bei den meisten Asus-Routern lässt sich beispielsweise über die Funktion „Dual-WAN“ ein zweiter WAN-Zugang oder der USB-Port über Smartphone oder Mobilfunk-Stick als Ausfallschutz nutzen. Mit der Option „Lastausgleich“ können Sie aber – anders als bei einer Fritzbox – auch zwei aktive Internetanschlüsse gleichzeitig verwenden, um die Bandbreite zu erhöhen oder die Onlineanbindung des Routers stabil zu halten.

Bei Asus können Sie im Routermenü unter „WAN → Dual-WAN“ neben dem Ausfallschutz auch einen Lastausgleich aktivieren, um beispielsweise für eine höhere Bandbreite beide Internetzugänge gleichzeitig zu nutzen.



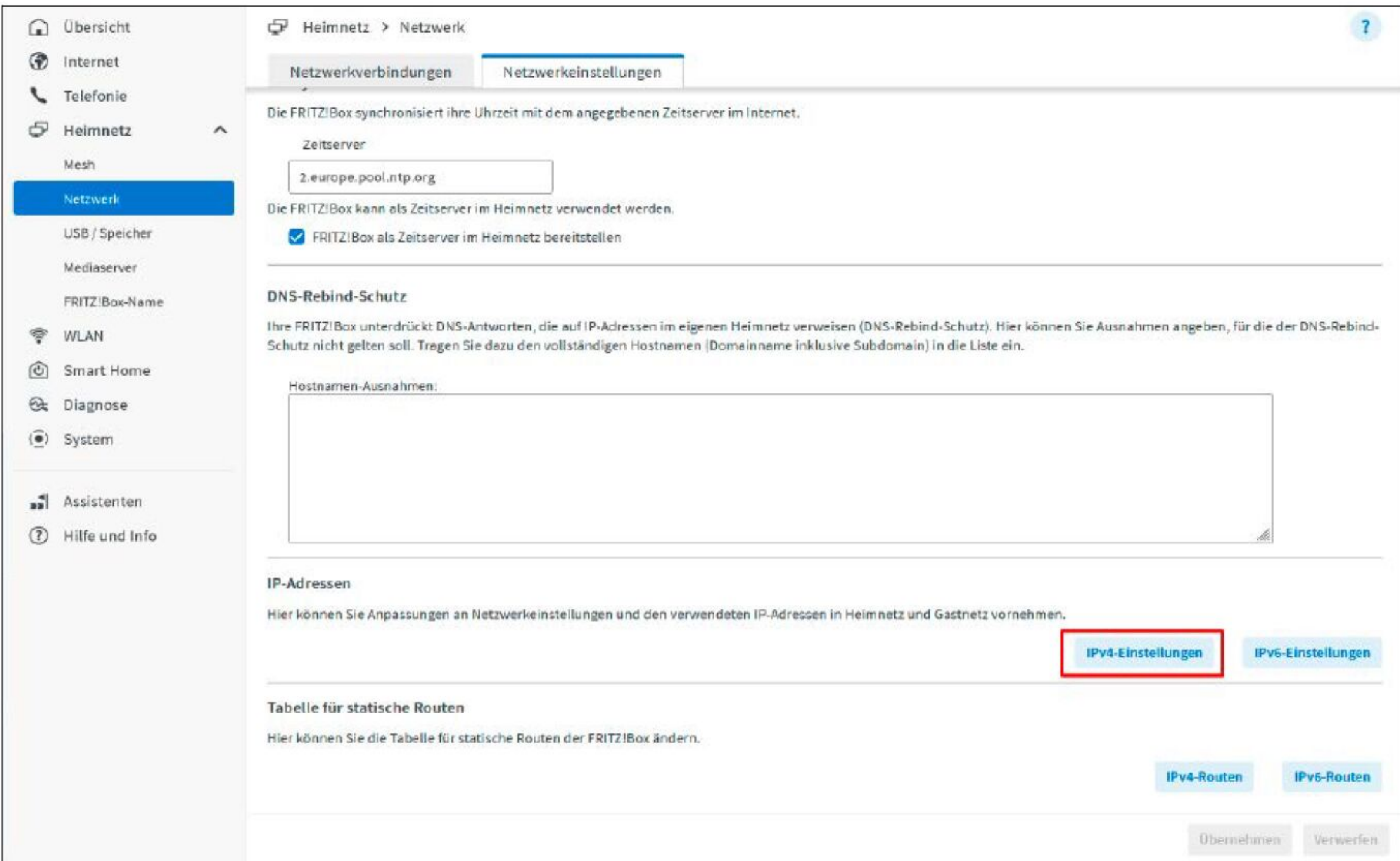
Telefonie und Fernzugriff beim LAN-Ausfallschutz

Auch bei einem per LAN-Port vorgeschalteten Mobilfunkrouter können Probleme beim Telefonieren auftreten. Denn zum Hindernis der öffentlichen IP-Adresse kommt in diesem Fall hinzu, dass die Datenpakete fürs Telefonieren ein zusätzliches NAT, nämlich das des vorgeschalteten Mobilfunkrouters, überwinden müssen. Das erfordert aufwendige Porteeinstellungen am vorgeschalteten Router, die vermutlich auch nur mit Telefonanschlüssen unabhängiger VoIP-Provider funktionieren. Rechnen Sie deshalb damit, dass Sie beim Ausfall Ihrer Hauptinternetverbindung wahrscheinlich nicht über Ihre gewohnte Festnetzrufnummer telefonieren können. Weichen Sie daher vorübergehend auf Ihr Smartphone aus. Ähnlich problematisch gestaltet sich der Fernzugriff auf Ihre Fritzbox per VPN: Auch in diesem Fall können Sie sich mit einem

cloudbasierten Zugang über Teamviewer oder Any-Desk behelfen.

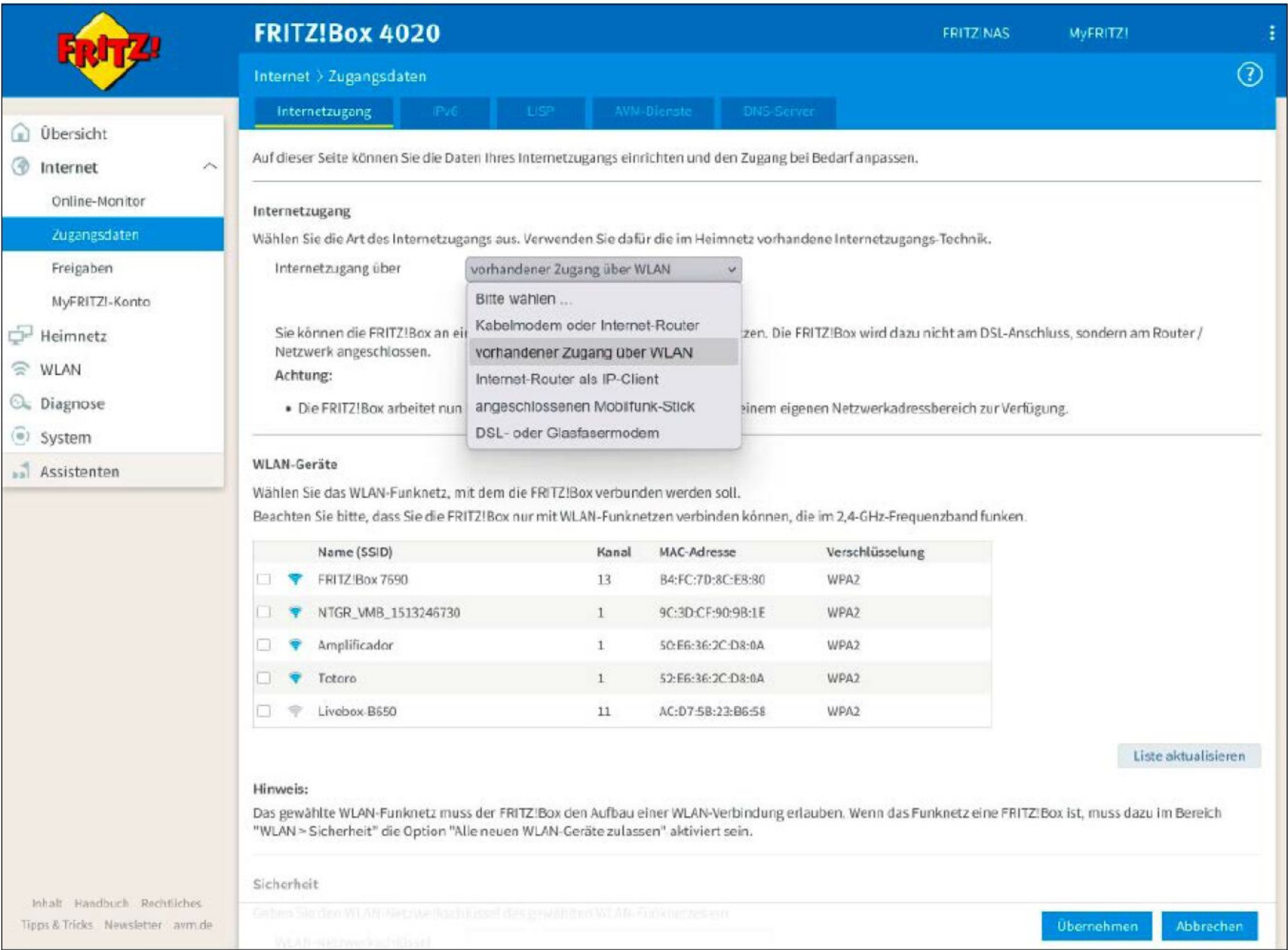
Hilfe vom Nachbarn: Online gehen über das WLAN nebenan

Wollen oder können Sie den Fritzbox-Ausfallschutz nicht nutzen, hilft Ihnen bei einem Internetausfall eventuell ein freundlicher Nachbar. Ist dessen Router noch online, können Sie Ihr Heimnetz vorübergehend über eine WLAN-Verbindung zum WLAN des Nachbarn ins Internet bringen. Dazu baut Ihre Fritzbox über das 2,4-GHz-Band eine Verbindung zum anderen WLAN auf. Diese besondere Internetzugangsfunktion, bei der ein vorhandenes WLAN als WAN-Zugang genutzt wird, nennen andere Routerhersteller „WISP“ (Wireless Internet Service Provider): Sie erlaubt es, dass der eigene Router sich trotz einer WLAN-Verbindung so verhält, als wäre er direkt im Internet. Er verbindet sich zunächst mit dem vorhandenen WLAN, holt sich per DHCP eine WAN-IP-Adresse von dessen Router, spannt aber ein eigenes, getrenntes Heimnetzwerk auf. Allerdings unterstützen nur bestimmte Modelle diese Funktion: Fritzbox 7590, 7490, 7583 VDSL, 7520, 7530, 7560, 7580, 7583, 4020, 4040, 4050, 4060, 6850 LTE, 6860 5G und 6850 5G. Einige dieser Modelle erhalten aber inzwischen keinen Support mehr und damit keine Firmware-Updates gegen Sicherheitslücken: Diese sollten Sie grundsätzlich nicht mehr direkt mit dem Internet verbinden. Falls Ihr Nachbar ebenfalls eine Fritzbox nutzt, nutzt diese wahrscheinlich denselben IPv4-Adressbereich. Ihre Fritzbox wird in diesem Fall bei der ersten Verbindung zum anderen WLAN selbstständig ihren Adressbereich ändern. Sie müssen dann das Webmenü Ihrer Fritzbox unter einer anderen IP-Adresse aufrufen. Auch die IP-Adressen Ihrer Clients im Heimnetz ändern sich dann entsprechend. Da Ihre Fritzbox weiterhin als Router mit aktivierter Firewall arbeitet, hat Ihr Nachbar keinen Zugriff auf Ihr Heimnetz. Umgekehrt könnten Sie sich hingegen aus Ihrem nachgeschalteten Heimnetz mit dem Heimnetz Ihres Nachbarn verbinden, weshalb er entsprechende Sicherheitsvorkehrungen treffen sollte: Am besten erlaubt er die WLAN-Verbindung zu Ihnen über das Gastnetz seines Routers: Dann sind die beiden Heimnetze auf jeden Fall getrennt. ■



Setzen Sie auch als Ausfallschutzrouter eine Fritzbox ein, müssen Sie den internen LAN-IPv4-Adressbereich ändern. Diese Einstellung ist im Fritzbox-Menü in den erweiterten Netzwerkeinstellungen versteckt.

Nach der Änderung der IPv4-Adresse in der Fritzbox wird Ihnen die neue Adresse noch einmal angezeigt. Notieren Sie sich diese, damit Sie auch künftig auf das Menü des Routers zugreifen können.



Vor allem ältere Fritzbox-Modelle wie zum Beispiel die Fritzbox 4020 kommen auch per WLAN-Verbindung zu einem anderen Router ins Internet und arbeiten dabei weiterhin mit Routerfunktionen.



Druckerprobleme gratis lösen

Drucker bieten unterschiedliche Wartungsseiten an, mit denen Sie feststellen können, ob und was mit einem Ausgabegerät nicht in Ordnung ist. Eine kostenlose Hilfestellung, die Sie sowohl bei Tintenstrahl- als auch Laserdruckern nutzen sollten. Es lohnt sich.

VON INES WALKE-CHOMJAKOV

Brief, Einladungskarte, Foto: Die Arbeit am Dokument ist fertig. Jetzt fehlt nur noch der Ausdruck. Doch wenn Sie auf dem gedruckten Resultat Mängel erkennen, geht das schnell an die Nerven. Streifen, verschobene Buchstaben oder falsche Farben stören nicht nur, sie machen den Ausdruck unbrauchbar. Und nicht immer ist sofort klar, wo die Ursache für die schlechte Druckqualität liegt.

„Jeder Printer hat Wartungsseiten, die Ihnen bei Druckproblemen helfen – und zwar gratis.“

Hier kommt es auf die richtige Druckerwartung an. Denn es lohnt sich, die drucker-eigene Hilfe anzunehmen. Mitgelieferte Serviceseiten in Treiber und Gerät unterstützen Sie dabei, gängigen Druckermängeln schnell auf den Grund zu gehen und sie zu beheben. Je nachdem, ob Sie einen Tintenstrahldrucker oder einen Laserprinter einsetzen, unterscheiden sich die Testseiten. Mit den Tipps aus diesem Beitrag wissen Sie, wo Sie die kostenlose Druckerhilfe finden, wie Sie die ausgedruckten Muster interpretieren und optimal zur Problemlösung einsetzen.

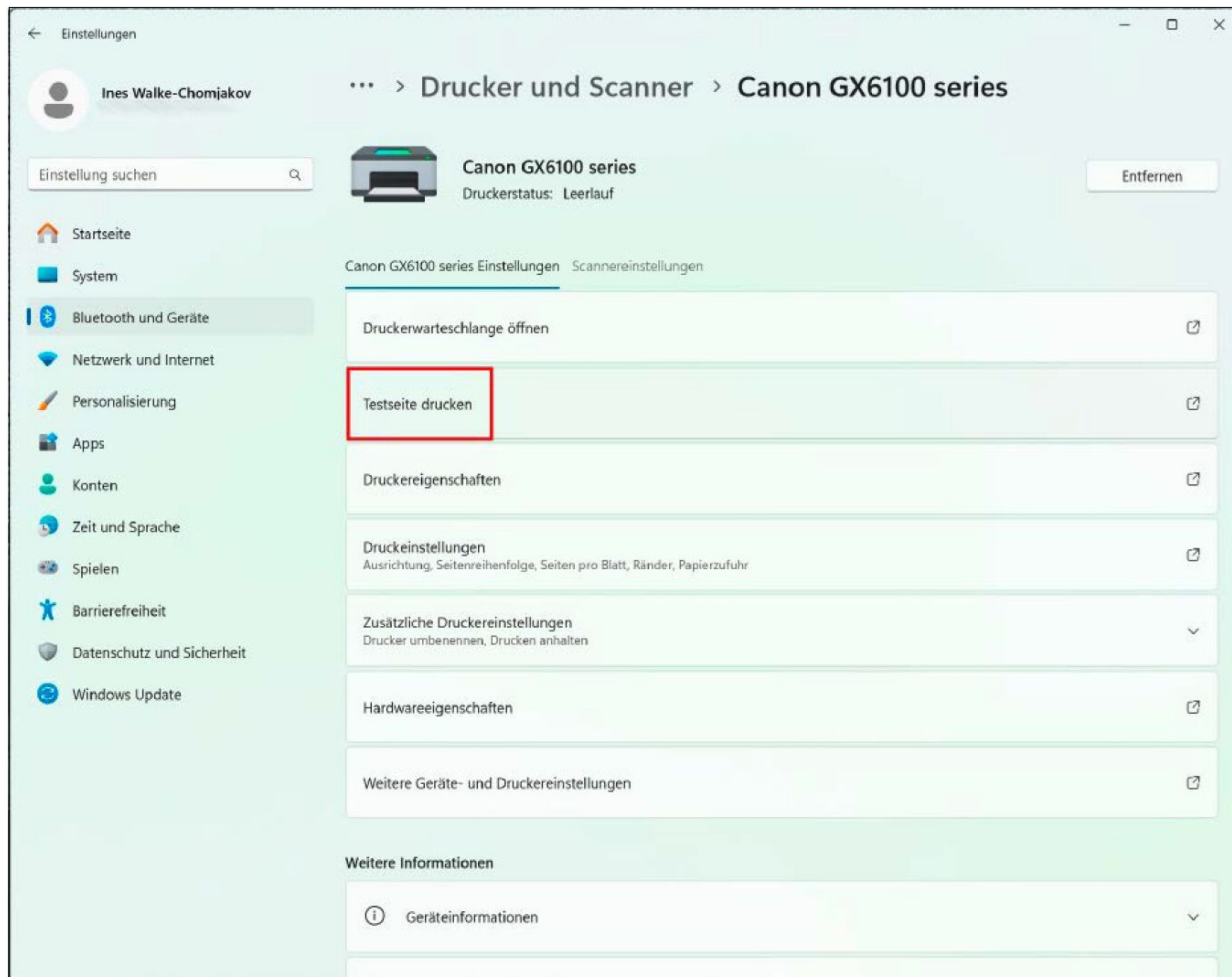
Über Windows: Druckertestseite für den Verbindungs-Check

Wer schon einmal einen Drucker installiert hat, kennt sie: die Windows-Druckertestseite. Mit ihr endet nahezu jede Treiberinstallation eines neuen Ausgabegeräts unter Windows. In der Regel ist die Testseite in

die Routine beim Aufspielen des Druckertreibers integriert. Ob Sie sie jedoch nutzen, bleibt Ihnen überlassen.

Für einen ersten Check, ob die Verbindung zwischen Windows-Rechner und Drucker korrekt funktioniert, ist die Testseite ein empfehlenswertes Mittel. Wird sie ausgegeben, können Drucker und Rechner oder Mobilgerät miteinander kommunizieren. Läuft der Druckauftrag ins Leere, merken Sie sofort, dass etwas mit der Verbindung nicht stimmt.

Auch zwischendurch ist der Einsatz der Windows-Testseite praktisch. So erkennen Sie schnell Verbindungsprobleme von Rechner und Drucker. Sie rufen sie in den Systemeinstellungen von Windows auf, indem Sie „Drucker und Scanner“ in die Suchzeile eingeben, auf die gleichlautende Auswahl und Ihr Druckermodell klicken. Mit einem Klick auf „Testseite drucken“ senden Sie das Dokument an den Drucker.



Bei der Erstinstallation oder zwischendurch: Dank der Windows-Druckertestseite wissen Sie schnell, ob die Kommunikation zwischen Drucker und Rechner reibungslos funktioniert.

Das Blatt liefert auch wertvolle Infos: Unter „Print Driver Properties“ sehen Sie den „Treibernamen“. Er enthält meist auch die Produktbezeichnung oder zumindest die Geräteserie, zu der das Modell gehört. Das ist immer dann wichtig, wenn Sie etwa ein Problem im Internet recherchieren wollen und die genaue Modellbezeichnung nicht parat haben. Um zu checken, ob Sie den Treiber aktualisieren sollen, finden Sie auf dem Blatt auch die derzeit eingesetzte Treiberversion. Sie lässt sich einfach mit einer eventuellen Aktualisierung vergleichen. Einen Testausdruck wie unter Windows gibt es in den Mobilbetriebssystemen Android und iOS nicht. Selbst die Drucker-Apps der Hersteller bieten keinen reinen Verbindungstest zwischen Smartphone/Tablet und Drucker an.

Tintenstrahldrucker: Düsentestseite bei streifigen Ausdrucken

Ein Tintenstrahldrucker bringt die Tinte über viele Druckdüsen aufs Papier. Diese sind am Druckkopf nach Farben angeordnet. Sie können ganz oder teilweise ausfallen oder durch Staub, Tintenreste und Papierabrieb verstopfen. Spätestens, wenn Sie einen Ausdruck in den Händen halten, der Streifen aufweist oder dessen Farben teilweise nicht stimmen, ist es Zeit für ei-

nen Düsentest. In allen Windows-Treibern von Tintenstrahldruckern sind spezielle Musterseiten für den Düsentest hinterlegt. Auch wenn sich die Vorlagen dafür je nach Druckerhersteller optisch unterscheiden, zeigen sie Motive, aus denen sich erschließen lässt, ob alle Düsen korrekt arbeiten. Meist sind das feine Linien und/oder farbige Balken. Richten Sie Ihr Augenmerk darauf, ob Ihnen fehlende Striche und streifige Balken auffallen. Auf dem Ausdruck sehen Sie alle Druckfarben. So finden Sie schnell heraus, welche Farbe(n) und damit welche Düsen Probleme machen. Die Düsentestseite für Ihr Druckermodell finden Sie im Druckertreiber unter „Wartung“ oder „Utility“. Bei Druckern und Multifunktionsgeräten, die sich auch ohne PC über ein Display bedienen lassen, ist sie meist zudem direkt im Drucker hinterlegt. Suchen Sie im Menü in den „Einstellungen“ nach dem Menüpunkt „Wartung“. Sehen Sie auf dem Testausdruck unterbrochene Linien und/oder Streifen, sind die Düsen an diesen Stellen ganz oder teilweise ausgefallen. In der Regel zeigt der Drucker im Treiber oder am Display nach der Ausgabe der Düsentestseite automatisch einen Mustervergleich an. Er hilft Ihnen, zu beurteilen, ob eine Düsenreinigung nötig ist. Nach der Reinigung wiederholt sich der



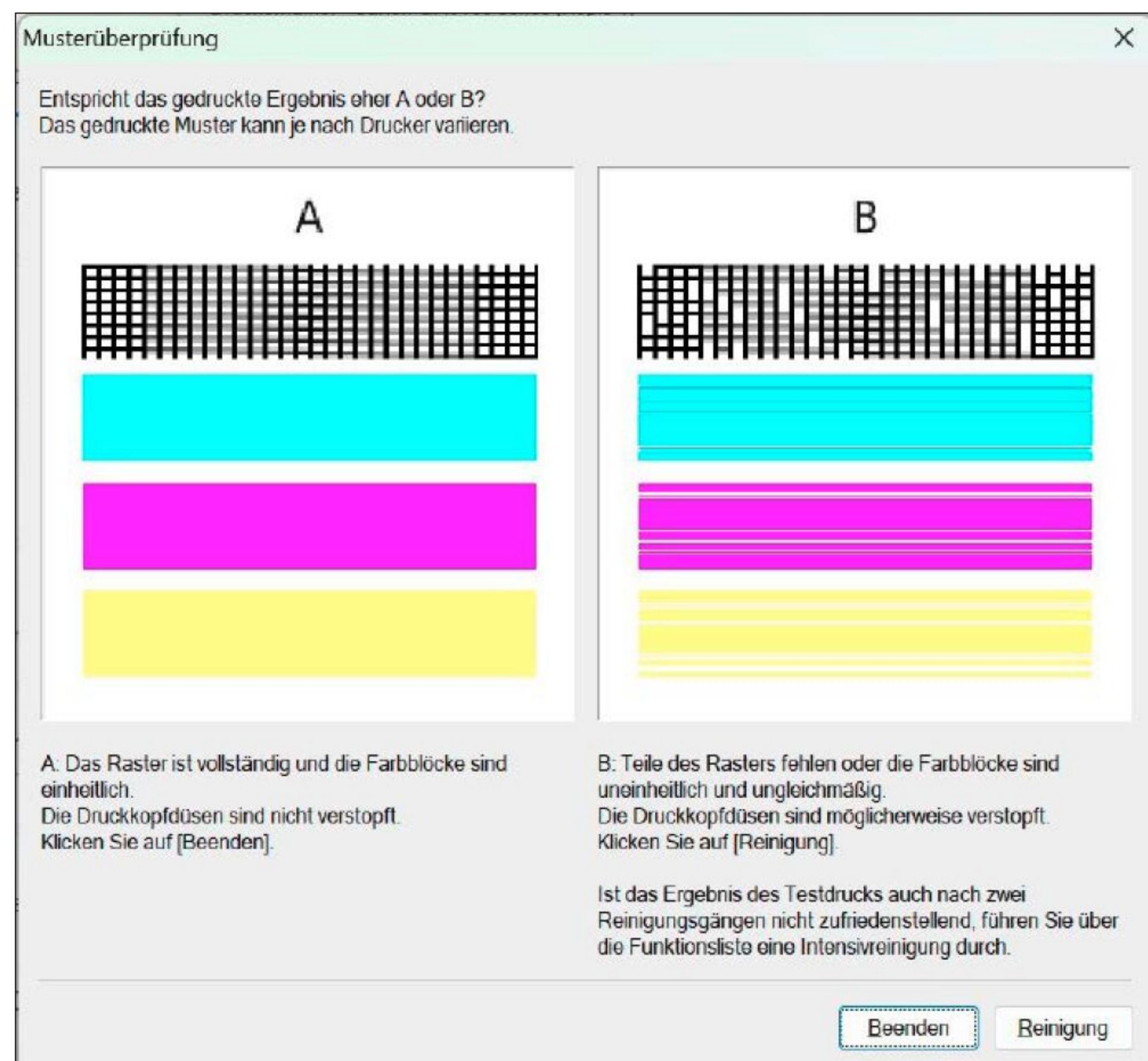
Wartungsvorgänge für Tintenstrahldrucker können Sie auch per App vom Smartphone oder Tablet aus starten – hier zum Beispiel einen Düsentest über die Smart-Panel-App des Herstellers Epson.

Vorgang. Sie werden aufgefordert, die Düsentestseite auszugeben, anhand der Sie beurteilen, ob Sie weitere Reinigungsgänge durchführen müssen.

Bei manchen Druckermodellen lassen sich Düsenreinigungen sogar auf bestimmte Farben begrenzen – etwa nur auf die Schwarz-Düsen. Das spart Tinte, die beim Reinigen zwangsläufig verbraucht wird.

Druckkopfausrichtung: Unschärfen bei Inkjetdruckern beheben

Bei einem Tintenstrahldrucker spielt neben einwandfrei funktionierenden Düsen auch die Position des Druckkopfs eine entscheidende Rolle für einen qualitativ hochwertigen Ausdruck. Stimmen Abstand vom Papier und Position des Druckkopfs nicht, sehen Sie auf dem Papier anstelle von geraden minimal versetzte Linien. Die Folge: Texte und Bilder sind auf dem Papier unscharf dargestellt. Auch Farbtöne sind ver-



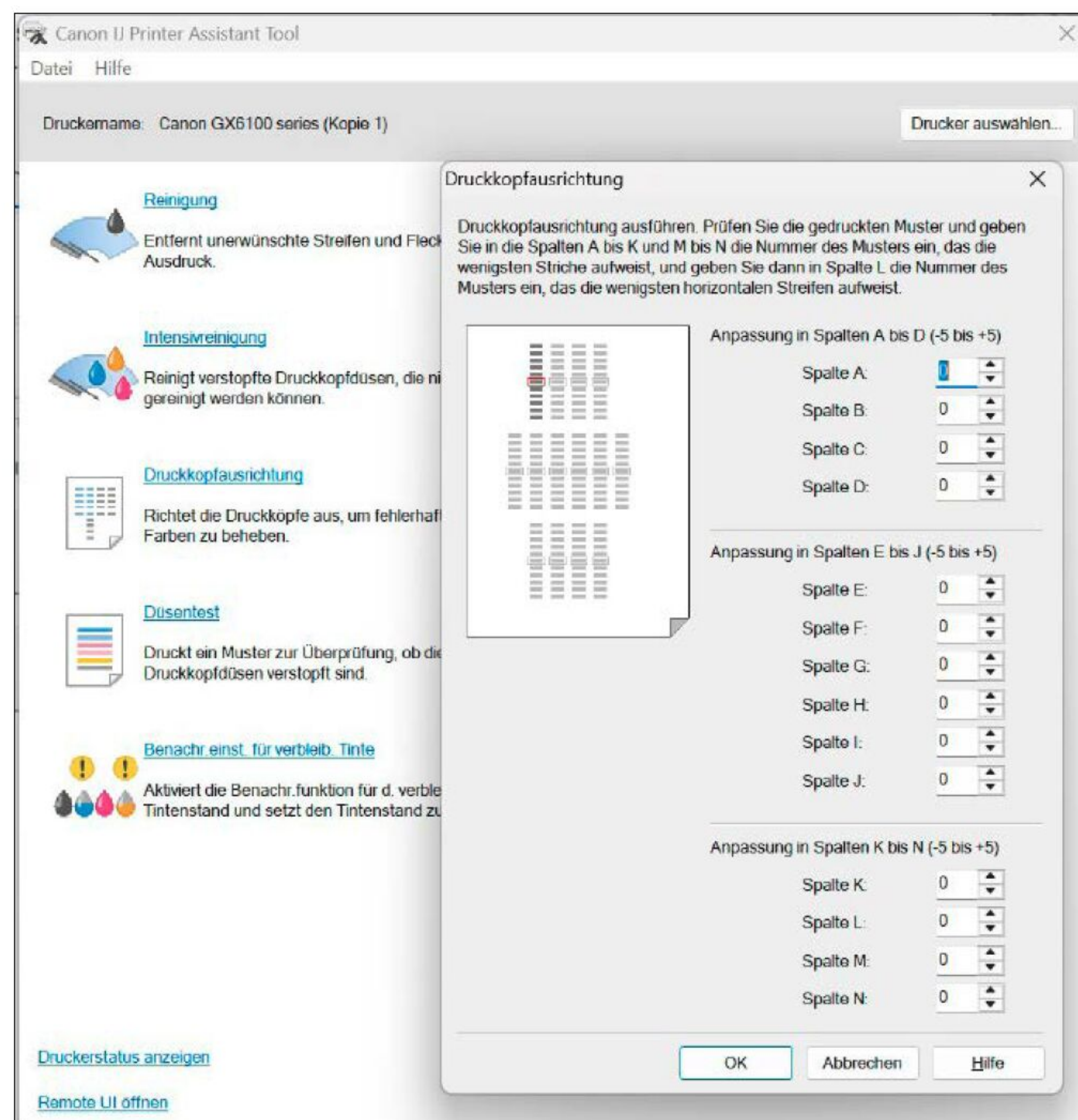
Beim Düsentest zeigt der Tintendrucker ein Muster an, das Ihnen die Entscheidung erleichtert, ob eine Düsenreinigung nötig ist. Fehlen Stellen oder sehen Sie Streifen auf dem Ausdruck, starten Sie den Vorgang.

fälscht. Eine inkorrekte Position des Druckkopfs beeinträchtigt die Farbmischung. Die Ursachen sind vielfältig: Oft verändert sich die Position des Druckkopfs schon einen Hauch, wenn Sie das Gerät an einen anderen Platz stellen oder länger transportieren. Auch ein Patronenwechsel kann sich negativ auf die Druckkopfposition auswirken. Bei Patronen mit integriertem Druckkopf ist das Ausrichten obligatorisch, sobald Sie eine neue Tintenpatrone eingesetzt haben. Der Druckkopf ist in diesem Fall genauso neu wie die Tinte und muss angepasst werden.

Bei einem Gerät mit separaten Tintenkartuschen wechseln Sie üblicherweise nur die Farbe, die Sie gerade leer gedruckt haben. Der Druckkopf selbst bleibt ungetastet. Er sollte nur ausgerichtet werden, wenn Sie Qualitätsmängel feststellen. Dasselbe gilt für einen Printer mit Tintentanks. Hier befinden sich Druckkopf und Tanks sogar an unterschiedlichen Stellen im Gerätinneren. Sie sind mit Schläuchen verbunden. Beim Nachfüllen wird der Druckkopf deshalb gar nicht tangiert.

Für die Druckkopfjustage bietet jedes Tintenstrahlgerät ein Prozedere im Treiber oder direkt im Bedienmenü am Gerät an. Sehen Sie unter „Wartung“ nach und starten Sie den Vorgang, indem Sie auf „Druckkopfausrichtung“ oder „Druckkopfjustage“ klicken. Danach unterscheiden sich die Verfahren abhängig vom Hersteller und sogar der Druckerserie. Im einfachsten Fall läuft der Prozess automatisch ab: Bei vielen Multifunktionsgeräten für zu Hause erhalten Sie einen Ausdruck, den Sie auf das Scannerglas legen. Die Justage übernimmt der Drucker im Zusammenspiel mit der Scaneinheit.

Bei der Mehrzahl der Drucker müssen Sie aktiv mitmachen: Sie entscheiden anhand mehrerer Ausdrücke mit Farbfeldern, die mit Buchstaben und Ziffern versehen sind. Es geht sowohl um die vertikale als auch horizontale Ausrichtung des Druckkopfs. Befolgen Sie genau die eingeblendeten Anweisungen. Schritt für Schritt geben Sie die jeweils beste Buchstaben-Ziffern-Kombination ein. In der Regel passt jene, deren Farbfeld am homogensten dargestellt ist – sprich: ohne Streifen, Striche oder durchscheinendes Weiß des Papiers (sogenannte Blitzer). Sind alle Felder der Musterseiten abgearbeitet, bestätigen Sie die Eingaben mit „Ok“. Der Druckkopf ist nun neu justiert.



Mit der Druckkopfjustage sorgen Sie beim Inkjetdrucker dafür, dass er Druckpunkte exakt setzt. Damit korrigieren Sie versetzte Linien und falsche Farbtöne. Über Musterseiten wählen Sie die besten Buchstaben-Ziffern-Kombinationen aus.



Gerade Multifunktionsgeräte für zu Hause nutzen Kombipatronen. Bei einem Wechsel tauschen Sie sowohl Tinten- als auch Druckköpfe aus. Das Ausrichten eines frisch eingesetzten Druckkopfs ist ein Muss.

tiert. Anhand eines Probedrucks überprüfen Sie, ob die Mängel verschwunden sind. Ist das nicht der Fall, können Sie den Druckkopf nachjustieren. Dazu starten Sie einen zweiten Ausrichtungsvorgang.

Laserdrucker: Verbesserte Farben durch Kalibrierung

Auch bei einem Laserdrucker oder -Multifunktionsgerät kommt es vor, dass Ausdrucke Mängel aufweisen – zum Beispiel Streifen oder zu blasser, auch leicht verschmierter Farben. Im Gegensatz zu Tintenstrahldruckern bieten Lasergeräte für den heimischen Einsatz vielfach keine integrierten Wartungsseiten an, die bei der Ursachenforschung helfen könnten.

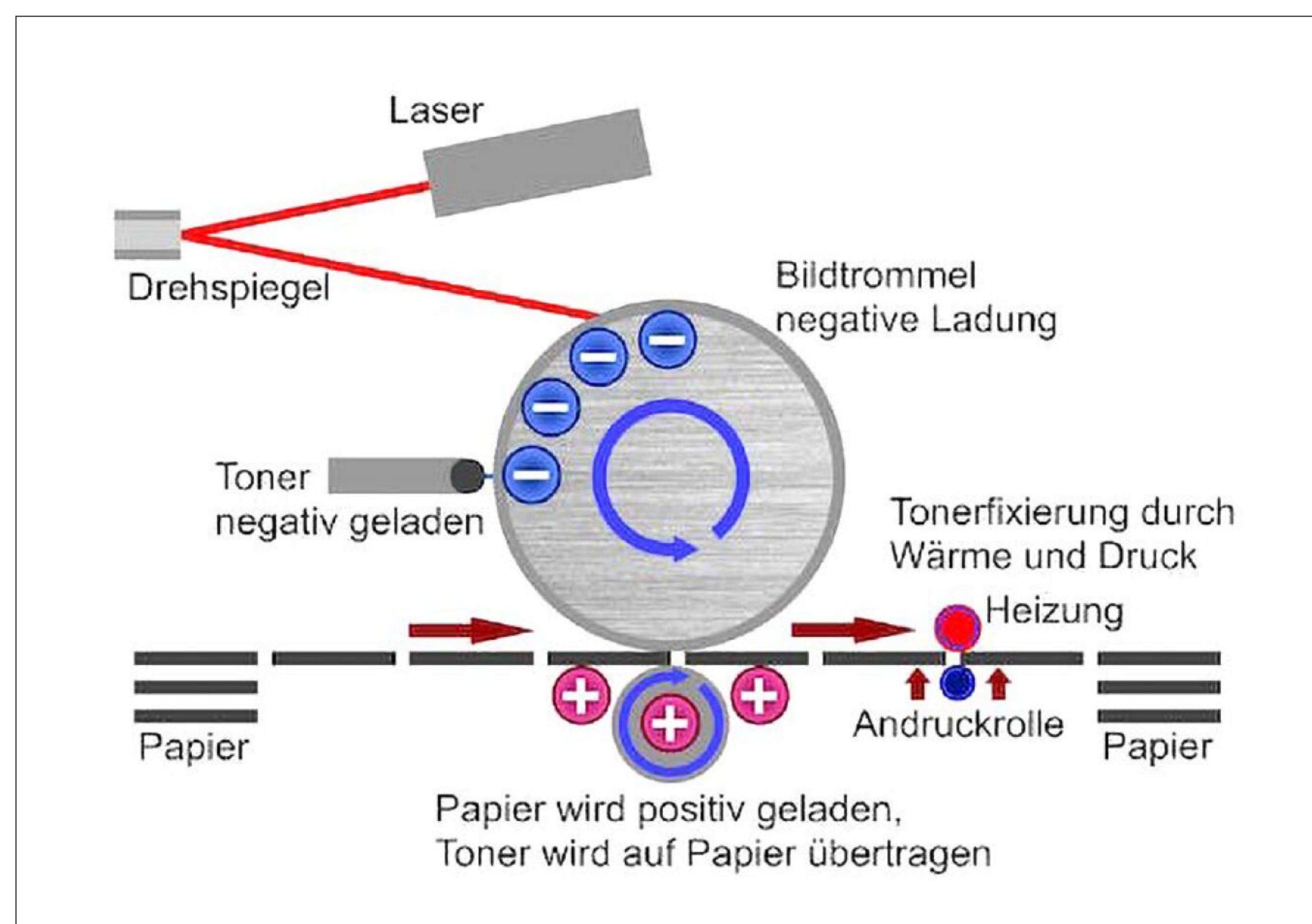
Vielmehr haben Laserprinter Verfahren integriert, die in bestimmten Zeitabständen automatisch ablaufen, um die Druckqualität konstant auf einem hohen Niveau zu halten. Dazu zählt die Farbkalibrierungsfunktion. Sie lässt sich bei manchen Modellen auch manuell anstoßen, sobald Defizite am Druckergebnis auffallen. Hat Ihr Drucker ein Display, suchen Sie im Bedienmenü nach Begriffen wie „Einrichtung“ oder „Systemkonfiguration“. Meist finden Sie die Funktion unter „Druckqualität“. Sobald Sie den Vorgang starten, erscheint ein entsprechender Hinweis auf dem Display. Warten Sie, bis die Farbkalibrierung vollständig abgeschlossen ist, und starten Sie erst dann einen Probedruck.

Laserdrucker, die übers Netzwerk betrieben werden, lassen sich auch über ein Webinterface verwalten. Um es aufzurufen, geben Sie die IP-Adresse des Druckers in die Adresszeile des Browsers ein. Hier sind oft Wartungsfunktionen integriert, auch wenn Sie die Services weder über den Druckertreiber noch direkt am Gerät aufrufen können. Ist das Webinterface Ihres Druckermodells durch ein Passwort geschützt, suchen Sie im Handbuch zum Drucker nach den Default-Zugangsdaten. Alternativ können Sie diese auch per Online-recherche herausfinden.

Besonderheit bei Laserdruckern: Reinigungsseite für Trommel

Bei Laserdruckern ist viel Mechanik im Spiel. Die Bildtrommeln, die – elektrisch aufgeladen – die Tonerpartikel anziehen. Die Transferrolle, die den Toner auf das Papier überträgt. Die Fixiereinheit, die mit hoher Temperatur den Toner auf dem Pa-

Viele Laserdrucker-Multifunktionsgeräte haben ein Display, über das Sie auch Wartungsvorgänge starten können. Als Mittel zur Farbverbesserung bietet sich die Farbkalibrierung an.



Laserdruck ist ein sehr mechanischer Vorgang. Deshalb sammeln sich viele Schmutzpartikel im Gehäuseinneren an. Über den Modus „Reinigungsseite“ lässt sich die Bildtrommel säubern.

pier fixiert. Sie alle begünstigen, dass sich mit der Zeit Papier-, Toner- und Staubpartikel im Gehäuseinneren ansammeln. Das ist nahezu unvermeidlich und kann auch mit dem Resttonerbehälter nicht ganz verhindert werden.

Deswegen bieten viele Laserdrucker den Modus „Reinigungsseite“ an. Damit lassen sich die Partikel entfernen, die auf Ausdruck zu Flecken, aber auch zu vertikalen Linien und verschmierten Druckbildern führen können. Ob bei Ihrem Laserdrucker ein solcher Reinigungsmodus integriert ist, entnehmen Sie dem Handbuch zum Modell. Teils lässt er sich über das Bedienmenü oder Display unter „Wartung“ starten. Gegebenenfalls müssen Sie auch bestimmte Tastenkombinationen am Gerät drücken, um den Drucker in einen Service-Modus zu versetzen. Alternativ

kann der Reinigungsvorgang auch über das Webinterface mit Admin-Rechten initiiert werden.

Der Begriff „Reinigungsseite“ führt etwas in die Irre. Gemeint ist, dass zum Säubern ein Blatt weißes Papier verwendet wird. Genauer beschreiben Begriffe wie „Trommelauffrischung“ oder „Trommelreinigung“ den Vorgang. Beachten Sie zudem, dass das Blatt Papier bei manchen Laserdruckermodellen über die Einzelblattzufuhr manuell ins Gerät eingeführt werden muss. Ist der Prozess einmal angestoßen, darf er nicht unterbrochen werden. In der Regel erzeugt Ihr Drucker dabei mechanische Laufgeräusche. Um die Trommel vom Schmutz zu befreien, sind oft mehrere Durchgänge nötig. Verwenden Sie jeweils ein neues Blatt Papier und entsorgen Sie die gebrauchte Seite. ■

So senken Sie Ihre Druckkosten

Beim Drucken addiert sich zu den Hardwarekosten der Verbrauch für Tinte oder Toner sowie Papier. Das ist unvermeidlich, lässt sich aber aufs Nötigste reduzieren. Folgen Sie dazu diesen Spartipps, oder verwenden Sie die Vollversion Cleverprint von der Heft-DVD.



© Africa Studio - AdobeStock

VON INES WALKE-CHOMJAKOV

Drucken ist und bleibt ein Vorgang, der Material verbraucht und damit Kosten verursacht. Sie kommen einfach nicht darum herum, für Patronen und Papier zu sorgen. Allerdings haben Sie Einfluss darauf, wie viele Drucke Sie mit den Kartuscheninhalten schaffen und welche Menge an Papier Sie für die Ausdrücke aufwenden müssen. Anlaufstelle Nummer eins ist dabei der Druckertreiber. Er bietet einige Einstellungen, mit denen Sie den Verbrauch von Druckfarbe und Papier auf ein Minimum reduzieren können. Wie umfangreich die Sparmaßnahmen ausfallen, hängt stark vom Druckermodell ab. Trotzdem lohnt es sich, mithilfe dieser Tipps einen genauen Blick auf ihn zu werfen. In der Vollversion

„Bei jedem Drucker lassen sich die Kosten für Papier und Farbe senken – auch bei Ihrem Modell.“

Cleverprint (auf Heft-DVD) finden Sie einen praktischen Helfer, mit dem Sie das Sparpotenzial für jedes Druckermodell noch weiter erhöhen.

Besten Druckertreiber installieren

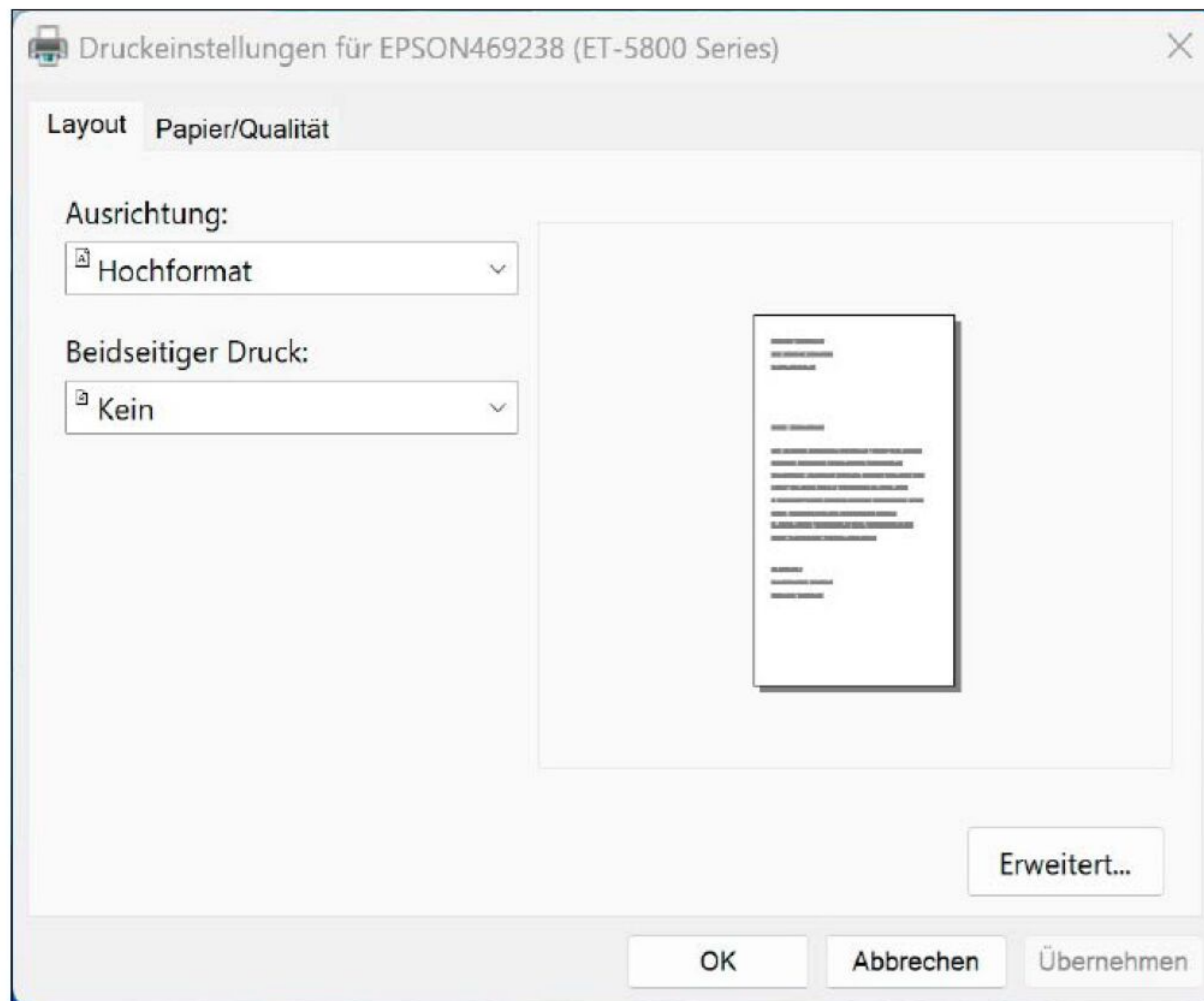
Bei Druckern kann es unterschiedliche Versionen von Treibern geben. Welche Fassung bei Ihnen vorhanden ist, hängt davon ab, wie Sie den Drucker in Betrieb nehmen. Überlassen Sie es Windows 10 oder 11, automatisch einen Treiber zu installieren, muss diese Version nicht vollständig mit dem Originaltreiber vom Hersteller übereinstimmen. Vielmehr kann sie abgespeckt sein, um zwar das Drucken zu ermöglichen, aber nicht unbedingt mit allen Einstellungsmöglichkeiten. Da darunter auch Optionen sein können, die Ihnen beim Senken von Druckkosten helfen, empfiehlt es sich, den vollständigen Herstellertreiber zu installieren. Dazu starten Sie eine Internetsuche mit der genauen Druckerbezeichnung – etwa HP Neverstop Laser MFP 1202nw. Wählen Sie den Treffer, der Sie auf die entsprechende Support-Webseite des Herstellers führt. Meiden Sie andere Angebote im Internet, da sie sich als Betrugsversuche entpuppen können. Suchen Sie das aktuelle Treiberpaket für Ihr

Modell und laden Sie es auf Ihren Rechner herunter. Nach einem Doppelklick auf die Datei startet in der Regel ein Installationsassistent. Folgen Sie den Anweisungen. Haben Sie ein Multifunktionsgerät, lässt sich oft gleichzeitig auch der Original-Scannertreiber installieren. Wiederum gilt, dass Sie so zur besten Lösung kommen.

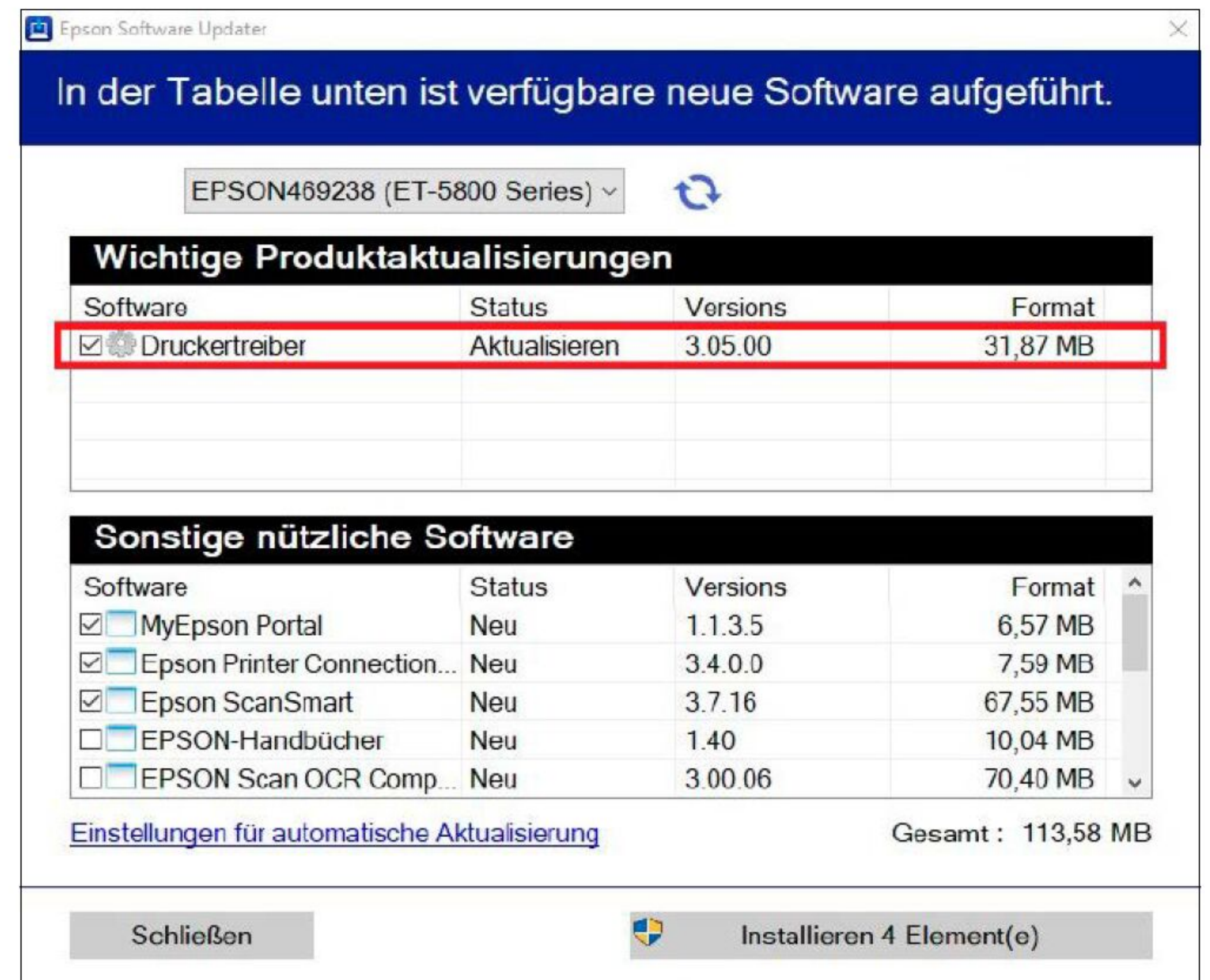
Tipp: Entfernen Sie den alten Druckertreiber bevor Sie das aktuelle Treiberpaket installieren. Dazu können Sie die Deinstallationsroutine des Druckers verwenden, die Sie bei Windows 10 im Bereich „Apps und Features“, bei Windows 11 unter „Apps → Installierte Apps“ finden. Auch Gratis-Tools wie Ccleaner (auf Heft-DVD) leisten gute Dienste bei der Deinstallation. Sie listen alle Programmbestandteile zum Gerät wie etwa Druck-Plug-ins auf. So werden sie alles bequem in einem Aufwasch los.

Druckertreiber aktualisieren

Meist läuft der Druckertreiber bei Updateaktionen unter dem Radar und ist deshalb nicht auf dem aktuellen Stand. Ein Update durchzuführen dient grundsätzlich der Sicherheit. Gleichzeitig ergänzt eine Aktualisierung häufig auch zusätzliche Talente – etwa, wenn so neue Papierformate und



Gerade bei Netzwerkversionen sind vom Betriebssystem automatisch installierte Druckertreiber oft sehr rudimentär mit Funktionen ausgestattet. Sie durch Originaltreiber zu ersetzen lohnt sich auf alle Fälle.



Hilfstoools zum Druckertreiber übernehmen oft die Suche nach Updates. Sie starten automatisch, wenn Sie im Treiber auf die Aktualisierungsfunktion klicken. Das ist komfortabel und bedienerfreundlich gelöst.

Papiersorten unterstützt werden. Auch das kann helfen, die Druckkosten zu senken. Denn so wählen Sie für jedes Druckprojekt das passende Format. Sie sparen den Papierabfall, den Sie sonst beim Zuschneiden verursachen würden. Außerdem vermeiden Sie Fehldrucke, weil Sie anhand der Druckvorschau mit dem idealen Format genau sehen, wie die Inhalte auf dem Blatt angeordnet sind. Gerade bei kreativen Projekten auf teuren Papieren können Fehldrucke die Kosten schnell in die Höhe treiben.

Das Treiberupdate bei Druckern für den Heim- und Homeoffice-Gebrauch geht in der Regel problemlos vonstatten. Meist ist die Aktualisierungsfunktion direkt im Treiber zu finden – etwa in den Bereichen „Wartung“ oder „Erweitert“. Sobald Sie auf den Update-Button klicken, startet die Onlinesuche nach einer neueren Version. Es kann auch ein Zusatztool verknüpft sein, das Sie bei der Drucker-Inbetriebnahme automatisch installiert haben. So nutzen zum Beispiel manche Epson-Druckermodele das Herstellerprogramm „Epson Software-Updater“. Es startet die Update-Suche automatisch. Folgen Sie einfach den angezeigten Hinweisen.

Richtig ausschalten spart Geld

Gerade wer selten druckt, schaltet das Ausgabegerät zwischen den Einsätzen aus. Besonders bei Tintenstrahlgeräten ist dabei auf den korrekten Ausschaltprozess zu ach-

ten. Er gewährleistet, dass der Druckkopf korrekt in die Parkposition fährt. Hier sind neben der Druckmechanik auch die Düsen am besten geschützt. Tintenreste können deshalb nicht so schnell antrocknen. Sie sparen sich so Düsenspülgänge, die in der Regel viel Tinte und damit Geld kosten. Um das Gerät korrekt abzuschalten, drücken Sie den Ausschalter am Gehäuse. Bei manchen Modellen müssen Sie etwas länger auf der Taste bleiben oder zusätzlich per Display den Ausschaltprozess bestätigen. Danach beginnt die Ausschaltoutine. Warten Sie sie auch dann ab, wenn die Düsen kurz durchgespült werden. Obwohl währenddessen Tinte verbraucht wird, schützt die Maßnahme die Düsen vor Tintenresten, die antrocknen und zu Verstopfungen führen können. Ist der Abschaltprozess beendet, können Sie den Stecker ziehen, um das Gerät komplett vom Stromnetz zu trennen.

Druckauflösung senken

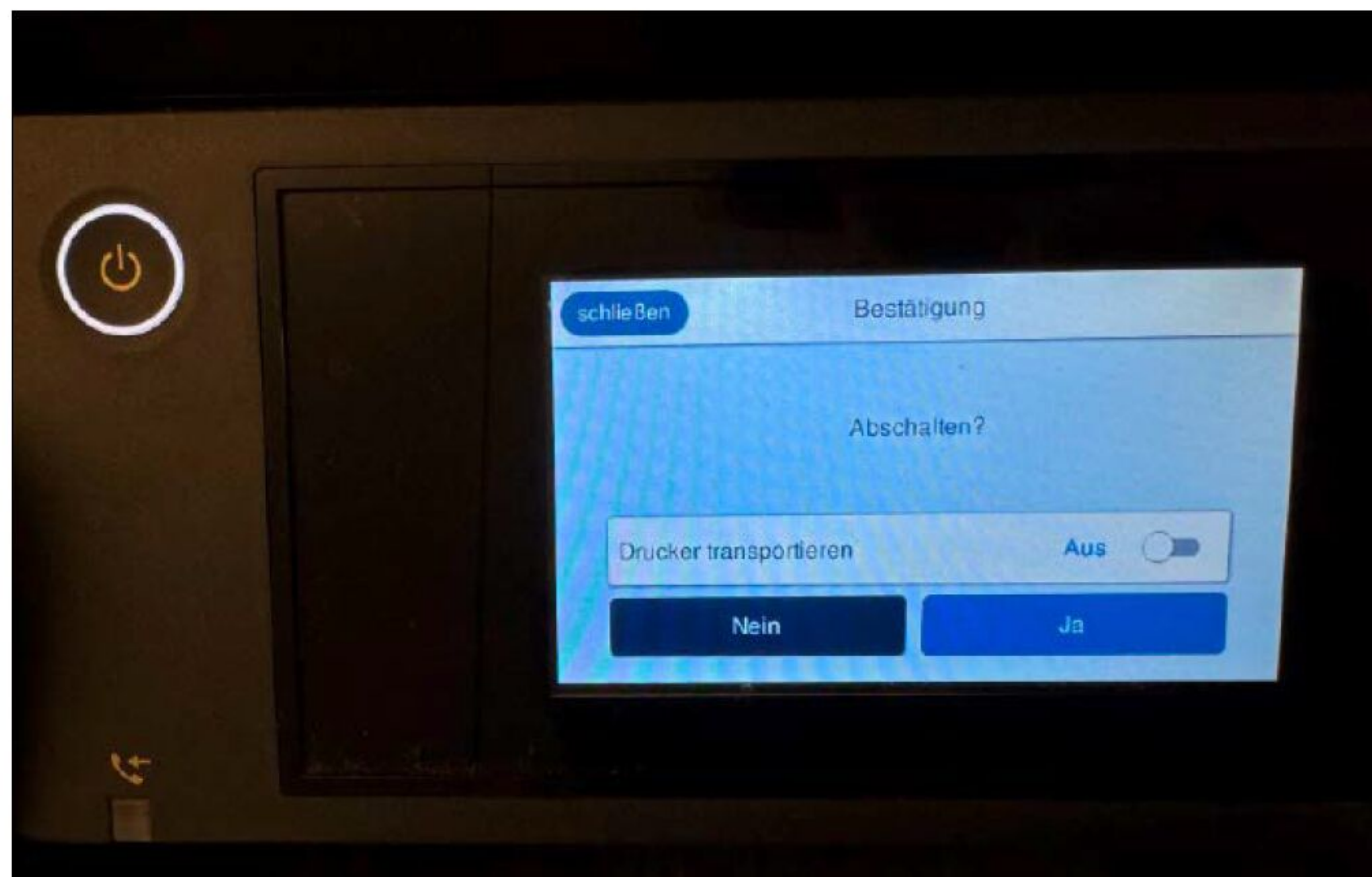
Viele Tintenstrahlprinter für zu Hause tendieren in der Standardauflösung dazu, relativ viel Tinte auf das Papier aufzubringen. Damit ist meist ein gutes Druckergebnis garantiert. Allerdings hat der hohe Tinten-auftrag zur Folge, dass sich die oft kleinen Patronen schnell leeren. Da ein Satz Nachkaufkartuschen – gerade als Originale vom Hersteller – schon bei Vierfarbgeräten 70 Euro und mehr kostet, sollten Sie mit der Flüssigkeit möglichst sparsam umgehen.

Eine Möglichkeit ist, die Auflösung zu senken. Probieren Sie ruhig einmal aus, wie die Deckung auf Normalpapier ausfällt, wenn Sie den Entwurfsmodus aktivieren. Teils lässt sich im Treiber auch ein spezieller Sparmodus einstellen, der die Reichweite der Tintenpatronen erhöht. Hier fallen Texte und Bilder nicht ganz so blass aus wie im Entwurfsmodus. Sie können Buchstaben in der Regel gut erkennen, auch wenn sie nicht so dunkel wie bei Standardauflösung gedruckt sind. Sollte Ihr Printer diese Einstellung unterstützen, finden Sie sie unter „Qualität“.

Auch beim Fotodruck können Sie die Auflösung senken, um Tinte zu sparen. Das gilt besonders dann, wenn Sie auf hochwertigen Fotopapieren drucken. Die hellweißen, glänzenden Oberflächen verstärken die Leuchtkraft der Farben. Dank der Papierschichten dringt die Tinte gesteuert ein – das erhöht die Präzision des Ausdrucks. Im Treiber wählen Sie zuerst den passenden Medientyp aus und senken dann die Auflösung. Oft erhalten Sie mit Standardauflösung bereits erstaunlich hochwertige Ergebnisse. Weiter sollten Sie die Auflösung aber nicht senken. Im Entwurfsmodus können Fotos nicht wirken.

Automatisch beidseitig drucken

Die einfachste Methode, dauerhaft möglichst wenig Papier zu verwenden, ist der automatische Duplex-Druck. Dazu muss der Drucker eine Wendeeinheit fürs Papier



Korrektes Ausschalten hilft, die Tintenkosten zu senken. Denn der Prozess sieht vor, die Düsen kurz zu spülen und den Druckkopf exakt zu parken. Beide Vorsichtsmaßnahmen ersparen später extra Spülgänge wegen verstopfter Düsen.



Multifunktionsgeräte mit Duplex-Druckeinheit können oft auch beidseitig kopieren. Die Einstellung finden Sie im Menü direkt am Gerät. In der Regel müssen Sie die Funktion für jeden Kopierauftrag erneut extra auswählen.

mitbringen. Sie sorgt dafür, dass das Blatt gedreht wird, sobald die Vorderseite bedruckt ist. Gleichzeitig können Sie sicher sein, dass Sie Fehler beim Bedrucken der Rückseite vermeiden – etwa, weil Inhalte auf dem Kopf stehen.

Um beim Papiersparen einen möglichst hohen Effekt zu erzielen, sollte der Duplex-

Druck für alle alltäglichen Druckaufträge gelten. Gerade bei Bürodrukern gilt er deshalb als Voreinstellung ab Werk. Bei Geräten für den heimischen Gebrauch müssen Sie das beidseitige Bedrucken meist erst im Treiber aktivieren. Einfacher machen Sie es sich mit einem Einstellungsprofil, das Sie bei Bedarf nur noch aufrufen

müssen. Nehmen Sie dafür zuerst die Einstellungen im Treiber vor – etwa Hochformat, zweiseitiges Drucken, Graustufen, Standardauflösung. Legen Sie dann eine neue Vorlage an, geben Sie ihr eine eindeutige Bezeichnung – etwa „Duplex Graustufen“ und sichern Sie sie. Die Einstellungen sind nun definiert und werden automatisch

UNNÖTIGE SEITEN LÖSCHEN MIT ABELSOFT CLEVERPRINT

Bei Ausdrucken von Webinhalten stören oft eingebaute Werbebanner, Bilder oder allgemeine Angaben am Ende der Webseite.

Mit der Vollversion Cleverprint von Abelssoft (auf Heft-DVD) lassen sie sich im Handumdrehen entfernen. Damit sinkt der Papierverbrauch deutlich.

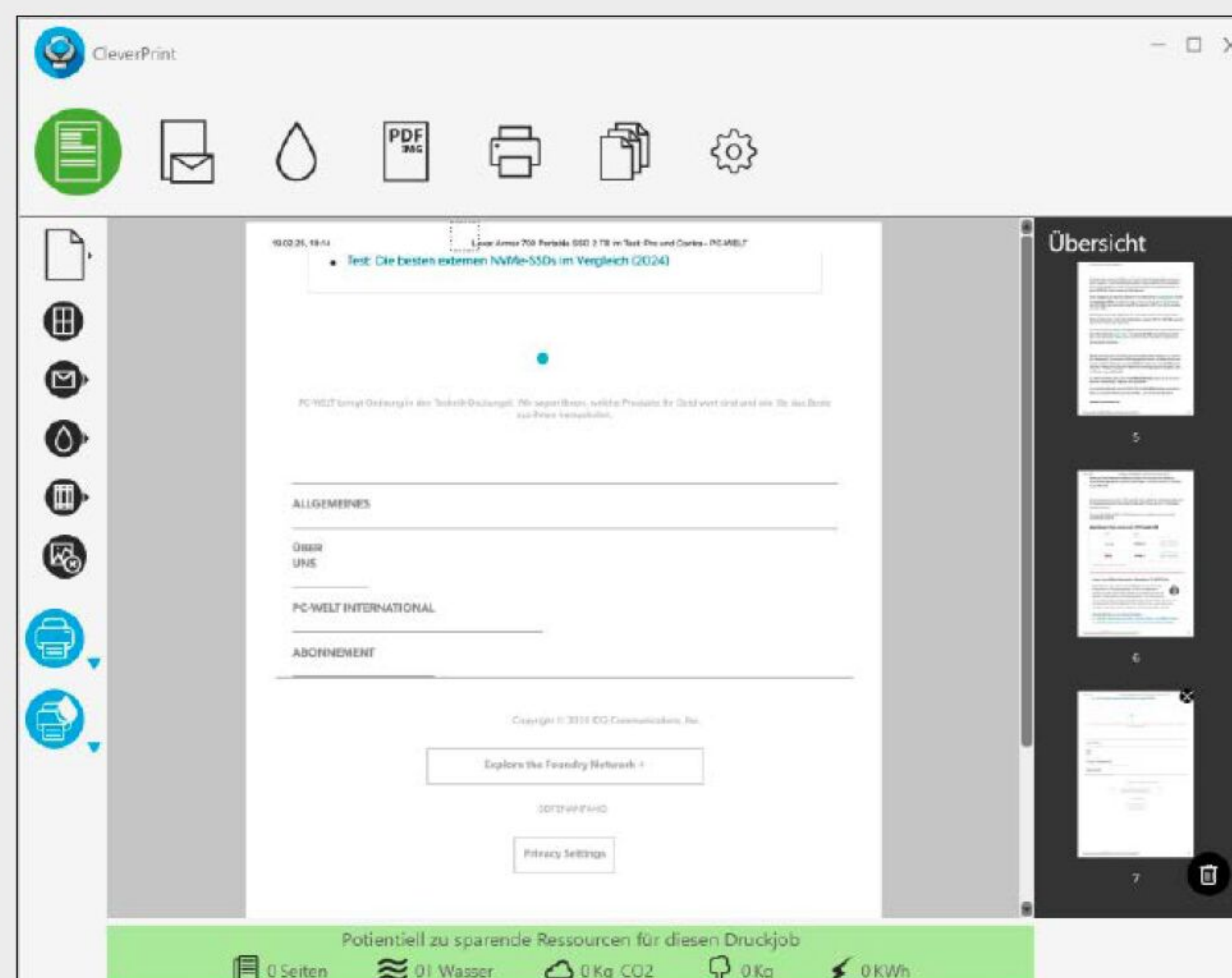
So geht's: Spielen Sie das Programm über den Installer auf unserer DVD auf Ihren PC, und starten Sie es. Um Onlineinhalte direkt über den Browser auszudrucken, gehen Sie etwa bei Google Chrome auf die drei Striche rechts oben im Fenster und auf „Drucken“. Wählen Sie nun aus den verfügbaren Druckern „Cleverprint“ aus, und klicken Sie auf „Drucken“. Das Programm bereitet den Druckjob nun auf – das dauert eine Weile, klappt aber auch, wenn Sie Cleverprint zuvor nicht aktiv gestartet haben.

Ist der Vorgang abgeschlossen, öffnet sich das Programmfenster. Sie sehen Ihren Druckauftrag als Vorschau. Rechts daneben unter „Übersicht“ finden Sie den Inhalt auf die Druckseiten verteilt. Hier können Sie durchscrollen und die Seiten identifizieren, auf die Sie verzichten wollen. Zum Löschen markieren Sie die betreffende Seite per Mausklick. Ein weiterer Klick auf das Papierkorb-Symbol rechts unten entfernt sie.

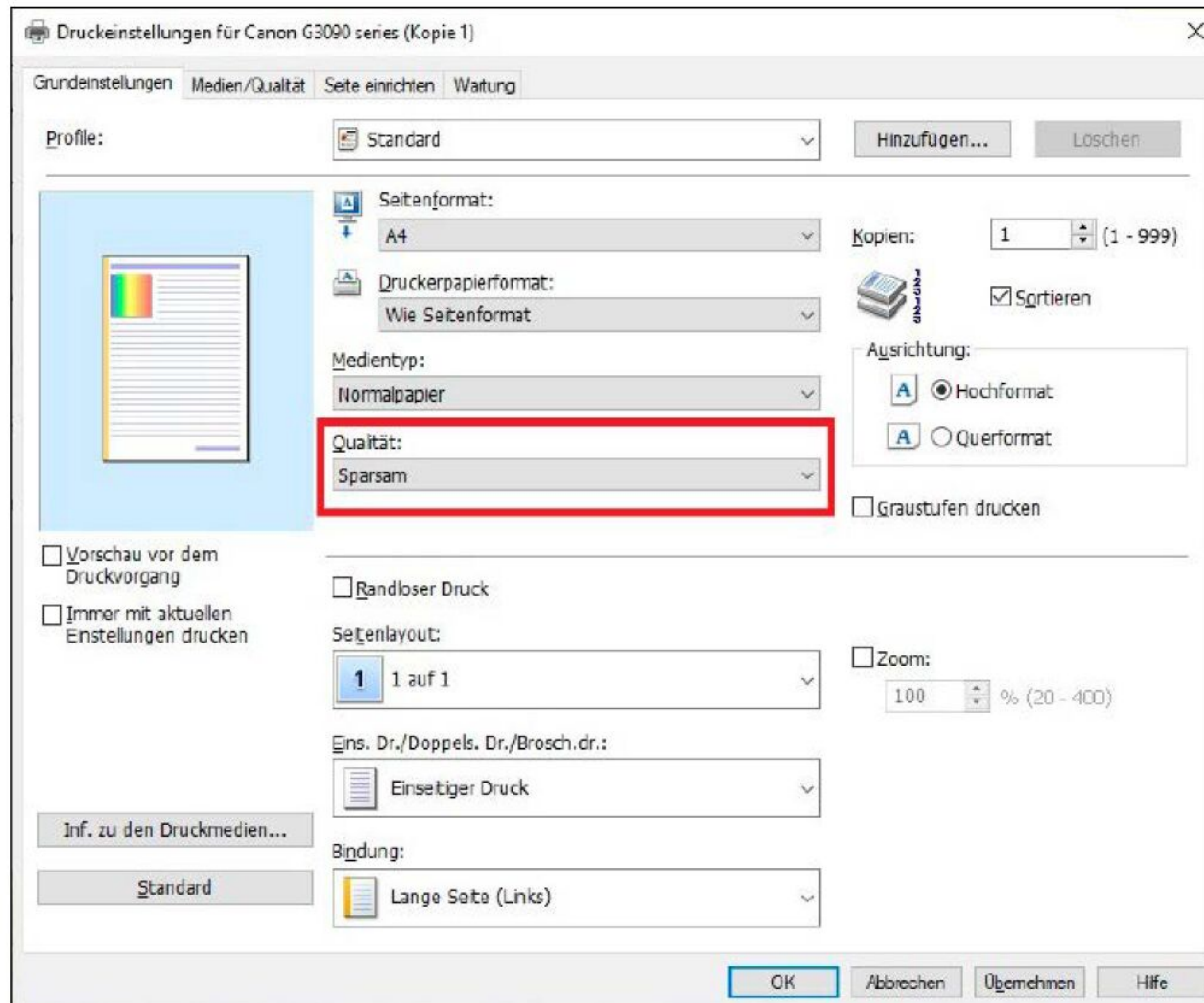
Wollen Sie zusätzlich zum Papier auch Tinte oder Toner sparen, können Sie links im Fenster unterschiedliche Maßnahmen ergreifen. Über das unterste Symbol drucken Sie automatisch im Entwurfsmodus mit stark vermindertem Farbauftrag. Zwei Symbole darüber finden Sie die Funktion „Grafiken aus den

Druckseiten entfernen“, über die Sie Abbildungen löschen und so weitere Druckfarbe einsparen können.

Über die obere Symbolleiste wählen Sie Ihren Drucker aus. Beherrscht er den automatischen Duplex-Druck, lässt dieser sich hier aktivieren – auch das erhöht das Sparpotenzial auf bequeme Weise.



Mit der Vollversion Cleverprint von Abelssoft identifizieren Sie flott Druckseiten, auf die Sie verzichten und so Papier sparen können. Sie lassen sich rechts in der „Übersicht“ mit nur zwei Mausklicks aus dem Druckjob entfernen.



Manche Druckermodelle bieten einen „Sparsam-Modus“, der den Tintenauftrag moderat senkt. Die Auflösung liegt zwischen Entwurfs- und Standard-Modi. So sparen Sie Tinte, ohne viel an Ausgabequalität einzubüßen.

übernommen, sobald Sie das Druckprofil aufrufen. Um es dauerhaft im Treiber zu aktivieren, klicken Sie einfach auf „OK“. Wählen Sie zusätzlich den Drucker als Standard-Ausgabegerät aus, um sicher zu sein, dass Sie von den Einstellungen bei jedem Druckjob profitieren.

Bei Multifunktionsgeräten mit Duplex-Einheit können Sie nicht nur automatisch beidseitig drucken, sondern auch papiersparend kopieren. Bei Geräten mit Display und Vorlageneinzug wählen Sie einfach im Kopiermenü die Einstellung für die Duplex-Kopie aus. Auch bei Modellen ohne ADF gelingt die Duplex-Kopie. Allerdings müssen Sie hier die Vorlagen nacheinander einzeln auf den Flachbettscanner legen. Dauerhaft voreinstellen lässt sich das Duplex-Kopieren meist nicht. Sie müssen es für jeden Kopierauftrag aktiv anstoßen.

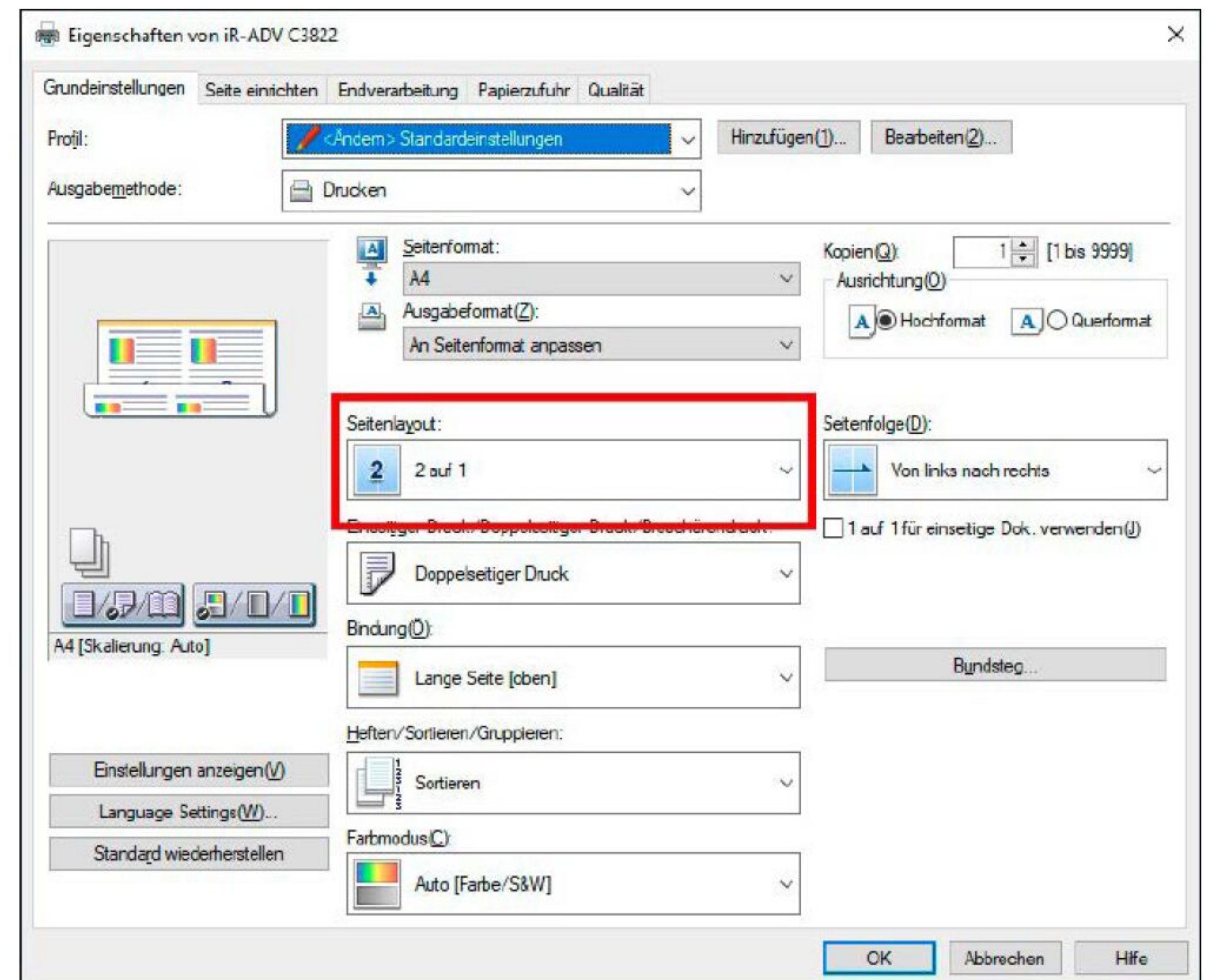
Mehrere Seiten auf ein Blatt

Weniger als permanente Einstellung als zum spontanen Papiersparen eignet sich die Multi-Page-Funktion. Darüber platzieren Sie auf einem DIN-A4-Blatt mehrere Seiten eines Dokuments. So können Sie zum Beispiel einen vierseitigen Brief auf zwei Blättern Papier ausdrucken.

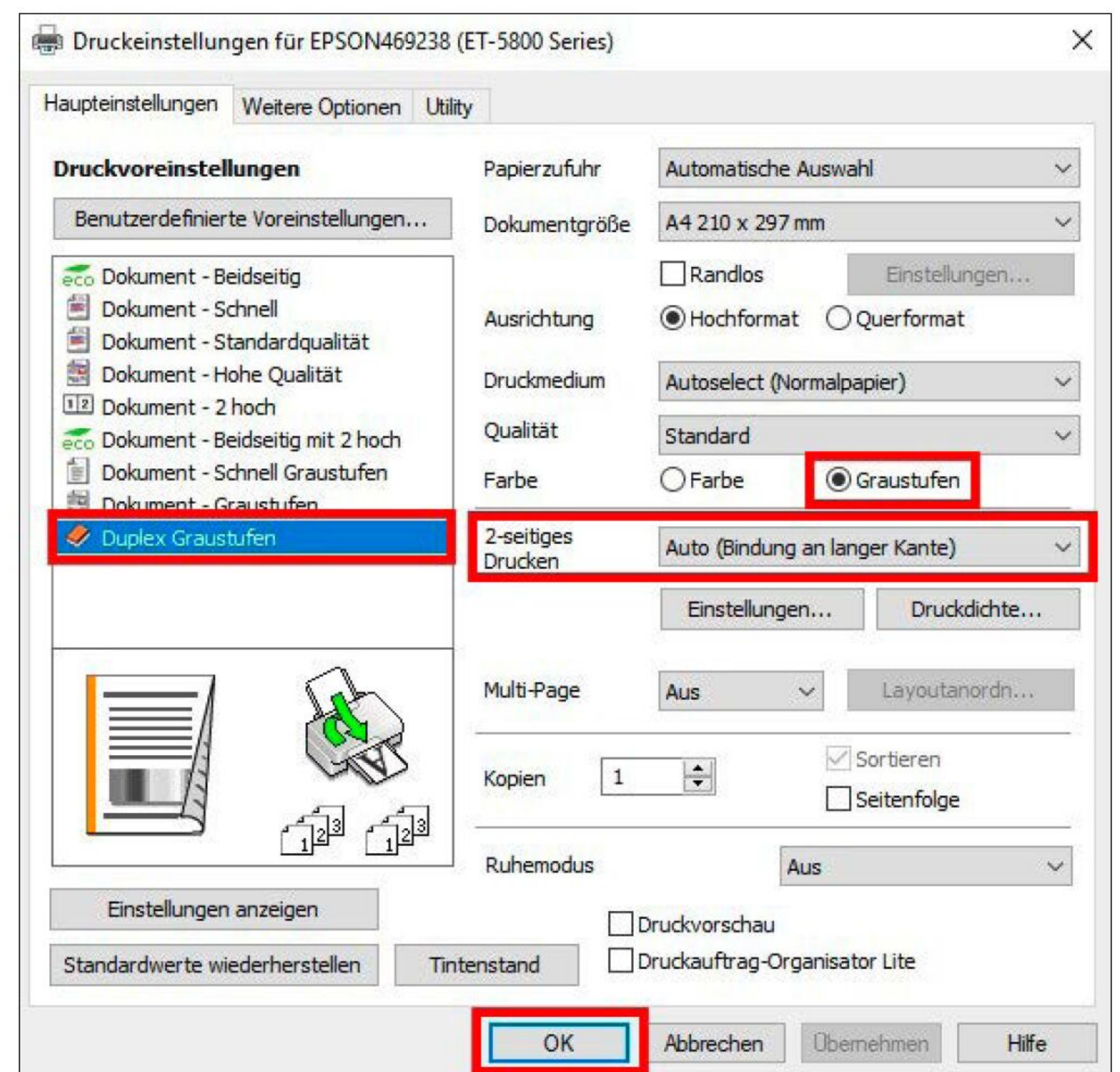
Um die Funktion für einen Druckauftrag zu nutzen, rufen Sie den Treiber aus dem gerade genutzten Programm auf – meist über „Datei → Drucken“. Klicken Sie auf „Druckereinstellungen“ oder „Druckereigenschaften“. Neben Multi-Page finden Sie die Funk-

Voreinstellungen lassen sich im Druckertreiber sichern, um sie jederzeit wieder aufzurufen. Neben Druckprofilen vom Hersteller können Sie eigene Varianten entwerfen, um möglichst sparsam zu drucken.

tion auch unter Bezeichnungen wie „Seitenlayout“ oder einfach nur „Layout“. Platzieren Sie nicht zu viele Seiten auf einem Blatt, wenn der Text noch lesbar sein soll. Ausschlaggebend sind die ursprünglich gewählten Einstellungen. Bei einem Word-Dokument mit einer Schriftgröße von 12 Punkt können Sie Texte auf zwei Seiten auf einem A4-Blatt noch gut lesen. Bei einer kleineren Schrift kann es schon schwierig werden, die Buchstaben leicht zu erkennen. Gleichzeitig sollten Sie bei Multi-Page die Seitenumbrüche des Dokuments im Auge



Indem Sie mehrere Seiten auf ein Blatt drucken, sparen Sie Papier. Die Treibereinstellung lohnt sich bei geraden Seitenumfängen besonders und ist in nahezu jedem Druckertreiber vorhanden.



behalten: Die Einstellung bietet sich für gerade Seitenumfänge (zwei, vier et cetera Seiten) an, da Sie die Papierfläche ideal ausnutzen und so den größten Spareffekt erzielen. Bei ungeraden Seitenumfängen nutzen Sie am besten die Druckvorschau im Treiber (falls vorhanden), um zu überprüfen, ob Sie wegen ein paar Zeilen am Ende des Dokuments ein neues Blatt benötigen. In diesem Fall brechen Sie den Druckauftrag ab und verschieben Sie die Zeilen. Alternativ schränken Sie den Druckauftrag auf die voll ausgenutzten Seiten ein. ■

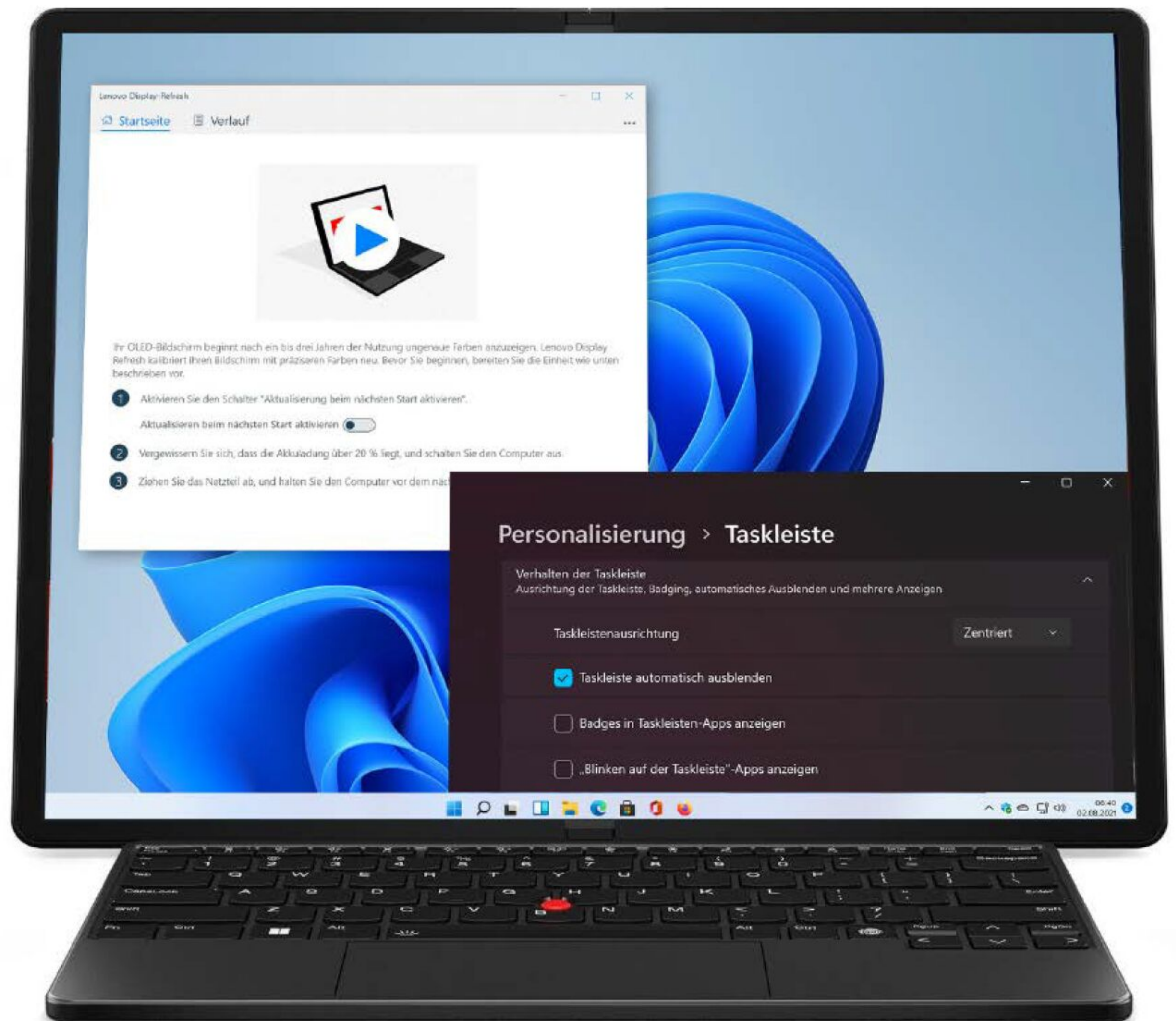
Oled-Pflege bei Notebook & Monitor

PC-Geräte wie Monitore und Notebooks mit Oled-Display werden immer beliebter. Die Gefahr von Defekten durch Einbrennen ist hier jedoch höher als bei Fernsehern. Mit den richtigen Pflegemaßnahmen können Sie bei Ihrem Oled-Schirm effektiv vorbeugen.

VON INES WALKE-CHOMJAKOV

Bildschirme mit Oled-Panels werden bei Notebooks und PC-Monitoren immer populärer. Der Grund: Die Preise für Oleds sind gesunken, was perspektivisch auch so weitergehen dürfte. Ein Notebook mit Oled-Display in Full-HD-Auflösung und mit 15 Zoll Diagonale bekommen Sie derzeit bereits ab 600 Euro, zum Beispiel das Modell Asus Vivobook Go 15 Oled. Sie finden hier zwar weder bei den Komponenten noch beim Schirm Top-Ausstattung. Allerdings meistert das in dieser Geräteklasse gebotene 60-Hertz-Display die meisten Alltagsaufgaben ohne Problem – solange es nicht ums Spielen geht.

„Oleds zeigen tolle Bilder, bergen aber die Gefahr von Schäden durch Burn-in. Mit den richtigen Maßnahmen beugen Sie vor.“



Ein Monitor mit Oled-Panel zielt oft auf spezielle Einsatzszenarien ab. Entweder unterstützt er das kreative Arbeiten mit überraschenden Details oder das Spielen am Rechner mit ultraschnellen Schaltzeiten. Ein Oled-Spielemonitor mit 27-Zoll-Diagonale, QHD-Auflösung und 240 Hertz Bildwiederholrate liegt preislich bei gut 550 Euro – wie zum Beispiel der LG Ultragear Oled 27GS95QE-B. Ein 4K-32-Zöller wie der Dell 32 Plus (S3225QC) schlägt mit 860 Euro aufwärts zu Buche. Damit sind Oled-Monitore zwar immer noch kein Schnäppchen, bewegen sich jedoch preislich immer mehr in erschwingliche Regionen.

Hemmschuh: Einbrennen durch statische Bildinhalte

Genau wie Oled-Fernseher bestechen Oled-Monitore mit ihrem überragenden Kontrast. Da sie pixelgenau dimmen und die

Bildpunkte ganz abschalten können, zeigen sie echtes Schwarz an. Die selbstleuchtenden Pixel überzeugen zudem dank satter Farben, sehr kurzer Schaltzeiten und äußerst stabiler Blickwinkel, bei denen sich Farben kaum bis gar nicht verändern, auch wenn Sie von der Seite auf den Bildschirm blicken.

Was die Begeisterung an Oled-Schirmen im Computerumfeld bremst, ist die Gefahr des Einbrennens (Burn-in). Diese Effekte können entstehen, wenn Bildinhalte lange statisch angezeigt werden. Beim Fernseher betrifft das etwa Logos von Sendern und Sendungen. Ungleich mehr Möglichkeiten ergeben sich bei der täglichen Arbeit an einem Desktopmonitor oder Notebookdisplay. Denn hier handelt es sich bei sehr vielen Anwendungsfällen um das Anzeigen statischer Inhalte – zum Beispiel von Tabellen, Texten oder auch der Windows-Task-



Bei Notebooks liegt der Oled-Einstieg momentan bei rund 600 Euro. In Sachen Bildschirm bekommen Sie ein Full-HD-Display mit 60 Hertz Bildwiederholrate – wie etwa beim Asus Vivobook Go 15 Oled.



Auch wenn das Oled-Panel bei PC-Monitoren noch kein Schnäppchen darstellt, sind viele Gaming-Bildschirme wie hier der LG Ultragear Oled 27GS95QE-B inzwischen preislich durchaus erschwinglich.

leiste, die in den Standardeinstellungen des Betriebssystems stets sichtbar bleibt.

Einbrenneffekte gibt es in unterschiedlichen Stufen: Image Sticking, Image Retention oder Ghost Image (Geisterbild) ist ein vorübergehender Effekt. Dabei bleiben ein leichtes Schattenbild oder ein Umriss sichtbar, obwohl sich das Bildsignal bereits geändert hat. Hervorgerufen wird der Effekt dadurch, dass Oleds sehr empfindlich auf Änderungen der Stromspannung reagieren. Verschiebt sich die Schwellenspannung der Pixeltransistoren, kann es zu der fehlerhaften Anzeige kommen.

Das richtige Einbrennen, Burn-in oder Image Retention, ist bei Oleds dagegen dauerhaft. Hier hinterlassen statische Inhalte, die über einen langen Zeitraum und wiederholt angezeigt werden, bleibende Spuren auf dem Panel. Sie sehen sie dann als Schattenbilder im Hintergrund, die nicht mehr verschwinden. Burn-in entsteht, weil sich Oled-Panels im Betrieb abnutzen. Sie altern und verlieren dabei an Leuchtkraft. Das ist jedoch ein sehr langsamer Prozess. Deshalb sind echte Defekte durch Burn-in bei den meisten Herstellern von der Gerätgarantie abgedeckt. Außerdem kann das Panel ein Defizit in der Leuchtkraft durch eine höhere Stromversorgung genau dieser Pixel kompensieren.

Mitgelieferte Unterstützung bei der Oled-Pflege

Sowohl für Desktopmonitore als auch für die meisten Notebooks mit Oleds bieten die Hersteller eingebaute Pflegemaßnahmen an. Sie sollten sie unbedingt durchführen,

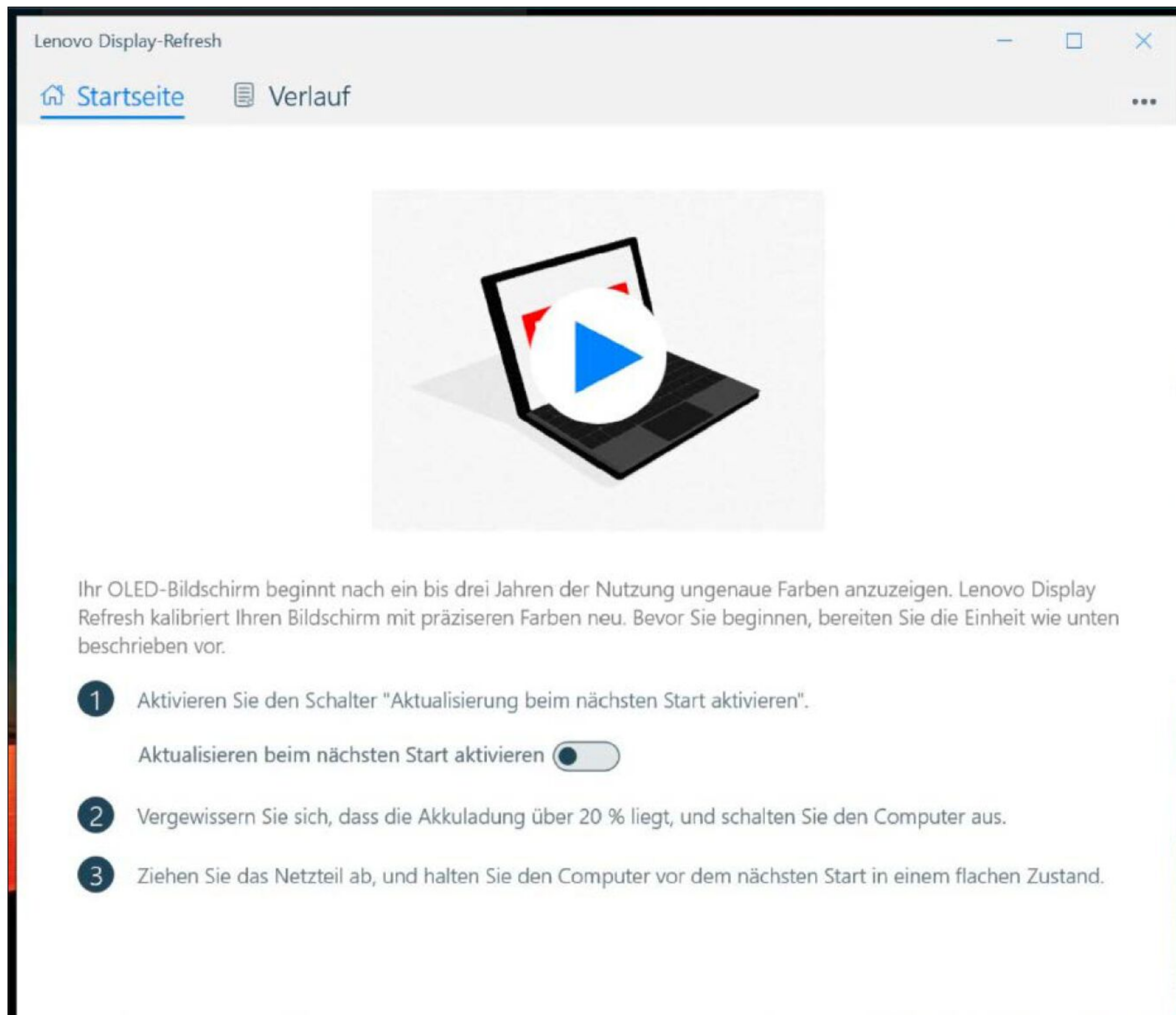
Selbst ein mit 32 Zoll üppig ausgestatteter 4K-Oled-Monitor wie der Dell S3225QC ist bereits unter die 1000-Euro-Grenze gesunken. Künftig dürften die Preise noch weiter fallen.



um die Panelqualität zu erhalten. Bei Monitoren finden Sie die integrierten Routinen zur Oled-Wartung im Onscreen Display (OSD). Oft sind sie unter dem Menüpunkt „Weitere“ oder „Sonstige“ untergebracht. Notebookhersteller integrieren die Funktionen vielfach in die herstellereigenen Wartungstools. So ergänzt etwa Asus das Dienstprogramm Myasus bei Laptops mit Oled-Panel um den Bereich „Asus OLED Care“. Vielfach gibt es für beide Gerätekategorien auch noch zusätzliche Apps, die Sie bei der Oled-Pflege unterstützen. Allerdings hängt das Angebot sehr stark vom spezifischen Gerät ab. So begrenzt zum Beispiel Lenovo das Dienstprogramm Lenovo Display Refresh auf das Thinkpad X1 Fold. Gleichzeitig schadet auch ein Update des jeweiligen Tools nicht. Manche Funktion zur Oled-Wartung wird nach unserer Erfahrung erst durch eine Aktualisierung ergänzt.

Pixel-Refresh: Basiswartung beim Oled-Bildschirm

Eine übliche Wartungsroutine, die der Gefahr von Burn-in von vornherein vorbeugen soll, ist der Pixel-Refresh oder die Pixelaktualisierung. Die Maßnahme überprüft und korrigiert die Schwellenspannung an den Pixeltransistoren. Diese kann sich im Laufe des Oled-Betriebs verschieben – insbesondere dann, wenn viele helle Stellen angezeigt werden. Hier fließt der meiste Strom und es entsteht in der Folge die höchste Temperatur. Ziel der Routine ist es, jene Schwellenspannung wiederherzustellen, die bei der Produktion des Panels festgelegt wurde. Durch die Korrektur verschwinden auch eventuell vorhandene Anzeigefehler. Der Pixel-Refresh startet bei den meisten Geräten nach einer bestimmten Anzahl von Betriebsstunden automatisch. Manche Monitormodelle, wie etwa unser Versuchskan-



Dienstprogramme für die Oled-Wartung sind empfehlenswerte Helfer, um die Qualität des Panels zu erhalten. Sie sind oft modellabhängig. So beschränkt Lenovo etwa das Tool Pixel-Refresh nur auf das Thinkpad X1 Fold.

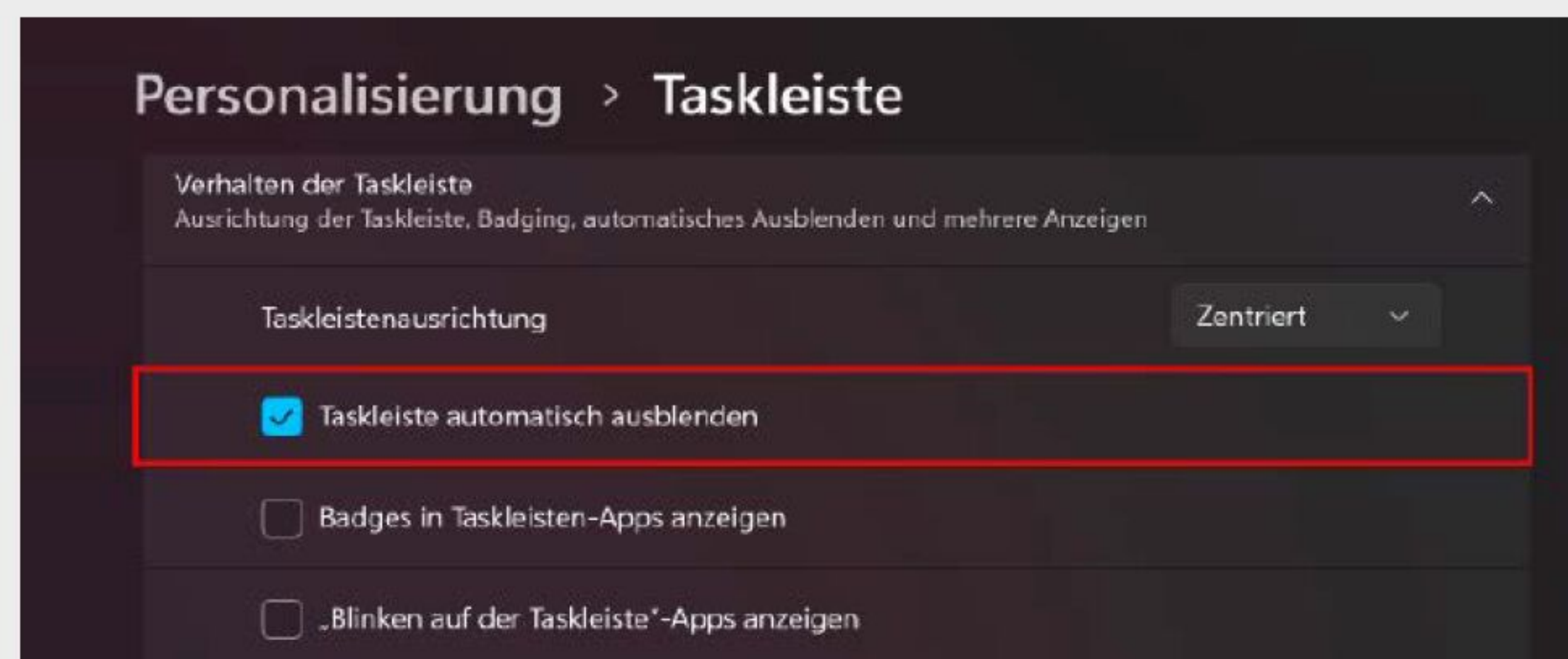
didat Dell S3225QC zeigt im OSD bereits nach vier Stunden an, dass eine Pixelaktualisierung nötig ist. Optisch wechselt ein grüner Punkt bei „OLED Bildschirmstatus“ auf Gelb. Einen aktiven Hinweis zum Eingreifen erhalten wir in diesem Fall jedoch nicht. Starten wir die Korrektur, läuft die Aktion automatisch ab und dauert sechs bis acht Minuten. Das Display schaltet sich am Ende ab. Die Einstellung im OSD lässt sich aus gutem Grund nicht deaktivieren. Sie können aber auswählen, dass der Refresh erst dann startet, wenn sich der Monitor im Standby-Modus befindet. Zwischendurch einen Blick ins OSD zu werfen und die Aktualisierung durchzuführen kommt der Lebensdauer Ihres Oled-Monitors zugute.

Panel-Refresh: Selbstkalibrierung der Oled-Pixel

Um irreversible Schäden durch echtes Burn-in zu vermeiden, haben alle Oled-Panels einen Selbstschutzmechanismus integriert – den Panel-Refresh, der auch als Panel Compensation bezeichnet wird. Das Schutzverfahren startet automatisch nach einer vorgegebenen Betriebsdauer. Die Ge-

OLED-SCHUTZMASSNAHMEN FÜR JEDERMANN

Mit diesen Maßnahmen können Sie den wertvollen Oled-Schirm selbst vor Einbrenneffekten schützen und die Lebensdauer der Pixel erhalten.



Indem Sie die Taskleiste ausblenden, unterstützen Sie die Oled-Gesundheit, denn damit ist ein statischer Inhalt weniger auf dem Desktop.

Ausblenden der Taskleiste: Am Rechner gehört die Windows-Taskleiste zu jenen statischen Inhalten, die immer angezeigt werden. Zum Schutz der Oled-Pixel verhindern Sie das durch das Ausblenden der Taskleiste. Unter Windows 11 führen Sie einen Rechtsklick auf dem Desktop aus und wählen „Weitere Optionen anzeigen → Anpassen“. Im Bereich „Personalisierung“ scrollen Sie nach unten zu „Verhalten der Taskleiste“. Hier setzen Sie ein Häkchen bei „Taskleiste automatisch ausblenden“.

Bildschirmschoner: Auch wenn Ihr Oled-Gerät keinen Bildschirmschoner mitbringt, können Sie diesen unter Windows 11

aktivieren. Wiederum unter „Personalisierung“ klicken Sie auf „Sperrbildschirm“ und gehen zu „Bildschirmschoner“. Idealerweise entscheiden Sie sich für ein dunkles Motiv. Sie können es sich in der Vorschau anzeigen lassen und eine Wartezeit in Minuten festlegen.

Dark Mode: Um die hellen Stellen auf dem Oled-Schirm weiter zu reduzieren, ist der Dunkelmodus ein geeignetes Mittel. Er schont nicht nur die Augen, sondern auch das Oled-Panel. Auch er lässt sich im Windows-Bereich „Personalisierung“ einschalten. Klicken Sie auf „Farben“ und entscheiden Sie sich unter „Modus auswählen“ für „Dunkel“.

Vollbildmodus: Gerade fürs Anschauen von Filmen und Videos empfiehlt sich der Vollbildmodus, damit sich die Videoanzeige möglichst auf die gesamte Schirmfläche skaliert. Kinofans sollten daher schon beim Kauf auf das 16:9-Format achten, um keine störenden Balken an den Seiten zu riskieren.

Helligkeitskontrolle: Bei Desktopmonitoren regeln oft Umgebungslichtsensoren die Helligkeit des Oled-Schirms abhängig von den Bedingungen am Aufstellort. Je nach Situation wird die Leuchtdichte automatisch zurückgefahren. Bei Bewegtbildern wie Filmen empfiehlt es sich, auf vorhandene Modi zurückzugreifen – etwa auf den Filmmodus. Wenn Sie HDR-Einstellungen nutzen, vergessen Sie nicht, diese wieder abzuschalten. Damit reduzieren Sie die Spitzenhelligkeit, schonen die Oled-Pixel und sparen auch Energie.

rätehersteller halten sich bedeckt, wann genau das passiert. Mehrere Hundert Betriebsstunden dürften aber schon vergangen sein. Der Panel-Refresh beginnt, sobald das Display ausgeschaltet ist. Deshalb sollten Sie einen Oled-Monitor auch nicht über eine schaltbare Steckerleiste komplett von der Stromzufuhr trennen.

Beim Panel-Refresh greift der Bildschirm auf eine Memory-Funktion zurück. Der interne Controller speichert alle Daten zu Leuchtdauer und Helligkeit – und zwar für jedes Pixel. Jene Oled-Pixel, die über einen besonders langen Zeitraum in hoher Helligkeit leuchten und daher bereits in der Leuchtkraft nachgelassen haben, bekommen eine höhere Stromversorgung. Das funktioniert, weil Oled-Panels üblicherweise nicht im Maximalbereich leuchten, sondern auf Grundlage des Average Picture Level (APL). Es beschreibt in Prozent, wie hoch die mittlere Helligkeit eines Bildes auf dem Schirm ausfällt.

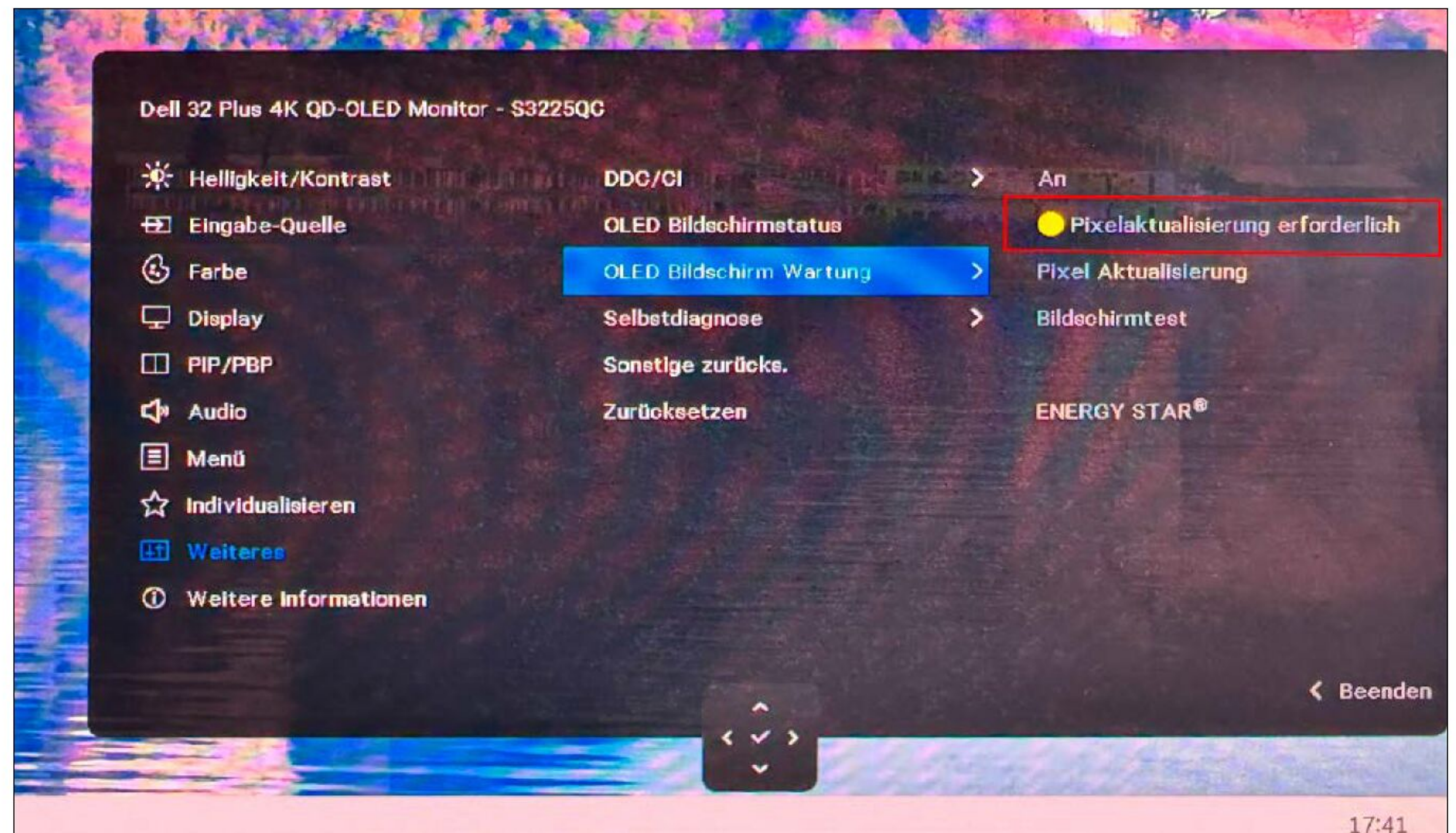
Weitere Schutzmaßnahmen: Pixel-Shifting, Logo-Dimming und Co.

Besonders bei Oled-Monitoren und -Notebooks, die fürs Gaming gedacht sind, integrieren die Hersteller zusätzliche Schutzmechanismen für den Oled-Bildschirm. Allerdings muss nicht jedes Modell alle Verfahren mitbringen.

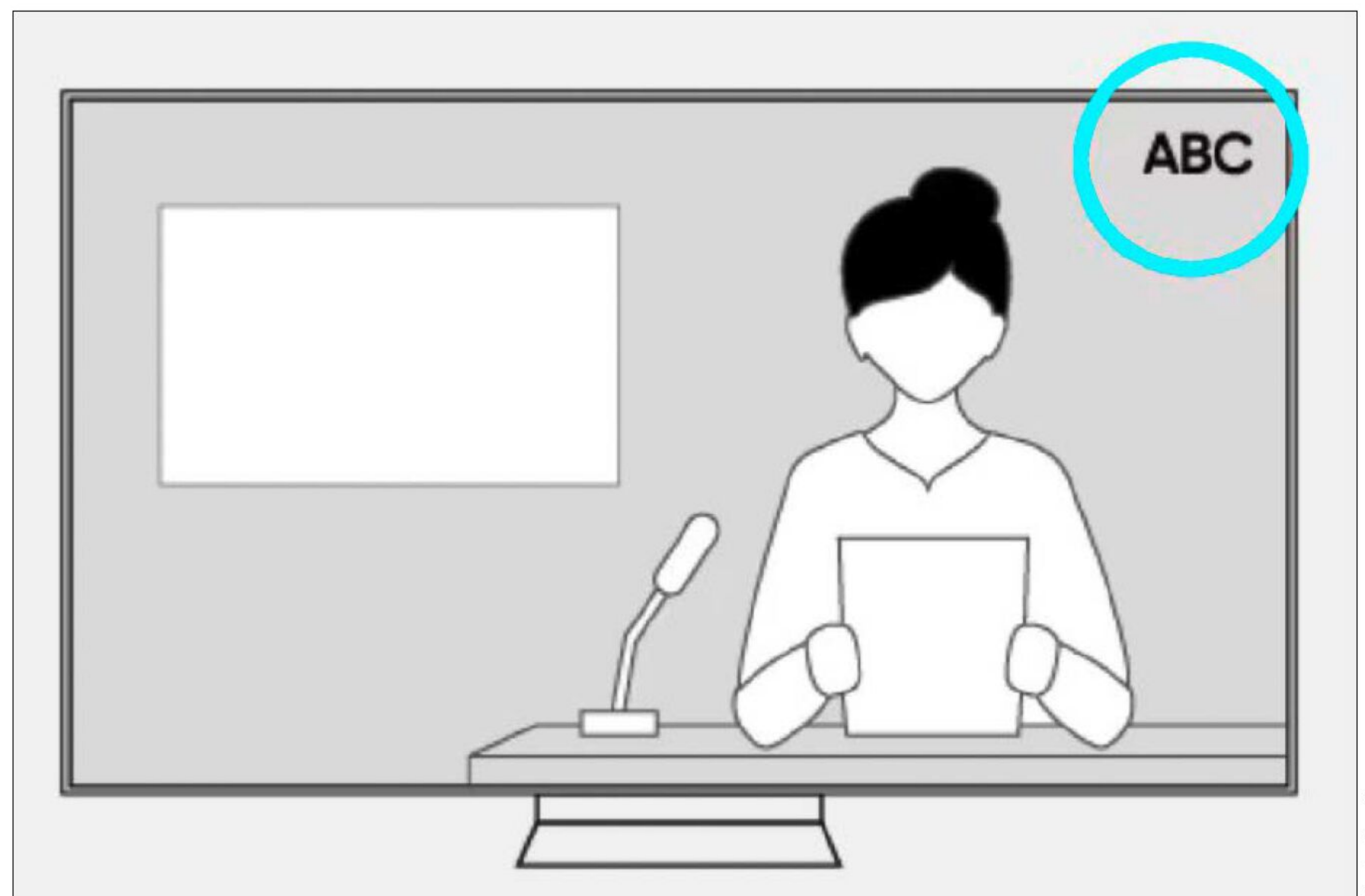
Pixel-Shifting: Die Funktion finden Sie auch unter der Bezeichnung Pixel-Orbiter. Ist sie aktiviert, wird das angezeigte Bild in vordefinierten Abständen – etwa alle drei Minuten – um einige wenige Pixel horizontal und vertikal verschoben. Damit verändert es die Position auf dem Display. Das soll verhindern, dass bestimmte Pixel überbeansprucht werden und damit schneller altern.

Logo-Dimming/Logo Detection: Bietet das Bedienmenü Ihres Monitors diese Funktion, erkennt das Display Logos und wiederkehrende Einblendungen automatisch und reduziert deren Helligkeit. Wie stark das passieren soll, können Sie meist selbst anhand mehrerer Stufen bestimmen. Die Einstellung ist eine Vorsichtsmaßnahme, die sich bei Symbolleisten in Spielen, eingeblendeten Senderlogos oder Programmnamen anbietet.

Bildschirmschoner: Für den Schutz der gesamten Anzeige können Sie übers Herstellertool einen Bildschirmschoner aktivieren. Er startet, sobald ein Eingangssignal ausbleibt – oft schon nach zwei Minuten. ■



Eine Grundfunktion zur Oled-Pflege ist der Pixel-Refresh (Pixelaktualisierung). Die Panelwartung lässt sich auch manuell anstoßen – idealerweise, wenn Sie einen Hinweis im Monitor-Bedienmenü (OSD) sehen.



Bei manchen Geräten mit Oled-Schirmen lässt sich eine Logo-Erkennung aktivieren. Sie macht den statischen Bildinhalt auf dem Schirm ausfindig und dunkelt ihn ab, um das Panel vor Einbrennen zu schützen.



Ein aktivierter Bildschirmschoner – hier bei einem Samsung-Oled-Monitor – schützt die Anzeige vor Schäden durch starre Inhalte, wenn der Rechner gerade nicht genutzt wird.



© RioPatuca Images - AdobeStock

Akkutausch leicht gemacht

Die Akkulaufzeit ist gerade bei Smartphones und Notebooks ein entscheidendes Qualitätskriterium. Wir sagen, wie Akkuspezifikationen zu interpretieren sind und wie Sie den Stromspender am besten tauschen, wenn die Leistung nachlässt.

**VON VERENA OTTMANN UND
ANDREAS HITZIG**

Bei einem aktuellen Smartphone hält der Akku trotz regelmäßiger Nutzung meist deutlich über einen Tag. Dies lässt jedoch

„Wenn der Akku von Phone oder Notebook zu schnell schlapp macht, sollten Sie an einen Austausch denken.“

von Jahr zu Jahr spürbar nach – bereits nach zwei Jahren muss das Gerät oftmals noch während des Tages an das Ladegerät. Ähnlich sieht es bei Notebooks aus: Hier sind zu Beginn bei leistungsstarken Akkus acht bis zehn Stunden Laufzeit keine Seltenheit. Dies reduziert sich aber bei intensiver Nutzung des Geräts schnell auf die Hälfte und weniger, abhängig von der Anzahl der Ladezyklen.

Im schlimmsten Fall ist es dann an der Zeit, den Akku zu tauschen. Dazu müssen Sie jedoch zuerst herausfinden, ob sich der Akku überhaupt tauschen lässt, welcher Akku in Ihrem Gerät steckt und wie Sie Ersatz dafür finden.

Smartphone und Notebook: Akkuangaben verstehen

Ein Akkumulator – auch kurz Akku – ist ein wiederaufladbarer Speicher für elektrische Energie, zumeist auf der Basis eines elektrochemischen Systems. Das Prinzip ist bei sämtlichen Akkus gleich: Sie wandeln beim Aufladen elektrische Energie in chemische Energie um. Sobald der Akku dann zum Einsatz kommt, findet der umgekehrte Prozess statt, und aus der chemischen wird wieder elektrische Energie.

Bei PCs, Smartphones und Tablets kommt am häufigsten ein Lithium-Ionen- oder ein Lithium-Polymer-Akku zum Einsatz. Sie haben eine niedrige Selbstentladung von le-



Möchten Sie einen Notebook-Akku austauschen, hilft eine genaue Typenbezeichnung dabei, den richtigen Ersatzakku zu finden. Alternativ suchen Sie nach dem Notebook-Modell.

diglich zwei bis acht Prozent pro Monat. Dazu ist der Temperaturbereich, in dem sich die Akkus einsetzen lassen, mit -20 Grad bis +60 Grad Celsius recht groß. Die zentralen Kennzahlen eines Akkus, die Hinweis auf die Leistungsfähigkeit geben, sind die Kapazität und die Entladespannung. Bei der Kapazität handelt es sich um die Ladungsmenge, die ein Akku speichern kann. Diese wird normalerweise in Milliamperestunden (mAh) oder Amperestunden (Ah) angegeben. Damit Sie die Leistungsfähigkeit des Akkus einschätzen können, ist als weitere Info die Entladespannung notwendig. Beispielsweise benötigen Smartphones in der Regel zwischen 3,7 und 4,4 Volt, ein Notebook meist 11 bis 15 Volt. Die Gesamtlaufzeit des Akkus lässt sich bei konstanter Leistungsaufnahme des Verbrauchers mit der folgenden Formel berechnen:
$$(\text{Nennkapazität Akku} \times \text{Spannung Akku}) / \text{Leistungsaufnahme Verbraucher} \times 60$$

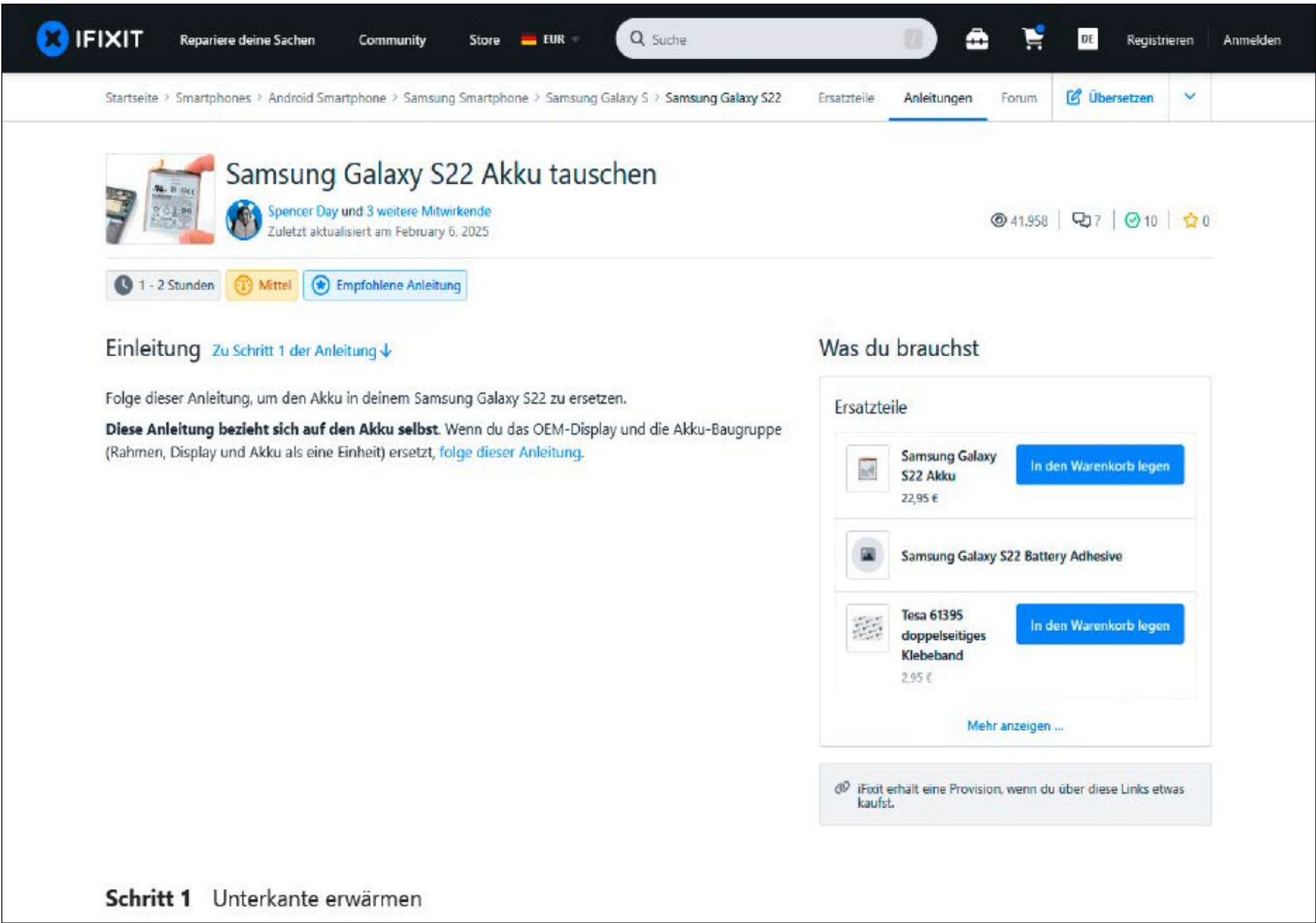
Ein Notebook mit einer Leistungsaufnahme von 40 Watt und einem 7,2-Ah-Akku mit 11,1 Volt lässt sich damit also knapp 120 Minuten betreiben. In der Regel können aktuelle Notebooks allerdings durch diverse Stromsparmaßnahmen die Laufzeit verlängern.

Alter Akku: Vor dem Tausch Informationen auslesen

Wenn die Leistung eines Akkus nachlässt und Sie mit dem Gedanken spielen, diesen auszutauschen, kann es hilfreich sein, sich einige Informationen über den alten Akku zu beschaffen. Vor allem die bereits absolvierten Ladezyklen und die verbliebene Leistungsfähigkeit sind hier interessant, da sie Auskunft über die Qualität des Strom-

spenders geben. Aber: Die Informationen lassen sich nicht bei allen Geräten auslesen. Deshalb können wir nicht garantieren, dass die vorgestellten Programme auch bei Ihnen funktionieren. Da die Tools jedoch kostenfrei sind, gehen Sie mit einem Versuch kein Risiko ein. Bei einem PC oder Notebook mit Windows 11 benötigen Sie nicht einmal ein Zusatzprogramm, um die Akkuinformationen zu ermitteln. Microsoft stellt Ihnen dazu die Funktion **Battery Report** zur Verfügung. Starten Sie hierfür mit der Tastenkombination Windows-X die „Windows PowerShell (Administrator)“, und geben Sie darin folgende Befehlszeile ein:

```
powercfg /batteryreport /output  
"C:battery_report.html"
```



iFixit ist wohl der Klassiker unter den Reparaturdiensten. Möchten Sie Ihrem Smartphone einen Ersatzakku spendieren, finden Sie auf der Seite diverse Anleitungen und können auch sämtliches Zubehör darüber bestellen.



Auch bei einem Smartphone muss der Ersatzakku mit dem Gerät kompatibel sein. Neben der Kapazität, also der Ladungsmenge, muss der Stromspender auch die richtige Spannung liefern.

Die Anwendung liest daraufhin die verfügbaren Daten des Akkus aus und speichert sie als HTML-Datei unter „C:\WINDOWS\system32\battery_report.html“. Beim Öffnen mit dem Browser sehen Sie, welche Informationen verfügbar waren: Neben dem Hersteller sind dies unter anderem auch die Kapazität des Akkus sowie die Anzahl der Ladezyklen. Letzteres gibt allerdings nicht jeder Akku preis. Möchten Sie herausfinden, wie oft Sie Ihr Android-Smartphone bereits aufgeladen haben, empfiehlt sich die App **aBattery - Battery Health** (<https://tinyurl.com/4x8p7cxw>).

Battery report

COMPUTER NAME	LAPTOP-J79RC08C
SYSTEM PRODUCT NAME	FUJITSU CLIENT COMPUTING LIMITED LIFEBOOK U7511
BIOS	Version 2.40 06/30/2023
OS BUILD	22621.1.amd64fre.ni_release.220506-1250
PLATFORM ROLE	Mobile
CONNECTED STANDBY	Supported
REPORT TIME	2025-02-14 11:17:50

Installed batteries

Information about each currently installed battery

BATTERY 1	
NAME	CP811122-01
MANUFACTURER	Fujitsu
SERIAL NUMBER	01A-P210423012380R
CHEMISTRY	Li-ion
DESIGN CAPACITY	64.714 mWh
FULL CHARGE CAPACITY	64.593 mWh
CYCLE COUNT	11

Windows gibt Ihnen über einen Shell-Befehl verschiedene Infos zum verbauten Akku aus. So können Sie neben dem Hersteller und der Typenbezeichnung beispielsweise auch herausfinden, wie oft der Akku bereits geladen wurde.

Sie benötigen eigentlich Root-Zugriff für die Anzeige aller Akkuangaben, allerdings können Sie dies mit der Installation einer weiteren App namens **Shizuku** (<https://tinyurl.com/uksf5ss6>) umgehen. Um Shizuku mit aBattery zu verbinden, sind jedoch einige Schritte notwendig: Starten Sie zuerst Shizuku, und tippen Sie auf „Über Wireless-Debugging starten“ (ist ab Android 11 möglich) und „Kopplung“. Aktivieren Sie nun in den Entwickleroptionen Ihres Smartphones die Funktionen „USB Debugging“ und „Wireless Debugging“ per Schiebeschalter. Tippen Sie auf „Wireless Debugging“ und auf „Gerät über einen Kopplungscode koppeln“. Sie erhalten sofort einen Code sowie eine Kopplungsanfrage von Shizuku. Übertragen Sie den Code in das dafür vorgesehene Feld. Wechseln Sie dann zurück zu Shizuku und tippen Sie auf „Starten“. Sie erhalten eine Bestätigung und können nun aBattery starten. Nach einer kurzen Analyse haben Sie Zugriff auf alle Akkuangaben, inklusive der Ladezyklen.

Smartphone: Akkutausch bei neueren Modellen oft knifflig

Noch vor ein paar Jahren war es problemlos möglich, den Akku eines Smartphones selbst zu tauschen: Sie mussten dazu einfach die hintere Abdeckung abnehmen, um an das Akkufach zu kommen. Seit die Akkus

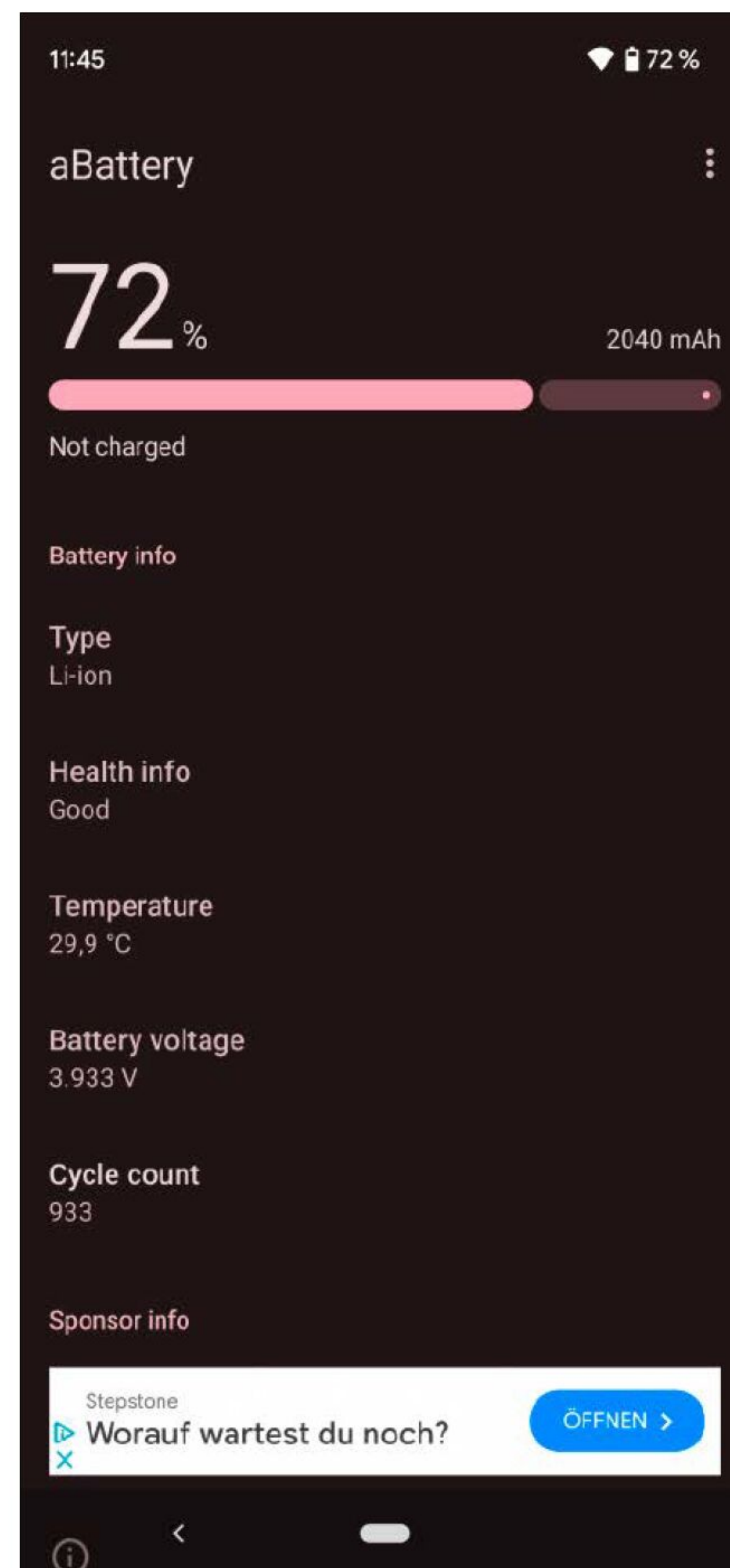
spritzwassergeschützt oder teilweise sogar wasserdicht sind, geht dies nicht mehr. Heute ist es nur noch mit Spezialwerkzeug und handwerklichem Geschick möglich, den Akku Ihres Smartphones zu tauschen.

Tipp: Auf Youtube finden Sie zu fast jedem Gerät mehrere Videos, in denen der Austausch eines Akkus gezeigt wird.

Auch bei iFixit (<https://de.ifixit.com>) finden Sie eine Vielzahl von Reparaturanleitungen zu den gängigsten aktuellen, aber auch zu älteren Geräten. Interessant sind an dieser Stelle vor allem die Einschätzungen zum Schwierigkeitsgrad, zu den Kosten und der Dauer einer Reparatur. Zusätzlich bekommen Sie eine Liste von Werkzeugen, die Sie für den Austausch des Akkus benötigen. Fehlt Ihnen davon eines, können Sie es gleich über die Seite bestellen, ebenso den Ersatzakku.

Aber auch bei Amazon finden sich komplette Austauschsets für gängige Smartphones inklusive Ersatzakku und dem zur Reparatur notwendigen Werkzeug. Solch ein Set kostet etwa für das Samsung Galaxy S22 rund 30 Euro, für das neuere Samsung Galaxy S23 ist es sogar noch ein paar Euro günstiger.

Haben Sie sich den Ersatzakku bereits auf anderem Wege beschafft, gibt es auch reine Werkzeugsets. Ihr Preis startet bei rund zehn Euro, das sehr gut bewertete „Essen-



Die kostenlose App aBattery gibt Ihnen unter anderem die Ladezyklen Ihres Android-Smartphones aus. Die Einrichtung ist zwar etwas umständlich. Anschließend stehen Ihnen aber einige wichtige Akkuinfos zur Verfügung.

tial Electronics Toolkit“ von iFixit kostet beispielsweise etwa 30 Euro.

Handyreparatur vom Spezialisten

Wenn Sie noch nie zuvor einen Smartphoneakku selbst getauscht haben, sollten Sie sich immer der Risiken bewusst sein. Ein zu starker Druck, und die Rückseite des Gehäuses oder das Display bekommen einen Sprung – und das Smartphone wird zum wirtschaftlichen Totalschaden. Das Samsung Galaxy S20 wird beispielsweise als Gebrauchtgerät im Internet aktuell noch zwischen 100 und 180 Euro gehandelt. In einem solchen Fall kann man das Risiko eventuell eingehen. Bei einem Samsung Galaxy S22 mit einem Restwert ab 270 Euro sollten Sie die Reparatur eher einem Fachmann überlassen, also dem Reparaturservice um die Ecke oder einem Serviceanbieter im Internet. Die lokale Lösung finden

Sie am besten über Google – ziehen Sie hier die Bewertungen für den jeweiligen Shop in Ihre Überlegungen mit ein. Die Kosten liegen meist auf einem ähnlichen Niveau wie bei der Selbstreparatur. Empfehlenswerte Onlinereparaturdienste sind etwa www.myphonerepair.de, www.mc-repair.de oder <https://handyreparatur123.de/>. Bei ihnen liegen die Preise für einen Akkutausch des S22 beispielsweise zwischen 70 und 90 Euro inklusive Versandkosten. Ob das wirtschaftlich Sinn macht, müssen Sie natürlich selbst entscheiden. Zumindest erhalten Sie von den Versandhändlern ein Jahr Garantie auf die Reparatur.

Notebook: Passenden Ersatzakku in Spezialshops finden

Auch hier ist die erste Frage im Zusammenhang mit einem neuen Akku: Lässt sich der Stromspender problemlos tauschen? Daran anschließend gibt es noch weiteren Klärungsbedarf, nämlich, ob es für das betreffende Gerät überhaupt noch einen Ersatzakku gibt, und falls ja, ob Sie den Tausch selbst vornehmen können. Bei vielen älteren Notebooks ist der Akku nicht fest verbaut und lässt sich sogar ohne Öffnen des Gehäuses wechseln. Dadurch kommen Sie auch direkt an die erste wichtige Information, nämlich die Typenbezeichnung. Über sie lassen sich bei Bedarf auch weitere Zusatzinformationen recherchieren, falls diese nicht auf dem Akku abgedruckt sind. Doch dazu später mehr. Vor allem können Sie so nach der Typenbezeichnung im Internet suchen, um einen Ersatzakku aufzutreiben. Für viele gängige Notebooks gibt es einen Originalakku vom Hersteller, aber auch (günstigere) Nachbauten von Drittanbietern. Diese sind in der Qualität jedoch oft sehr unterschiedlich, weswegen Sie hier die Bewertungen, falls vorhanden, genau lesen sollten. Falls Ihr Gerät einen fest verbauten Akku hat oder Sie die Typenbezeichnung Ihres Notebooks nicht genau kennen, nehmen Sie am besten den Umweg über die Windows-Systeminformationen. Diese rufen Sie über Ausführen (Windows-R) und die Eingabe `msinfo32.exe` auf. In der Übersicht sehen Sie unter „Systemmodell“ die Herstellernummer beziehungsweise die genaue Bezeichnung Ihres Notebooks und unter „System-SKU“ den Typennamen. Mit diesen Angaben suchen Sie nun in einem

Mein Konto · Anmelden · Partner werden! Fragen? Tel: 0621/ 545 672 85 Mo - Fr: 09:00 - 18:00 Uhr Service/Hilfe

MyPhoneRepair Kleben, Schicken, Fertig!

HOME APPLE SAMSUNG SONY MICROSOFT XIAOMI MOTOROLA HUAWEI ONEPLUS NOKIA GOOGLE

Übersicht Samsung S-Reihe Galaxy S22

Galaxy S22

Reparatur Möglichkeiten

	Preis
Display (Glas/Touchscreen + LCD) Reparatur	229,99 €
Display Glas Reparatur	169,00 €
<input checked="" type="checkbox"/> Akku Austausch	89,99 €
Fehlerdiagnose	34,99 €
Wasserschadenreinigung	49,99 €
Backcover/ Akkudeckel Reparatur	94,99 €
Hauptkamera Reparatur	89,99 €
Ladebuchse Reparatur	84,99 €
Software Zurücksetzen	34,99 €

*inkl. MwSt. inkl. Versandkosten **89,99 € ***

Zahlungsmöglichkeiten

SOFORT ÜBERWEISUNG, VISA, PayPal, SEPA Lastschrift, Kauf auf Rechnung, Vorkasse / Überweisung

Extrem schnell reparieren

Rund 70 Prozent der Handys reparieren und verschicken wir innerhalb von 24 Stunden zurück.

Die 24h Express-Reparatur vom Handy, Smartphone oder Tablet steht allen Nutzern aus Deutschland bei ausgewählten Handys und Reparaturen zur Verfügung.

Trauen Sie sich bei Ihrem Smartphone den Austausch des Akkus nicht zu oder ist er nur sehr aufwendig durchzuführen, gibt es Onlinedienste, die dies für Sie erledigen. Überprüfen Sie jedoch unbedingt, ob es sich preislich lohnt, denn der Tausch durch einen Serviceanbieter ist oft kostspielig.

Info-Hotline: Mo. - Fr. 10 - 17:30 Uhr 0 2151 7 501600 eMail: info@akku500.de Service/Hilfe 4,5 Google Kundenrezensionen

akku500.de

Suchbegriff...

Mein Konto 0,00 €

Home Handy / Smartphone Akkus Apple Akkus & Zubehör Kamera-Akkus (Foto & Video) Werkzeug-Akkus **Notebook-Akkus**

Startseite > Notebook-Akkus

Preiswerte Notebook- und Netbook-Akkus in Top-Qualität

Entdecken Sie in unserem Onlineshop ein großes Produktsortiment an Notebook- bzw. Laptop- und Netbook-Akkus. Jeder von uns angebotene Notebook- und Netbook-Akku ist mit Qualitätszellen namhafter Hersteller ausgerüstet und mit allen erforderlichen Maßnahmen für einen sicheren Betrieb bestückt. Unsere über 500 verschiedenen Notebook- und Netbook-Akku-Modelle sind für alle führenden Hersteller ab Lager lieferbar. Des Weiteren führen wir das passende Zubehör, wie zum Beispiel Reise-Ladegeräte und Kfz-Ladekabel.

Wählen Sie hier den gesuchten Hersteller:

ABACUS	Acer	ADS	Advent
AHTEC	AJP	ALPHATOP	AOPEN
APPLE	ARM COMPUTER	ASCENTIA	Asi
ASI NOTEBOOK	AST	ASUS	BELINEA
BenQ	BSI	CANON	CASPER
CHEM USA	CHICONY	Clevo	CMS
COMIMAX	COMPAL	COMPAQ	COMPOWER
CTX	DAEWOO	DATRON	Dell
DPI	DIGITAL STAR	DUAL TECHNOLOGIES	ECS
ELASCO	EMACHINES	EPSON	EUROCOM

Käuferschutz 4,60 Sehr gut

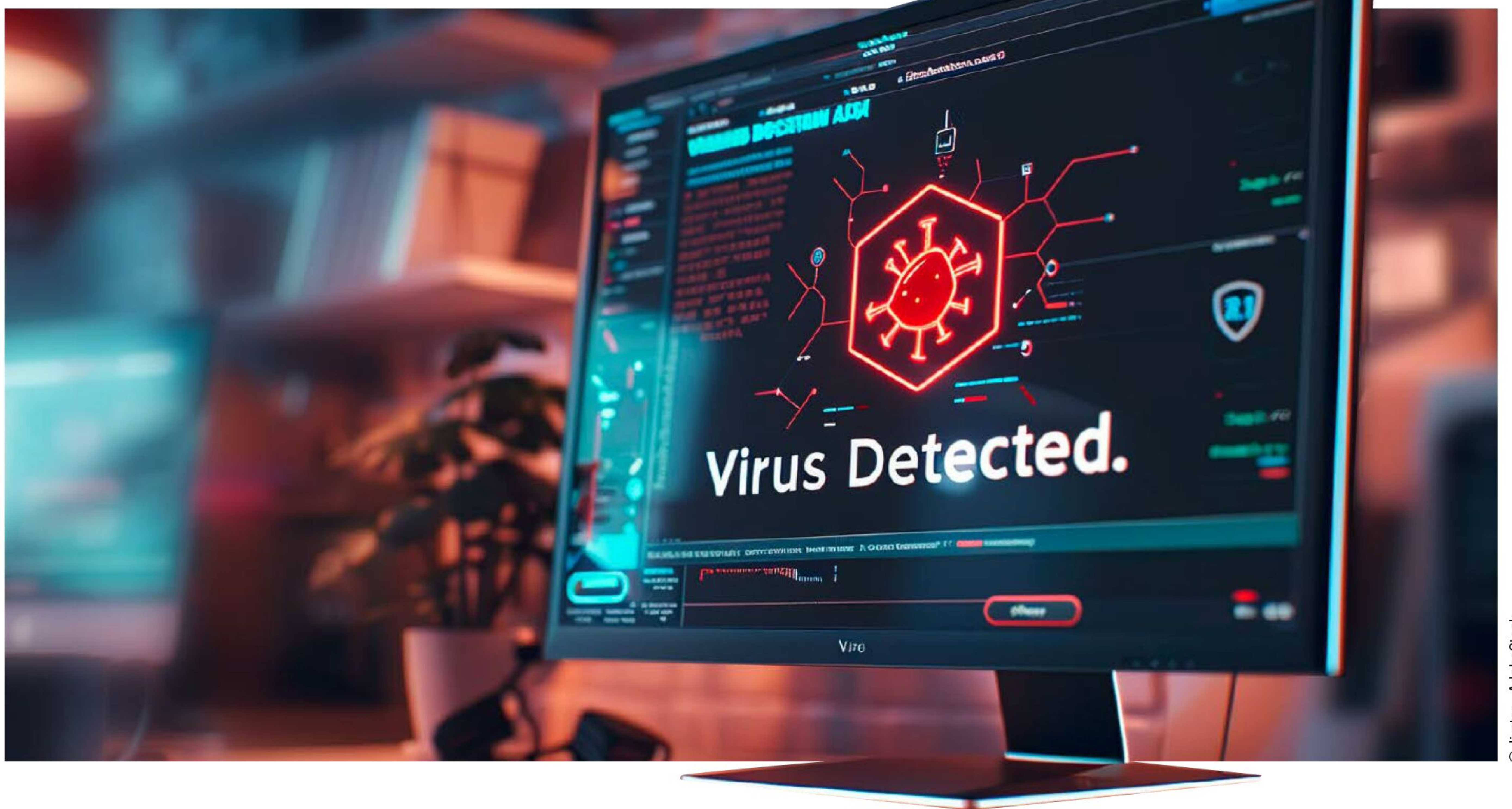
Spezielle Akkushops wie Akku500.de (Bild) oder Akkushop.de sind eine optimale Anlaufstelle, wenn Sie einen neuen Akku für Ihr Notebook oder ein anderes Gerät suchen. Sie sollten jedoch genau wissen, welchen Akku Sie brauchen. Dazu gibt es Apps fürs Smartphone und Windows-Funktionen.

auf Akkus spezialisierten Onlineshop wie www.akku500.de oder www.akkushop.de Ihren Ersatzakku. Alternativ können Sie auch über den Hersteller und das Gerätemodell suchen.

Fazit: Akkutausch statt neuem Gerät ist oft sinnvoll

Der Tausch eines Akkus lässt sich bei den meisten Smartphones und Notebooks pro-

blemlos bewerkstelligen. Geräte mit noch recht hohem Tageswert sollten Sie aber in jedem Fall von einem qualifizierten Betrieb reparieren lassen, da sonst das Risiko eines Totalschadens droht. Mit etwas handwerklichem Geschick, den nötigen Ersatzteilen und einer guten Anleitung aus dem Internet lässt sich aber die Lebensdauer eines Geräts in jedem Fall um ein oder zwei Jahre verlängern. ■



© Jivster - Adobe Stock

Neues Jahr 2026, neue Gefahren?

Es hört nicht auf. Angreifer nutzen weiterhin neue Lücken und Tricks, um in Rechner einzudringen. Um geschützt zu sein, sollten Sie die aktuellen Hacks kennen. Auf der Heft-DVD gibt es dazu das große Profi-Schutzpaket mit aktuellen Sicherheits-Tools.

VON ARNE ARNOLD

Vom smarten, aber unsicheren Türschloss bis hin zur Deepfake-Keynote von Nvidia gibt es aktuell etliche Angriffsformen, die

„Achtung: Die Deepfake-Version eines Livestreams von Nvidia hat mehr Zuschauer als das Original und will die Leute mit Kryptobetrug abzocken.“

brandgefährlich sind. Die folgenden zehn Angriffe stechen besonders hervor und können in ähnlicher Form auch im Jahr 2026 zur Bedrohung werden.

1. WLAN-Passwort aus Balkonkraftwerk geklaut

Balkonkraftwerke boomen. In Deutschland sollen bereits über eine Million dieser kleinen Solaranlagen installiert sein, die sich problemlos an fast jedem Balkon montieren lassen. Sie bestehen aus einem oder zwei Solarmodulen, einem Wechselrichter, Kabeln und einer Befestigung. Der Wechselrichter wandelt den Gleichstrom der Module in netzkompatiblen Wechselstrom um. Oft bieten die Geräte auch ein WLAN-Modul. Damit kann man drahtlos die aktu-

ellen Stromerzeugungsdaten einsehen.

Gefahr: In mehreren weitverbreiteten Wechselrichtern wurden Sicherheitslücken entdeckt. Damit sind Hunderttausende Nutzer betroffen. Viele dieser Lücken hängen mit der Verbindung zur Cloud des Herstellers zusammen. Über diese sind die Geräte angreifbar. Viele Wechselrichter lassen sich fernsteuern und somit gezielt abschalten. Dies hat der Sicherheitsspezialist Valentin Conrad in seiner Masterarbeit an der TU Darmstadt herausgefunden. Ein weiteres Problem ist die WLAN-Verbindung des Wechselrichters. Ein IT-Profi aus dem Westerwald hat eine Lücke im weitverbreiteten Wechselrichter Hoymiles HMS 800W entdeckt. Wer den Stromstecker des Geräts in einer bestimmten Fre-

quenz ein- und aussteckt, veranlasst einen Neustart, bei dem das WLAN-Modul einen Hotspot eröffnet, damit man es neu konfigurieren kann. Wer sich nun per Smartphone mit dem Hotspot verbindet (das nötige Passwort ist in der Regel auf dem Gehäuse des Wechselrichters zu finden), erhält automatisch das WLAN-Passwort des Eigentümers zugesendet.

Schutz: Gegen diesen Angriff gibt es seit Juli 2025 ein Firmware-Update für den Wechselrichter. Außerdem helfen folgende Tipps: Entfernen Sie das werksseitige Passwort des Wechselrichters, sollte es sich auf dem Gerät befinden, und verwahren Sie es an einem sicheren Ort. Wenn möglich, sollte der Schuko-Stecker des Wechselrichters nicht für fremde Personen zugänglich sein.

Grundsätzlich sind Sie besser geschützt, wenn Sie dem Wechselrichter nur das Passwort für das Gastnetzwerk Ihres Routers verraten und nicht das WLAN-Passwort für Ihr Heimnetzwerk. Gegen Angriffe über die Verbindung zur Herstellercloud schützt das allerdings nicht. Überlegen Sie deshalb, ob der Wechselrichter überhaupt eine Internetverbindung benötigt.

2. Malware in Open-Source-Software nimmt weiter zu

Im Jahr 2024 ist die Computerwelt nur knapp einer Katastrophe entkommen. Über mehrere Jahre hinweg hatten Angreifer daran gearbeitet, eine Hintertür in das Betriebssystem Linux einzubauen. Eine Lücke in diesem System betrifft nahezu alle Nutzer, da fast jeder Internetserver mit Linux läuft.

Die Angreifer standen kurz davor, unbemerkt Zugriff auf einen Großteil dieser Server zu erhalten. Sie hatten sich als Mitarbeiter in das Open-Source-Projekt XZ eingeschlichen, das ein Komprimierungstool herstellt. Dies gelang ihnen durch Social Engineering und viel Geduld. Der Angriff auf die Open-Source-Software begann vermutlich im Jahr 2021 und lief bis Anfang 2024. Zu diesem Zeitpunkt war die Hintertür in Vorabversionen von Debian und anderen Linux-Systemen vorgedrungen. Damit war sie nur noch Monate davon entfernt, weltweit auf die meisten Internetserver verteilt zu werden.

Entdeckt wurde die Hintertür nicht von einem Antivirenspezialisten, sondern von Andres Freund, einem Microsoft-Mitarbeiter.

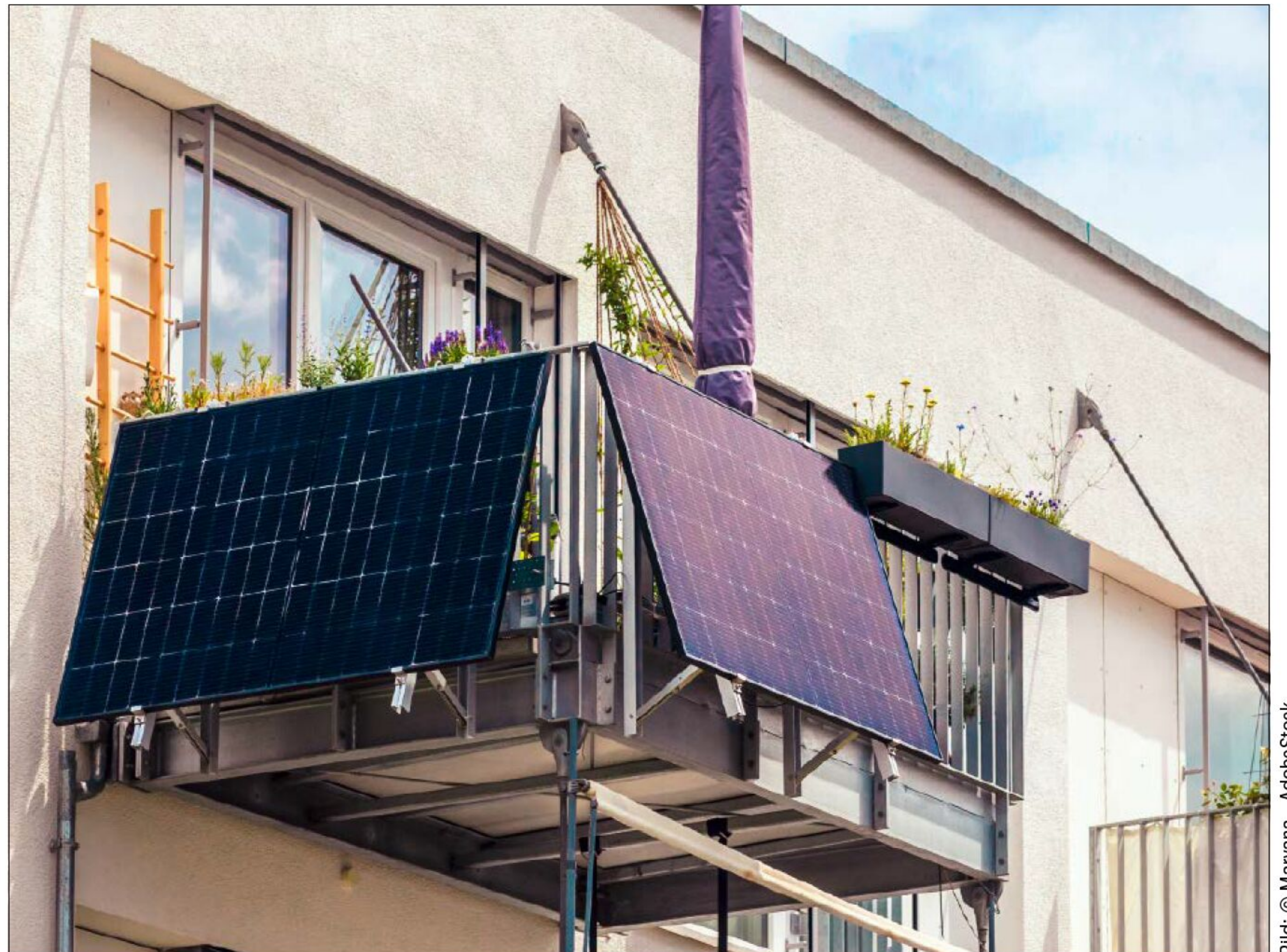


Bild: © Maryana - AdobeStock

Verrät Ihr WLAN-Passwort: Balkonkraftwerke bestehen aus den Solarpanels und einem Wechselrichter. Viele dieser Geräte haben aber Schwachstellen. Eine davon verrät bis Juli 2025 das WLAN-Passwort des Heimnetzwerks.

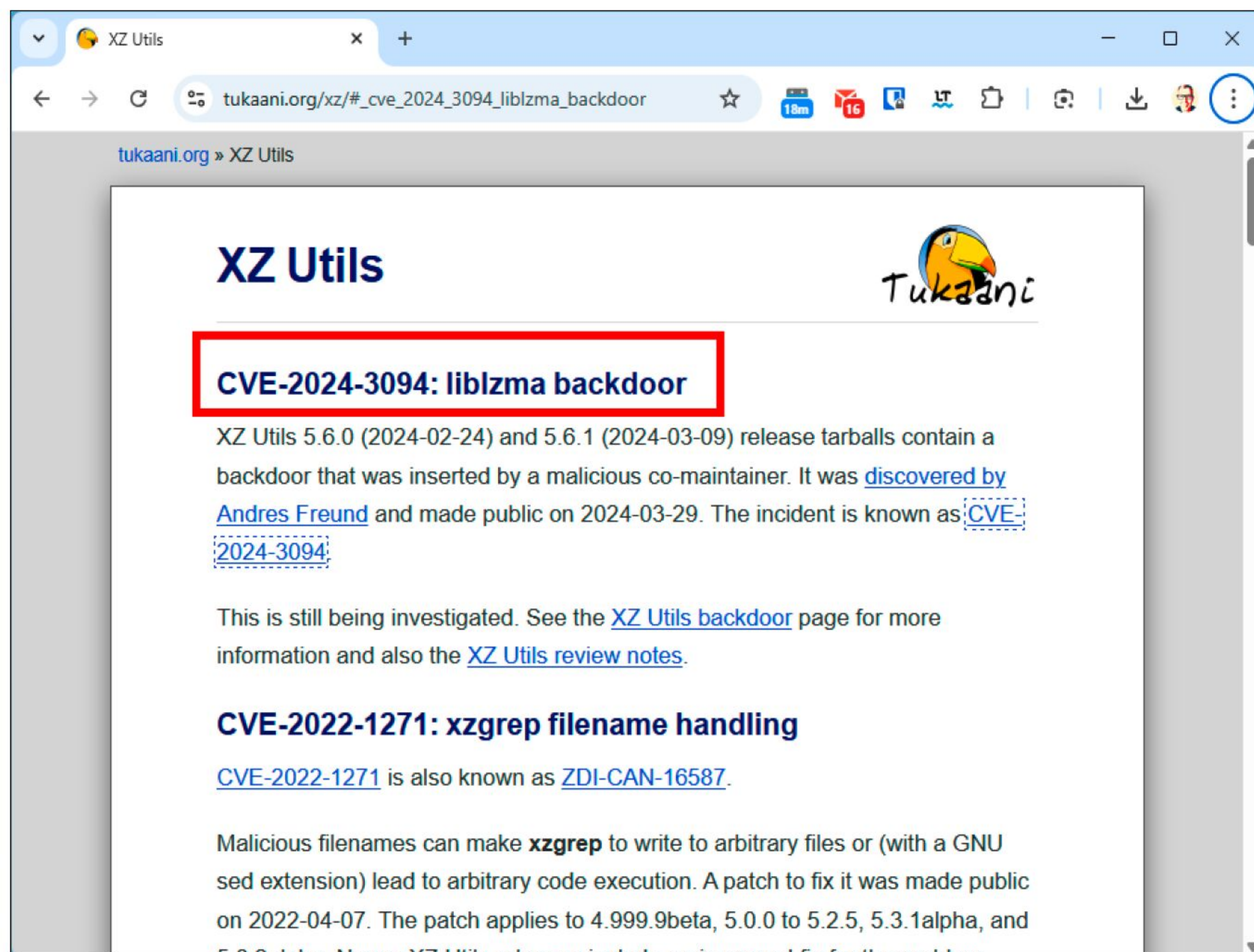
```
Terminal
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
Di, 08.06.2021 | 21:17 lw on mint20 MB free=564 CPU=0% [2] ~/.ssh
ssh -X ha@192.168.0.6
The authenticity of host '192.168.0.6 (192.168.0.6)' can't be established.
ECDSA key fingerprint is SHA256:ox6W0582CzWuLkzL0JAhuFZY5jVZbsVJz/WzeHdeLzU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.6' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.9.241-113 aarch64)

* Documentation: https://help.ubuntu.com
* Management:   https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage
Last login: Mon Jun 7 18:30:01 2021 from 192.168.178.31
```

Per SSH verbinden Sie einen PC mit einem Linux-Server. Zur Absicherung werden Schlüssel ausgetauscht. Im Jahr 2024 gelangte beinahe eine Hintertür in Linux-Server, die sich per SSH ausnutzen ließ.

Freund ist Entwickler und arbeitet an der Open-Source-Datenbank PostgreSQL unter Linux. Ihm war aufgefallen, dass die Anmeldung per SSH (Secure Shell) mit der neuen Vorabversion von Debian etwas länger brauchte. Anstatt der üblichen Viertelsekunde dauerte die Anmeldung eine Dreiviertelsekunde. Andere Entwickler hätten diesen Unterschied womöglich entweder nicht bemerkt oder ignoriert. Freund wurde jedoch misstrauisch und suchte nach der Ursache. Vier Tage später hatte er die Hintertür gefunden und warnte die Öffentlichkeit. Sicherheitsforscher vergaben für die XZ-Hintertür dann einen CVSS-Wert (Common Vulnerability Scoring System) von 10, den höchstmöglichen Wert.

Der Angriff auf XZ ist aus mehreren Gründen besonders. Einerseits ist da die Dauer. Der Angreifer nahm sich Jahre Zeit, um Mitglied in einem Open-Source-Projekt zu werden, das Vertrauen des Projektleiters zu gewinnen und seinen Code einzupflegen. Bemerkenswert sind auch der feindliche Code und die gesamte Angriffskette. Sie umfasst die XZ Utils, Systemd und SSH. Dieselbe Hintertür öffnet sich nur für den Angreifer, der einen geheimen Schlüssel senden muss. Alle anderen SSH-Nutzer erhalten keinen Zugriff auf die Backdoor. Schließlich ist auch die Entdeckung des Schadcodes außergewöhnlich – noch zur rechten Zeit und dank eines einzigen aufmerksamen Entwicklers.



Die Sicherheitslücke in den XZ Utils erhält einen Score von 10. Das ist der höchstmögliche Wert. Er zeigt, dass sich eine Lücke leicht ausnutzen lässt und großen Schaden zulässt.

Erschreckend ist, dass dieser außergewöhnliche Angriff auf ein Open-Source-Projekt kein Einzelfall ist. Zwar sind die anderen Attacken weniger spektakulär, dafür aber umso zahlreicher. Das wird möglich, da Open-Source-Software auf Offenheit basiert: Der Code ist für jedermann zugänglich, anpassbar und überprüfbar. Es gibt zwar Sicherheitsmechanismen, trotzdem ist es relativ einfach, verseuchte Pakete bereitzustellen, die wiederum von Entwicklern genutzt werden.

Darauf macht auch der Antivirenhersteller Kaspersky (www.kaspersky.de) aufmerksam. Laut einer Analyse versteckten Cyberkriminelle im Jahr 2024 insgesamt 14.000 schädliche Pakete in Open-Source-Projekten. Dies entspricht einem Anstieg von 50 Prozent im Vergleich zum Vorjahr. Die Experten des Cybersicherheits-Anbieters untersuchten 42 Millionen Versionen von Open-Source-Projekten auf Schwachstellen. Für das Jahr 2025 liegen uns noch keine Zahlen vor. Einen nennenswerten Rückgang erwarten wir aber nicht.

Gefahr: Für Endanwender besteht eher eine indirekte Gefahr. Die meisten Angriffe zielen auf den Diebstahl von Daten in Unternehmen. Entsprechend ist überwiegend Unternehmenssoftware betroffen. Doch Datendiebstahl aus Firmen betrifft am Ende auch die Kunden.

Schutz: Für Entwickler, die Open Source in ihre Projekte einbinden, sowie für Unternehmen, die mit Open Source arbeiten, bietet der Sicherheitsanbieter Kaspersky einen Informations-Feed zu problematischem Code an. Der Feed meldet die folgenden Bedrohungsarten: Pakete mit Schwachstellen, Pakete mit Schadcode, Pakete mit Riskware wie Krypto-Miner, Hacktools usw., kompromittierte Pakete, die politische Slogans enthalten.

Ein Zugang zu dem Feed lässt sich unter www.kaspersky.com/open-source-feed beantragen. Softwareunternehmen können auch auf die Tools von Sicherheitsexperten wie Xygeni Security (<https://xygeni.io>) zugreifen. Das Unternehmen hat sich auf den Schutz der Software-Lieferkette spezialisiert. Endanwender müssen sich auf ihren installierten Virenschutz verlassen.

3. Abmelde-Button stiehlt persönliche Daten

Jeder Newsletter muss einen Abmelde-Button enthalten, über den man ihn abbestellen kann.

Gefahr: Nicht jeder Abmelde-Link ist harmlos. Einer von 650 dieser Buttons führt nicht zur gewünschten Abmeldeseite, sondern zu einer Phishing-Website, die Daten stehlen oder Malware verbreiten will. Das meldet das Sicherheitsunternehmen

DNS Filter (www.dnsfilter.com). Wer auf einen Abmelde-Link klickt, bestätigt damit automatisch, dass seine Mailadresse existiert und er auch ins Postfach schaut. Für Spammer, die ihre Mailadressen meist aus großen Datenpaketen ziehen, ist allein diese Information schon etwas wert. Wenn sich die Spammer dann noch Mühe geben, gestalten sie die vermeintliche Abmeldeseite so, dass sie Daten von Besuchern abzieht. Mit Social-Engineering-Tricks entlocken sie ihren Opfern Passwörter und andere sensible Informationen.

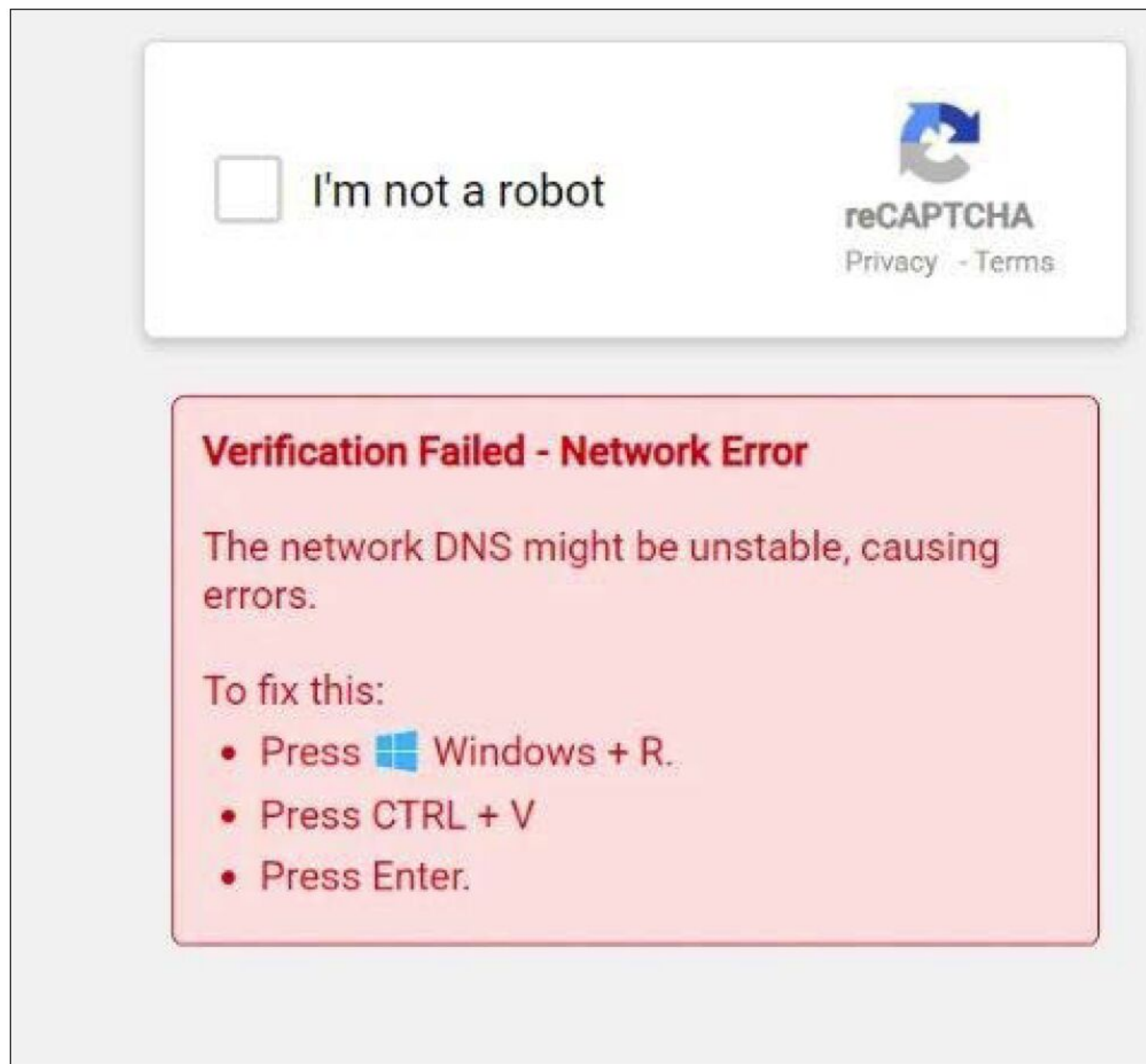
Schutz: Anstatt auf den Abmelde-Button zu klicken, können Sie den Absender in Ihrem E-Mail-Programm oder in der Weboberfläche Ihres E-Mail-Providers sperren. Falls das nicht möglich ist, können Sie die E-Mail und damit den Absender auf eine Spam-Liste setzen. So gelangen keine weiteren Nachrichten von diesem Absender in Ihr Postfach. Sie müssen dann nur daran denken, den Absender wieder zu entsperren, falls Sie doch einmal wieder Nachrichten von ihm erhalten möchten. Das wird bei den Phishing-Mails, um die es hier geht, aber nie der Fall sein. In Outlook klicken Sie mit der rechten Maustaste auf eine E-Mail und wählen „Sperren“ → „Absender sperren“. In Thunderbird wählen Sie die Mail aus und klicken oben auf „Junk“. Auf den Webseiten von GMX und Web.de markieren Sie die Mail und wählen oben im Menü „Spam“ aus. Bei Gmail öffnen Sie die Nachricht und wählen dann das Drei-Punkte-Menü rechts oben in der E-Mail aus. Klicken Sie im Menü auf „Als Spam melden“ oder auf „Absender sperren“.

4. Ein Captcha auf Webseiten schleust Malware ein

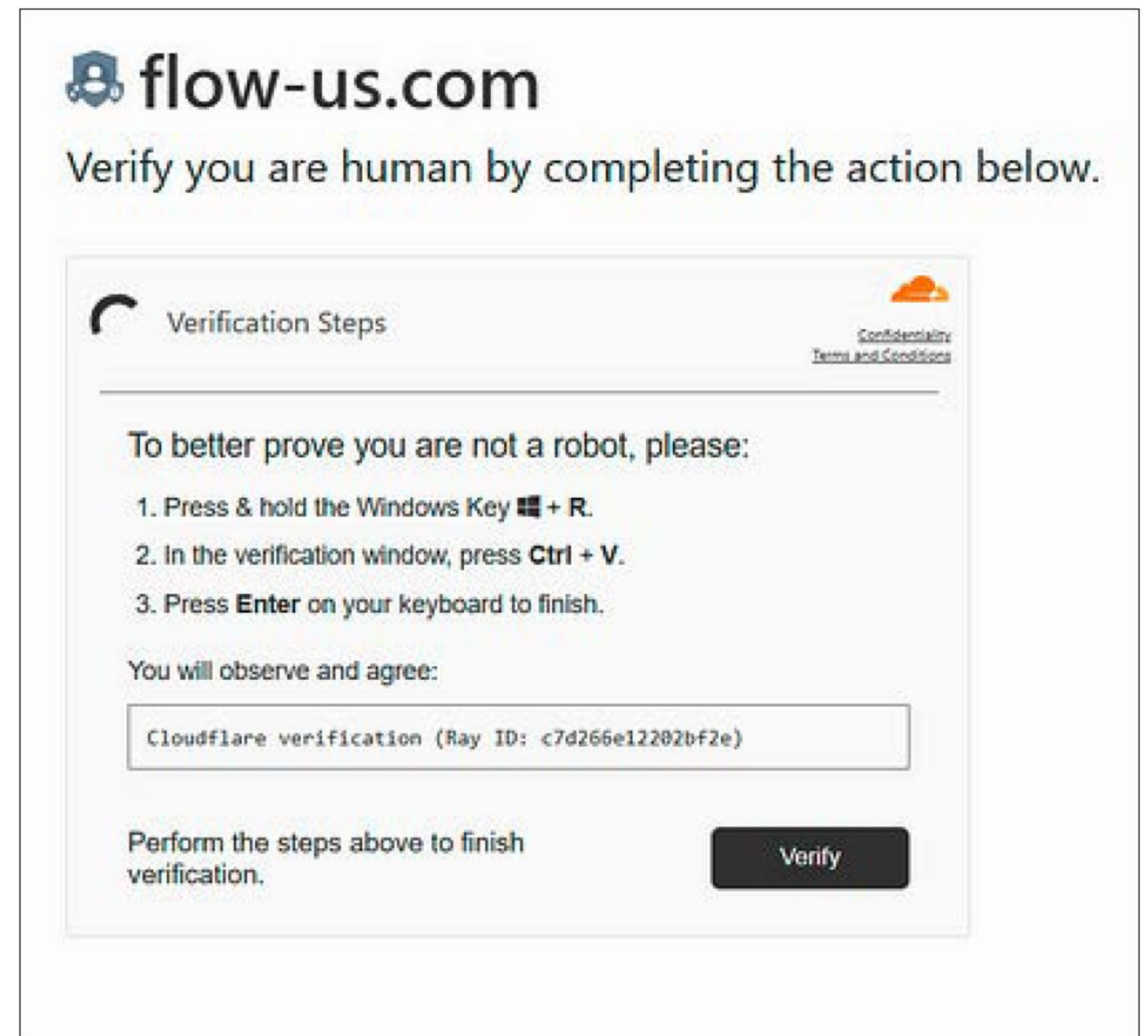
Captchas sollen Webseiten vor automatisierten Anfragen schützen, indem sie echte Menschen von Bots unterscheiden. Inzwischen genügt dafür oft ein Klick auf die Checkbox „I’m not a robot“ (Ich bin kein Roboter). Früher musste man auf kleinen Fotoquadraten Autos, Ampeln oder Motorräder anklicken.

Gefahr: Seit einiger Zeit nutzen Kriminelle Captchas, um Viren wie den Schädling Qakbot in die PCs von Seitenbesuchern zu schmuggeln, und zwar so:

Mit dem ersten Klick auf die Checkbox bei „I’m not a robot“ kopiert die Website schädlichen Code in die Zwischenablage des Sei-



Quelle: DNS Filter



Quelle: Dark Atlas

Neue Falle bei Captchas: Nach dem Anklicken des feindlichen Captchas „I'm not a robot“ erscheint anschließend eine dieser Anleitungen. Wenn Sie ihr folgen, fügen Sie einen zuvor kopierten Schadcode in den Ausführen-Dialog von Windows ein, der dann den eigentlichen Virus herunterlädt.

tenbesuchers. Anschließend erscheint eine Anleitung, der man folgen soll, da angeblich gerade ein Netzwerkfehler aufgetreten ist, oder um weiterhin zu überprüfen, dass man ein Mensch und keine Maschine ist. Die Anleitung gibt die Tastenkombinationen Win-R und Strg-V, gefolgt von der Enter-Taste, vor. Was man damit jedoch tatsächlich ausführt, ist das Öffnen des Ausführen-Dialogs von Windows (Win-R), das Einfügen des feindlichen Codes aus dem Zwischenspeicher dorthin (Strg-V) und dessen Ausführung (Enter). Der Code lädt dann den eigentlichen Schädling, meist Qakbot, herunter. Dieser fügt den PC einem Botnetz hinzu oder lädt Ransomware nach, die alle Daten verschlüsselt und anschließend Lösegeld verlangt.

Schutz: Der Ausführen-Dialog sollte als klare Warnung dienen. Kein legales Captcha der Welt sollte dort Code einfügen wollen. Bleiben Sie misstrauisch und trauen Sie sich, eine Aktion auch abzuberechnen.

5. Spionage-Trojaner Spark Cat und Kitty im App Store

Ein neuartiger Spionage-Trojaner bestiehlt Nutzer von Android- und iOS-Smartphones. Der als Spark Cat bezeichnete Schädling steckte in Apps, die es in den offiziellen App Stores von Google und Apple gab. Nach der Installation der verseuchten App fordert diese Zugriff auf den Fotospeicher. Das weckt in der Regel kein Misstrauen,

denn Spark Cat und sein Nachfolger Spark Kitty verstecken sich beispielsweise in Chat-Apps. Das Versenden von Fotos per Chat-App ist verbreitet und erfordert natürlich Zugriff auf die Fotos.

Gefahr: Allein bei Google Play zählten die Sicherheitsforscher von Kaspersky zehn mit Spark Kitty verseuchte Apps, die über 240.000 Mal heruntergeladen wurden. Im App Store von Apple steckte der Schädling in elf verseuchten Apps. Der Schädling durchsucht den Fotospeicher des Handys nach Screenshots, auf denen sich Passwörter oder andere geheime Informationen befinden. Per OCR-Erkennung wird der Text extrahiert und dient den Angreifern dann als Zugang zu Krypto-Wallets. Auf diese Weise können sie hohe Summen von den Konten ihrer Opfer stehlen.

Schutz: Die bewährte Methode, nur Apps aus den offiziellen App Stores zu laden, hilft hier leider nicht weiter. Der Schädling steckte schließlich in Apps aus diesen Stores. Achten Sie deshalb künftig auch darauf, wie oft eine App bereits heruntergeladen wurde. Apps mit einer Million oder mehr Downloads sind höchstwahrscheinlich sicher. Achten Sie außerdem darauf, welche Berechtigungen eine App einfordert. Den Zugriff auf den Fotospeicher sollten Sie nur nach reiflicher Überlegung gewähren. Und grundsätzlich sollten sensible Informationen wie Passwörter nicht auf Screenshots gespeichert

werden. Diese gehören in einen Passwortmanager. Ein kostenloses Programm ist etwa Bitwarden (<https://bitwarden.com>).

6. Angriffe auf Drucker: Fast 750 Modelle sind betroffen

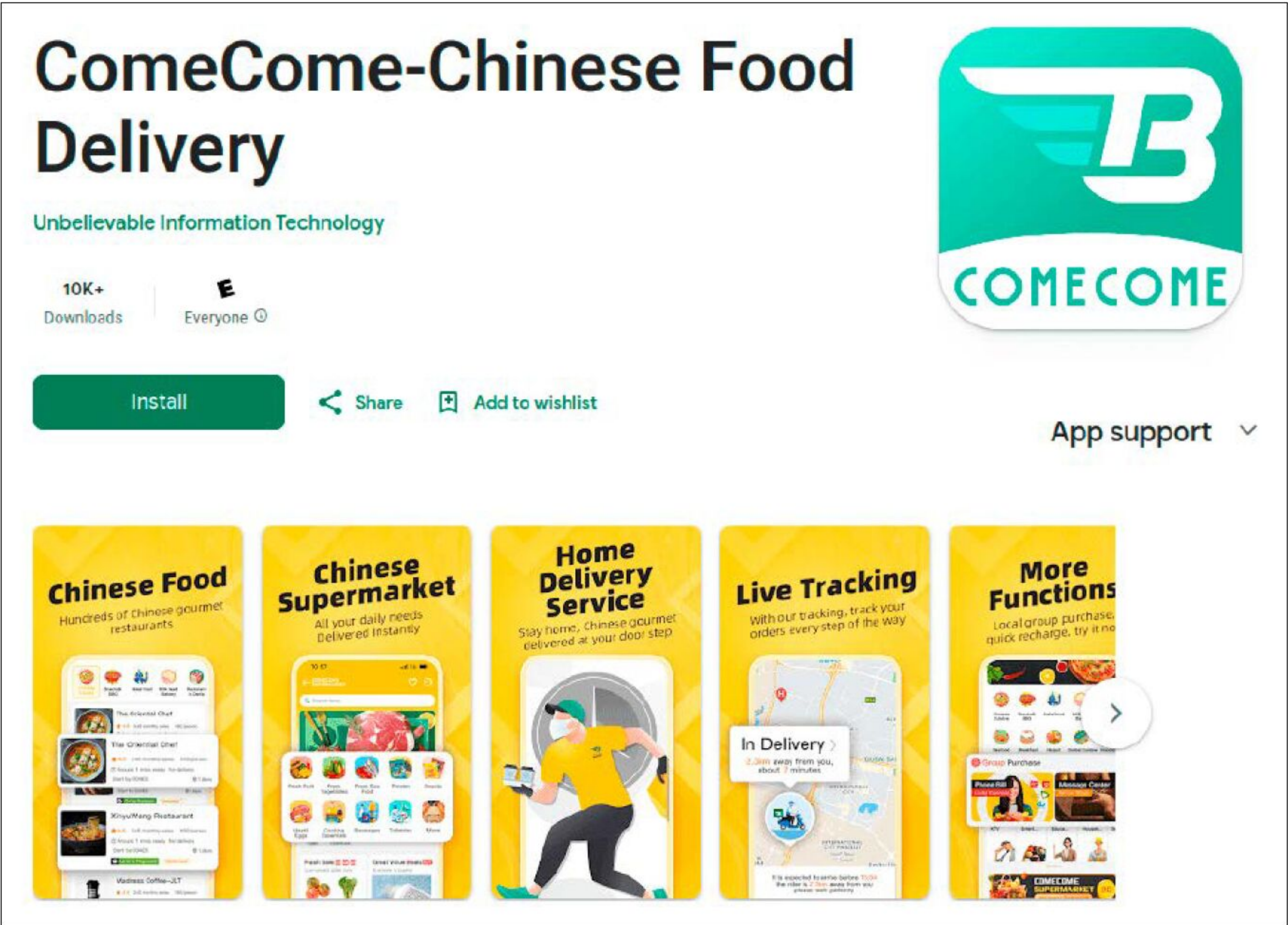
Im Juni 2025 haben Sicherheitsforscher von Rapid 7 (www.rapid7.com) acht Schwachstellen in Hunderten von Druckern verschiedener Hersteller entdeckt.

Gefahr: Über diese Lücken können sich Angreifer Zugang zum Netzwerk und zu Daten verschaffen. Betroffen sind die Unternehmen Brother, Fujifilm, Ricoh, Toshiba und Konica Minolta. Zwar haben die Unternehmen Firmware-Updates bereitgestellt, doch eine Sicherheitslücke kann lediglich mit einem Workaround geschlossen werden. Diese Lücke hebt die Authentifizierung aus, wodurch Angreifer die Kontrolle über das Gerät erlangen können. Für den Log-in nutzen die Angreifer das Standardpasswort des Geräts, das aus dessen Seriennummer besteht. Diese lässt sich über eine andere Lücke abfragen.

Schutz: Ändern Sie das Standardpasswort Ihres Druckers und installieren Sie die neuesten Updates für Ihr Gerät.

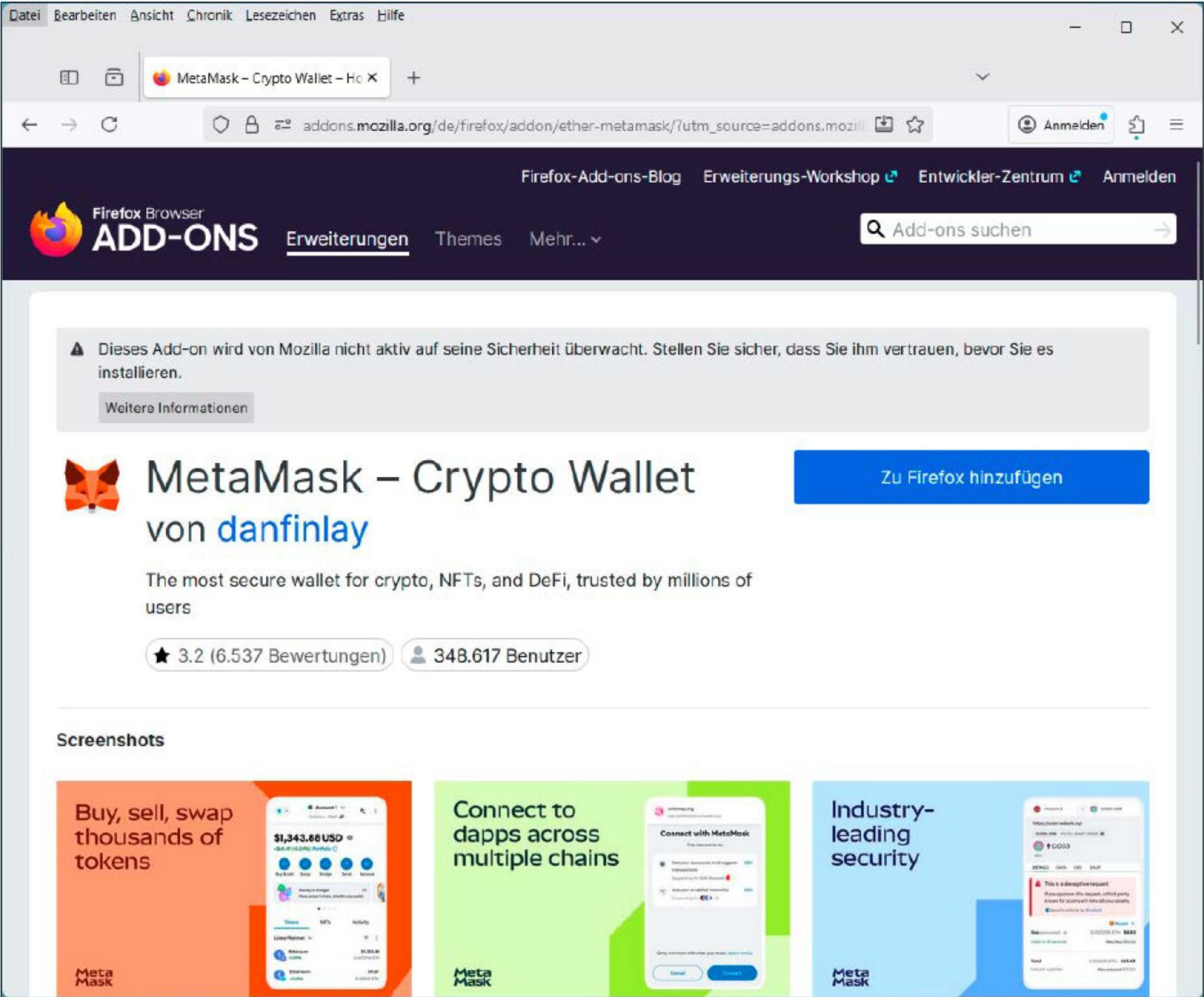
7. Browsererweiterungen leeren Krypto-Wallets

Immer wieder tauchen Browsererweiterungen mit Schadcode auf. Zuletzt hatten es die Kriminellen hinter diesen Erweite-



Diese App stand im offiziellen App Store von Google und war mit dem Spionage-Trojaner Spark Cat verseucht. Der Schädling sucht im Bilderspeicher des Smartphones nach Passwörtern, die er per OCR extrahiert.

Quelle: Kaspersky



Dies ist eine Firefox-Erweiterung für die Kryptobörse Meta Mask. Ob diese Erweiterungen harmlos sind oder nicht, lässt sich oft nicht leicht entscheiden. Eine hohe Zahl an Downloads spricht jedoch dafür, dass ein Add-on harmlos ist. Auch ein Blick auf die Website des Entwicklers hilft bei der Einschätzung.

rungen auf die Besitzer von Krypto-Wallets abgesehen.
Gefahr: Dutzende gefälschter Browser-Add-ons für Firefox zielen darauf ab, Zugangsdaten für Wallets mit Kryptowährun-

gen zu stehlen. Die Erweiterungen geben sich als legitime Wallet-Tools bekannter Plattformen wie Coinbase, Meta Mask oder Trust Wallet aus. Einige der rund 40 gefährlichen Add-ons sollen es sogar in

den offiziellen Add-on-Marktplatz von Firefox (<https://addons.mozilla.org>) geschafft haben, wie der Entdecker Koi (www.koi.ai) berichtet. Dafür haben die Angreifer den Open-Source-Code bekannter Add-ons genutzt und ihren Schadcode darin platziert. Anschließend wurde das Add-on unter einem ähnlichen Namen wie das Original online gestellt.
Schutz: Laden Sie Browsererweiterungen ausschließlich von vertrauenswürdigen Quellen herunter. Achten Sie auch dort darauf, dass das Add-on bereits sehr oft heruntergeladen wurde. Da sich Erweiterungen automatisch aktualisieren können, besteht zudem die Gefahr, dass zunächst harmlose Add-ons nach einem Update mit Schadcode ausgestattet werden. Deinstallieren Sie deshalb Erweiterungen, die Sie nicht mehr benötigen.

8. Deepfakes: Abzocke mit Kryptowährungen

Deepfakes sind Fälschungen von Fotos, Audios oder Videos. Damit lässt sich jede Menge Unheil anrichten, denn selbst vorsichtige Menschen können durch die Fälschungen zu Fehlern verleitet werden. Ein Beispiel ist ein gefälschter Livestream von Nvidias Keynote im Oktober 2025: Zeitgleich zum echten Livestream auf Youtube sendeten Betrüger ein Deepfake-Video mit einem KI-generierten Jensen Huang, dem CEO von Nvidia. Dieser sprach jedoch nicht von neuen Chips bei Nvidia, sondern von einem neuen Kryptowährungsprojekt. Der Fake-Stream soll zu Beginn mehr Zuschauer als der echte gehabt haben: 100.000 für das Deepfake gegenüber 12.000 bei Nvidia. Grund dafür war vermutlich, dass Youtube bei einer Suche nach „Nvidia Keynote“ zuerst den Deepfake in der Ergebnisliste angezeigt hatte. Erst nach einer halben Stunde nahm Youtube damals die Fälschung offline.

Gefahr: Kriminelle nutzen Kryptowährungen, um unvorsichtigen Nutzern das Geld aus der Tasche zu ziehen. Diese Betrügereien laufen meist über falsche Versprechen von schnellen Gewinnen mit tatsächlich wertlosen Krypto-Coins. Dazu werden oft Deepfakes eingesetzt. Durch Manipulation wird dann der scheinbare Wert der Coins schnell gesteigert, was die Opfer zum Kauf bewegt. Ab einem bestimmten Wert verkaufen die Betrüger ihre Anteile auf einen Schlag und machen damit Ge-

winn. Der Kurs der Kryptowährung fällt rapide, sodass alle anderen meist einen kompletten Verlust erleiden.

Schutz: In Kryptowährungen sollte man nur investieren, wenn man sich mit der Materie sehr gut auskennt. Dann lassen sich die typischen Kryptoabzocken leicht erkennen.

9. Ransomware mit Künstlicher Intelligenz agiert autonom

Sicherheitsforscher von Eset (www.eset.de) haben eine Schadsoftware namens Prompt Lock entdeckt. Diese setzt Künstliche Intelligenz gezielt für Ransomware-Angriffe ein.

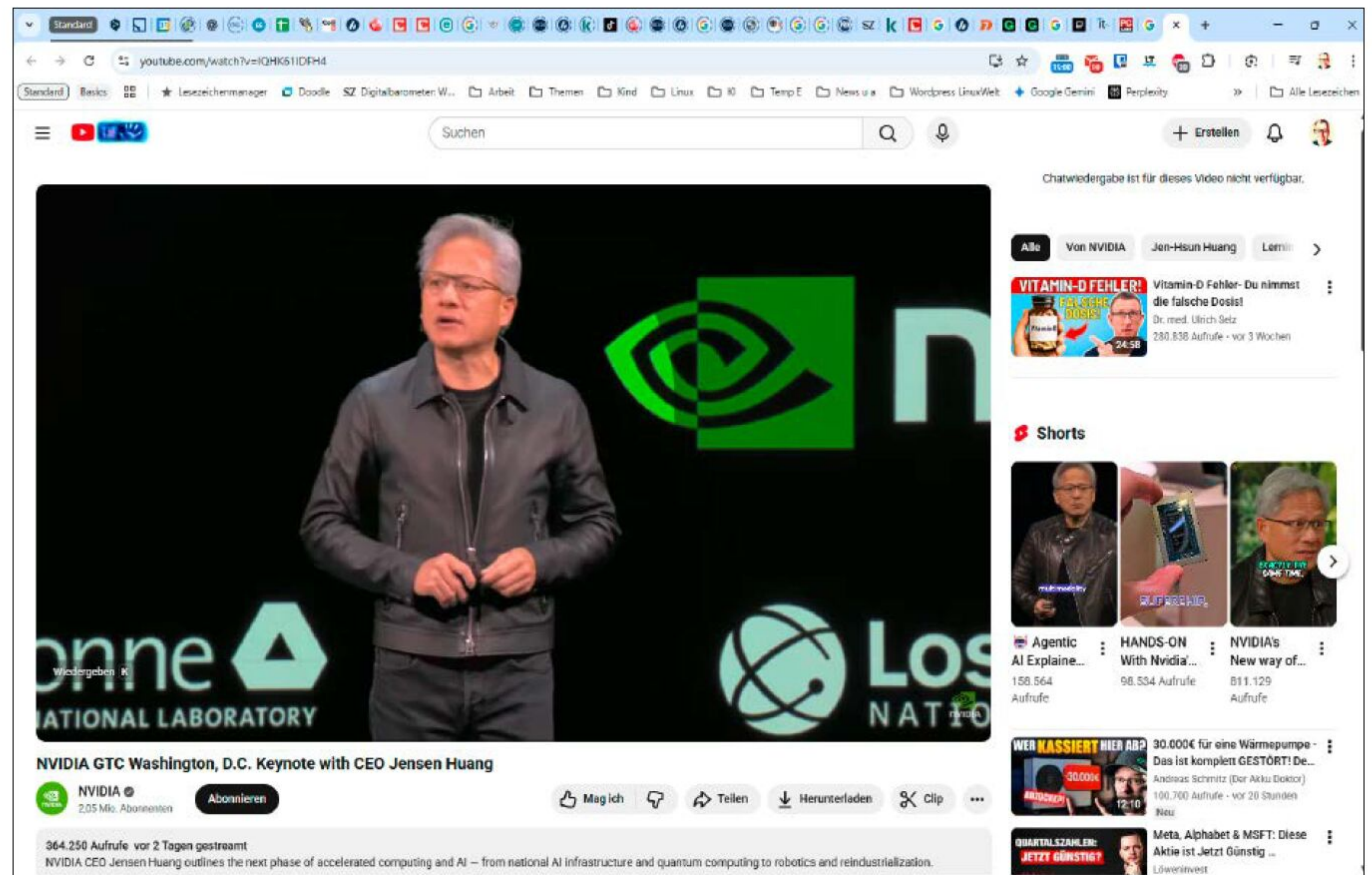
Gefahr: Der Erpresservirus nutzt ein lokal installiertes Sprachmodell, das im laufenden Angriff eigenständig Scripts generiert und somit selbst entscheidet, welche Dateien durchsucht, kopiert oder verschlüsselt werden. Eine Funktion zur endgültigen Zerstörung von Dateien ist offenbar bereits integriert, jedoch bislang noch nicht aktiviert. Prompt Lock erstellt plattformübergreifende Lua-Scripts (www.lua.org), die sowohl unter Windows als auch unter Linux und Mac-OS lauffähig sind.

Schutz: Der beste Schutz gegen Erpresserviren ist eine aktuelle Datensicherung, die vom System getrennt gelagert wird. Weitere Tipps gegen Ransomware finden Sie in unserem Ratgeber unter www.pcwelt.de/1152984.

10. Smart-Home-Geräte: Angreifer knacken Türen

Smarte Geräte fürs Heimnetzwerk bieten in der Regel auch einen Internetzugriff auf ihre Funktionen. Das ist zwar bequem, birgt aber auch Risiken.

Gefahr: Bedrohlich werden Lücken in smarten Geräten, wenn ein Angreifer darüber in das Heimnetzwerk eindringen und Daten stehlen kann. Ebenfalls sehr unangenehm ist folgender Fall: Eine smarte Türklingel hat eine Lücke, über die Angreifer die Verriegelung öffnen können. Das war wohl im Oktober 2025 bei den Türschlössern der Firma Unifi der Fall. In der Zutrittssoftware Unifi Access Application steckte eine Sicherheitslücke (<https://tinyurl.com/5a9bwzsc>) mit dem CVSS-Wert von 10, wie der Hersteller selbst bekannt gab. Wie die Lücke und die passenden Angriffsmethoden genau aussehen, verriet er nicht. Doch der CVSS-Score von 10, also die höchstmögliche Bewertung, legt nahe,



Der echte Jensen Huang, CEO von Nvidia, auf der echten Keynote im Oktober 2025. Gleichzeitig lief auf YouTube ein Deepfake der Keynote mit Jensen Huang, in der er für eine Kryptowährung Werbung machte.



In der Verwaltungssoftware für die smarten Türschlösser von Unifi steckte eine Sicherheitslücke mit dem höchsten Verwundbarkeitswert (CVSS 10). Hacker konnten eine mit Unifi geschützte Tür vermutlich leicht knacken.

dass sich die Lücke leicht und mit massiven Folgen ausnutzen lässt.

Schutz: Von der Lücke betroffen ist die Version 3.4.31 von Unifi Access Application, die sich an Unternehmen richtet. Administratoren sollten ein Update auf die neueste

Version durchführen. Generell sollten Sie bei allen Smart-Home- und Netzwerkgeräten regelmäßig nach Updates für die Firmware und für Verwaltungssoftware Ausschau halten. Lücken in diesen Geräten können gravierende Folgen haben. ■

Sicherheitstipps der Experten

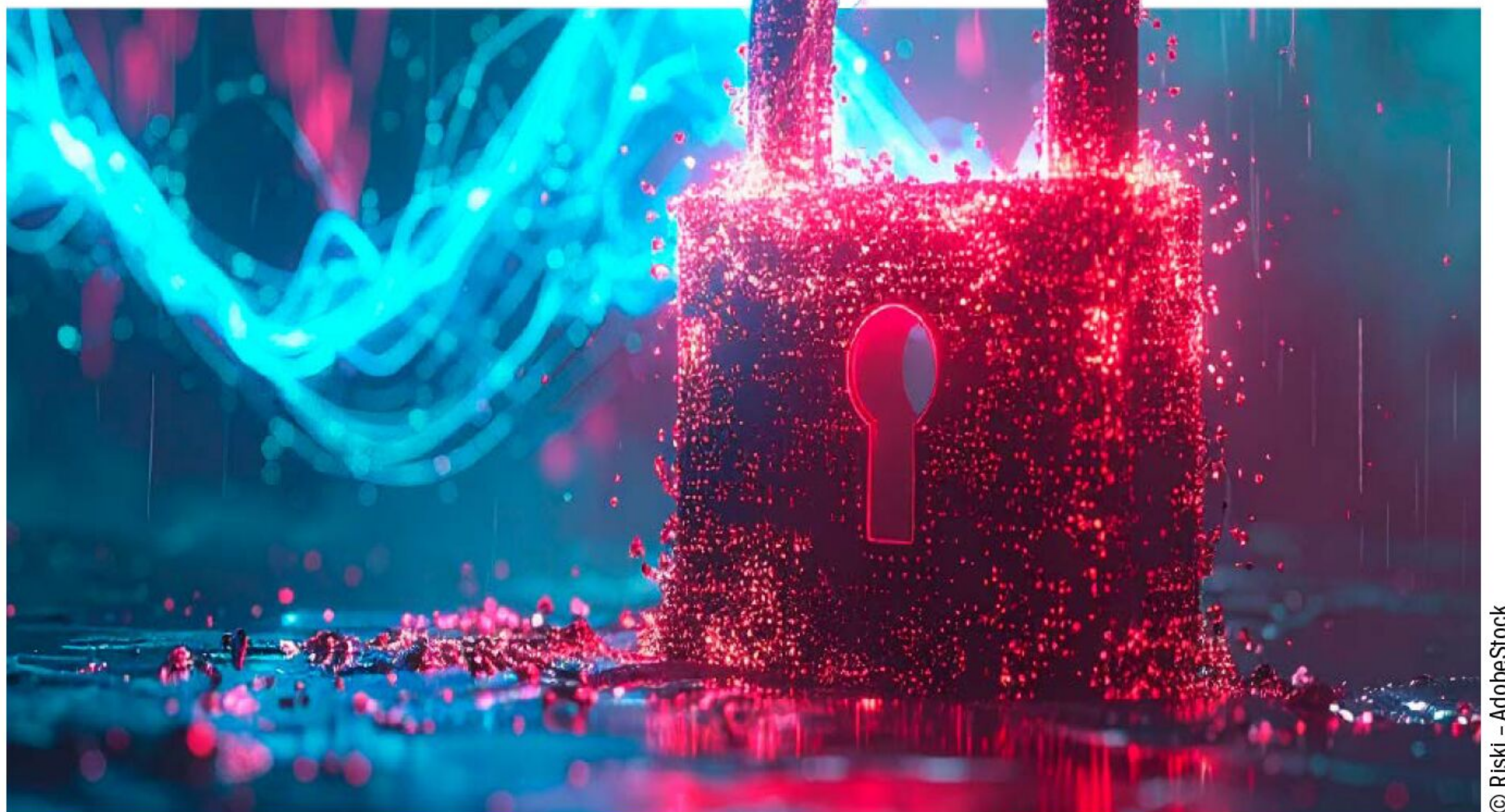
Die Zahl der Fälle von Cyberkriminalität ist in Deutschland nach wie vor hoch. Doch wo liegen die größten Gefahren für die Anwender, und wie begegnet man ihnen? Wir haben sechs Experten befragt.

VON ROLAND FREIST

Wenn es um die Gefahren im Cyberspace geht, beherrschen bereits seit Jahren Themen wie Phishing-Mails, Ransomware und Betrug über Onlineshops die öffentliche Debatte. Doch wie sieht die aktuelle Sicherheitslage tatsächlich aus? Und was sollte man tun, wenn man den Verdacht hat, selbst Opfer eines Onlinebetrugs geworden zu sein? Wir haben Experten von der Verbraucherzentrale NRW, vom Chaos Computer Club, von Trend Micro und vom Dezernat Cybercrime des Bayerischen Landeskriminalamts befragt. Auf Heft-DVD finden Sie passende Schutztools für Windows.

Verbraucherschutz: So können sich Internetnutzer absichern

Die Website der Verbraucherzentrale NRW (www.verbraucherzentrale.nrw) liefert umfangreiche Informationen zu aktuellen Betrugsfällen und immer wieder neuen Maschinen von Kriminellen im Internet. Unsere Fragen wurden beantwortet von David Riechmann, Fachanwalt für Bank- und Kapitalmarktrecht, Iwona Husemann, Referentin Gruppe Verbraucherrecht, und Dr. Ralf Scherfling, wissenschaftlicher Mitarbeiter in der Gruppe Finanzen und Versicherungen.



© Riski - AdobeStock



Iwona Husemann, Referentin Gruppe Verbraucherrecht bei der Verbraucherzentrale NRW

PC-WELT: Wie sicher sind Zahlungsdienste wie Klarna oder Paypal aus Sicht der Verbraucherzentrale?

Riechmann: Technisch können wir die Dienste nicht auf Sicherheitslücken prüfen. Grundsätzlich können Verbraucher:innen diese Zahlungsdienste nutzen, wenn sie sich an die Vorsichtsmaßnahmen halten, die auch im Onlinebanking gelten, insbesondere ist eine Zwei-Faktor-Authentifizierung empfehlenswert.

PC-WELT: Was sind aktuell die größten Risiken für Verbraucher beim Surfen, Einkaufen oder Kommunizieren im Internet?

Riechmann: Verbraucher:innen werden durch Werbung häufig auf Seiten gelenkt, bei denen entweder ihre Daten abgegriffen werden, oder auf Seiten, die sich im Nachgang als Fakeshops oder unseriöse Geldanlagen herausstellen.

PC-WELT: Was sollte ich tun, wenn ich Ware im Internet bestellt und bezahlt, aber nicht erhalten habe?

Husemann: Sie sollten sich zunächst mit dem Shop in Verbindung setzen. Existiert dieser nicht (mehr), sollten Sie versuchen, über die Bank oder den Zahlungsdienstleister das bereits gezahlte Geld zurückzufordern. Bei Überweisungen ist das in der Regel allerdings nicht mehr möglich. Haben Sie das Gefühl, betrogen worden zu sein, sollten Sie Strafanzeige bei der örtlichen Polizeidienststelle erstatten.

PC-WELT: Eine unbekannte Person verschickt unter meinem Namen Spamnachrichten. Wie kann ich mich wehren?

Dr. Scherfling: Wenn Sie vermuten, dass sich ein Unbefugter Zugang zu Ihrem Mailkonto verschafft hat, sollten Sie als Erstes prüfen, ob es in Ihrem Account fremde Zu-

griffe gibt. Viele Anbieter bieten auch die Möglichkeit, online im Kundencenter oder den Mailbox-Einstellungen die Log-ins zu prüfen und unbekannte Log-ins zu trennen. In dem Zusammenhang sollte man auch nachsehen, ob Kontoeinstellungen geändert und beispielsweise Weiterleitungen eingerichtet wurden.

Gab es unbefugte Zugriffe, sollte zeitnah das Passwort geändert und der Mailprovider informiert werden. Selbst wenn es keine fremden Zugriffe gab, sollte man überlegen, sicherheitshalber das Passwort zu ändern. Sofern noch nicht geschehen, sollten Sie ferner darüber nachdenken, eine Zwei-Faktor-Authentifizierung zu aktivieren. Außerdem sollten Sie in jedem Fall Strafanzeige stellen.

Biometrische Verfahren: Was spricht dafür, was dagegen?

Jochim Selzer gehört zum Kreis der Sprecher des Chaos Computer Clubs und gibt seit Jahren Seminare zu Datenschutz- und Sicherheitsthemen.

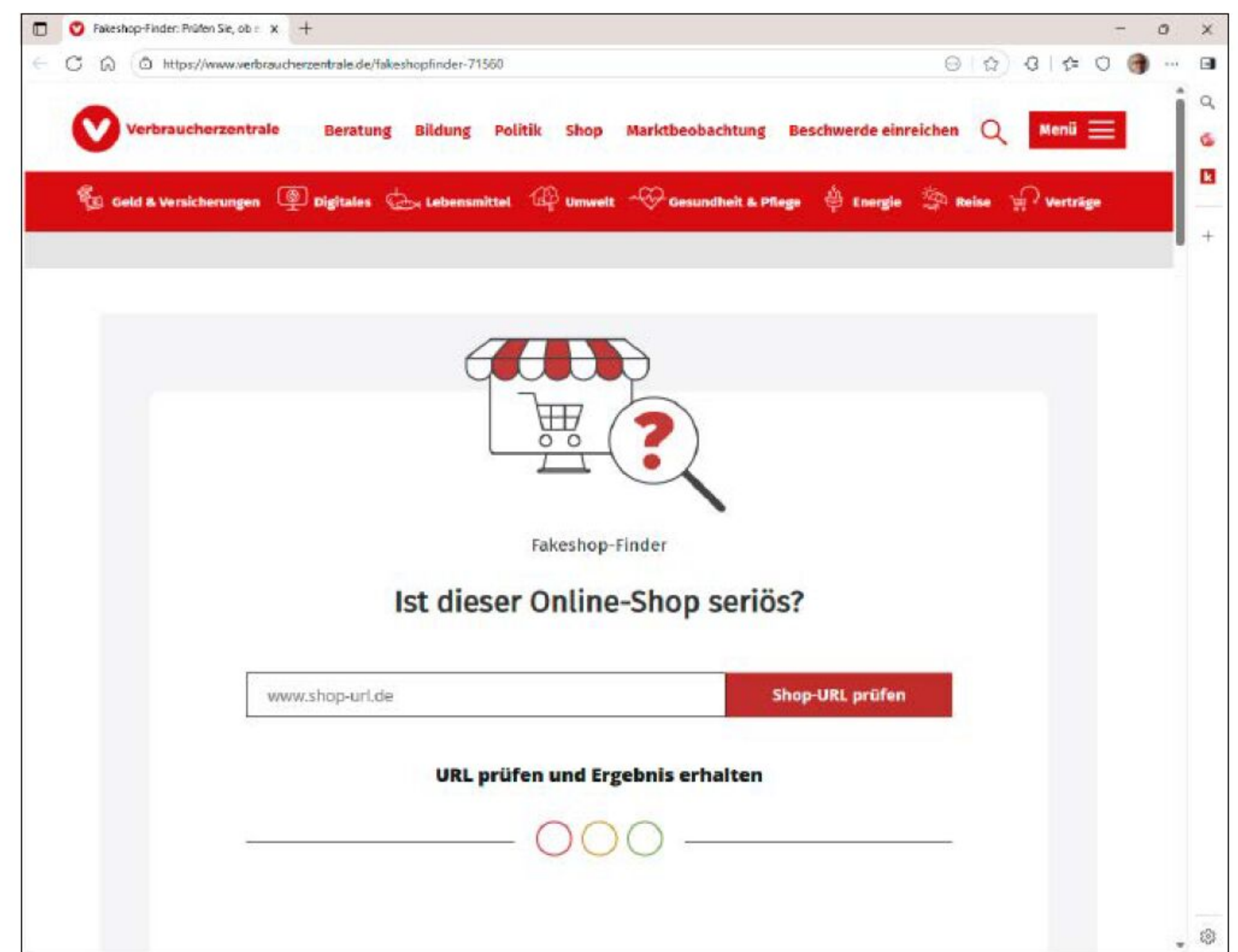


Jochim Selzer, Sprecher beim Chaos Computer Club

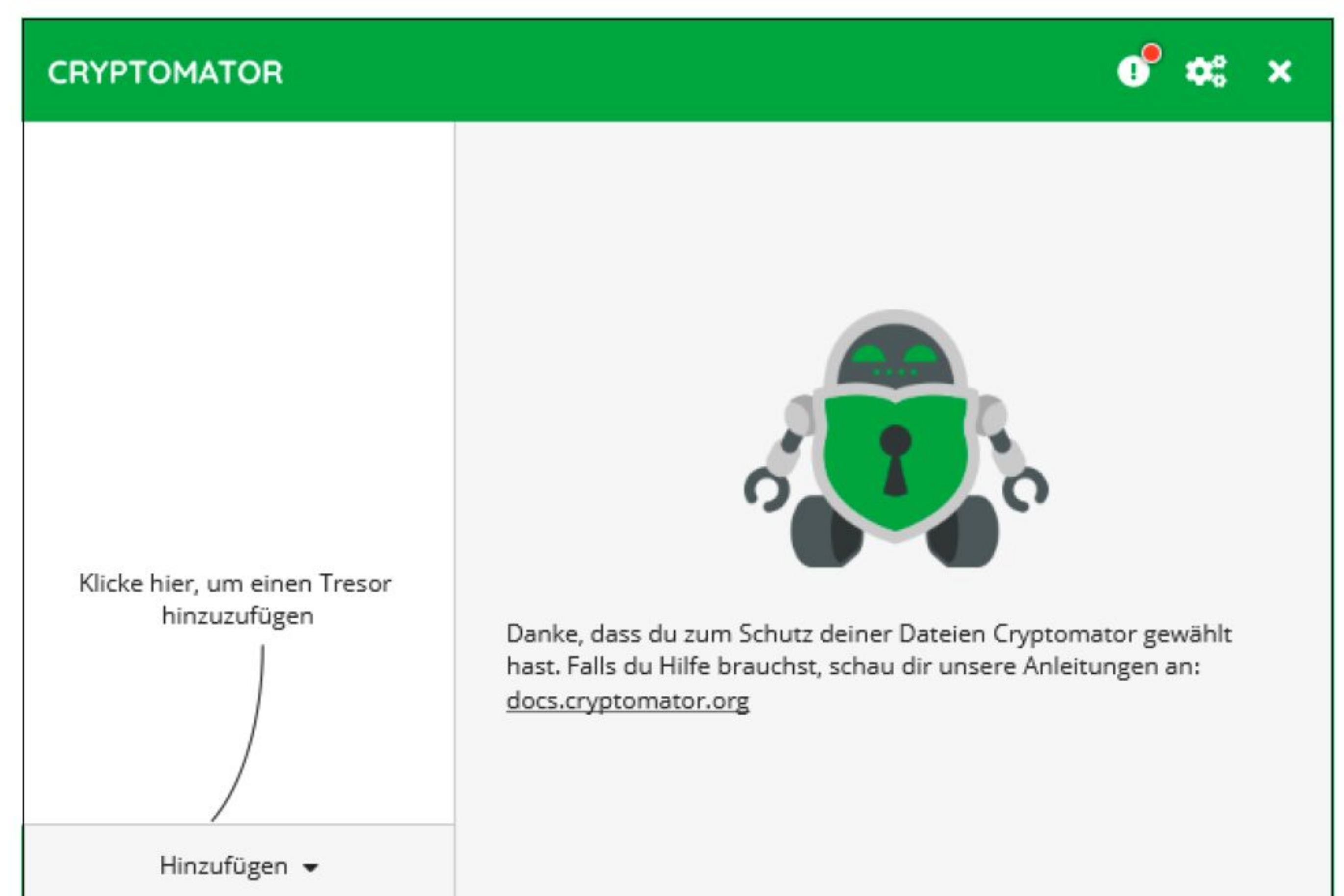
PC-WELT: Wie gut schützt eine biometrische Authentisierung – etwa per Fingerabdruck oder Gesichtserkennung?

Selzer: Biometrische Merkmale haben das Problem, dass sie kopiert und nachgemacht werden können. Die Qualität einer biometrischen Authentifizierung hängt zudem von der Qualität des Geräts oder der Technologie ab. Fingerabdrucksensoren etwa lassen sich in vielen Fällen überlisten, indem man einen Fingerabdruck von einer Oberfläche abnimmt und in ein Bildbearbeitungsprogramm überträgt. Dann erfolgt

Auf der Seite der Verbraucherzentrale findet sich unter anderem ein Fakeshop-Finder, mit dem der Besucher überprüfen kann, ob ein Onlineshop seriös ist oder ob es sich um einen Fakeshop handelt.



Mit der Open-Source-Software Cryptomator kann man die eigenen Daten bei einem Cloud-Dienst wie Onedrive sicher verschlüsseln und vor fremden Blicken schützen.



ein Ausdruck auf eine Plastikfolie, die anschließend mit Holzleim bestrichen wird, was einen Latexfilm ergibt, den man sich auf den Finger legen kann. Außerdem lässt sich die digitale Kopie des Abdrucks verschicken, sodass jedermann ihn nachbilden und nutzen kann.

Wenn Sie jedoch nur ein Smartphone entsperren wollen, dann finde ich in einem normalen Kontext das Verwenden eines Fingerabdrucks in Ordnung. Auch als zweiter Faktor für eine Authentifizierung sind biometrische Merkmale aus meiner Sicht zulässig.

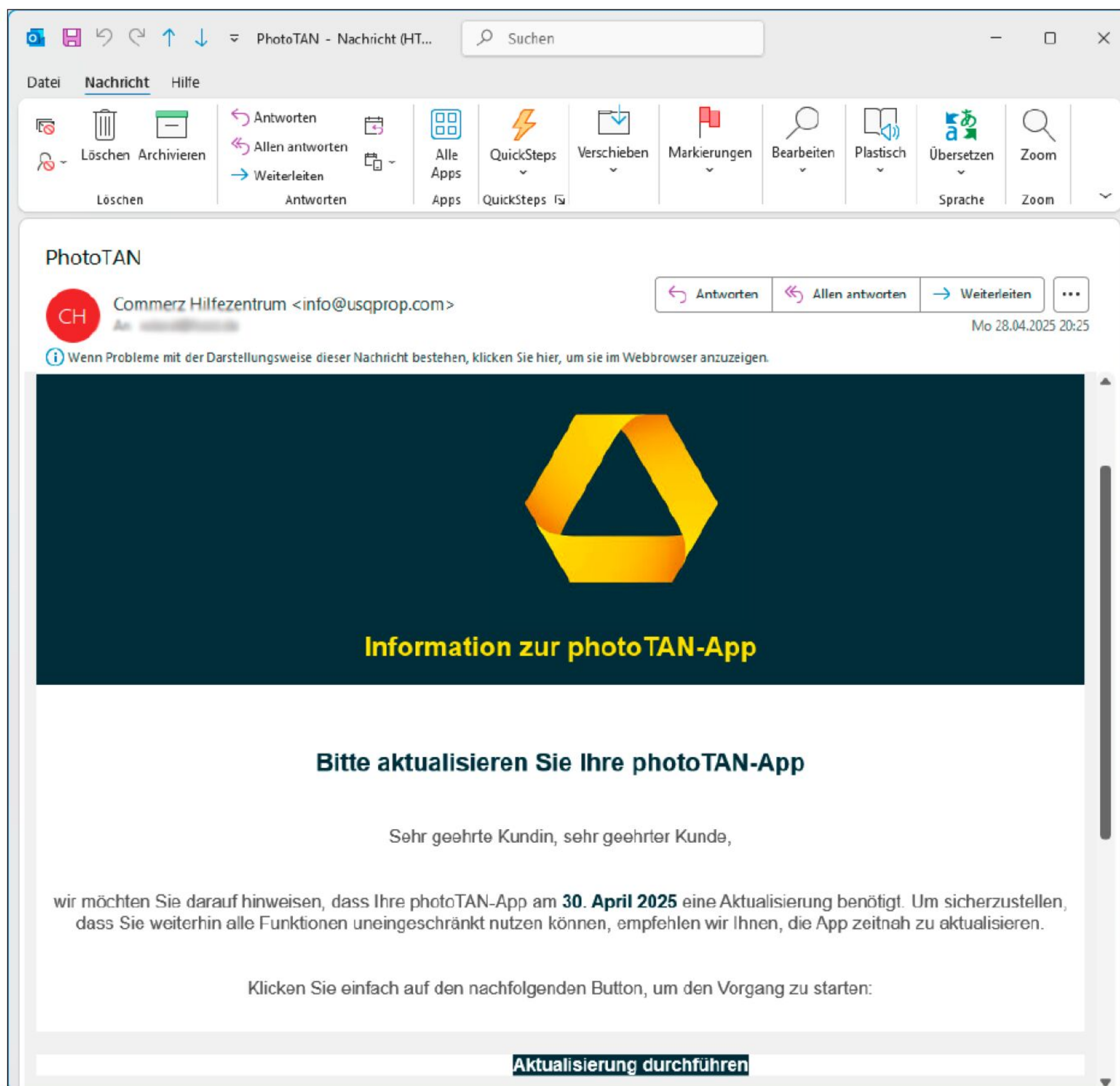
PC-WELT: Wie sieht es mit Passkeys aus?

Selzer: Passkeys halte ich von der Idee her für das, was man haben möchte. Sie arbeiten mit einem Challenge-Response-Verfahren, bei dem das Gerät, bei dem Sie sich einloggen wollen, Ihnen eine sich ständig ändernde Frage stellt, die Sie nur dann korrekt beantworten können, wenn Sie im Besitz des Geheimnisses hinter dem Passkey sind. Allerdings sind Passkeys üblicher-

weise an ein Gerät gebunden oder sie befinden sich auf einem Stick, Smartphone oder Notebook. Und so ein Gerät kann ja auch abhandenkommen, sodass andere Personen Zugriff auf den Passkey erhalten. Passkeys sollten daher niemals der einzige Anmeldefaktor sein, sondern immer mit einem zweiten Faktor kombiniert werden.

PC-WELT: Müssen private Anwender davon ausgehen, dass bei amerikanischen Clouddiensten ihre Daten gescannt und ausgewertet werden? Sind europäische Clouds sicherer? Wie können sie ihre Daten schützen?

Selzer: In den USA ist der rechtliche Schutz für Daten sehr schlecht. Die amerikanischen Ermittlungsbehörden haben nahezu unbegrenzten Zugriff auf ausländische Daten. An Onedrive komme ich als Windows-User jedoch praktisch nicht vorbei. Allerdings können Sie mit Programmen wie Cryptomator (gratis, auf Heft-DVD und unter <https://cryptomator.org>) Daten in der Cloud so ver-



Phishing-Nachrichten wie diese werden heute häufig von einer KI geschrieben. Rechtschreibung und Aufmachung haben sich dadurch deutlich verbessert. Die Nachrichten sehen oft täuschend echt aus.

schlüsseln, dass sie vom Cloudanbieter nicht gelesen werden können.

PC-WELT: Welche Programme und Apps zur sicheren Kommunikation empfehlen Sie den Anwendern?

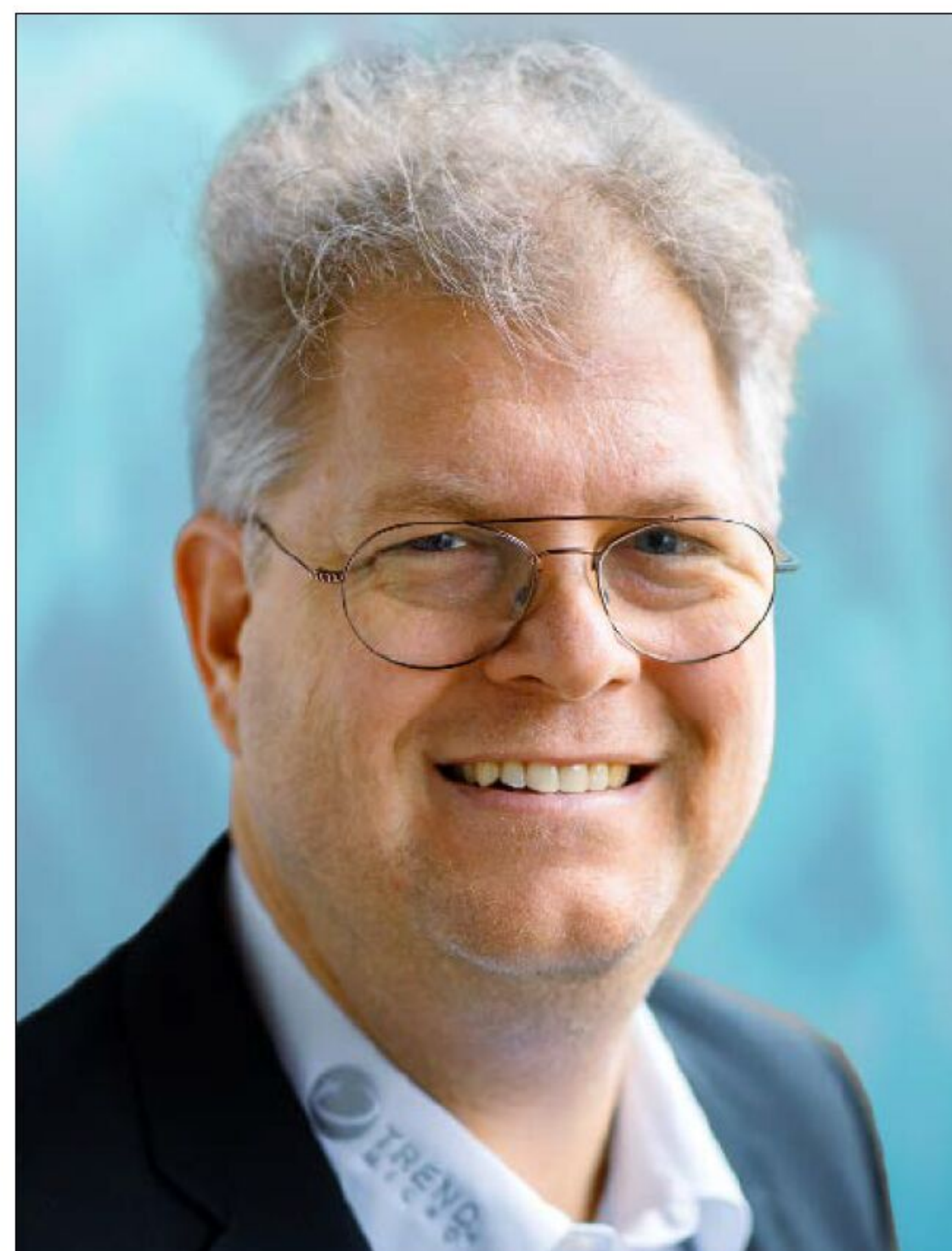
Selzer: Wenn man sich die E-Mail-Kommunikation ansieht, dann zeigt sich, dass Mails im privaten Umfeld maximal von einem Prozent der Benutzer mit Verschlüsselungsverfahren wie PGP geschützt werden. Deswegen sage ich heute, wenn Sie sicher kommunizieren wollen, dann nehmen Sie Whatsapp (www.whatsapp.com), das ist wenigstens ordentlich asymmetrisch verschlüsselt. Aber auch Signal (<https://signal.org>) und Threema (<https://threema.com>) bieten eine sichere Verschlüsselung. Bei Whatsapp ist das Problem, dass Besitzer Meta die Metadaten des Messengers liest und auswertet.

Ransomware: Weiterhin sind die Erpresserviren gefährlich

Der Cybersecurity-Anbieter Trend Micro, ursprünglich als Hersteller von Antivirensoftware bekannt, macht oft Tricks von Kri-

minellen im Internet publik. Viele der Analysen stammen von Richard Werner, dem Security Advisor der Firma in Europa.

PC-WELT: Müssen private Anwender Angst vor Ransomware-Angriffen haben?



Richard Werner, Security Advisor bei der Sicherheitsfirma Trend Micro Europe

Werner: Die meisten Ransomware-Angriffe konzentrieren sich heute auf Unternehmen. Die ganz großen Angriffswellen, die wir noch vor zehn Jahren im Privatbereich hatten, gibt es nicht mehr. Aber man muss immer eines beachten: Im Privatbereich sehen wir vor allem automatisierte Angriffe. Da wird nicht mit dem Opfer gesprochen. Das System ist verschlüsselt, und entweder derjenige zahlt oder er zahlt nicht. Punkt. Muss man davor noch Angst haben? Ich würde sagen: Ja.

PC-WELT: Wie stark nutzen Kriminelle mittlerweile Systeme mit generativer Künstlicher Intelligenz wie ChatGPT?

Werner: Sehr stark. KI wird für alle Formen von Betrug genutzt, die mit Sprache zusammenhängen. Es gibt Voice-Cloning-KI-Systeme, die es erlauben, Menschen eine andere Stimme zu verleihen und ihnen eine professionell wirkende Ausdrucksweise zu geben.

Die Technik kommt aus dem Callcenter-Bereich. Dort wird sie eingesetzt, um die Herkunft etwa eines Support-Mitarbeiters zu verschleiern. Man hat die Erfahrung gemacht, dass ein Support-Mitarbeiter, der akzentfrei Englisch spricht, für viele Amerikaner vertrauenswürdiger ist als jemand mit einem fremdländischen Akzent. Voice Cloning ist eine Technologie, die es ermöglicht, dass jemand seinen Akzent verliert. Dafür wurde sie ursprünglich mal entwickelt. Im Privatbereich wird sie zusammen mit Deepfakes häufig für Sextortion eingesetzt, also für gefälschtes Bild- oder Tonmaterial, mit dem ein Krimineller droht, eine Person in ein schlechtes Licht zu setzen, um sie damit zu erpressen.

Auch Textnachrichten werden von einer KI geschrieben. Es kommt eine E-Mail von der Bank und besagt, dass Sie die Zugangsdaten für Ihr Konto aktualisieren müssen. Mit der KI lässt sich die Mail so formulieren, dass sie wirklich überzeugend klingt. Die KI kann nicht nur einen vorgegebenen Text schreiben und übersetzen, sondern man kann die KI so programmieren, dass die Aussage tatsächlich so wirkt, als käme sie von einem Bankmitarbeiter.

PC-WELT: Wie sinnvoll ist die Installation einer Antivirensoftware, wenn in Windows mit dem Defender bereits ein Schutzprogramm enthalten ist?

Werner: Windows ist nicht deswegen so häufig das Ziel von Hacker-Angriffen, weil

es sich um eine schlechte Software handeln würde. Es wird angegriffen, weil neunzig Prozent der Weltbevölkerung dieses Betriebssystem einsetzen. Der Defender ist nur eine Erweiterung von Windows. Eine Angriffssoftware muss sich daher aufgrund der weiten Verbreitung immer daran messen lassen, ob sie an diesem Verteidigungswall vorbeikommt oder nicht. Die Software anderer Hersteller ist solchen zielgerichteten Angriffen weniger stark ausgesetzt.

Betrugsversuche im Internet: Gesundes Misstrauen hilft

Dieter Hausberger ist der Dezernatsleiter Cybercrime beim Bayerischen Landeskriminalamt. Er ist besorgt über die hohe Zahl von Betrugsversuchen, die Privatpersonen im Internet bedrohen, und weist auf die Tausenden von Betrugsfällen im Zusammenhang mit dem Handel von Kryptowährungen hin.



Dieter Hausberger, Dezernatsleiter Cybercrime beim Bayerischen Landeskriminalamt

PC-WELT: Bedrohen KI-Systeme wie Chat-GPT oder Bildgeneratoren Sicherheit und Datenschutz?

Hausberger: Während noch vor wenigen Jahren Phishing-Mails oft schon an der Rechtschreibung als zumindest unstimmtig erkannt wurden, können diese – nicht zuletzt durch Einsatz von KI – mittlerweile so täuschend echt gestaltet sein, dass die E-Mail selbst keinerlei Verdacht erweckt. Und bereits jetzt gibt es für jedermann zugängliche KI, die ausgehend von einem

Eine neue Masche krimineller Banden ist der betrügerische Handel mit Kryptowährungen. In diesem Zusammenhang ermittelt die ZCB derzeit gegen rund 3000 Cybertrading-Plattformen.

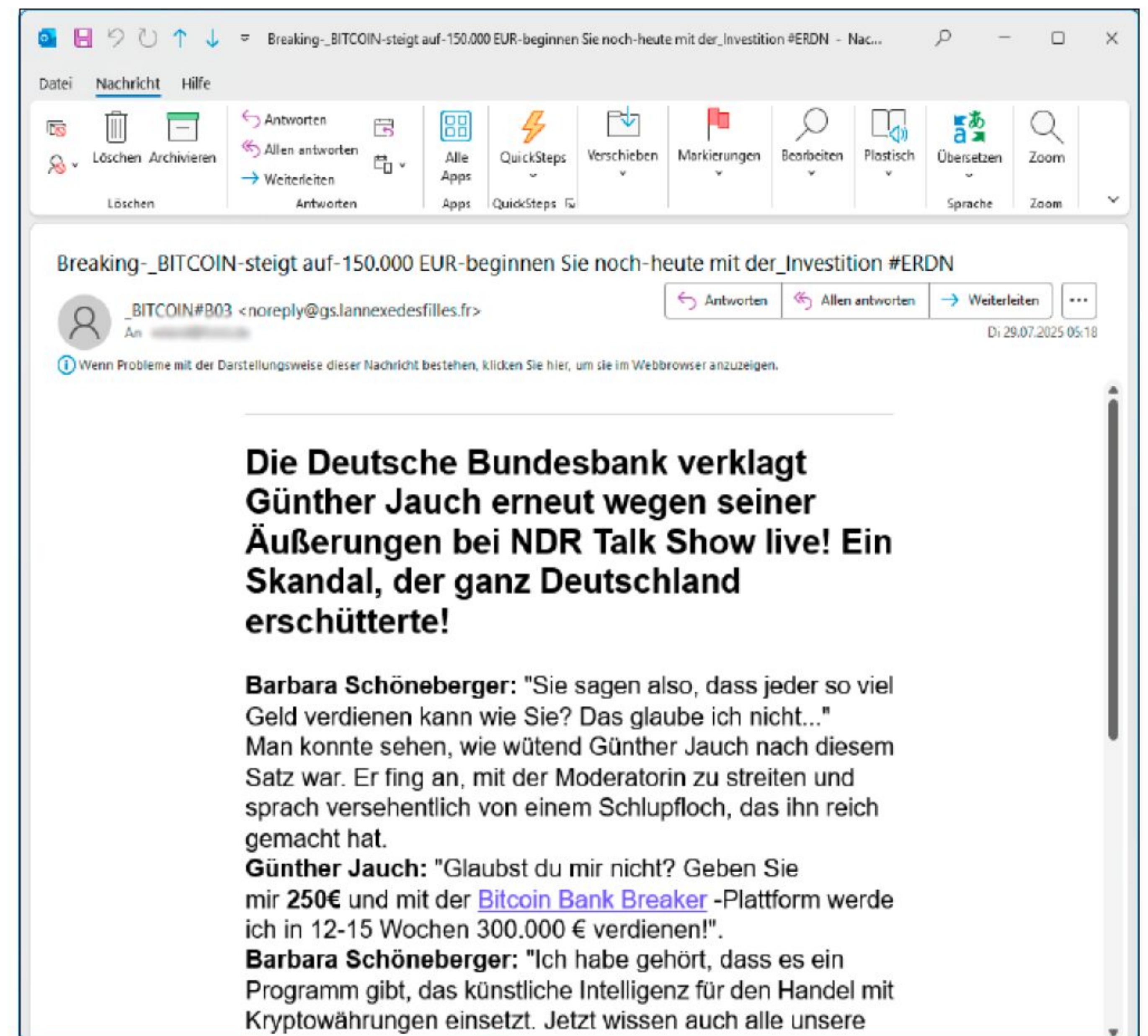


Bild echt wirkenden Film inklusive Sprachuntermalung generiert.

PC-WELT: Wie kann man sich vor KI-generierten Fake-Nachrichten und -Bildern schützen?

Hausberger: Hier kann ich Ihnen nur den Rat geben, ein gesundes Misstrauen an den Tag zu legen. Es gibt beispielsweise Videos, in welchen von Betrügern per KI generierte Prominente über soziale Medien davon berichten, extrem erfolgreich in Kryptowährungen investiert zu haben. Ich weiß nicht, ob es künftig Warnmechanismen geben wird, die uns ähnlich einer Firewall vor derartigen Fakes schützen werden. Naheliegender bietet es sich hier an, KI zur Abwehr einzusetzen.

PC-WELT: Ist das Bewusstsein der Bürgerinnen und Bürger für die Gefahren im Internet ausreichend geschärft?

Hausberger: Laut einer aktuellen Pressemeldung der Generalstaatsanwaltschaft Bamberg, Zentralstelle Cybercrime Bayern (ZCB), liefen und laufen dort Ermittlungen gegen etwa 3000 Cybertrading-Plattformen, auf denen betrügerischer Handel mit Kryptowährungen stattfindet beziehungsweise stattfand. Bisher kam es zum Eingang von 14.000 Anzeigen von überwiegend bayerischen Geschädigten mit einem geschätzten Gesamtschaden von ca. 500 Millionen Euro. Ich denke, dass wir es noch nicht geschafft haben, die Vorsicht vor Gefahren des Internets auf dieselbe Stufe wie vor Gefahren in der analogen Welt zu heben.

PC-WELT: Was sagen Sie, wenn das Opfer eines Betrugsfalls im Internet keine Anzeige bei der Polizei stellt, mit der Begründung, dass es sich ja um ausländische Straftäter handelt, die für die deutsche Polizei ohnehin nicht greifbar seien?

Hausberger: Da hat die Person nur bedingt recht. Die ZCB führt in ihrem aktuellen Bericht zum Thema Cybertrading mehr als 180 Festnahmen im In- und Ausland seit 2019 auf. Wir selbst haben als Zielgruppe Hightech-Kriminelle und konnten Anfang des Jahres zusammen mit Partnerbehörden vier Beschuldigte in Südostasien festnehmen. In manchen Ländern sind Festnahmen natürlich sehr schwierig. Aber da ist es mittlerweile so, dass die Täter mit Sanktionen belegt werden können und aufgrund von internationalen Haftbefehlen Probleme haben, zu reisen.

Jede Anzeige ist wichtig, und eine einzelne Anzeige bringt nur vermeintlich wenig. Letztlich ist es oft so, dass eine auf Opferseite als wenig bringend bewertete Einzelanzeige die initiale Spur erzeugt, um einen großen Tatkomplex und viele dahinterstehende Einzelanzeigen zu klären.

PC-WELT: In welchem Bereich sehen Sie derzeit die größten Gefahren für Privatpersonen im Internet?

Hausberger: Alles rund um den Betrug und das Abfangen von Daten, wodurch Kriminelle in der Verlängerung wieder Betrug begehen können, ist für Privatpersonen das Deliktfeld, das wohl am meisten unmittelbare Auswirkungen hat. ■



© Mit Material von MCGORIE – AdobeStock

Im Test: Virenschutz für 2026

Antivirenprogramme werden immer besser. Der diesjährige Antivirentest zeigt, dass die Erkennungsraten mittlerweile bei allen Herstellern knapp unter 100 Prozent liegen. Und auch bei der Performance haben die Testkandidaten zugelegt.

VON ROLAND FREIST

Der diesjährige Antivirentest bestätigt einige Tendenzen, die sich bereits seit mehreren Jahren zeigen. So gleichen sich die Ergebnisse bei der Virenerkennung und -bekämpfung immer weiter einander an. Bei der Effektivität trennen die Programme nur noch einige Zehntelprozente.

„Auch kostenlose Antivirenprogramme bieten einen zuverlässigen Schutz vor Schädlingen.“

Dass die Antivirenprogramme sich bei den Erkennungsraten mittlerweile kaum noch unterscheiden, ist natürlich zum einen auf die Arbeit der Forschungsabteilungen bei den Herstellern zurückzuführen, die ihre Produkte ständig verbessern und optimieren. Zum anderen kommen diese eng beieinander liegenden Ergebnisse aber auch zustande, weil die Firmen bereits seit etlichen Jahren über Branchenorganisationen wie die Cyber Threat Alliance (CTA) oder die Malware Information Sharing Platform (MISP) einen automatisierten Austausch von „Indicators of Compromise“ (IoC) organisieren, also eine Weitergabe von Virensignaturen, Hashcodes, verdächtigen Domains und IP-Adressen. Mit STIX (Structured Threat Information eXpression) und TAXII (Trusted Automated eXchange of Intelligence Information) existieren sogar

unabhängige Standards für den automatisierten Austausch von Bedrohungsdaten. Echte Ausreißer bei den Erkennungsraten gibt es daher kaum mehr, alle Programme arbeiten bei der Virenbekämpfung ähnlich gut. Nennenswerte Unterschiede zeigen sich im Test lediglich bei den „False Positives“, also den Fehllarmen. Einige Programme erweisen sich bei der Zuordnung zu den beiden Gruppen „Virus“ und „Kein Virus“ als sehr treffsicher, andere dagegen melden in mehreren Dutzend Fällen einen Virus, wo keiner ist.

Defender wird immer besser

Ein weiterer Trend ist, dass es auch zwischen kostenlosen und kostenpflichtigen Programmen kaum mehr Leistungsunterschiede gibt. So landen die kostenlosen, baugleichen Produkte von Avast und AVG

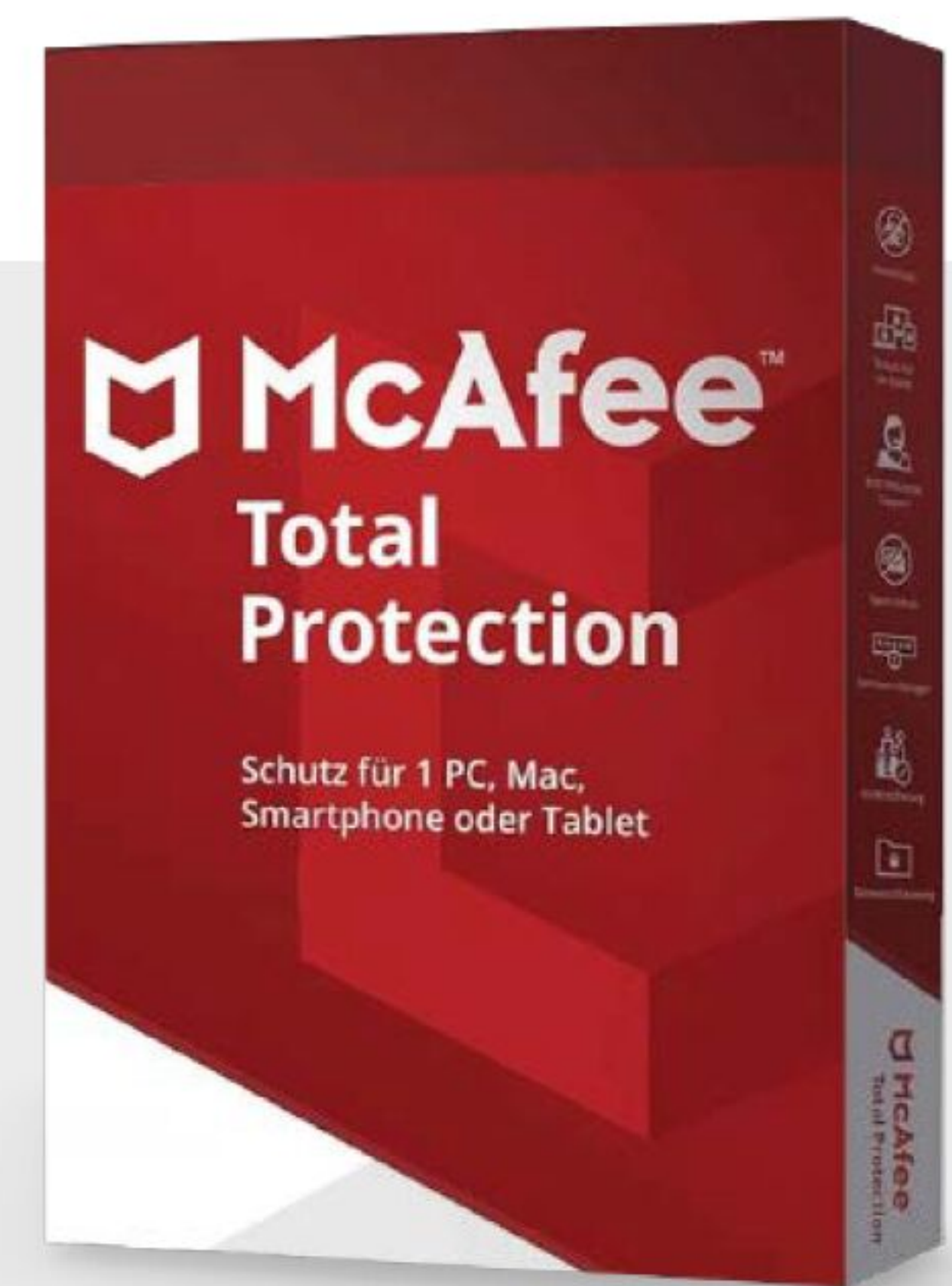
bei jedem Test in der Spitzengruppe. Auch der in Windows enthaltene Defender kann mit den Produkten der spezialisierten Antivirenfirmen problemlos mithalten. Microsoft hat seinen Virenwächter jedes Jahr ein Stück verbessert. Während die Erkennungsraten in der Anfangszeit noch bei katastrophalen 70 Prozent lagen, was dem Defender in Tests regelmäßig den letzten Platz bescherte, braucht sich die Software heute nicht mehr zu verstecken und kommt regelmäßig auf einen Platz im Mittelfeld der Ergebnistabelle.

Wenig Unterschiede beim Ressourcenverbrauch

Neben der Qualität der Virenerkennung untersucht dieser Test auch den Ressourcenverbrauch der Programme. Antivirensoftware muss kontinuierlich im Hintergrund laufen, damit sie eindringende oder plötzlich aktiv werdende Schädlinge sofort erkennen und bekämpfen kann. Dafür belegt sie Arbeitsspeicher und CPU-Ressourcen und greift auf das Speichermedium zu, also die SSD. Je nach Konfiguration und innerem Aufbau der Antivirenprogramme wirkt sich das mehr oder weniger stark auf die Performance des Rechners aus, er wird also langsamer. Bemerkbar macht sich das in Windows unter anderem an träge startenden Programmen, gebremsten Streifzügen durchs Web und bei älteren Festplatten auch an verlangsamten Kopieraktionen.

TESTSIEGER: MCAfee TOTAL PROTECTION

Die amerikanische Firma McAfee gehört bei jedem Test von Antivirenprogrammen zum Kreis der Favoriten. Dieses Jahr hat es mal wieder für die oberste Stufe auf dem Treppchen erreicht. Die Software fährt sowohl bei den Erkennungsraten wie auch bei der Geschwindigkeit Spitzennoten ein. Der Vorsprung gegenüber den baugleichen Programmen von Avast und AVG ist allerdings nur hauchdünn und wird erst bei der dritten Stelle hinter dem Komma sichtbar.



Allerdings hat die Entwicklung der Hardware in den vergangenen Jahrzehnten dazu geführt, dass auch ressourcenhungrige Vertreter aus der Riege der Antivirenprogramme moderne PCs kaum noch ins Schwitzen bringen. In unserem Test führt das dazu, dass viele Kandidaten bei der Messung der Performance die Bewertung „sehr schnell“ erhalten, was bedeutet, dass die Unterschiede sehr klein sind und die meisten Programme die Leistung des PCs kaum beeinträchtigen.

Das BSI warnt vor Kaspersky-Produkten

Die russische Firma Kaspersky liefert mit der gleichnamigen Software ein Antiviren-

tool, das seit Jahren regelmäßig im oberen Drittel der Testtabellen landet. Allerdings besteht seit 2022 eine Warnung des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI), die sich insbesondere an Behörden und Betreiber kritischer Infrastruktur richtet. Grund ist ein Gesetz, das der russischen Regierung Zugriff auf Unternehmensdaten erlaubt. Das BSI sieht darin ein Risiko, da Antivirenprogramme Systemrechte besitzen und sich daher für Spionage oder Sabotage geradezu anbieten. Kaspersky betont dagegen seine Unabhängigkeit und verweist darauf, dass es bereits vor Jahren seine Rechenzentren mit allen Daten in die Schweiz verlagert hat.

PC-WELT: WIE WIR TESTEN

In diesem Test untersuchen wir die Virenerkennung und die Geschwindigkeit der Programme. Den teilweise stark variierenden Funktionsumfang der Tools berücksichtigen wir dabei nicht.

Für den Test der Antivirenprogramme greifen wir auf die Messdaten des österreichischen Prüfinstituts AV-Comparatives (www.av-comparatives.org) zurück. Als Hardwarebasis dient dem Institut ein Low-End-Rechner mit einem Intel Core i3, 8 GB RAM und einer SSD.

Um die Leistung beim Virenschutz zu ermitteln, wird im Test Real World Protection beobachtet, wieviel Prozent der eingesetzten Schädlinge erkannt und abgeblockt werden können.

Der Malware-Protection-Test hingegen geht davon aus, dass Schadsoftware bereits in den Rechner eingedrungen ist. Er misst, wieviel Prozent der zunächst noch inaktiven Viren erkannt und unschädlich gemacht werden. Beide Tests registrieren zudem die Zahl der Fehlalarme.

Die Performance-Tests messen, wie schnell typische Dateiaktionen unter Windows trotz aktivierter Antivirensoftware ausgeführt werden. Hinzu kommen die Ergebnisse aus mehreren Benchmarktests. AVC-Score steht für den AV-Comparatives-Score, einen Performance- und Security-Test, der mehrere Testroutinen in sich vereint. Procyon steht hingegen für die Procyon-Benchmark-Suite von UL Solutions, und dabei vor allem für den Office-Productivity-Benchmark. Die Ergebnisse beider Benchmarks ergeben zusammengeordnet den Impact-Score. Für die Bewertung berücksichtigen wir allein das Ergebnis des Impact-Scores. Die Ergebnisse der Virenschutz- und Performance-Tests ergeben zwei Einzelnoten, die wir im Verhältnis 60:40 werten und daraus unsere Gesamtnote berechnen.



IM ÜBERBLICK: 19 INTERNET-SICHERHEITSPROGRAMME



Testergebnisse		Platz 1	Platz 2	Platz 2	Platz 4
Produkt		McAfee Total Protection	Avast Free Antivirus	AVG Antivirus Free	Norton Antivirus Plus
Internet		www.mcafee.com	www.avast.de	www.avg.com	www.nortonlifelock.com
Virenschutz (60 %)		Gewichtung			
Real World Protection Test: Blockiert (%) / Note	35 %	99,6 / 1,2	100 / 1,0	100 / 1,0	100 / 1,0
False Positives I / Note	15 %	2 / 1,1	5 / 1,2	4 / 1,2	3 / 1,1
Malware Protection Test: Blockiert (%) / Note	35 %	99,96 / 1,03	99,96 / 1,03	99,96 / 1,03	99,96 / 1,03
False Positives II / Note	15 %	15 / 1,7	10 / 1,5	10 / 1,5	10 / 1,5
Zwischennote Virenschutz	60 %	1,2	1,12	1,12	1,1
Geschwindigkeit (40 %)					
Kopieren von Dateien (erster Lauf)		sehr schnell	sehr schnell	sehr schnell	sehr schnell
Kopieren von Dateien (zweiter Lauf)		sehr schnell	sehr schnell	sehr schnell	sehr schnell
Komprimieren/Dekomprimieren		sehr schnell	sehr schnell	sehr schnell	sehr schnell
Programme installieren		sehr schnell	sehr schnell	sehr schnell	sehr schnell
Programme starten (erster Lauf)		sehr schnell	sehr schnell	sehr schnell	sehr schnell
Programme starten (zweiter Lauf)		sehr schnell	sehr schnell	sehr schnell	sehr schnell
Dateien herunterladen		sehr schnell	sehr schnell	sehr schnell	sehr schnell
Surfen im Web		sehr schnell	sehr schnell	sehr schnell	sehr schnell
AVC-Score (höher ist besser)		90	90	90	90
Procyon-Score (höher ist besser)		97,4	96,2	96,2	95,4
Impact-Score (niedriger ist besser)		2,6	3,8	3,8	4,6
Zwischennote Geschwindigkeit	40 %	1,18	1,31	1,31	1,4
Gesamtnote		1,192 / sehr gut	1,196 / sehr gut	1,196 / sehr gut	1,22 / sehr gut
Preis*		- / 110 Euro (Angebot: 35 Euro)	kostenlos	kostenlos	35 Euro (Angebot: 20 Euro) / -
Jahreslizenz für 1 Gerät / 5 Geräte					

ⓘ Voll- bzw. Testversion auf Heft-DVD * unverbindliche Preisempfehlung des Herstellers

Testergebnisse		Platz 11	Platz 11	Platz 13	Platz 14
Produkt		Avira Free Security	TotalAV Antivirus Pro	Panda Free Antivirus	F-Secure Internet Security
Internet		www.avira.com	www.totalav.com	www.pandasecurity.com	www.f-secure.com
Virenschutz (60 %)		Gewichtung			
Real World Protection Test: Blockiert (%) / Note	35 %	99,1 / 1,45	99,1 / 1,45	96,9 / 2,55	98,7 / 1,65
False Positives I / Note	15 %	0 / 1,0	1 / 1,0	8 / 1,4	0 / 1,0
Malware Protection Test: Blockiert (%) / Note	35 %	99,98 / 1,02	99,97 / 1,03	99,3 / 1,35	99,99 / 1,0
False Positives II / Note	15 %	28 / 2,9	28 / 2,9	35 / 2,7	65 / 4,2
Zwischennote Virenschutz	60 %	1,45	1,45	1,98	1,71
Geschwindigkeit (40 %)					
Kopieren von Dateien (erster Lauf)		sehr schnell	sehr schnell	sehr schnell	sehr schnell
Kopieren von Dateien (zweiter Lauf)		sehr schnell	sehr schnell	sehr schnell	sehr schnell
Komprimieren/Dekomprimieren		schnell	schnell	sehr schnell	schnell
Programme installieren		sehr schnell	sehr schnell	sehr schnell	sehr schnell
Programme starten (erster Lauf)		schnell	schnell	sehr schnell	schnell
Programme starten (zweiter Lauf)		sehr schnell	sehr schnell	sehr schnell	sehr schnell
Dateien herunterladen		sehr schnell	sehr schnell	sehr schnell	sehr schnell
Surfen im Web		sehr schnell	sehr schnell	sehr schnell	sehr schnell
AVC-Score (höher ist besser)		85	85	90	85
Procyon-Score (höher ist besser)		86,7	86,6	95,2	86,5
Impact-Score (niedriger ist besser)		18,3	18,4	4,8	18,5
Zwischennote Geschwindigkeit	40 %	3,14	3,17	2,65	3,17
Gesamtnote		2,13 / gut	2,13 / gut	2,25 / gut	2,29 / gut
Preis*		kostenlos	19 Euro (3 Geräte) / -	kostenlos	50 Euro / 80 Euro
Jahreslizenz für 1 Gerät / 5 Geräte					

ⓘ Voll- bzw. Testversion auf Heft-DVD * unverbindliche Preisempfehlung des Herstellers



Platz 5	Platz 6	Platz 7	Platz 8	Platz 9	Platz 10
Kaspersky Premium	Eset Internet Security	K7 Total Security	Microsoft Defender	G Data Total Security	Trend Micro Internet Security
www.kaspersky.de	www.eset.com	www.k7computing.com	www.microsoft.com	www.gdata.de	www.trendmicro.com
99,1 / 1,45	99,1 / 1,45	98,7 / 1,65	99,1 / 1,45	99,1 / 1,45	99,6 / 1,2
1 / 1,0	1 / 1,0	20 / 2,0	3 / 1,1	7 / 1,3	43 / 3,1
100 / 1,0	99,95 / 1,03	99,6 / 1,2	99,94 / 1,07	99,97 / 1,03	98,07 / 1,97
3 / 1,1	6 / 1,3	7 / 1,3	10 / 1,5	3 / 1,1	4 / 1,2
1,17	1,21	1,49	1,26	1,23	1,76
sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell
sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell
schnell	sehr schnell	schnell	schnell	schnell	schnell
sehr schnell	schnell	sehr schnell	schnell	sehr schnell	sehr schnell
schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell	schnell
sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell
sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell
sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell
85	85	85	80	85	85
97,5	95,5	95,6	96,5	85,6	92,2
7,5	9,5	9,4	13,5	19,4	12,8
1,94	2,05	2,04	2,61	3,16	2,53
1,48 / sehr gut	1,55 / gut	1,71 / gut	1,8 / gut	2,00 / gut	2,07 / gut
40 Euro / 55 Euro	40 Euro / 60 Euro	15 Euro / 68 Euro	kostenlos	50 Euro / 82 Euro	25 Euro (3 Geräte) / -

Platz 15	Platz 16	Platz 17	Platz 18	Platz 19
Vipre Advanced Security	Bitdefender Total Security	Malwarebytes Premium	Quick Heal Total Security	Total Defense Essential Anti-Virus
www.totaldefense.com	www.bitdefender.de	www.malwarebytes.com/de	www.quickheal.com	www.totaldefence.com
97,8 / 2,1	98,2 / 1,9	97,8 / 2,1	93 / 4,5	98,2 / 1,9
0 / 1,0	1 / 1,0	28 / 2,49	6 / 1,3	1 / 1,0
99,93 / 1,03	99,97 / 1,03	99,51 / 1,25	99,19 / 1,41	99,98 / 1,02
8 / 1,4	5 / 1,2	53 / 3,51	16 / 1,8	3 / 1,1
1,46	1,36	2,07	2,53	1,34
schnell	schnell	sehr schnell	schnell	mittel
sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell
mittel	mittel	sehr schnell	sehr schnell	mittel
schnell	sehr schnell	schnell	mittel	mittel
schnell	schnell	mittel	schnell	sehr schnell
sehr schnell	schnell	mittel	sehr schnell	sehr schnell
sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell
sehr schnell	sehr schnell	sehr schnell	sehr schnell	sehr schnell
73	73	75	78	60
94,7	91,9	97,7	97,6	95,5
22,3	25,1	17,3	14,4	35,5
3,92	4,23	3,37	2,93	5,5
2,44 / gut	2,51 / befriedigend	2,59 / befriedigend	2,69 / befriedigend	3,0 / befriedigend
20 Euro / 30 Euro	- / 95 Euro (Angebot: 50 Euro)	50 Dollar (2 Geräte) / 80 Dollar	32 Euro / -	46 Euro (3 Geräte) / -

Fehlalarm oder gefährlicher Virus?

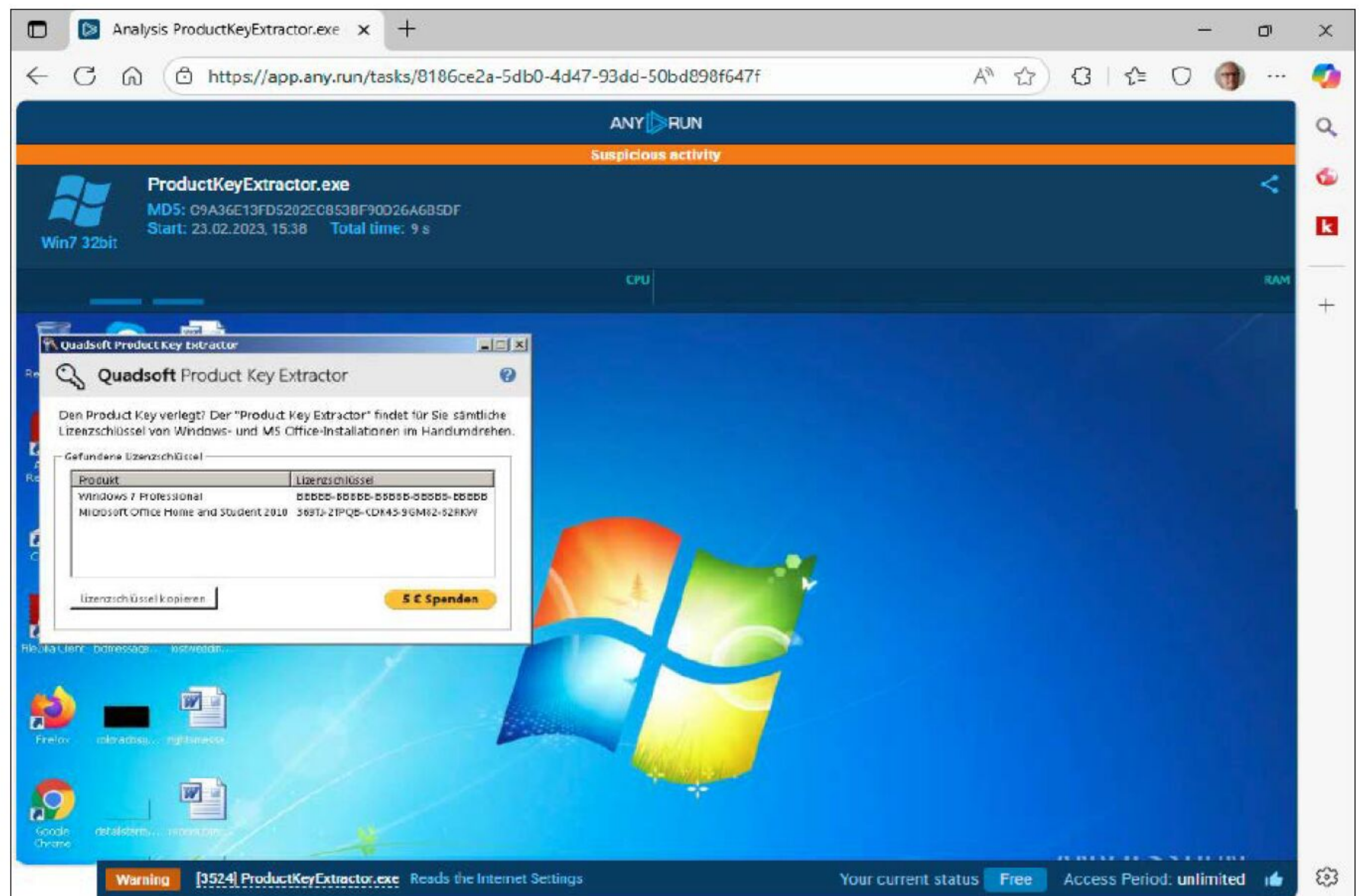
Wenn das Antivirenprogramm Alarm schlägt, löst das beim Anwender immer einen Schreckmoment aus. Doch nicht immer ist die Warnung berechtigt. Denn auch ein Virens Scanner kann sich mal irren.

VON ROLAND FREIST

Antivirensoftware ist nicht frei von Fehlern und meldet auch mal Computerviren, wo keine sind. Aus diesem Grund wehrte sich die Firma Procolored, ein Hersteller von Textildruckern, vehement gegen die Meldung eines Druckertesters, die Software eines ihrer Geräte enthalte einen Virus. Er hatte der Firma geschrieben, dass sowohl Google Chrome wie auch der Microsoft Defender beim Download der Druckersoftware Alarm ausgelöst und sie in Quarantäne genommen hatten.

Trotz des Protests von Procolored blieb der Tester hartnäckig. Er schickte die Software an die Securityfirma G Data, einen deutschen Hersteller von Antivirenprogrammen. Bei der Untersuchung stellte sich dann heraus, dass die Druckersoftware tatsächlich einen Backdoorvirus namens Xred und einen Trojaner enthielt. Als G Data

„Ein perfekt arbeitendes Antivirenprogramm, das keine Fehlalarme produziert, ist eine Illusion.“



Die Onlinesandbox Any.run lässt Sie in einer virtuellen Windows-Umgebung verdächtige Programme starten und deren Verhalten studieren.

Procolored mit den Ergebnissen konfrontierte, musste die Firma eingestehen, dass sich in ihren Downloadbereich ein Virus eingeschlichen hatte, und stellte eine neue Version ihrer Software bereit.

Wie Fehlalarme entstehen

Die zunächst abwehrende Haltung von Procolored ist verständlich. Denn es kommt tatsächlich vor, dass Antivirentools Schadsoftware erkennen, wo keine ist. Allerdings nicht häufig. Langzeittests zeigen immer wieder, dass Fehlalarme üblicherweise weniger als ein Prozent aller Virenmeldungen ausmachen. Ärgerlich sind sie jedoch, denn viele Anwender erschrecken erst einmal, wenn ihr Computer eine Schadsoftware meldet.

Wie kommen solche auch „False Positives“ genannten Fehlalarme zustande? Das hängt mit der Arbeitsweise von Antivirenprogrammen zusammen. Sie greifen zum einen auf täglich aktualisierte Virendefinitionen zu,

anhand derer sie Eindringlinge sehr sicher erkennen können. Da jedoch auch viele bislang unbekannte Schädlinge im Internet verkehren, für die noch keine Virendefinitionen existieren, bauen die Hersteller in ihre Software zusätzlich heuristische und Methoden der Verhaltensanalyse ein. Heuristisch heißt, dass die Programme auf verdächtige Merkmale einer Datei oder eines Programms achten. Die Verhaltensanalyse wiederum beobachtet die laufenden Programme auf dem PC. Beide Verfahren arbeiten mit Wahrscheinlichkeiten und berechnen, ob es sich bei einem Programm mit diesen oder jenen Eigenschaften um einen Virus handeln könnte. Dabei kommt es immer mal wieder zu Fehlalarmen.

Systemprogramme besonders betroffen

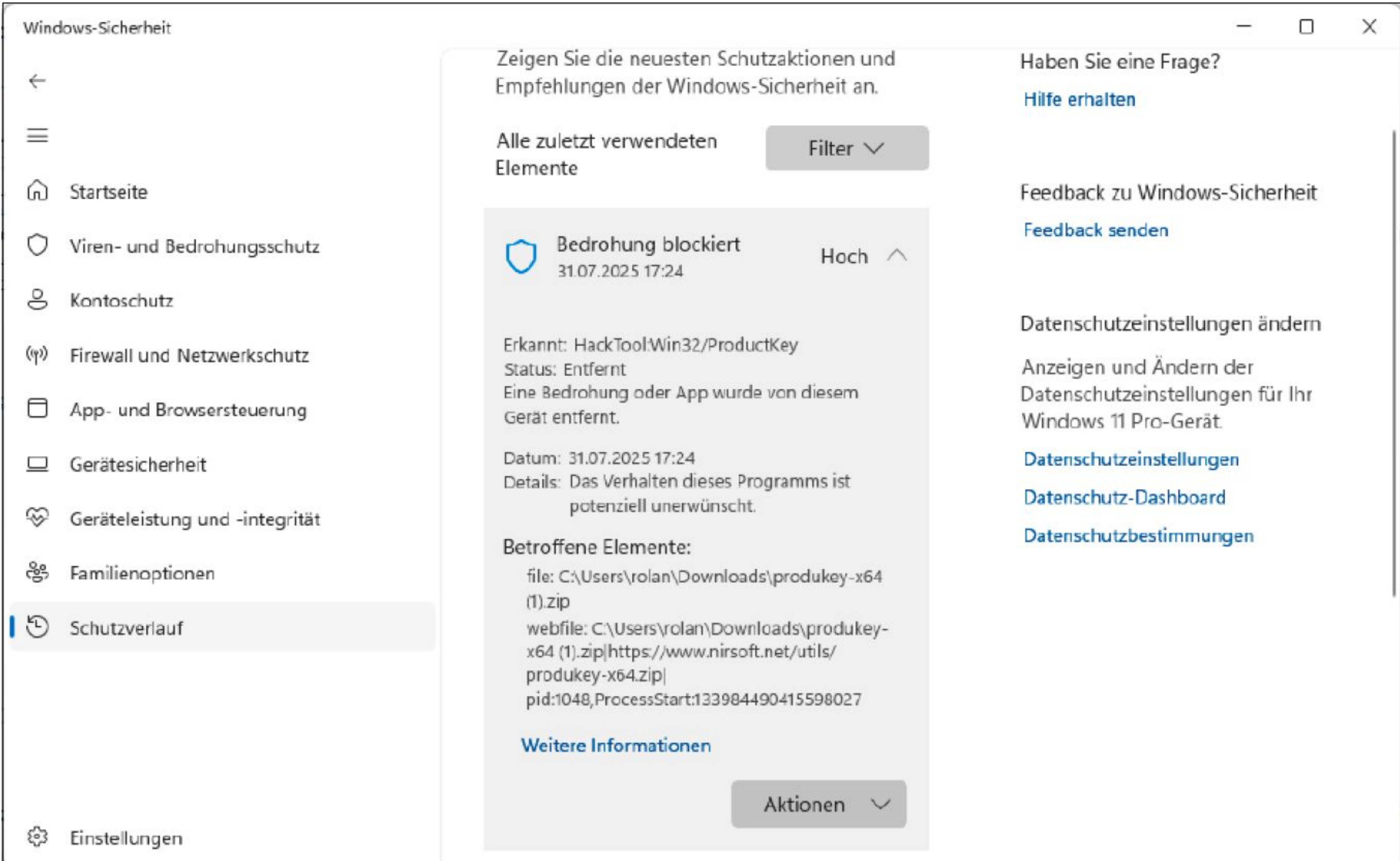
Besonders häufig treten Fehlalarme bei Programmen auf, die auf Systemeinstellungen oder Daten zugreifen, die das Antiviren-

programm als vertraulich oder sogar geheim einstuft. Das gilt beispielsweise für mehrere Tools der Softwareschmiede Nirsoft, so etwa für das Programm **Produkey**. Es liest die Lizenzschlüssel von Windows und Office 2003/2007 aus und zeigt sie in seinem Fenster an. An und für sich ein harmloser Vorgang, doch er liefert der Antivirensoftware offenbar genügend Verdachtsmomente, um die Anwendung als Virus einzustufen.

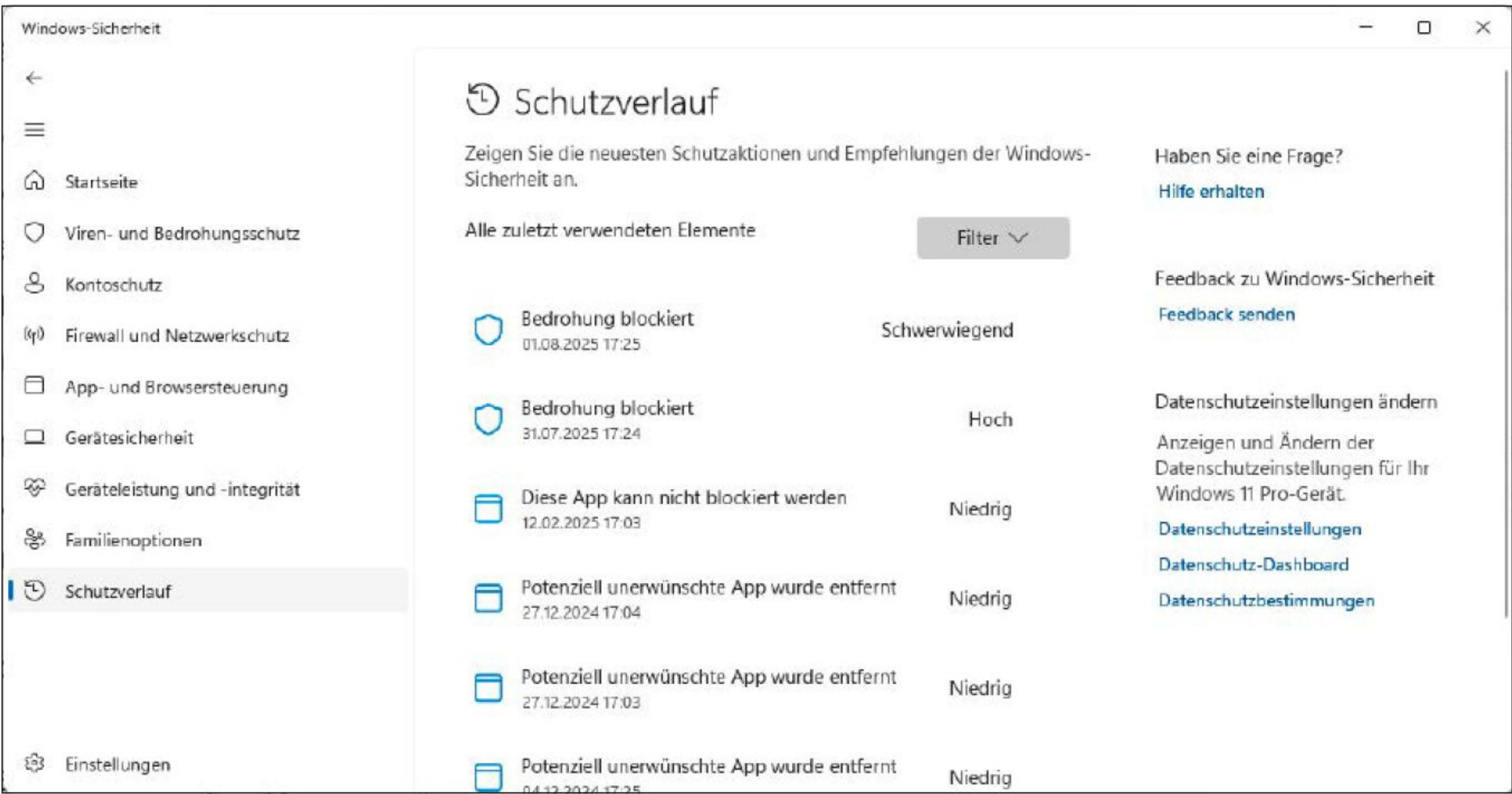
Das Gleiche gilt für zahlreiche andere Programme, die Daten wie Lizenzschlüssel oder Passwörter auslesen oder Systemeinstellungen verändern. Die Heuristik der Antivirensoftware achtet unter anderem auf Kombinationen bestimmter Systemaufrufe, wie sie für Malware typisch sind. Aber auch bekannte Hackertools, die etwa zum Knacken von Passwörtern dienen, werden von den Virenwächtern blockiert. Und das, obwohl sie legal zum Download angeboten werden. Denn das Hacken der eigenen Computer, etwa um ein vergessenes Passwort zu rekonstruieren, ist nicht verboten. Ein perfekt arbeitendes Antivirenprogramm, das keine Fehlalarme produziert, ist eine Illusion. Einerseits darf die Software auf keinen Fall einen Schädling übersehen, auf der anderen Seite soll sie harmlose Programme als solche erkennen. So ist es unvermeidlich, dass der Virenjäger im Zweifelsfall auf Nummer sicher geht und eine Software auch dann als gefährlich meldet, wenn sie das nicht ist.

Den Auslöser eines Fehlalarms überprüfen

Wenn Ihr Virenschutz Alarm auslöst, müssen Sie den Auslöser immer auch selbst unter die Lupe nehmen. Denn ansonsten besteht die Gefahr, dass das Antivirenprogramm Teile einer Software blockiert, die für ihr Funktionieren unbedingt erforderlich sind. Dabei



Das Nirsoft-Tool Produkey zeigt die Produktschlüssel von Windows und einigen Anwendungen an. Das genügt, um bei den meisten Virenwächtern, hier dem Microsoft Defender, Alarm auszulösen.



Der Defender listet die zuletzt gefundenen Bedrohungen auf und zeigt Ihnen auf Wunsch Details an. Dafür müssen Sie mit der Maus auf einen Bereich zeigen. Anschließend wird ein Pop-down-Menü angezeigt.

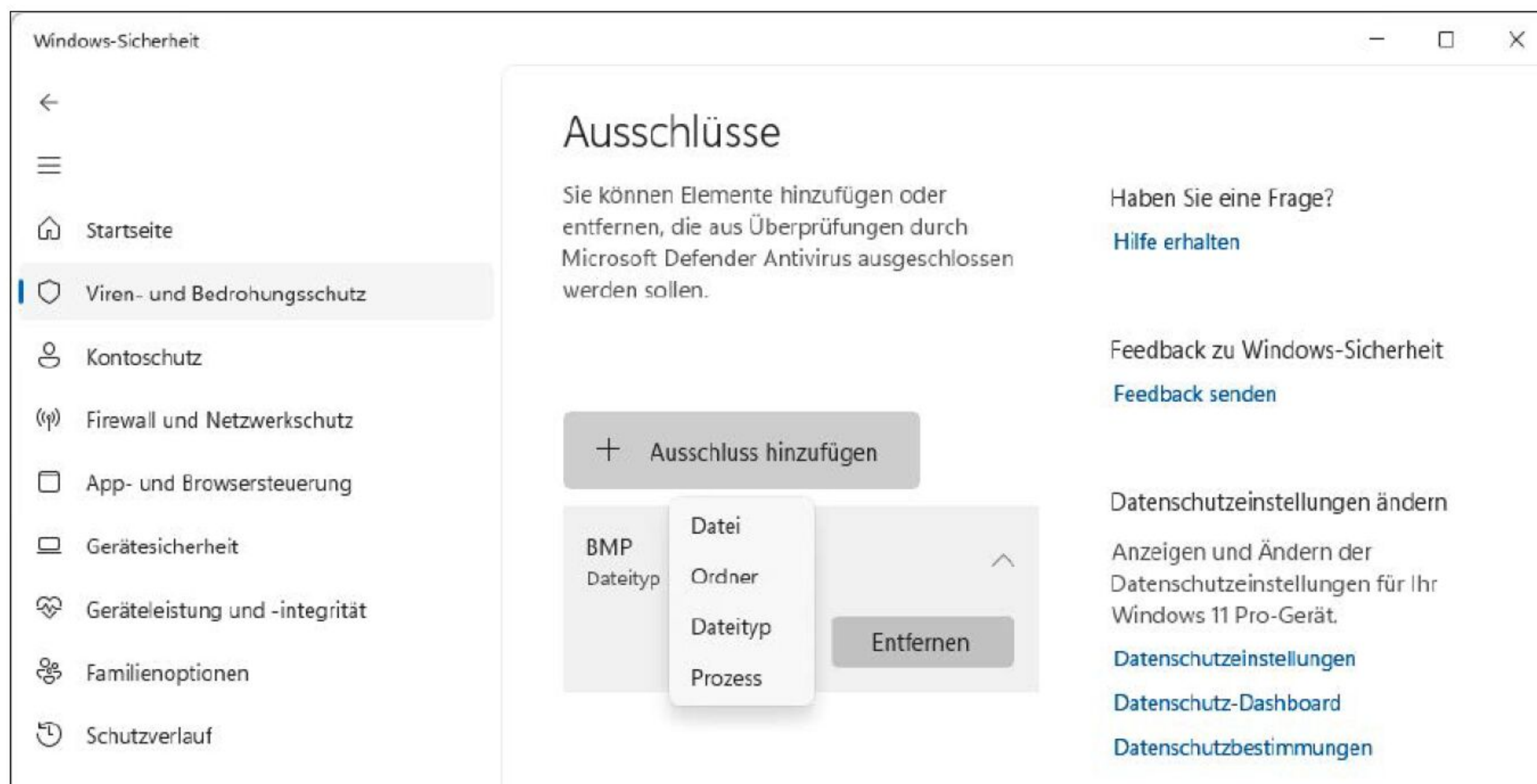
empfiehlt sich ein mehrstufiges Vorgehen. **Zweck des Tools prüfen:** In einem ersten Schritt sollten Sie überlegen, was Sie da heruntergeladen haben. Handelt es sich um eines der bereits erwähnten Tools zum Ermitteln

von Lizenzcodes oder Passwörtern, so können Sie von einem Fehlalarm ausgehen. **Auf Reputation prüfen:** Überprüfen Sie jedoch zusätzlich, von wo Sie die Software bezogen haben, und machen Sie sich Ge-

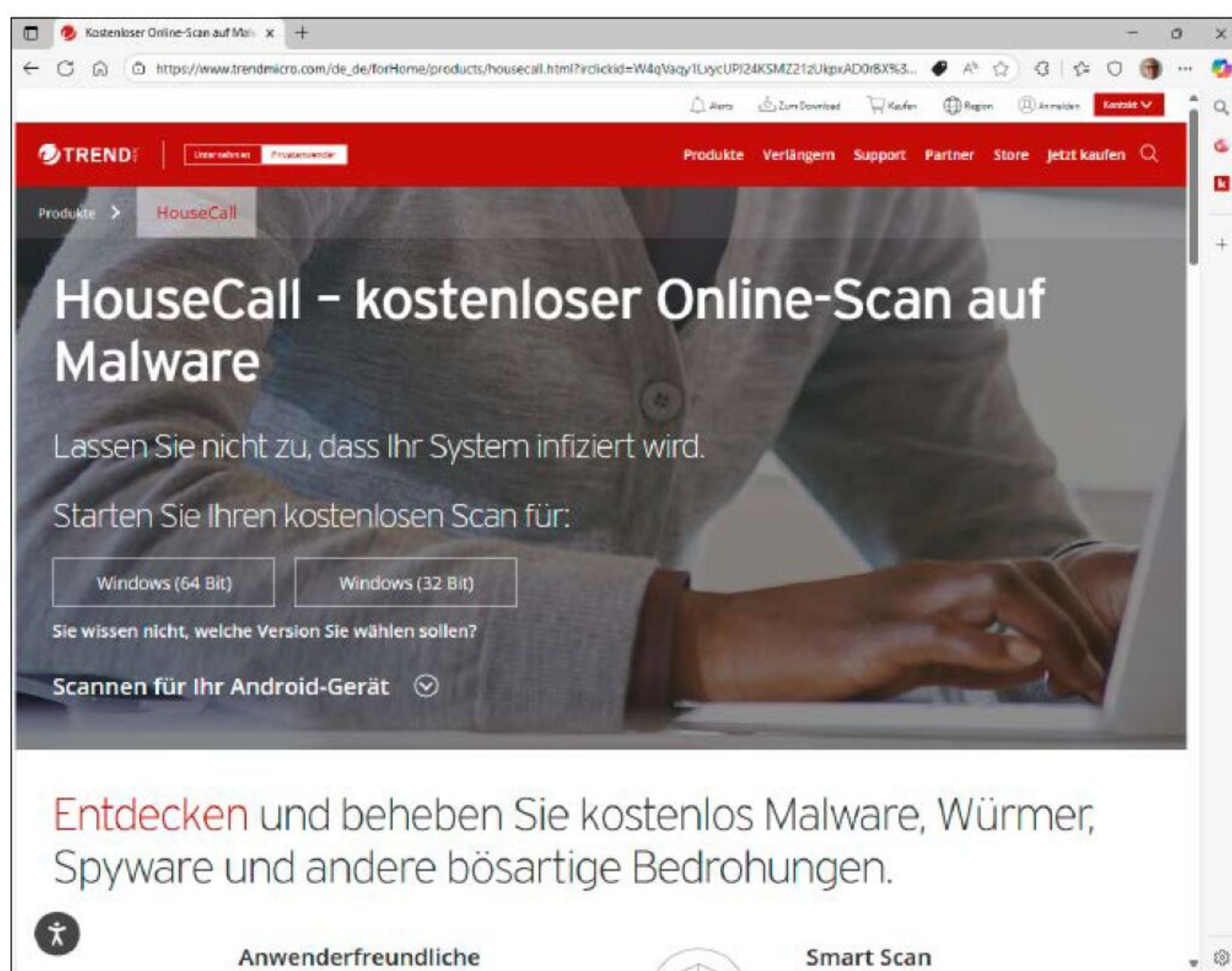
IM ÜBERBLICK: SCHUTZTOOLS

Name	Beschreibung	Auf	Internet	Sprache	Preis
Avast Free Antivirus	Antivirenprogramm	Heft-DVD	www.pcwelt.de/1135344	Deutsch	Kostenlos
AVG Antivirus Free Edition	Antivirenprogramm	Heft-DVD	www.pcwelt.de/1134904	Deutsch	Kostenlos
Avira Antivir Rescue System	Rettungs-DVD oder -Stick	Heft-DVD	https://tinyurl.com/mts4b8a2	Deutsch	Kostenlos
Kaspersky Rescue Disk *	Rettungs-DVD oder -Stick	Heft-DVD	https://tinyurl.com/bdjkm22f	Deutsch	Kostenlos
Norton Antivirus	Antivirenprogramm	-	https://de.norton.com	Deutsch	35 Euro pro Jahr
Produkey	Auslesen von Produktschlüsseln	Heft-DVD	https://tinyurl.com/2s4zf2hr	Englisch	Kostenlos
Sandboxie	Sandbox anlegen	Heft-DVD	www.pcwelt.de/1142998	Deutsch	Kostenlos
Sardu	Bootstick anlegen	Heft-DVD	www.sarducd.it	Deutsch	Kostenlos

* Das BSI (Bundesamt für Sicherheit in der Informationstechnik) empfiehlt, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen.



Wie bei anderen Antivirentools auch, können Sie beim Defender einzelne Dateien oder Ordner von der Überprüfung durch den Scanner ausnehmen, wenn Sie sicher sind, dass dort alle Dateien harmlos sind.



Mit dem Onlinescanner von Trend Micro untersuchen Sie Ihren Computer auf vorhandene Schadsoftware. Eine Installation ist dabei nicht erforderlich.

hängen zu bleiben droht, wenn man nicht schnell aktiv wird und ein Servicetool installiert. Dabei handelt es sich aber um einen Virus. Wenn das Antivirenprogramm jetzt einen Schädling meldet, ist die Wahrscheinlichkeit hoch, dass es sich tatsächlich um einen handelt. Typisch für Social Engineering sind die Techniken Druck, Dringlichkeit, Notlagen und Hilfesuche.

Auf Trickbetrug achten: Im Internet gilt generell: Wenn etwas zu gut ist, um wahr zu sein, dann ist es das in der Regel auch nicht. Das können etwa sehr günstige Kaufangebote sein. Tritt in einem solchen Zusammenhang eine Virenmeldung auf, dann ist sie wahrscheinlich berechtigt.

Was tun bei einem Fehlalarm?

Wenn Ihre Antivirensoftware ein heruntergeladenes Programm zur Malware erklärt, Sie aber sicher sind, dass es keine ist, können Sie die Downloaddatei oder auch die Adresse der Quelle im Internet als Ausnahme definieren. Eine entsprechende Funktion bietet jedes Schutzprogramm an.

Alternative Virens Scanner nutzen

Hat Ihr Antivirenprogramm eine Schadsoftware gemeldet, und Sie sind sich nicht sicher, ob es sich tatsächlich um einen Schädling oder um einen Fehlalarm handelt, können Sie in einem weiteren Schritt eine zweite Meinung von einem anderen Antivirentool einholen. Es ist nicht erforderlich, dass Sie dazu Ihre vorhandene Software deinstallieren und dann ein Konkurrenzprodukt herunterladen und einrichten. Schneller und einfacher ist die Überprüfung der verdächtigen Datei mit einem Onlinescanner.

Einige Antivirenhersteller bieten Onlinescanner als kostenlosen Service auf ihrer Website an. Dort gibt es einen Bereich, über den Sie verdächtige Dateien zu den Herstellerservern hochladen und überprüfen lassen können. Entsprechende Angebote gibt es von Eset (<https://tinyurl.com/2adr2dpf>), F-Secure (<https://tinyurl.com/3272vbav>) und Trend Micro (<https://tinyurl.com/yzch9fjk>).

Oder Sie gehen gleich zu Virustotal (www.virustotal.com), dem Onlinescanner von Google. Er legt die verdächtige Datei mehreren Dutzend Antivirenprogrammen verschiedener Hersteller vor und zeigt deren Untersuchungsergebnisse an. Obwohl es in der Vergangenheit vereinzelt Fälle gab, in

danken über deren Reputation. Dazu müssen Sie sich die Datei ansehen, die den Alarm hervorgerufen hat, und ihre Herkunft klären. Arbeiten Sie mit dem Microsoft **Defender** als Virenschutz, so finden Sie das File und seinen Ursprung in den „Einstellungen“ unter „Datenschutz und Sicherheit → Windows-Sicherheit → Viren- und Bedrohungsschutz → Schutzverlauf“. Dort sind alle vom Defender gefundenen Schadprogramme aufgelistet. Klicken Sie auf einen der Einträge, um den Dateinamen und die Herkunft zu erfahren. Ähnliche Verzeichnisse gibt es auch in jedem anderen Antivirenprogramm.

Wichtig ist, von wo Sie die Datei bekommen haben und ob diese Downloaddatei eine gute oder eher schlechte Reputation besitzt. Der Downloadbereich von www.pcwelt.de beispielsweise hat eine sehr gute Reputation. Stammt die Datei von dort, handelt es

sich mit hoher Wahrscheinlichkeit nicht um einen Schädling und damit um einen Fehlalarm. Eine schlechte Reputation haben dagegen Sites, die geknackte Programme und Spiele oder Tools zum Hacken von Lizenzabfragen et cetera anbieten. Hacker benutzen diese Software häufig, um Schadsoftware auf die Computer der Anwender zu übertragen. Auch Websites, die illegal Filme und Videos zum Download bereitstellen, gehören in diese Kategorie.

Auf Zeichen von Social Engineering prüfen: Social Engineering bezeichnet Tricks, die eine Person zu bestimmten Verhaltensweisen veranlassen, die sie ohne diese Tricks nicht zeigen würde. Social Engineering wird regelmäßig beim Phishing von privaten Daten und etwas seltener auch bei der Verbreitung von Malware eingesetzt. So behaupten E-Mails oder SMS beispielsweise, dass eine Bestellung auf dem Postweg

denen auch Virustotal einen Schädling nicht erkannte, ist dies die wohl sicherste Möglichkeit, um einen Fehlalarm auszuschließen. Alternativen zu Virustotal gibt es auch, darunter etwa Metadefender Cloud (<https://metadefender.com>), Hybrid Analysis (<https://hybrid-analysis.com>) und Jotti's Malware Scan (<https://virusscan.jotti.org>).

Offlinescan mit bootfähigen USB-Sticks und DVDs

Wenn Sie häufig an anderen Rechnern sitzen, können Sie auch einen Virens Scanner auf einem bootfähigen USB-Stick oder einer DVD installieren. Auf diese Weise können Sie den jeweiligen PC überprüfen, bevor Sie mit Ihrer Arbeit beginnen.

Es gibt mehrere Möglichkeiten, an einen solchen Stick oder eine DVD zu gelangen. So enthalten einige Antivirenprogramme Assistenten, um direkt aus der Software heraus eine portable Version auf Stick oder DVD anzulegen. Das gilt für die baugleichen Programme von **Avast** und **AVG** sowie für das kostenpflichtige **Norton Anti-virus**. Der Nachteil: Sie müssen zunächst das jeweilige Antivirenprogramm installieren, um die Disk anzulegen.

Andere Hersteller bieten Rescue Disks als fertige Downloads an. Diese Disks basieren in der Regel auf einem Linux-Livesystem, das um einen Virens Scanner ergänzt wurde. Sie sind erhältlich von **Avira** (<https://tinyurl.com/y39354x4>) und **Kaspersky** (<https://tinyurl.com/2bwbuwr4>).

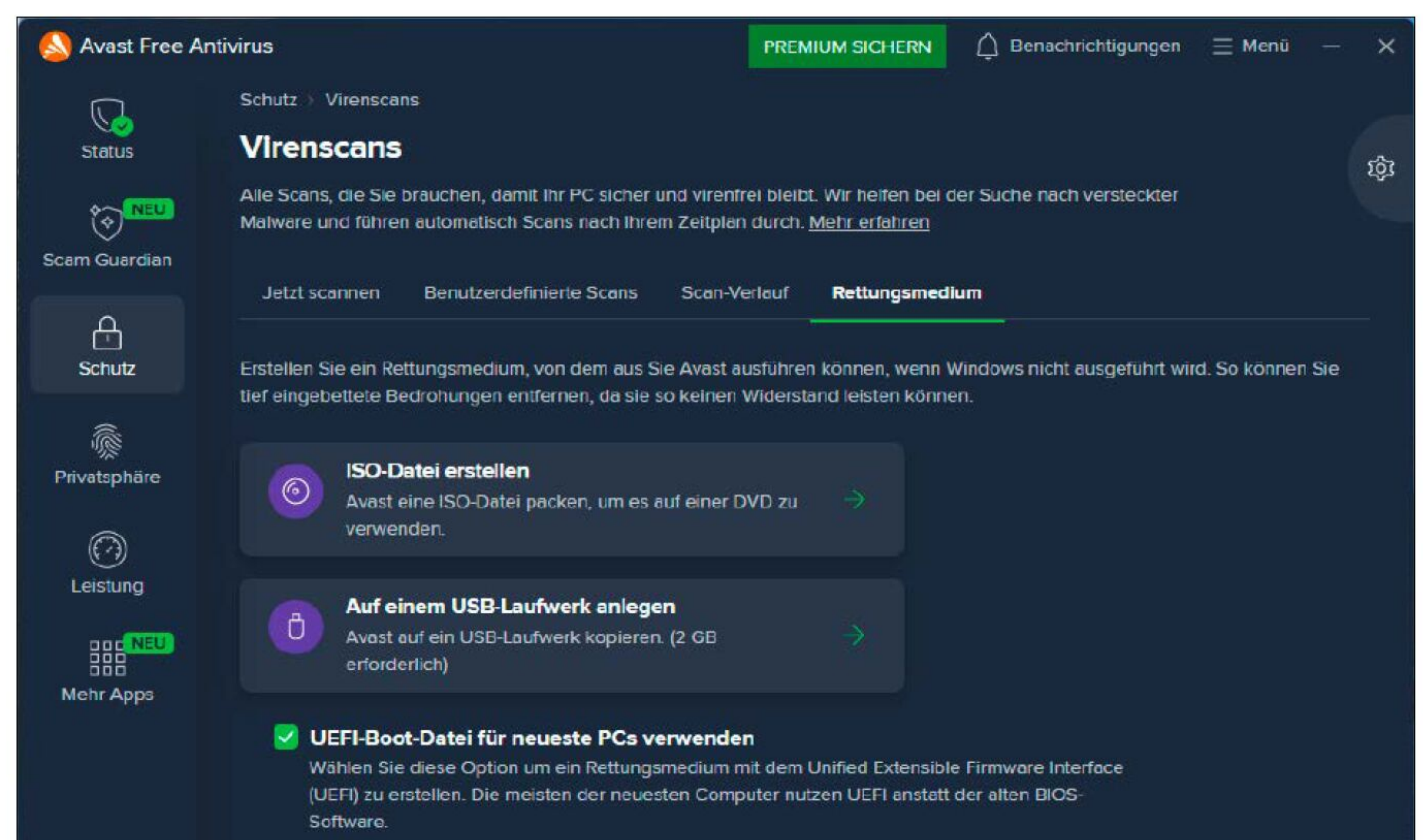
Zum Dritten können Sie aber auch auf **Sardu** zurückgreifen. Mit dieser Freeware legen Sie bootfähige USB-Sticks und DVDs an und bestücken sie mit einem Antivirentool Ihrer Wahl. Sardu stellt zu diesem Zweck Links zu frei verfügbaren Rettungssystemen von Antivirenherstellern zur Verfügung und bietet an, die Programme direkt herunterzuladen und in den Stick oder die DVD zu integrieren.

Verdächtige Programme gefahrlos starten

Eine weitere Methode, um Fehlalarme zu entdecken, ist die Ausführung eines verdächtigen Programms in einer gesicherten Umgebung. Das kann zum einen eine virtuelle Maschine sein, in der Sie Windows installieren und anschließend die zu untersuchende Software starten (www.pcwelt.de/article/1149707). Sollte sie einen Virus mitbringen, bleibt er in der virtuellen Ma-



Jotti's Malware Scan ist eine Alternative zu Virustotal und schickt hochgeladene Dateien an insgesamt dreizehn verschiedene Antivirens Scanner. Pro Datei besteht ein Datenlimit von 250 MB.



Nach der Installation einer zusätzlichen Komponente bietet der Avast-Virens Scanner das Anlegen einer Rettungsdisk auf DVD oder USB-Stick mit integriertem Virens Scanner an.

schine eingesperrt. Ein Überspringen auf Ihr Desktop-Windows ist in der Regel nicht möglich. Sie können daher in aller Ruhe beobachten, ob es sich beispielsweise um eine Ransomware handelt, die nun beginnt, die virtuelle SSD zu verschlüsseln.

Eine Alternative ist die Nutzung einer Sandbox. Auch dabei handelt es sich um eine abgeschirmte Umgebung, die der Schadsoftware keine Möglichkeit bietet, auszu brechen. Einfach zu handhaben sind dabei

Onlinesandboxen wie Any.run (<https://app.any.run>), Sie können aber auch auf lokal installierbare Sandboxsoftware wie **Sandboxie** zurückgreifen.

Achtung: Viele Viren sind so programmiert, dass sie erst nach einer Zeitspanne von mehreren Stunden, Tagen oder sogar Wochen aktiv werden. Wenn also ein Programm in einer Sandbox zunächst keine Auffälligkeiten zeigt, heißt das nicht mit Sicherheit, dass es ungefährlich wäre. ■

VIRENWARNUNGEN ALS LOCKMITTEL



Vor allem in den dunklen Ecken des Internets poppen immer wieder Browserfenster auf, die einen angeblichen Virenfund auf Ihrem PC melden. Um das Problem zu beheben, sollen Sie sofort dem Download eines Antivirenprogramms zustimmen. **Vorsicht:** Bei diesen Meldungen handelt es sich ausnahmslos um Betrug. Die angebotene Software besitzt normalerweise keine Funktion. Sie will Sie jedoch mit regelmäßig eingeblendeten Hinweisen zu einer kostenpflichtigen Lizenzierung überreden. Und schlimmer noch: Häufig enthalten diese Programme selbst einen Virus, der Ihren PC beispielsweise zum Teil eines Botnetzes macht.

Mobil und gut verschlüsselt

Notebooks, mobile Festplatten und USB-Sticks sind durch Datendiebstahl besonders gefährdet. Mit Windows und einigen Tools können Sie sie jedoch per Verschlüsselung sicher schützen.

VON ROLAND FREIST



© Mit Material von adam121 – AdobeStock

Mobilgeräte gehen schon mal verloren. Die Laptoptasche bleibt in Bus oder Bahn auf dem Nebensitz liegen, das Smartphone rutscht aus der Hosentasche, oder der USB-Stick fällt auf dem Parkplatz beim Ziehen des Autoschlüssels unbemerkt zu Boden. Gehen ein Notebook oder Telefon auf diese Weise verloren, bedeutet das zunächst einmal einen herben finanziellen Verlust. In vielen Fällen wiegt jedoch der damit einhergehende Datenverlust noch erheblich schwerer. Auf dem Notebook liegen oft wichtige und vertrauliche Dokumente wie etwa Steuerunterlagen, eventuell sind dort sogar Firmenpapiere abgelegt. Und ein Smartphone speichert neben E-Mails auch Kontaktlisten und Whatsapp-Chats.

Der Zugang zu einem Notebook ist zwar durch ein Passwort geschützt, die Dateien sind jedoch frei zugänglich. Wird das Gerät

über ein Livesystem gebootet, lassen sie sich einfach lesen und kopieren. USB-Sticks müssen in der Regel lediglich an einen Computer angeschlossen werden, und schon geben sie ihre Inhalte preis. Bei Smartphones hingegen ist das Dateisystem zwar grundsätzlich sicher verschlüsselt. Wurde das Gerät jedoch gerade benutzt, ist eventuell die Displaysperre noch nicht wieder aktiv, und der Finder kann die gespeicherten Daten lesen und per E-Mail oder Chatprogramm verschicken.

Besonders heikel ist der Verlust eines Geräts, wenn es nicht verloren, sondern gezielt gestohlen wurde, etwa weil der Dieb auf vertrauliche Firmenunterlagen oder Kreditkartendaten aus war. Wichtige Unterlagen auf Mobilgeräten sollten daher grundsätzlich verschlüsselt werden. In der Folge stellen wir Ihnen eine Reihe von sicheren Verschlüsselungstools vor.

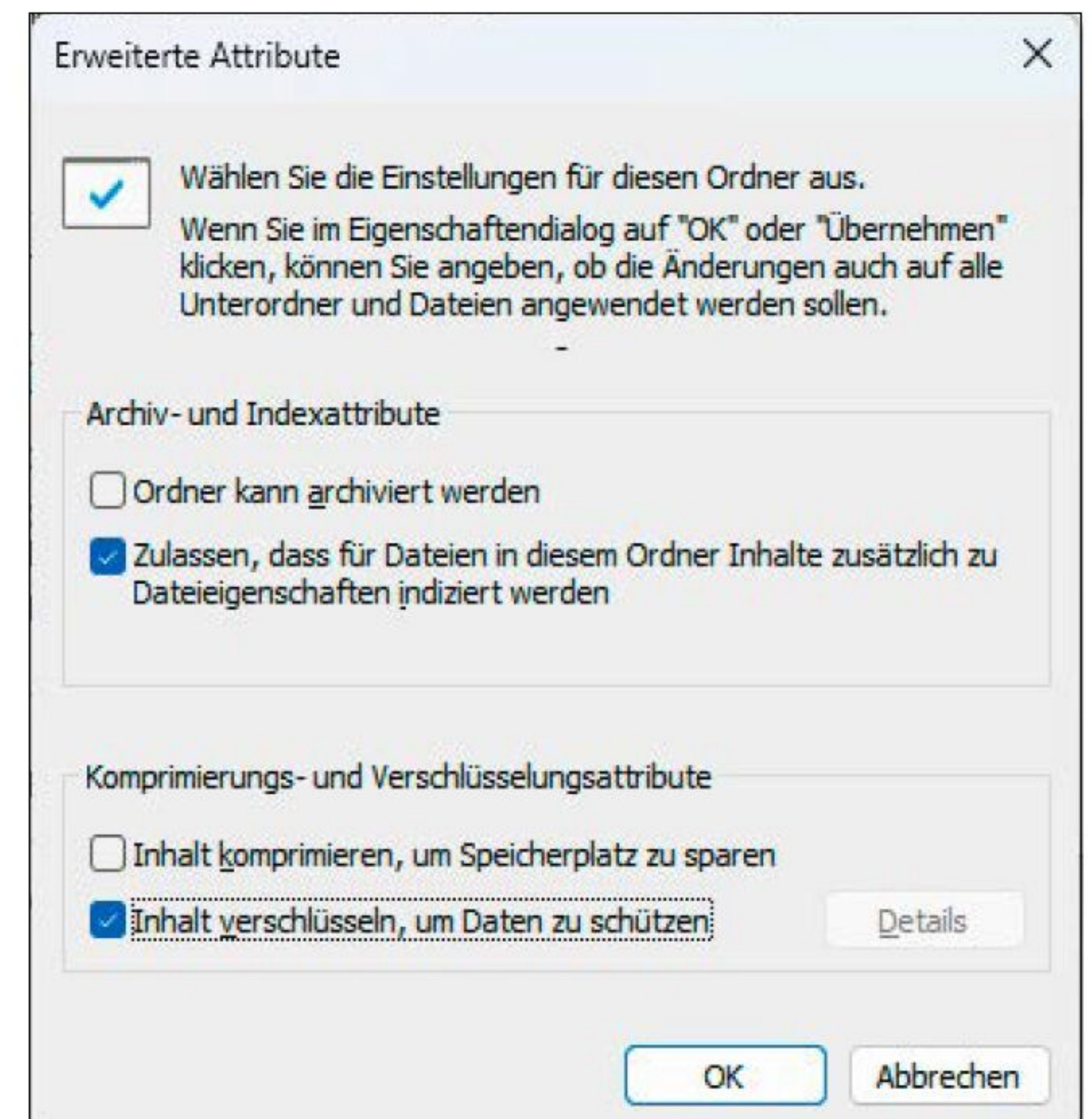
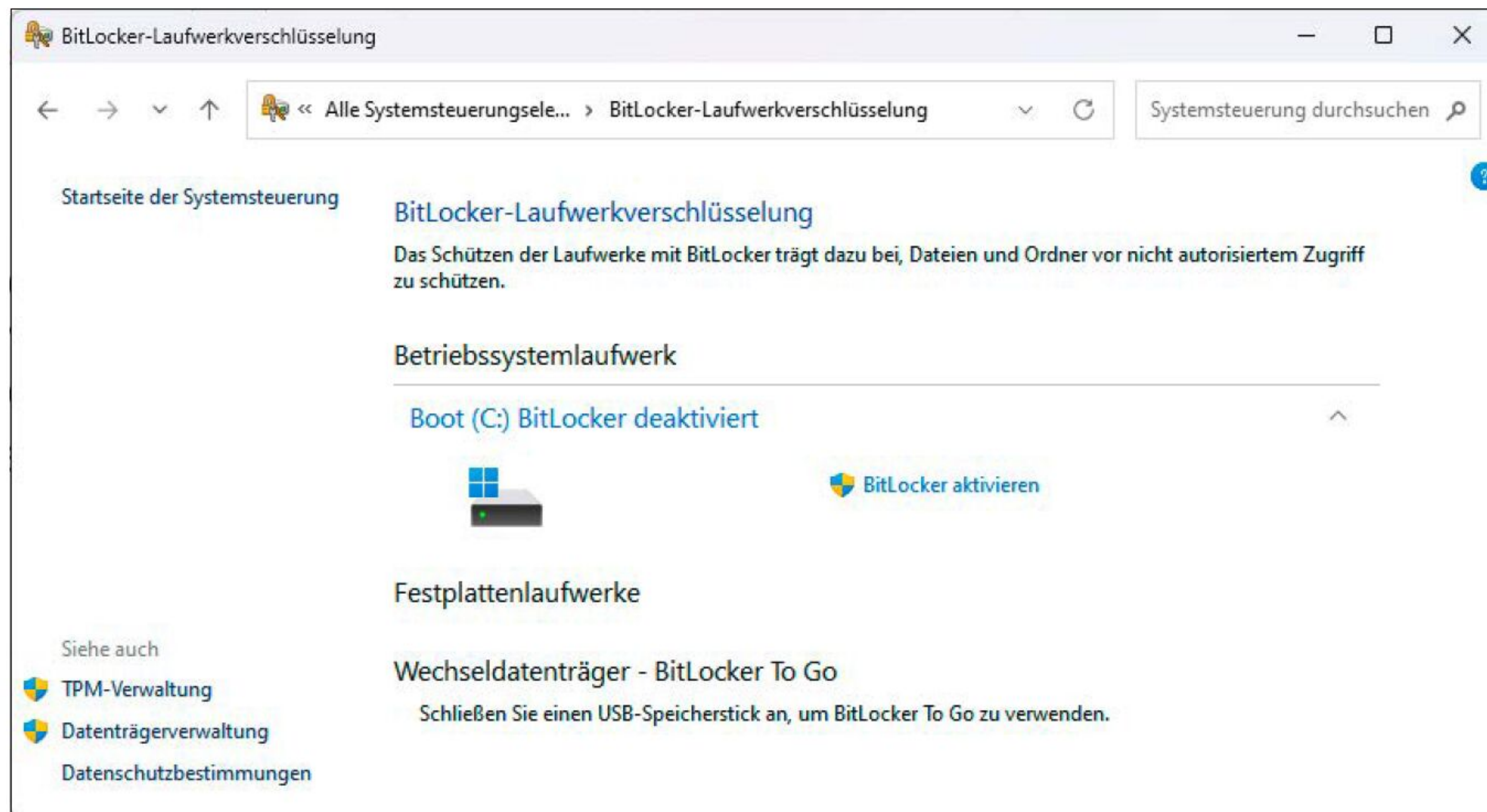
Systemlaufwerk und externe Festplatte verschlüsseln

Bei der Verschlüsselung der SSD eines Notebooks oder einer externen Festplatte haben Sie die Wahl zwischen zwei Verfahren: Full Disk Encryption (FDE) und File Level Encryption (FLE). Bei der Full Disk En-

ryption verschlüsselt eine Software den kompletten Datenträger, und zwar inklusive des Betriebssystems. Zum Lieferumfang von Windows Pro und Education gehört mit Bitlocker auch eine FDE-Verschlüsselung. Sie finden die Funktion in der Kategorieansicht der Systemsteuerung unter „System und Sicherheit → Bitlocker-Laufwerkverschlüsselung“. Nachdem Sie sie aktiviert haben, muss jeder Benutzer beim Hochfahren des Computers das definierte Bitlocker-Passwort eingeben. Im Unterschied zum Zustand vor der Verschlüsselung ist es jetzt nicht mehr möglich, ohne dieses Passwort auf die Dateien auf der SSD zuzugreifen. Die Bitlocker-Verschlüsselung nutzt die Funktionen des TPM-Chips des Computers und gilt als sehr sicher.

Eine Full Disk Encryption hat allerdings den Nachteil, dass die Daten auf der SSD nur dann geschützt sind, wenn das Notebook nicht benutzt wird und Sie sich nicht bei Windows angemeldet haben. Sobald Sie durch die Eingabe des Passworts die SSD entsperrt haben, können Hacker über ein Netzwerk oder das Internet auf die gespeicherten Dateien zugreifen. Das Gleiche gilt, wenn einem Kriminellen ein eingeschaltetes Gerät in die Hände fällt.

„Vertrauliche Daten sollten dringend verschlüsselt werden. Mit den richtigen Tools ist das ganz einfach.“



Die BitLocker-Laufwerkverschlüsselung wird in der Systemsteuerung von Windows aktiviert. Anschließend müssen Sie bei jedem Start des Rechners ein Passwort eingeben, um das Systemlaufwerk zu entschlüsseln.

Zum Verschlüsseln einer Datei oder eines Ordners aktivieren Sie im Windows-Explorer in den Eigenschaften einfach ein zusätzliches Attribut.

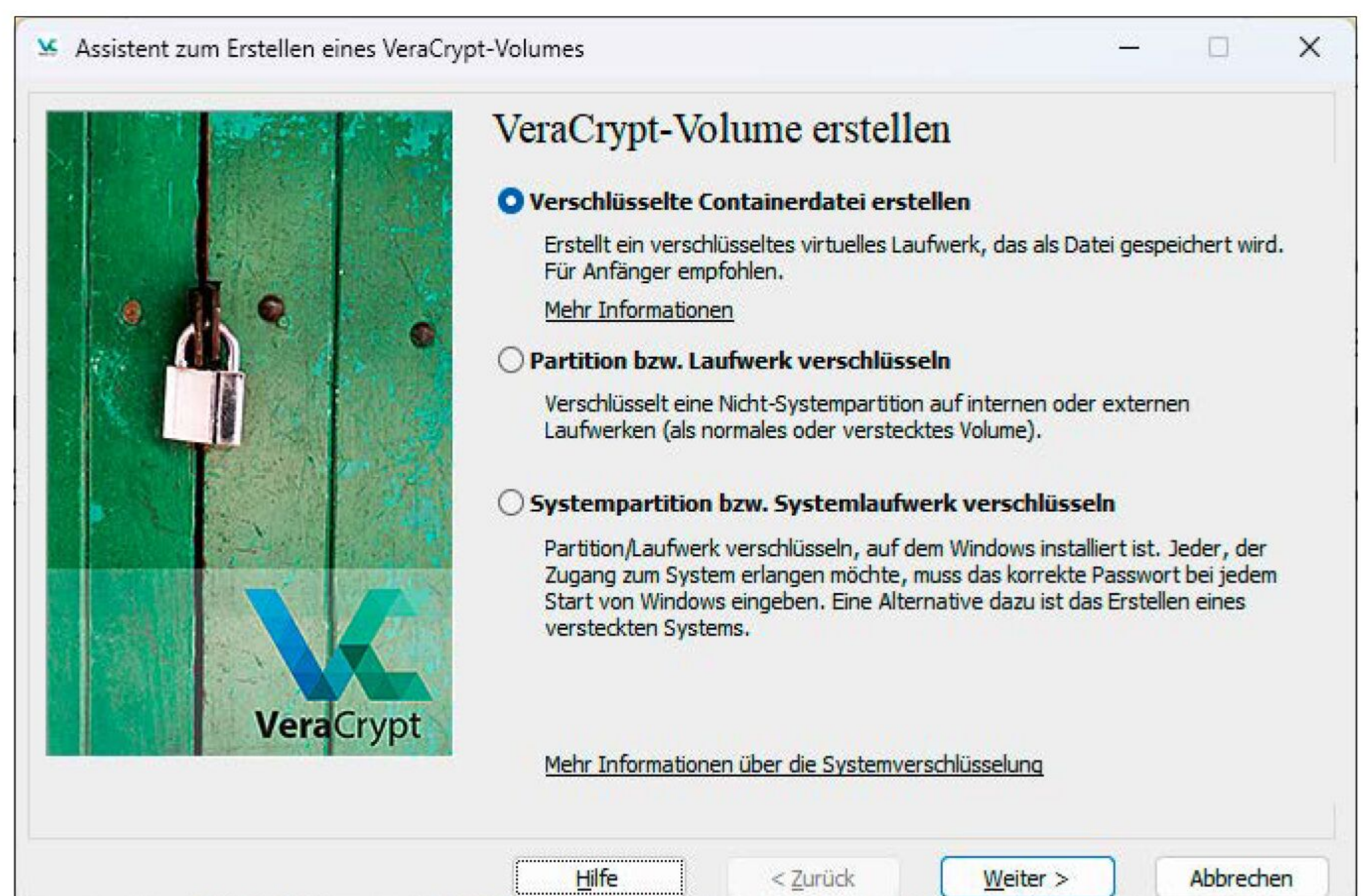
Notebookdaten mit Encrypting File System (EFS) verschlüsseln

Die Alternative zur FDE ist die File Level Encryption (FLE). Sie verschlüsselt lediglich ausgewählte Dateien und Ordner. Die FLE hat den Vorteil, dass sie kontinuierlich aktiv ist. Um auf die Daten zugreifen zu können, ist in der Regel die Eingabe eines Kennworts erforderlich.

Eine Ausnahme von dieser Regel ist die FLE von Windows. Microsoft nennt seine Dateiverschlüsselung EFS, Encrypting File System, und hat sie direkt ins Dateisystem NTFS integriert. Sie finden die Funktion im Kontextmenü des Explorers: Klicken Sie eine Datei oder einen Ordner mit der rechten Maustaste an, gehen Sie auf „Eigenschaften“, klicken Sie im Bereich „Attribute“ auf den Button „Erweitert“, setzen Sie ein Häkchen vor „Inhalt verschlüsseln, um Daten zu schützen“ und bestätigen Sie mit „OK“. Allerdings entschlüsselt Microsoft diese Daten, sobald Sie sich mit Ihrem Benutzerkonto anmelden. Es liegen hier also dieselben Probleme vor wie bei der Full Disk Encryption. Zudem ist die Entschlüsselung an das Passwort Ihres Benutzerkontos gebunden; haben Sie dieses vergessen oder wird das Benutzerkonto gelöscht, geht der Zugriff auf die Daten verloren.

Verschlüsseltes Laufwerk anlegen mit Veracrypt

Die Verschlüsselung mit dem EFS ist einfach und effektiv, hat jedoch auch den Nachteil, dass die Namen der enthaltenen Dateien sichtbar sind und andere Personen daraus auf den Inhalt schließen können. Um das



Veracrypt kann komplette Laufwerke verschlüsseln, aber auch einen verschlüsselten Container in Form eines virtuellen Laufwerks anlegen. Darin lassen sich Dateien und Ordner sicher speichern.

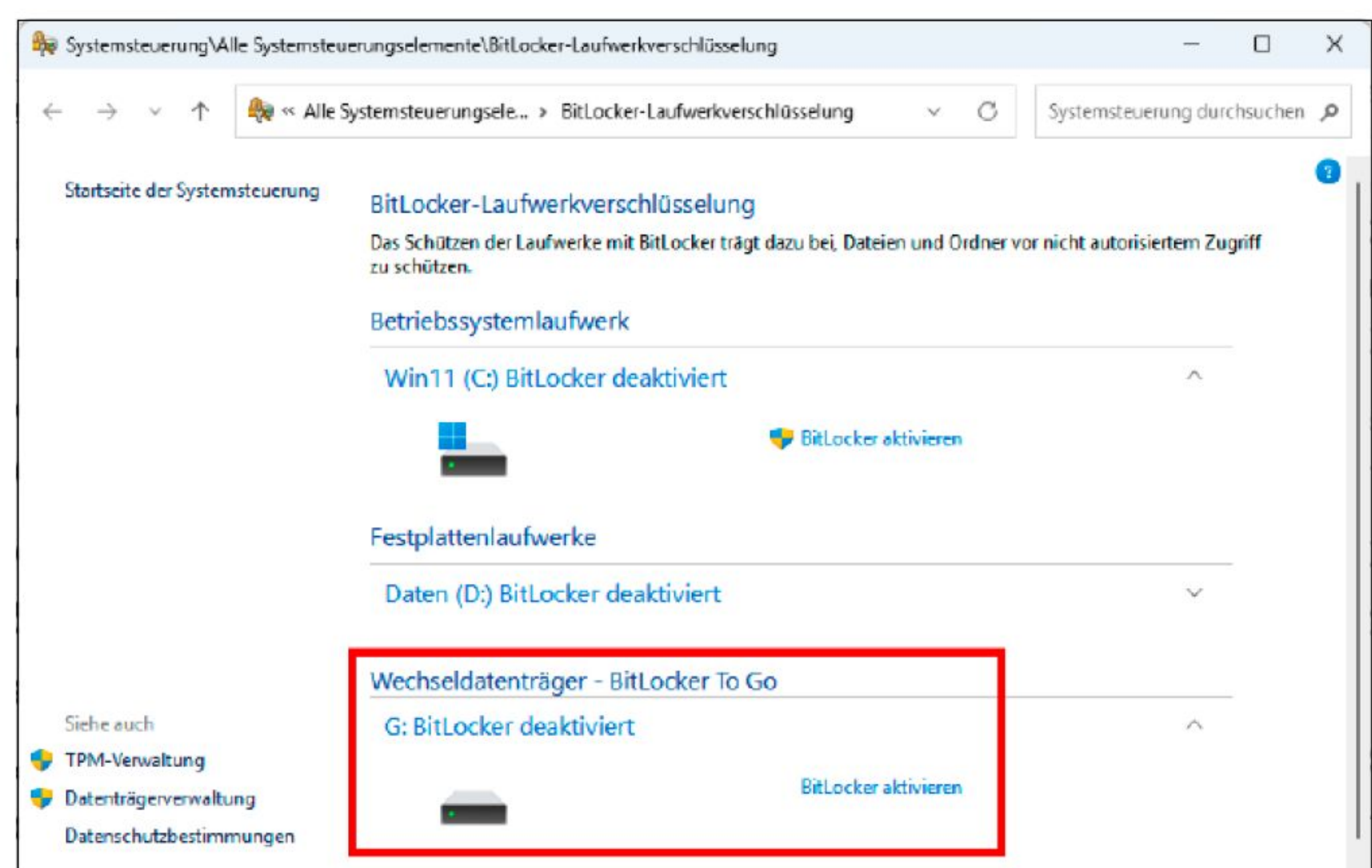
zu vermeiden, können Sie auf die Open-Source-Software **Veracrypt** (kostenlos, auf der Heft-DVD sowie unter www.pcwelt.de/1152564) zurückgreifen. Das Programm arbeitet etwas anders als die bisher vorgestellten Funktionen. Es kann einerseits ganze Laufwerke verschlüsseln, bietet aber auch an, einen verschlüsselten Container in Form eines gemounteten Laufwerks zu erzeugen, in das Sie die zu verschlüsselnden Dateien und Ordner einfach hineinkopieren oder -verschieben. Andere Benutzer sehen dann nur den Namen des Containers, nicht aber dessen Inhalt. Die Container-Verschlüsselung von Veracrypt eignet sich in erster Linie für die SSDs von Notebooks.

Öffnen Sie Veracrypt und klicken Sie auf „Volume erstellen“. Damit starten Sie einen Assistenten, in dessen erstem Fenster Sie „Verschlüsselte Containerdatei erstellen“ markieren. Klicken Sie auf „Weiter“ und wählen Sie „Standard-VeraCrypt-Volume“. Klicken Sie auf „Weiter → Datei“ und geben Sie den Pfad und den Dateinamen für den Container an. Bestätigen Sie dann mit „Speichern“.

Das nächste „Weiter“ bringt Sie zu den Verschlüsselungseinstellungen, die Sie einfach übernehmen können. Klicken Sie „Weiter“ und geben Sie die Größe des Containers an, den Veracrypt erzeugen soll. Das Programm zeigt an dieser Stelle an, wie viel Platz auf



Durch Mausbewegungen erzeugen Sie einen Zufallswert für die Verschlüsselung. Je länger Sie die Maus hin- und herbewegen, desto besser.



Sobald Sie einen USB-Stick an Ihren Windows-Rechner anschließen, haben Sie in der Systemsteuerung Zugriff auf die mobile Verschlüsselung Bitlocker To Go.

dem gewählten Laufwerk noch frei ist. Entscheiden Sie sich für einen passenden Umfang und klicken Sie auf „Weiter“. Nun will Veracrypt ein Passwort von Ihnen haben.

Tippen Sie eine lange und komplexe Buchstaben-Zahlen-Zeichen-Kombination ein und gehen Sie auf „Weiter“. Das Fenster „Große Dateien“ können Sie mit „Weiter“

überspringen. Im Fenster „Volume-Format“ wählen Sie als Dateisystem am besten „NTFS“ aus. Bewegen Sie den Mauszeiger mindestens 30 Sekunden lang hin und her, bis sich die Farbe des Fortschrittsbalkens von rot über gelb nach grün geändert hat. Klicken Sie auf „Formatieren“, um die Containerdatei zu erzeugen. Sobald der Vorgang beendet ist, wird das Assistentenfenster geschlossen.

Nun öffnet sich neben dem Assistenten auch wieder das Startfenster von Veracrypt. Markieren Sie einen Laufwerksbuchstaben, unter dem die Containerdatei erreichbar sein soll. Klicken Sie dann auf „Datei“ und steuern Sie das File an. Klicken Sie auf „Einhängen“, geben Sie das Passwort für den Container an, und bestätigen Sie mit „OK“. Der Container taucht nun unter dem gewählten Laufwerksbuchstaben im Explorer auf. Alles, was Sie hier hineinkopieren, wird automatisch verschlüsselt.

Externe SSDs mit Bitlocker To Go verschlüsseln

Veracrypt bietet sich vor allem für die dauerhafte Installation auf der SSD eines Notebooks an. Für externe Disks benutzen Sie am besten das mit Windows ausgelieferte **Bitlocker To Go**, das auch in der Home-Version enthalten ist.

Tippen Sie *Bitlocker* ins Suchfeld der Taskleiste und klicken Sie auf den Treffer „Bitlocker verwalten“. Damit öffnen Sie ein Fenster der Systemsteuerung, in dem unter „Wechseldatenträger – Bitlocker To Go“ bereits der Laufwerksbuchstabe des Sticks mit der Beschreibung „Bitlocker deaktiviert“ erscheint. Nach einem Klick auf den Link gehen Sie auf „Bitlocker aktivieren“ und set-

SICHERER ORDNER FÜRS SMARTPHONE

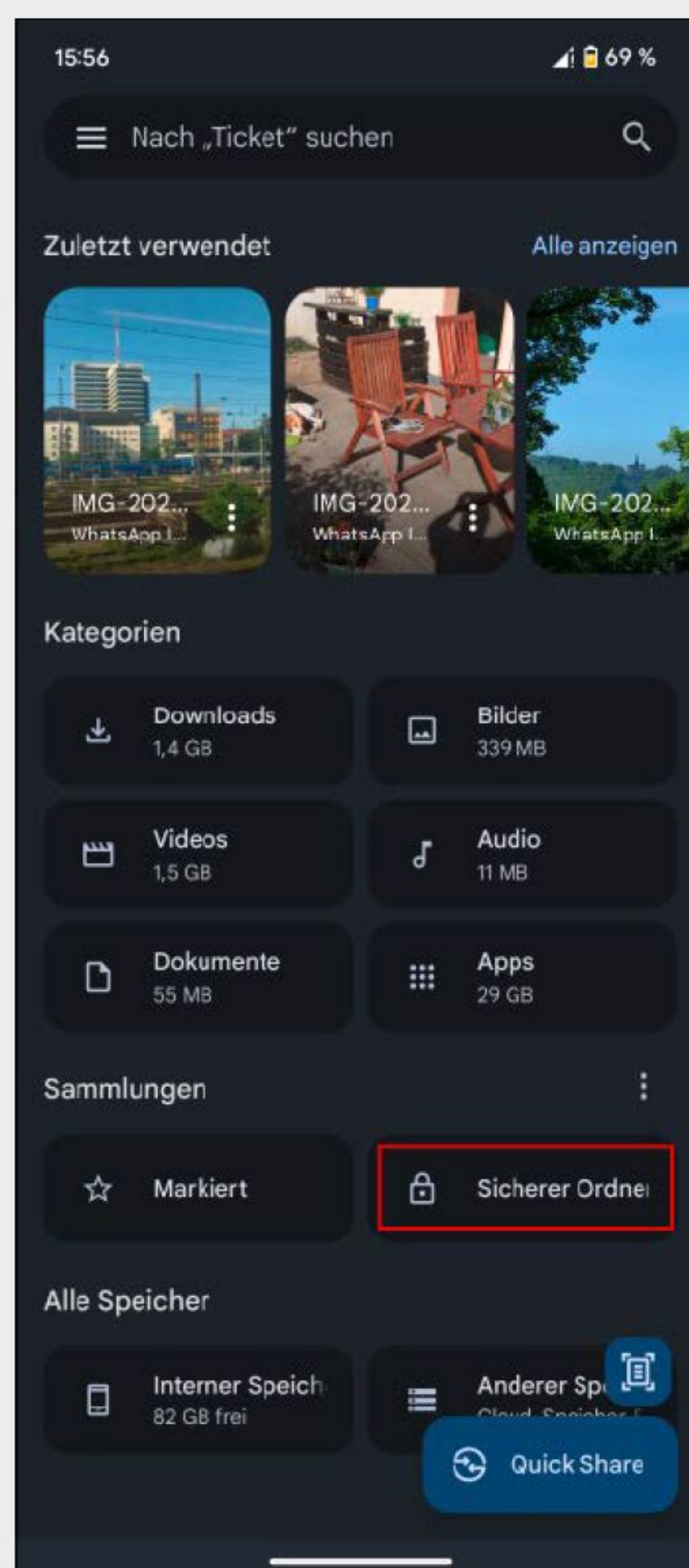
Die Datenspeicher von Smartphones und Tablets sind bereits bei Auslieferung mit einer Funktion des Betriebssystems sicher verschlüsselt. Das hilft Ihnen jedoch wenig,

wenn Sie das Gerät verlieren oder wenn es Ihnen gestohlen wird und die Displaysperre noch nicht wieder aktiv ist. Android bringt jedoch seit Version 8 einen Tresor mit, in dem Sie vertrauliche Daten sicher verstauen können. Der Tresor heißt in Android „Sicherer Ordner“ und ist Bestandteil des Dateimanagers Google Files, der auf vielen Smartphones und Tablets installiert ist. Falls Sie diese App auf Ihrem Gerät nicht finden, können Sie sie über den Play Store nachinstallieren.

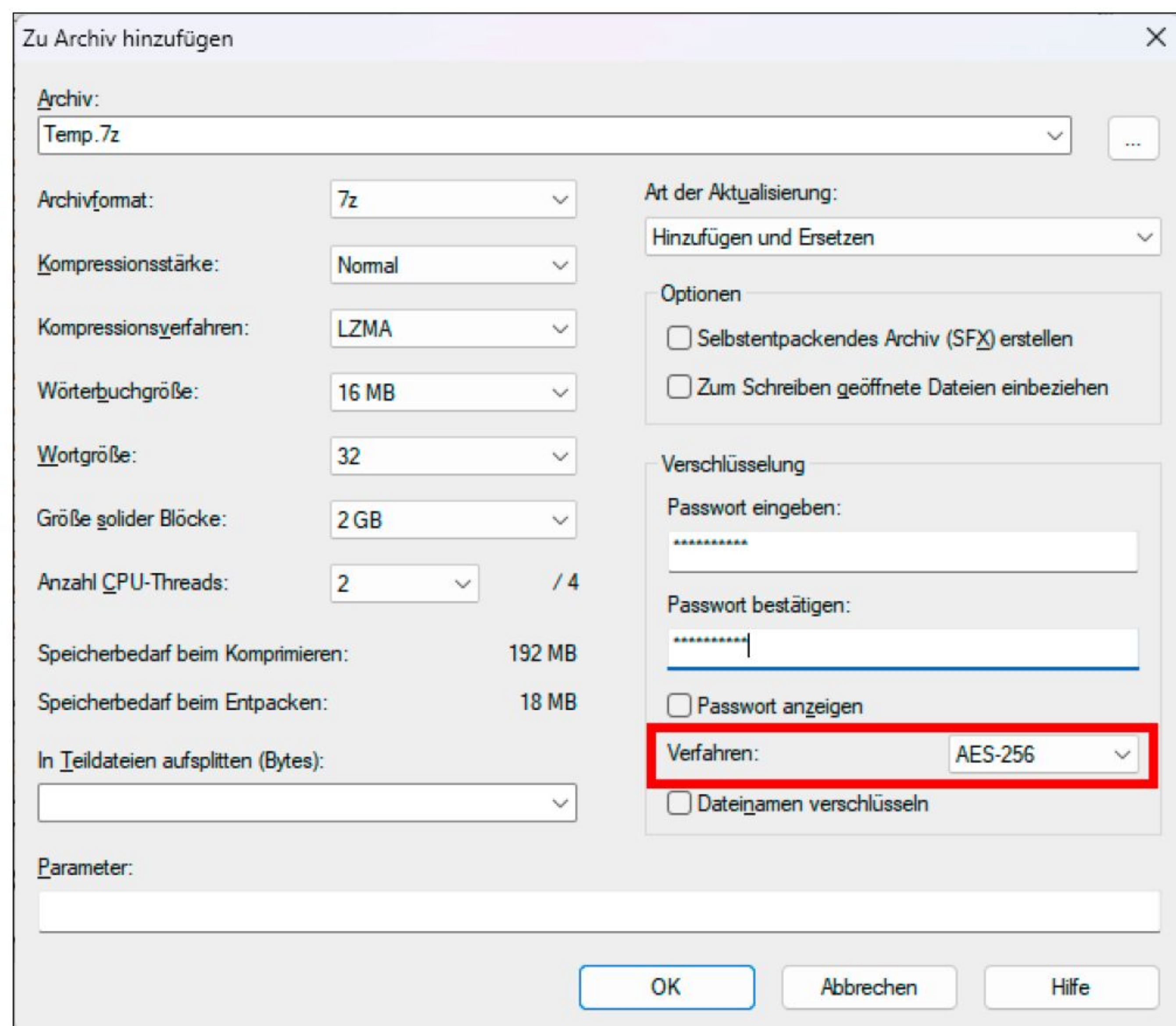
In Google Files rufen Sie dann „Sammlungen → Sicherer Ordner“ auf. Definieren Sie eine PIN oder ein Muster für den Zugriff, beide sollten sich von der PIN beziehungsweise dem Muster unterscheiden, die/das Sie für die Anmeldung an Ihrem Gerät benutzen.

Um Dateien in den Ordner zu verlagern, halten Sie den Finger auf dem File gedrückt, tippen danach auf die drei Punkte und gehen auf „In sicheren Ordner verschieben“. Um eine Datei wieder zurückzuholen, öffnen Sie in Google Files „Sammlungen → Sicherer Ordner“, geben die PIN oder das Muster ein, tippen eine Datei an und wählen „Mehr → Aus sicherem Ordner entfernen“.

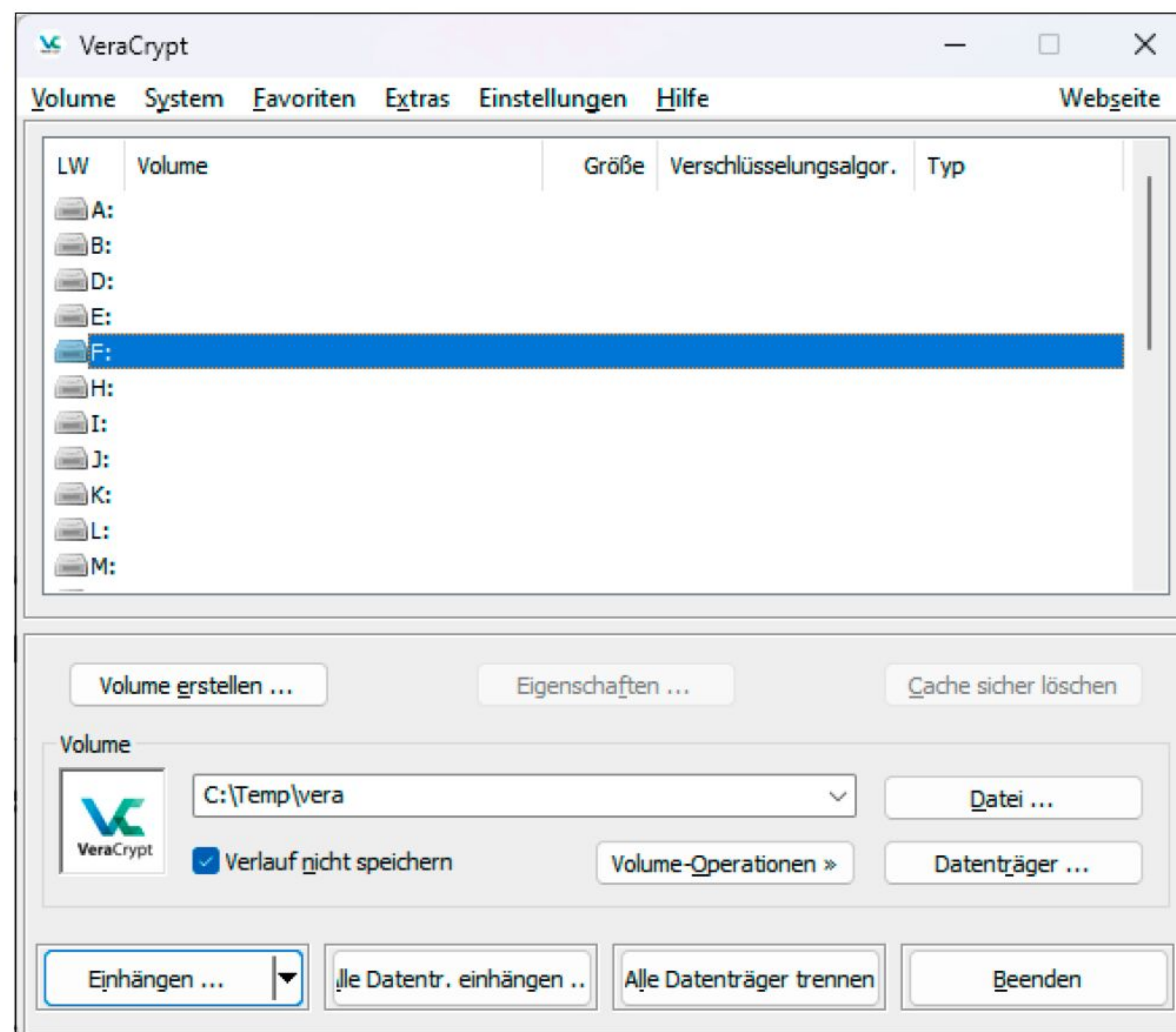
Achtung: Wenn Sie die PIN oder das Muster vergessen, gibt es keine Möglichkeit mehr, den Tresor zu öffnen.



Die Dateimanager-App Google Files bringt eine Funktion zum Anlegen eines sicheren, verschlüsselten Ordners für vertrauliche Daten mit.



Mit dem Packprogramm 7-Zip können Sie ZIP-Dateien auch sicher verschlüsseln. Achten Sie darauf, dass als Verschlüsselungsverfahren AES-256 eingestellt ist.



Sobald der Container erzeugt ist, binden Sie ihn über das Startfenster von VeraCrypt als eigenes Laufwerk ins Dateisystem ein.

zen ein Häkchen vor „Kennwort zum Entsperren des Laufwerks verwenden“. Geben Sie ein Kennwort ein und klicken Sie auf „In Datei speichern“, um den Wiederherstellungsschlüssel in einer TXT-Datei auf der SSD Ihres Desktop-PCs abzulegen. Abhängig davon, ob der Stick bereits Daten enthält oder nicht, wählen Sie „Nur verwendeten Speicherplatz verschlüsseln“ oder „Gesamtes Laufwerk verschlüsseln“. Um den Stick auch an anderen Windows-Rechnern verwenden zu können, markieren Sie im folgenden Fenster „Kompatibler Modus“ und klicken im letzten Fenster auf „Verschlüsselung starten“. Wenn Sie den Stick danach an einen Rechner anschließen, fordert Windows Sie jedes Mal zur Eingabe des Passworts auf.

Daten auf USB-Sticks mit 7-Zip verschlüsseln

Für die schnelle Verschlüsselung von Dateien und Ordnern auf einem USB-Stick schließlich ist das Freeware-Packprogramm **7-Zip** (kostenlos, auf DVD und unter www.pcwelt.de/1142558) gut geeignet. Sie können mit dem Tool ZIP-Dateien sicher mit dem Algorithmus AES-256 verschlüsseln und mit einem Passwort schützen. Zum Öffnen und Entpacken ist dann lediglich die Eingabe dieses Passworts notwendig. So gehen Sie vor: Markieren Sie die Dateien im Windows-Explorer, klicken Sie sie mit der rechten Maustaste an und gehen Sie auf „Weitere Optionen anzeigen → 7-Zip →

Zu einem Archiv hinzufügen“. Geben Sie der Archivdatei einen beliebigen Namen, die Endung sollte allerdings „zip“ heißen. Wählen Sie rechts unten im Abschnitt „Verschlüsselung“ ein sicheres und komplexes Passwort, wiederholen Sie es eine Zeile tiefer und stellen Sie – das ist wichtig – bei „Verfahren“ die Option „AES-256“ ein. Be-

stätigen Sie die Verschlüsselung zum Schluss mit „OK“. Nach einem Doppelklick auf die ZIP-Datei zeigt der Explorer nun zwar den Inhalt an; der Versuch, die Files zu extrahieren, führt jedoch zu einer Fehlermeldung. Nur wenn Sie das ZIP-File mit 7-Zip öffnen und das Passwort eingeben, lassen sich die Inhalte lesen. ■

HARDWAREBASIERTE VERSCHLÜSSELUNG

Bei allen im Artikel beschriebenen Verfahren handelt es sich um softwarebasierte Verschlüsselungen. Bei ihnen erfolgt die Ver- und Entschlüsselung während der Schreib- und Lesevorgänge durch die CPU. Daneben existiert eine hardwarebasierte Verschlüsselung, die heute vor allem bei externen USB-Festplatten zum Einsatz kommt.

Diese Geräte besitzen einen eigenen AES-Verschlüsselungschip, der zwischen das System-Bios und das Betriebssystem geschaltet wird. Dieser Chip führt beim Schreiben und Lesen der Daten sämtliche Ver- und Entschlüsselungsvorgänge auf der Disk aus, der gesamte Datenträger ist damit kontinuierlich verschlüsselt. Der Zugriff ist erst nach Eingabe eines Passworts möglich, das auf der externen Festplatte gespeichert ist.



Festplatten mit integrierter Hardwareverschlüsselung sind vor allem in Form von externen USB-Disks mit AES-Chip verfügbar.





© Mit Material von phj.domingos, kras99 – AdobeStock

10 Sicherheitsfragen

Neue Angriffe, neue Sicherheitstechniken, neue Fragen: Mit diesem Beitrag liefern wir die Antworten auf aktuelle Probleme der Sicherheit am PC und im Internet. Auf Heft-DVD finden Sie dazu ein großes Sicherheitspaket mit unverzichtbaren Schutztools.

VON ARNE ARNOLD

1. Was versteht man unter Suchparameter-Injection?

Angriffe mit Suchparameter-Injection sind eine neue, raffinierte Methode von Kriminellen, um an Ihre Daten zu kommen oder gar Zugriff auf Ihren PC zu erhalten. Kriminelle schalten bei Google Werbung, die immer dann angezeigt wird, wenn jemand nach dem Wort Support und nach einer bestimmten Firma sucht, etwa „Support Netflix“. Die angezeigte Werbung erscheint direkt über dem ersten Suchtreffer und ist so gestaltet,

„Passkeys sind nicht so sicher, wie man meint. Trotzdem sollten Sie sie unbedingt nutzen.“

als stamme sie von Netflix selbst. Wer auf diese Anzeige klickt, wird – und das ist das Besondere an dieser Masche – nicht auf eine gefälschte Website geleitet, sondern auf die originale Support-Website von Netflix. In die Suchfunktion der Support-Seite haben die Angreifer aber ihre eigene Telefonnummer eingetragen (siehe Abbildung). Ein Opfer, das bei dieser Nummer anruft, gibt dann dort den Kriminellen seine Daten preis, etwa das Passwort für das Netflix-Log-in. Teilweise werden die Opfer auch dazu überredet, eine scheinbare Support-Software zu installieren. Dabei handelt es sich aber tatsächlich um einen Trojaner, der den Angreifern Zugriff auf den PC ermöglicht.

Betroffen von der Masche ist nicht nur Netflix, auch die Websites anderer großer Unternehmen wie etwa HP, Dell & Co. werden von den Kriminellen gekapert.

So schützen Sie sich: Viele Sicherheits-suiten bieten einen Webfilter für den Browser. Dieser sollte solche Attacken erkennen. Entdeckt hat die aktuelle Malware-Kampagne der Antivirenspezialist Malwarebytes.

Der Website-Filter von **Malwarebytes** sollte entsprechend diese Angriffe zuverlässig blockieren.

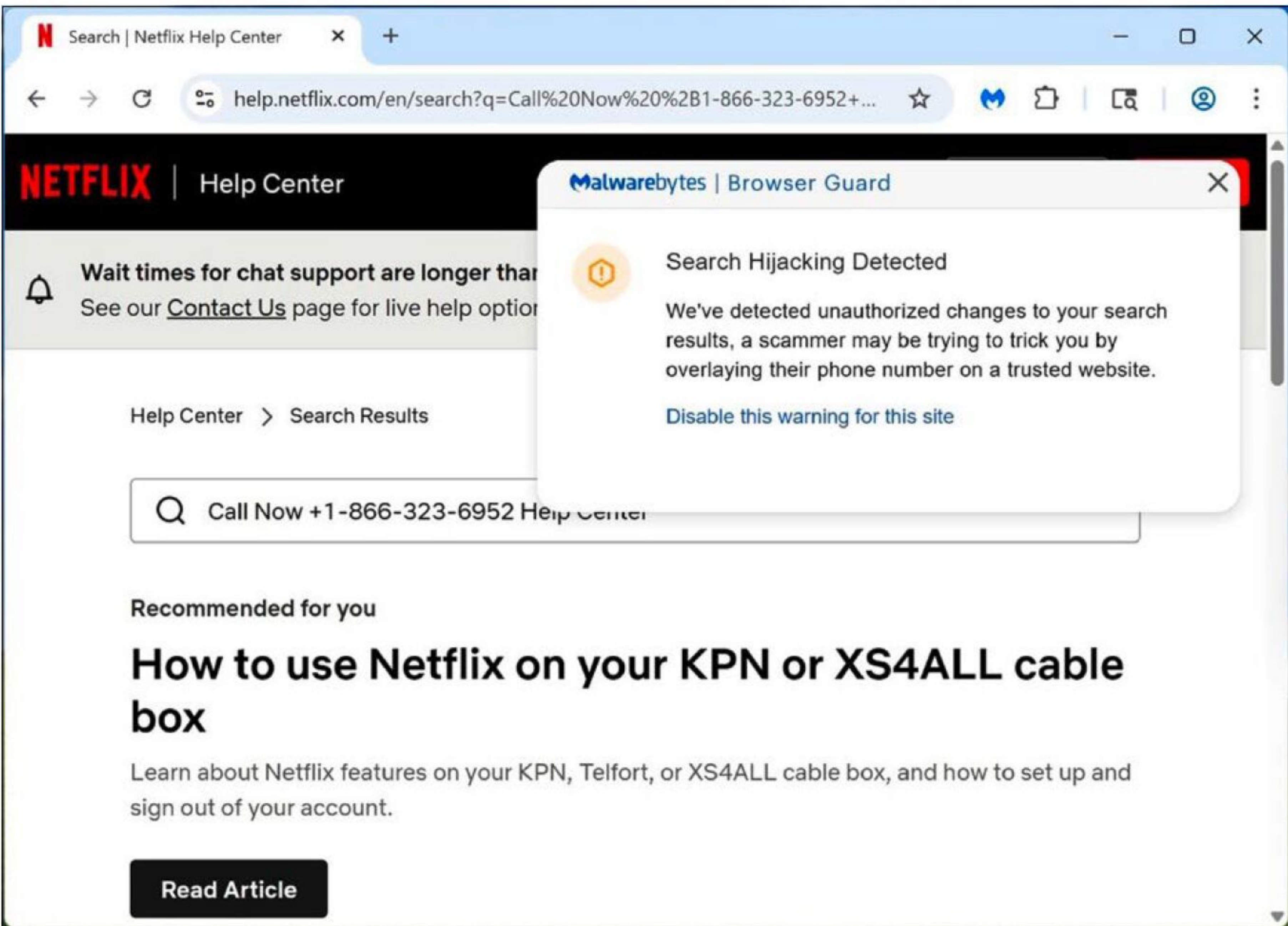
2. Genügt der Defender oder benötige ich Kaufsoftware?

Das Antivirenprogramm Microsoft Defender ist standardmäßig in Windows integriert. Seine Nutzung ist kostenlos, es aktualisiert sich automatisch, und die Verzahnung mit Windows könnte nicht enger sein – schließlich stammt das Tool vom Windows-Hersteller selbst. Zudem schnitt die Virenerkennung von Microsoft Defender in den vergangenen Tests fast immer sehr gut ab. Daher genügt der Defender für jeden IT-interessierten Anwender, der ein gesundes Maß an Misstrauen gegenüber E-Mails und Websites mitbringt. Wer sich aber überhaupt nicht für IT-Sicherheit interessiert und noch nie etwas von Phishing-Mails und gefährlichen Websites gehört hat, ist mit einer umfangreichen Antiviren-suite besser beraten, da diese mehr zusätzliche Schutzfunktionen bietet.

3. Sind Passkeys wirklich so viel sicherer als Passwörter?

Passkeys sind die neuen Superstars, wenn es um die sichere Anmeldung bei Online-diensten geht. Anstatt sich mit einem Passwort zu authentifizieren, nutzen Sie einen Passkey. Dieser wird auf einem kompatiblen Gerät (jedes aktuelle Smartphone oder Computer) gespeichert und per Fingerabdruck-, Gesichtsscan- oder PIN-Authentifizierung (Windows Hello) freigegeben. Da es bei einer Anmeldung per Passkey kein Passwort gibt, kann Ihnen dieses auch nicht gestohlen werden. Zudem schützen Passkeys sehr gut vor Phishing-Angriffen. Also: Ja. Passkeys sind viel sicherer als Passwörter. Sie sollten, wo immer es möglich ist, Passkeys zur Anmeldung bei einem Dienst nutzen.

Wenn Sie jedoch Ihr Smartphone verlieren, verlieren Sie auch Ihren Passkey. In einem solchen Fall ist es für einen Online-Dienst schwer, einen Nutzer sicher zu identifizieren. Ihm also wieder Zugriff auf sein Konto zu gewähren. Deshalb gibt es nur wenige Dienste, bei denen Sie sich ausschließlich per Passkey authentifizieren können. Es gibt immer noch ein Passwort für die Anmeldung. Eine Ausnahme stellt das Microsoft-Konto dar, das seit vergangenem Jahr passwortlos genutzt werden kann. Außerdem ist die Handhabung von Passkeys nicht so unkompliziert, wie viele mei-



Hier haben Kriminelle auf der echten Support-Website von Netflix ihre eigene Telefonnummer eingefügt. Wer dort anruft, gibt seine Daten preis und riskiert im schlimmsten Fall, sich einen Trojaner einzufangen.

nen. Probleme gibt es etwa, wenn man Passkeys sowohl im Betriebssystem (etwa Android) als auch in einem Passwortmanager gespeichert hat.

4. Wie schütze ich mich vor Krypto-Minern?

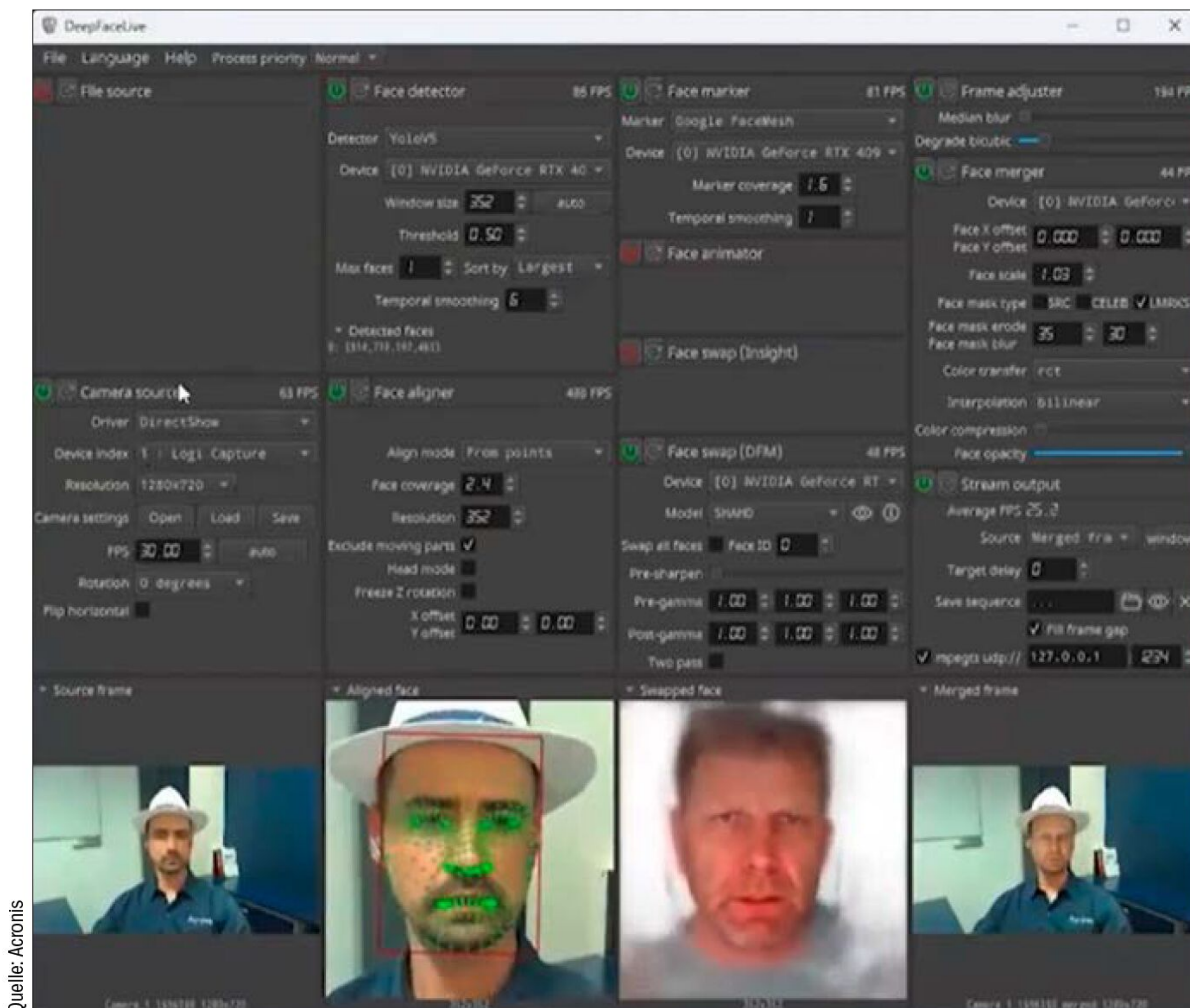
Krypto-Miner sind Schädlinge, die Ihren PC nutzen, um digitales Geld zu errechnen. Die

Bedrohung erfolgt auf zwei Arten: Erstens als klassische Malware, die sich in Ihrem Rechner einnistet. Diese Schädlinge blocken Sie mit einer guten Antivirensoftware. Andererseits lauern Krypto-Miner im Web: Auf präparierten Websites ist Javascript-basiertes Mining eingebettet, das direkt beim Seitenaufruf aktiv wird. In diesem Fall läuft der Schädling ausschließlich während

IM ÜBERBLICK: SICHERHEITSTOOLS



Name	Beschreibung	Auf	Internet	Preis	Sprache
Aomei Backupper Standard	Backup-Programm	Heft-DVD	www.pcwelt.de/article/1686627	Gratis	Deutsch
Avast Free Antivirus	Antivirenprogramm	Heft-DVD	www.avast.com	Gratis	Deutsch
AVG Antivirus Free Edition	Antivirenprogramm	Heft-DVD	www.pcwelt.de/article/1134904	Gratis	Deutsch
Avira Free Security	Antivirenprogramm	Heft-DVD	www.avira.com/de	Gratis	Deutsch
Bitwarden	Passwortmanager	Heft-DVD	www.pcwelt.de/article/1915554	Gratis	Deutsch
Cryptomator	Verschlüsselung für die Cloud	Heft-DVD	https://cryptomator.org	Gratis	Deutsch
Cryptsync	Verschlüsselung für die Cloud	Heft-DVD	https://tinyurl.com/4vjk29zf	Gratis	Englisch
Defender UI	Sicherheitstool	Heft-DVD	www.defenderui.com	Gratis	Deutsch
Free Firewall	Firewall	Heft-DVD	www.evorim.com/de/free-firewall	Gratis	Deutsch
Hard Configurator	Sicherheitstool	Heft-DVD	https://tinyurl.com/yc62d368	Gratis	Deutsch
Hardentools	Sicherheitstool	Heft-DVD	https://tinyurl.com/mtpj6b26	Gratis	Deutsch
Malwarebytes Adwcleaner	Anti-Adware	Heft-DVD	www.malwarebytes.com/de	Gratis	Deutsch
Malwarebytes Anti-Malware	Internet-Sicherheitspaket	Heft-DVD	www.malwarebytes.com/de	50 Euro pro Jahr	Deutsch
Opera	Internetbrowser	Heft-DVD	www.opera.com/de	Gratis	Deutsch
Privazer	Datenschutztool	Heft-DVD	https://privazer.com/de/	Gratis	Deutsch
Proton VPN	VPN-Client	Heft-DVD	https://protonvpn.com/de	Gratis	Deutsch
Veracrypt	Verschlüsselung	Heft-DVD	www.pcwelt.de/article/1152564	Gratis	Deutsch
Wise Folder Hider Free	Sicherheitstool	Heft-DVD	www.wisecleaner.eu	Gratis	Deutsch



Quelle: Acronis

Ein Sicherheitsexperte von Acronis zeigt in einem Webinar, wie sich mit einem kostenlosen Tool ein Gesicht in einem Livevideo austauschen lässt. Mit einem weiteren Tool lässt sich auch die Stimme auswechseln.

der geöffneten Browsersitzung und verschwindet mit dem Schließen der Seite.

So schützen Sie sich: Gegen Mining im Browser nutzen Sie für unbekannte und damit vielleicht verseuchte Websites den Browser **Opera**. Er blockiert Mining-Code automatisch.

5. Wie gefährlich sind Angriffe mit Künstlicher Intelligenz?

Künstliche Intelligenz erstellt innerhalb von Minuten überzeugende Texte, geklonte Stimmen, gefälschte Videos und funktionsfähigen Programmcode. Sie findet Sicherheitslücken in Software und Serverdiensten und ist äußerst preisgünstig. Das nutzen auch Cyberkriminelle. Die Frage, wie gefährlich KI-Angriffe dadurch sind, wird allerdings unterschiedlich beantwortet. Es gibt jedoch einige Experten, die in den nächsten Jahren mit einer Flut von äußerst gefährlichen Attacken rechnen. Im Folgenden finden Sie ein paar konkrete Beispiele dafür, wie KI Cyberangriffe verändert. Künstliche Intelligenz verbessert bestehende Angriffe und erleichtert Kriminellen die Arbeit. Während sich Phishing-Mails mit etwas Misstrauen noch leicht von echten E-Mails unterscheiden ließen, erschei-

nen die aktuellen, mit KI erstellten Phishing-Mails teilweise täuschend echt. Das bedeutet, sie sind nach Form und Inhalt kaum noch von echten E-Mails zu unterscheiden.

Weiter bedrohen sogenannte Deepfakes die Internetnutzer. Dabei geht es zum Beispiel um Videos mit bekannten Persönlichkeiten, etwa einem Nachrichtensprecher. Dieser liest auf einer Website jedoch nicht die Nachrichten der Tagesschau, sondern macht Werbung für dubiose Kryptowährungen und Aktien.

Zudem entstehen solche Angriffe heute deutlich schneller, da neue KI-Tools den Kriminellen dabei helfen. Diese Tools heißen etwa FraudGPT, WormGPT, AI Phish oder ScamGPT. Sie erzeugen innerhalb von Minuten neue Angriffe, für die die Kriminellen sonst Tage gebraucht hätten.

So schützen Sie sich: Gegen verbesserte Phishing-Mails hilft es, die Absenderadresse und die enthaltenen Links genau zu prüfen. Weitere Informationen dazu finden Sie in unserem Ratgeber unter www.pcwelt.de/1184128.

Gegen Deepfakes hilft Misstrauen und ein ganz genauer Blick auf das fragliche Foto oder Video. Wie Sie den Betrug erkennen,

erfahren Sie im Ratgeber unter www.pcwelt.de/article/1187442. Tipps gegen Angriffe mit gefälschten Stimmen finden Sie unter www.pcwelt.de/article/2417165.

6. Warum sind Zero-Day-Lücken so gefährlich?

Eine Zero-Day-Lücke ist eine bislang unbekannte Sicherheitslücke in einer Software oder einem Betriebssystem, für die noch kein Update verfügbar ist. Der Begriff „Zero-Day“ bezieht sich darauf, dass dem Hersteller null Tage Zeit blieb, um auf die entdeckte Schwachstelle zu reagieren. Entweder wurde sie noch nicht gemeldet oder sie wird bereits aktiv ausgenutzt. Gleichzeitig sind Schwachstellen in einer Software – zumindest wenn es sich um gravierende Schwachstellen handelt – ein gefundenes Fressen für Hacker. Denn darüber können sie sich in das System einklinken, ohne den Anwender überlisten zu müssen.

So schützen Sie sich: Gegen Zero-Day-Lücken kann sich die Software selbst nicht schützen, da das entsprechende Update noch fehlt. Die Heuristik einer Antivirensoftware kann den Schadcode jedoch meist erkennen. Bei Zero-Day-Lücken mit hohem Risiko kann es jedoch auch nötig sein, das betroffene System vom Internet zu trennen, bis ein Update gegen die Lücke vorliegt.

7. Wo finde ich einen Online-Virens scanner?

Tatsächlich gibt es heute keine Online-Virens scanner mehr, die Ihre gesamte Festplatte nach Malware durchsuchen könnten. Das liegt unter anderem daran, dass Code aus dem Browser heute deutlich weniger Rechte auf dem PC hat als vor rund 20 Jahren, als viele Online-Virens scanner per ActiveX im Browser arbeiteten. Heutige Browser bieten aber keine ActiveX-Unterstützung mehr. Der Begriff „Online-Virens scanner“ hat sich zwar erhalten, doch was Sie heute unter diesem Namen bekommen, sind einfache Antivirenprogramme. Sie werden als EXE-Datei auf Ihren PC geladen. Einige müssen installiert werden, andere starten ohne Installation. Als zweite Meinung zu dem Ergebnis Ihres bereits installierten Antivirenprogramms haben sie durchaus ihre Berechtigung. Beispiele für solche Virens scanner stammen von Eset (www.eset.com/de/home/online-scanner), Trendmicro (<https://tinyurl.com/m43fexpr>) und F-Secure (www.f-secure.com/de/online-scanner).

Unter dem Begriff „Online-Virens Scanner“ gibt es außerdem Websites, bei denen sich eine begrenzte Zahl an verdächtigen Dateien hochladen lässt. Diese werden dann auf Gefährlichkeit hin untersucht. Der bekannteste Vertreter dieser Art ist Virustotal, der eine Datei mit über 40 Antivirentools überprüft. Der Dienst ist immer dann einen Besuch wert, wenn Sie eine verdächtige Datei vor sich haben.

8. Kann ich durch Ransomware verschlüsselte Dateien retten?

Gegen viele Erpresserviren gibt es passende Entschlüsselungstools. Das richtige Tool zu finden ist jedoch meist nicht einfach, da der Erpresservirus den verwendeten Code nicht offenlegt. Hilfe finden Sie auf der Website www.nomoreransom.org. Ein Assistent führt Sie durch einen Prozess, an dessen Ende Ihnen, wenn alles gut geht, ein Entschlüsselungstool für Ihre Dateien angeboten wird. Wenn Sie dort nichts finden, probieren Sie es bei ID Ransomware (<https://id-ransomware.malwarehunterteam.com>). Wenn auch dort keine Hilfe angeboten wird, sollten Sie die verschlüsselten Dateien aufbewahren und in ein paar Monaten erneut nachsehen. Oft knacken Sicherheitsforscher die Verschlüsselungscodes von Ransomware erst nach einiger Zeit, oder die Kriminellen veröffentlichen den Generalschlüssel – das ist zumindest in der Vergangenheit schon vorgekommen.

9. Wie schütze ich mich vor Ransomware?

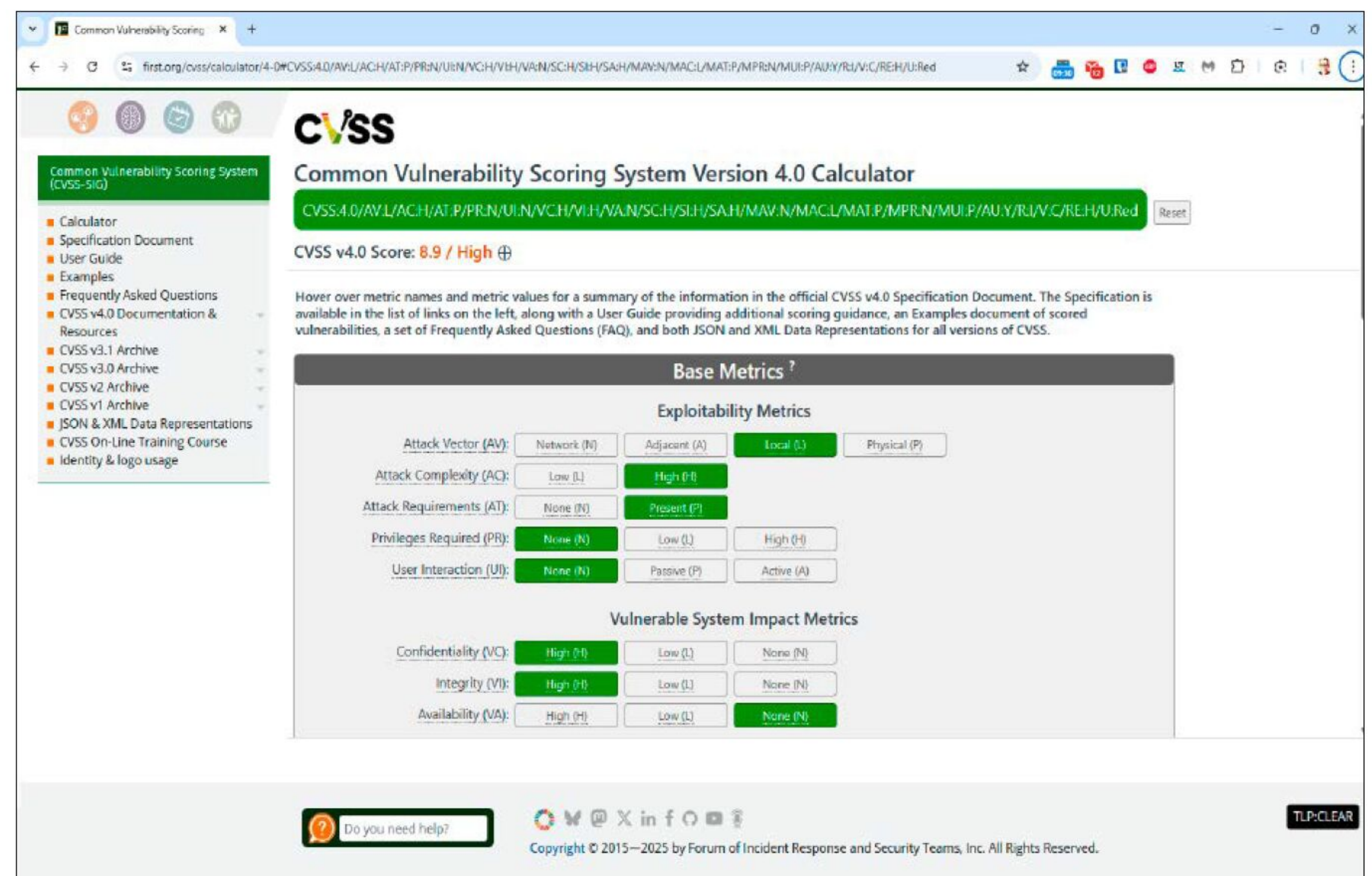
Idealerweise erkennt und blockiert zuverlässige Antivirensoftware Ransomware, bevor der Schädling aktiv wird und persönliche Daten verschlüsseln kann. Doch selbst moderne Schutzlösungen bieten keine hundertprozentige Sicherheit.

Der wirksamste Schutz gegen Ransomware ist deshalb ein aktuelles und extern gesichertes Backup. Der Ratgeber unter www.pcwelt.de/64840 zeigt, wie es geht.

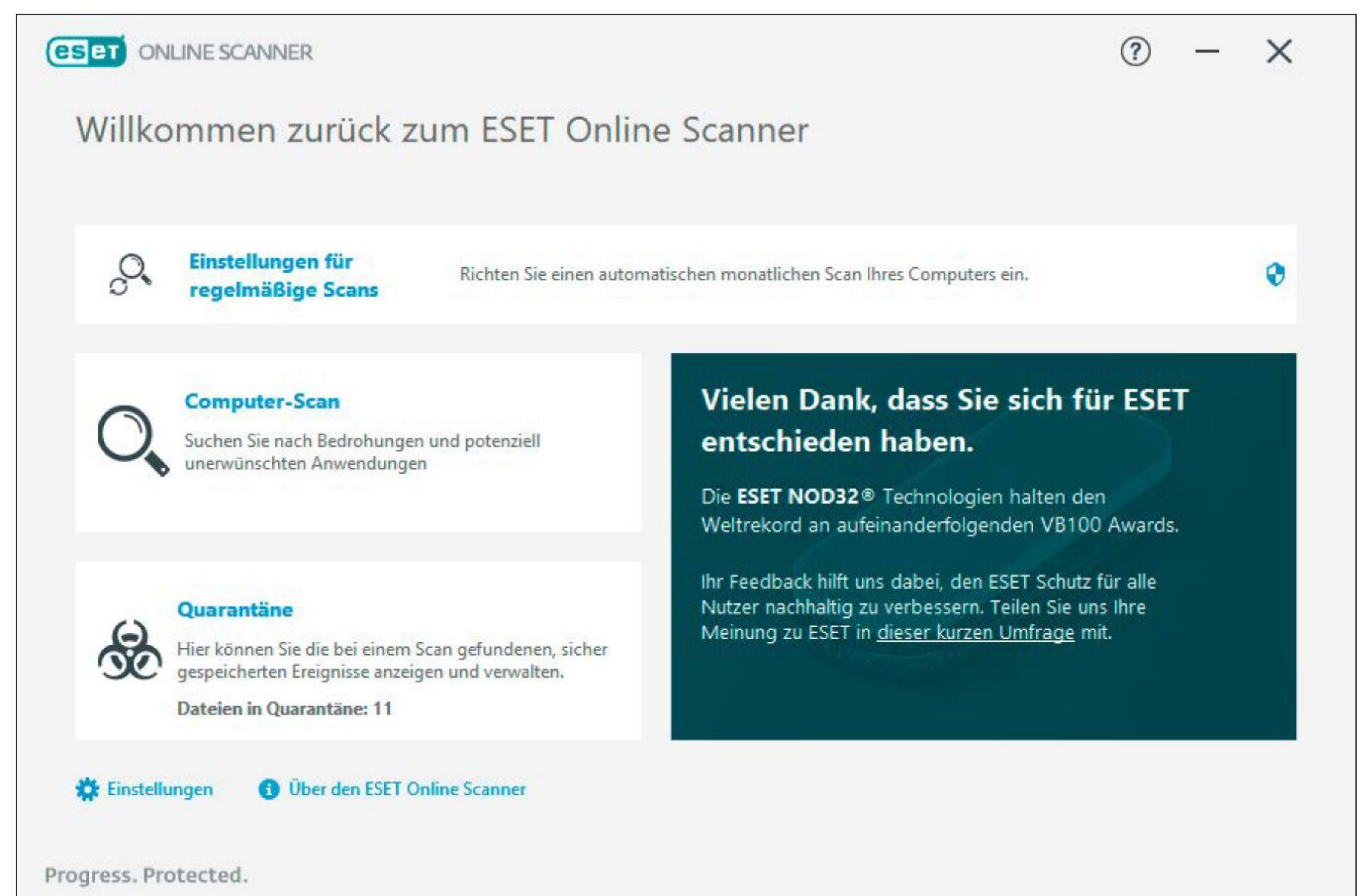
Zudem bietet Windows 11 seit einigen Jahren einen speziellen Schutz gegen Ransomware. Wie Sie ihn aktivieren, verrät dieser Artikel: www.pcwelt.de/article/2254566.

10. Sind meine privaten Dateien in der Cloud sicher?

Sicher sind Cloudspeicher nicht, man kann sie aber sicher machen. Bedroht werden



Der CVSS-4.0-Rechner zeigt an, wie gefährlich eine Sicherheitslücke nach dem Common Vulnerability Scoring System ist, und gleichzeitig, wie hoch das Risiko ist, dass sie ausgenutzt wird.



Das Tool Eset Online Scanner lässt sich parallel zu einem installierten Antivirenprogramm nutzen. Es verfügt zwar nicht über einen Virenwächter, untersucht aber alle Dateien auf der Festplatte.

sensible Daten in der Cloud von mehreren Seiten: Hacker können sich Zugang zur Cloud verschaffen. Der Cloudanbieter hat Zugriff auf die Daten, ebenso staatliche Stellen. Außerdem kann der Cloudanbieter Sie von Ihrem Konto aussperren, etwa wenn er Sie verdächtigt, gegen die Regeln verstoßen zu haben. Etwas, das in der Vergangenheit bei Microsoft angeblich häufiger vorgekommen ist.

So schützen Sie sich: Gegen Spionage können Sie sich mit einer guten End-to-End-Verschlüsselung schützen. Empfeh-

lenswert ist dafür etwa das Tool **Cryptomator**. Es stehen Apps für Android und iOS sowie Tools für Windows, Linux und MacOS bereit. Die Windows-Software von Cryptomator ist Donationware. Die Android- und die iOS-App kosten jeweils 19 Euro. Gegen den Ausschluss aus einem Cloudkonto schützt man sich am besten, indem man ein Backup der Daten auf dem eigenen PC erstellt. Das lässt sich etwa mit dem Tool **Cryptsync** recht problemlos einrichten. Tipps zu diesem Tool gibt es unter www.pcwelt.de/article/1199425. ■

Neue Sicherheits-Checklisten des BSI

Auf der Website des BSI finden Sie Tipps und Anleitungen in übersichtlichen PDFs, um die Sicherheit Ihres PCs zu verbessern. Zu den neuen Themen gehören unter anderem die sichere Nutzung Künstlicher Intelligenz und Erpressung mit Nacktbildern.

VON ROLAND FREIST

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht unter der Überschrift „Wegweiser für den digitalen Alltag“ in unregelmäßigen Abständen Broschüren, in denen Sicherheitsrisiken für private Anwender beim Umgang mit dem PC beschrieben werden. Sie können sich diese Ratgeber unter <https://tinyurl.com/2nkzzvfb> kostenlos als PDFs herunterladen. Ausgehend von den neuesten BSI-Broschüren geben wir Sicherheitstipps, mit denen Sie den beschriebenen Gefahren vorbeugen oder sie abwehren können.

Künstliche Intelligenz sicher und anonym nutzen

KI-Tools und Plattformen machen Fehler. Auch wenn die Hersteller daran arbeiten, die Fehlerrate ihrer Produkte zu verringern

„Die Broschüren des BSI enthalten interessante Informationen, die einen Blick lohnen.“



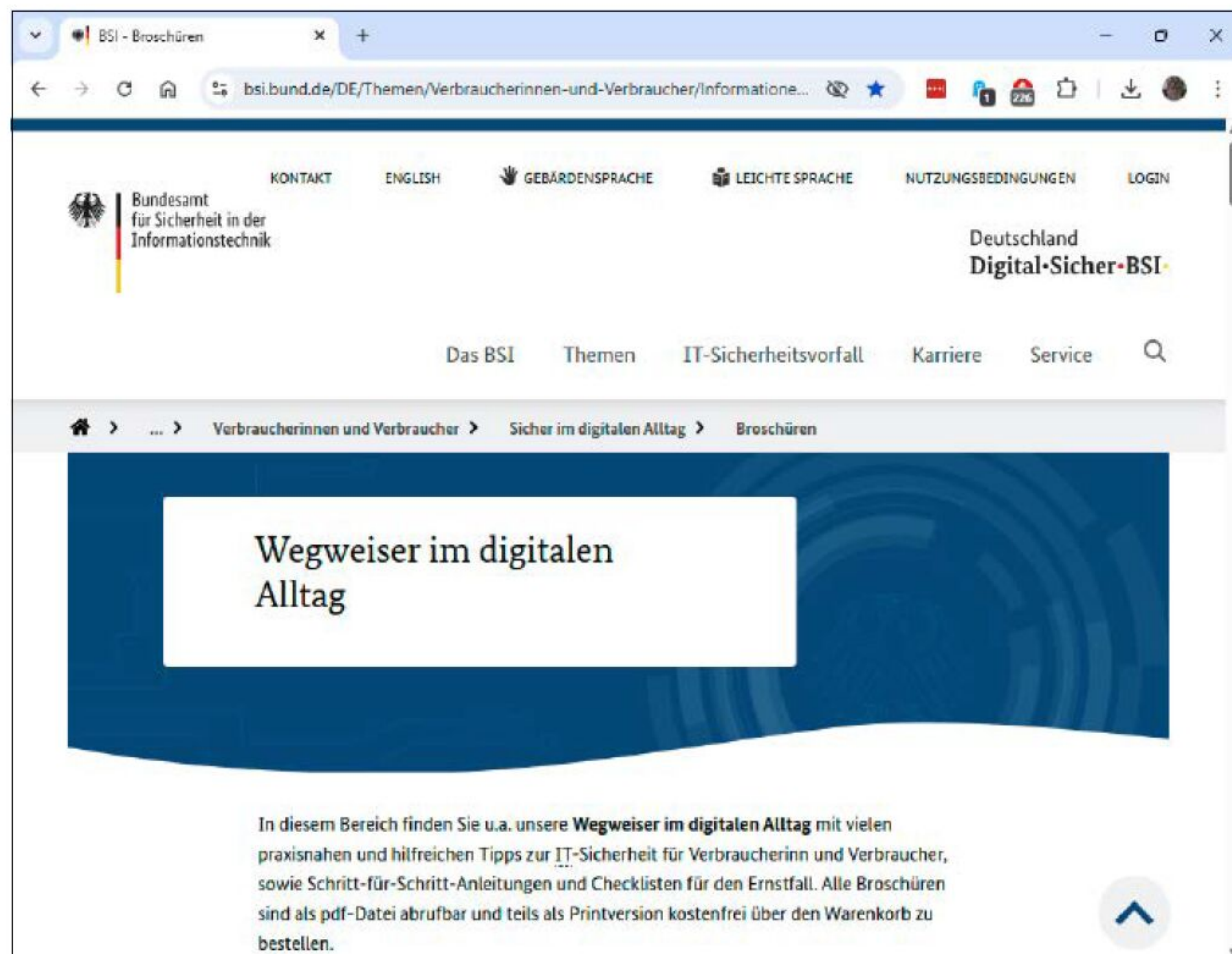
– komplett fehlerlos werden ChatGPT und seine Konkurrenten vermutlich niemals sein. Benutzer müssen sich also immer bewusst sein, dass eine Antwort der KI auch falsch sein kann.

Dabei gilt es abzuwägen, welche Folgen eine falsche Antwort hätte. Wenn ein Large Language Model (LLM) wie ChatGPT sich bei der Aufzählung der fünf bevölkerungsreichsten Städte der Welt verhaspelt, bleibt das normalerweise folgenlos. Doch wenn es auf die Frage nach dem richtigen Medikament gegen eine Krankheit die falsche Antwort liefert, kann das fatale Folgen haben. Je nach Thema sollten Sie die Antworten von KI-Systemen daher immer gegenchecken. Sie sollten zudem darauf achten, keine persönlichen Daten an die KI-Systeme weiterzugeben. Eröffnen Sie keine Accounts bei den LLMs, sondern bleiben Sie bei Ihren

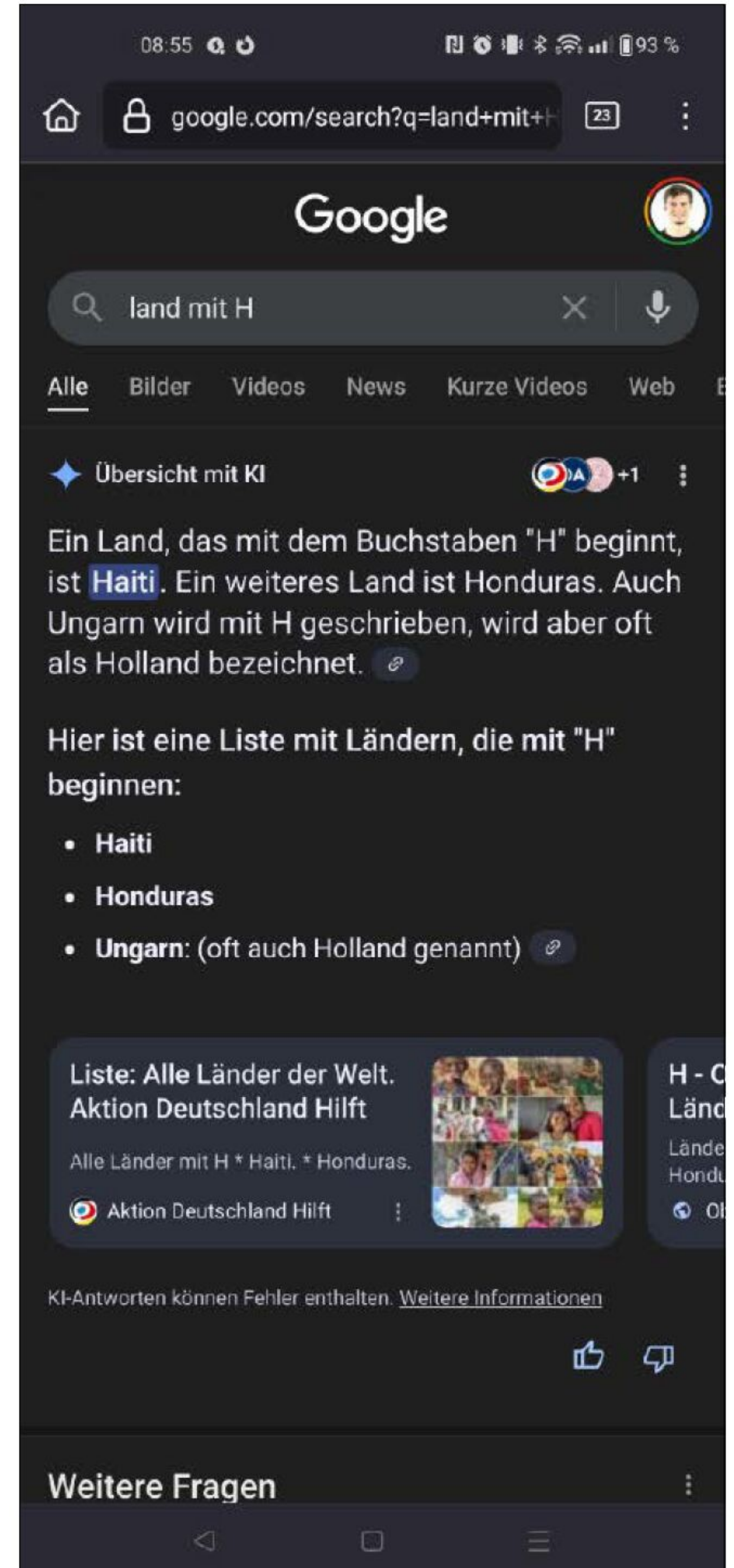
Fragen anonym. Geben Sie im Kontakt mit der KI niemals Daten wie Wohnort, E-Mail-Adresse, Telefonnummer oder Passwörter preis. Denn einige KI-Anbieter sammeln laut den Infos des BSI diese Daten und benutzen sie zum Anlegen von Profilen oder verkaufen sie weiter.

Phishing-Mails erkennen und Filter aktivieren

KI kann aber nicht nur falsche Antworten liefern, sondern wird von Kriminellen auch verwendet, um Phishing-Mails mit grammatikalisch perfekten Texten zu optimieren, Fake-Videos zu produzieren oder Stimmen von anderen Personen täuschend echt nachzuahmen. Umso wichtiger ist es, dass Sie bei eingehenden E-Mails und Sprachnachrichten die Adressen und Rufnummern sorgfältig kontrollieren.



Das BSI veröffentlicht unter der Überschrift „Wegweiser für den digitalen Alltag“ in unregelmäßigen Abständen Broschüren mit Tipps und Anleitungen zur Computer-Sicherheit.



Mit Phishing-Nachrichten versuchen Kriminelle, Sie auf gefälschte oder mit Schadsoftware verseuchte Websites zu locken. In allen drei großen Browsern (Chrome, Edge, Firefox) ist daher eine Schutzfunktion eingebaut, die Sie vor dem Besuch gefährlicher Websites warnt. Sie greift auf Datenbanken mit den Adressen von Phishing-Sites zu, kann aber auch andere Sites auf Gefahren checken. Allerdings bietet dieser Schutz keine hundertprozentige Sicherheit. Teilweise müssen Sie den Schutz auch erst aktivieren. Eine Anleitung dazu finden Sie unter <https://tinyurl.com/n4fudty5>.

Auf Erpressung mit Nacktbildern richtig reagieren

Bei Dating-Plattformen, aber auch bei sozialen Netzwerken versuchen Kriminelle häufig, Kontakt zu potenziellen Opfern herzustellen. Sobald sie deren Vertrauen gewonnen haben, schlagen sie einen Austausch von Nacktbildern oder einen Wechsel zu Videochats vor. Wenn es später zu sexuellen Handlungen vor der Kamera kommt, zeichnen sie die Bilder auf und drohen den Betroffenen mit Veröffentlichung. Man bezeichnet diese Erpressungsversuche mit dem Fachbegriff Sextortion.

Das BSI rät, auf die folgenden Lösegeldforderungen nicht einzugehen. Denn es bleibt nicht bei der einmaligen Zahlung, die Erpresser wollen immer mehr Geld. Stattdessen sollten Betroffene den Kontakt sofort abbrechen, Anzeige bei der Polizei erstatten und den Betreiber der Onlineplattform verständigen mit der Bitte, ihre Inhalte zu löschen. Der Betreiber kann zudem auch die Profile der Kriminellen blockieren.

Etwas anders gelagert ist der Fall, wenn die Absender dieser Mails nur behaupten, Zugriff auf die Webcam des Empfängers zu haben und so sein Verhalten vor der Kamera ausspioniert zu haben. In der Regel stimmt das nicht, Sie können diese Nachrichten also einfach ignorieren und löschen.

Was tun, wenn das E-Mail-Konto gehackt wurde?

Wenn Ihnen Freunde und Geschäftspartner plötzlich melden, dass sie von Ihnen Spam oder sogar virenverseuchte E-Mails erhalten haben, oder wenn Sie selbst von einem Tag auf den anderen keinen Zugriff auf Ihre E-Mails mehr haben, wurde Ihr Konto vermutlich gehackt. In den meisten Fällen wollen die Hacker über Ihr Konto Spam und andere Werbung verschicken, teilweise verkaufen sie unter Ihrer Mailadresse jedoch auch illegal Waren oder nutzen sie, um Passwörter bei Webdiensten wie etwa Onlineshops zurückzusetzen.

Auf jeden Fall sollten Sie unverzüglich handeln. Wenn Sie noch auf Ihren Account zugreifen können, sollten Sie sofort das Passwort ändern. Kontrollieren Sie dann die Einstellungen, ob jemand vielleicht Weiterleitungen der eingehenden Mails eingerichtet hat. Verständigen Sie außerdem Ihre Kontakte, dass Ihr Konto gehackt wurde. Haben Sie keinen Zugriff auf Ihren Account mehr, melden Sie dies Ihrem E-Mail-Provider und bitten Sie ihn um Hilfe. Er kann Ihre Anmeldeinformationen zurücksetzen oder wiederherstellen. Verständigen Sie auch in diesem Fall Ihre Kontakte. Schützen können Sie sich, indem Sie für den Zugriff auf Ihr Mailkonto, falls möglich,

KI-Systeme machen Fehler. Sie sollten ihren Antworten daher nicht blind vertrauen, sondern die Ergebnisse gegenchecken.

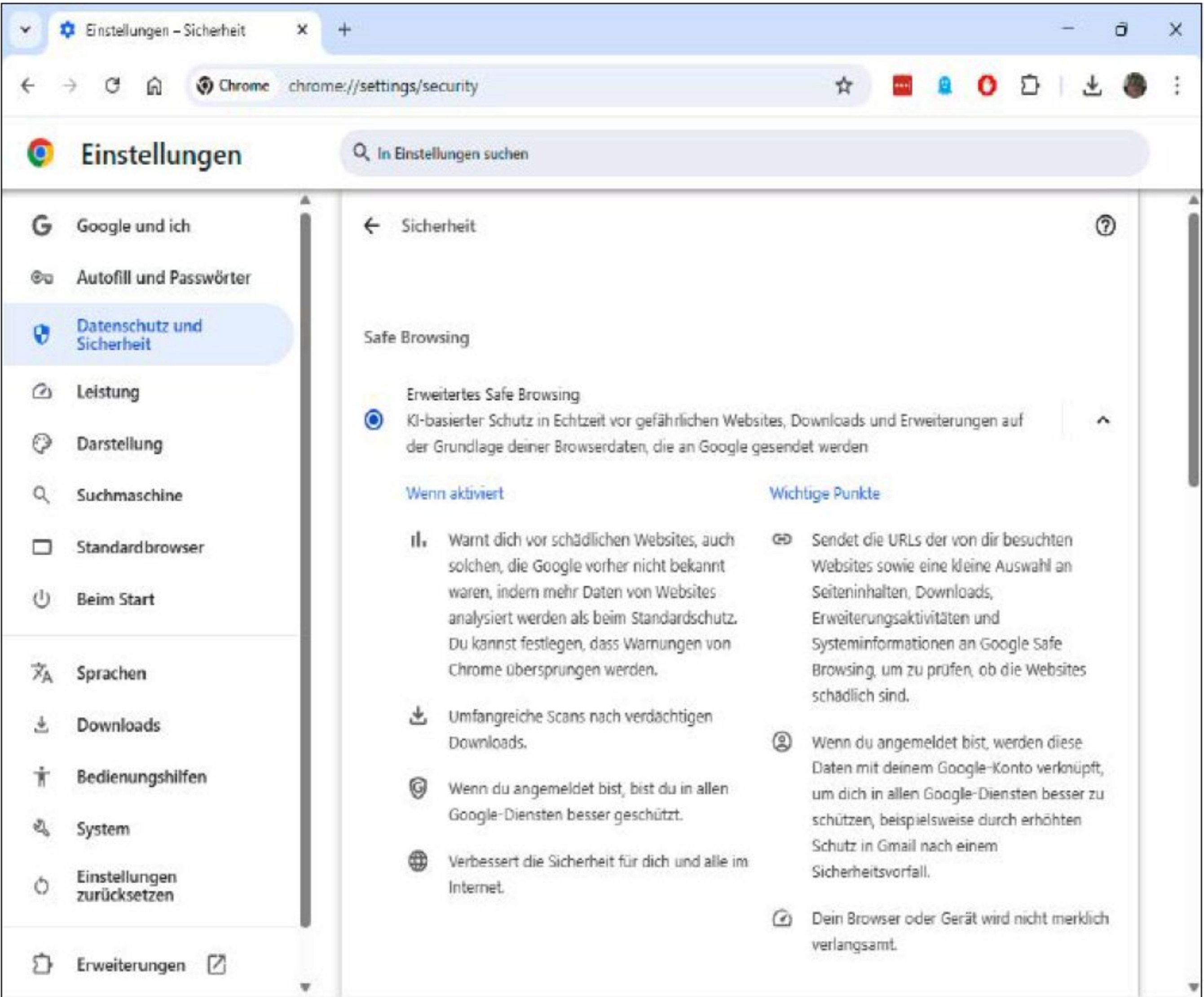
eine Zwei-Faktor-Authentisierung oder einen Passkey einrichten. Das Gleiche sollten Sie auch bei allen anderen Webdiensten machen, die Sie benutzen.

Die PC-WELT hat das Thema der gehackten Mail-Accounts bereits in der Vergangenheit aufgegriffen. Einen Artikel mit weiteren Tipps und Hinweisen finden Sie unter <https://tinyurl.com/mvjvnr8x>.

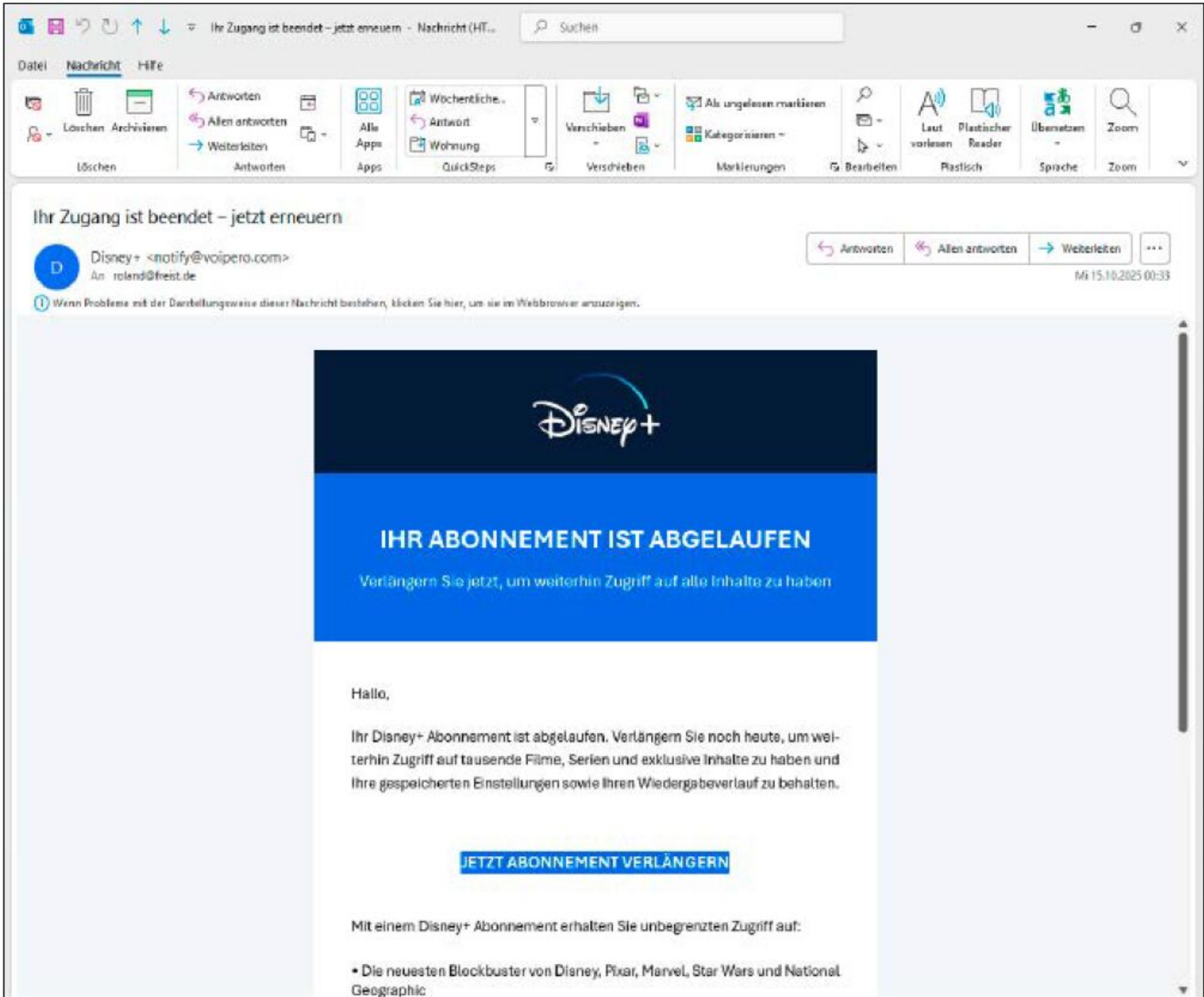
Betrug beim Onlinebanking erkennen

Die verpflichtende Zwei-Faktor-Authentisierung macht es Betrügern in der EU schwer, auf die Konten und das Geld von Bankkunden zuzugreifen. Dennoch gelingt es ihnen von Fall zu Fall, indem sie Kunden mit gefälschten Mails zur Preisgabe ihrer Zugangsdaten verleiten und sie auf gefälschte Bankseiten locken.

Wenn Sie bei der Kontrolle Ihres Kontostands ungewöhnliche Abbuchungen fest-



Aktivieren Sie in Google Chrome das erweiterte Safe Browsing, sodass Sie vor dem Besuch von Phishing- und anderen kriminellen Sites eine entsprechende Warnung erhalten und den Aufruf der Seiten abbrechen können.



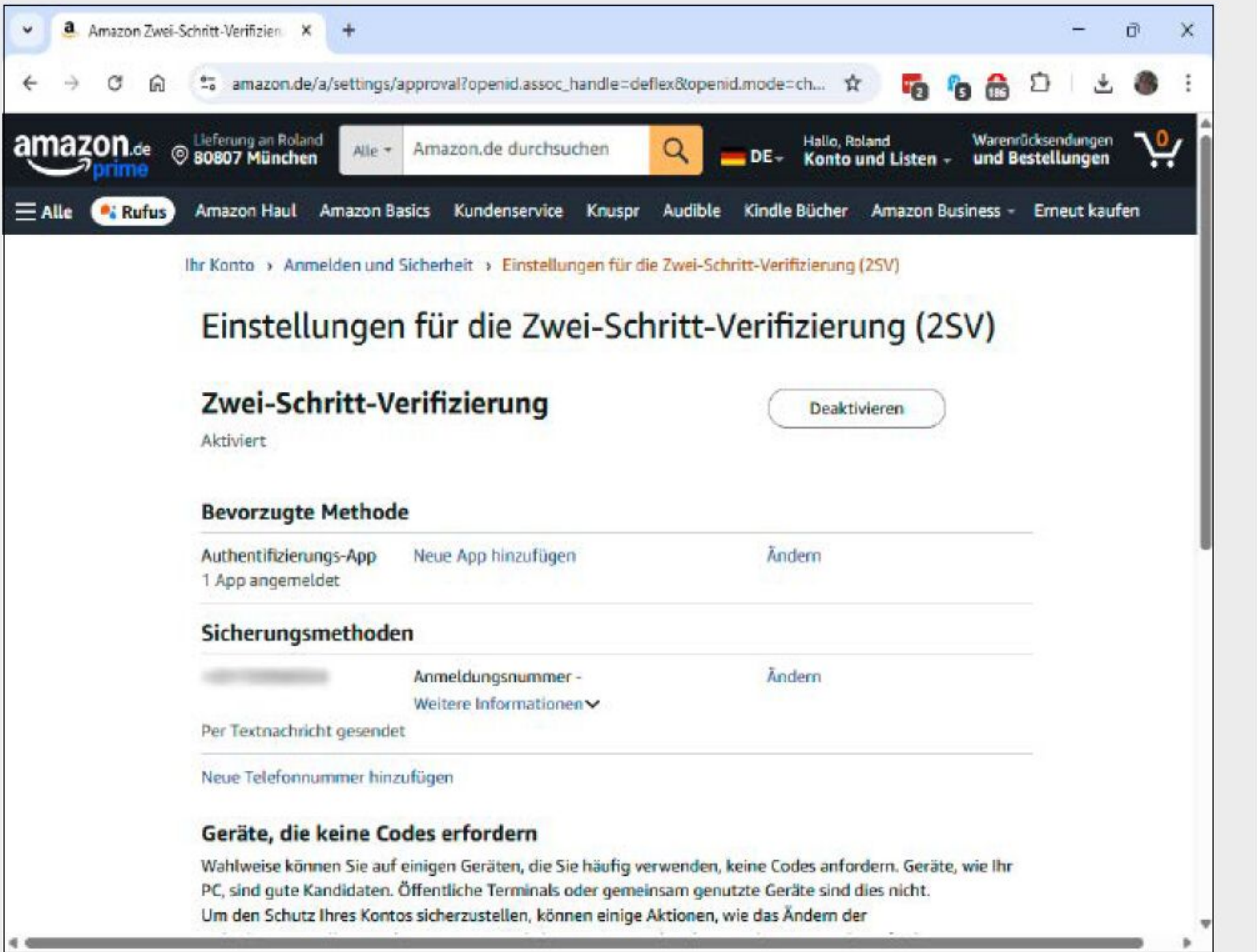
Häufig versuchen Kriminelle, mit solchen Phishing-Mails die Empfänger dazu zu bewegen, auf den Link zu klicken und ihre Benutzerdaten für den Streamingdienst einzugeben. Diese Daten lassen sich anschließend gut weiterverkaufen.

stellen, sollten Sie sofort die Telefonnummer 116 116 anrufen und Ihr Konto sperren lassen. Auch wenn Sie feststellen, dass Sie auf einer gefälschten Seite Ihre Zugangsdaten eingegeben haben, ist eine Sperrung des Kontos ratsam. Rufen Sie dann bei Ihrer Bank an, melden Sie Ihren Verdacht und fragen Sie nach ungewöhnlichen Kontobewegungen. Sollte tatsächlich eine fremde Person Geld von Ihrem Konto gestohlen haben, erstatten Sie umgehend Anzeige bei der Polizei.

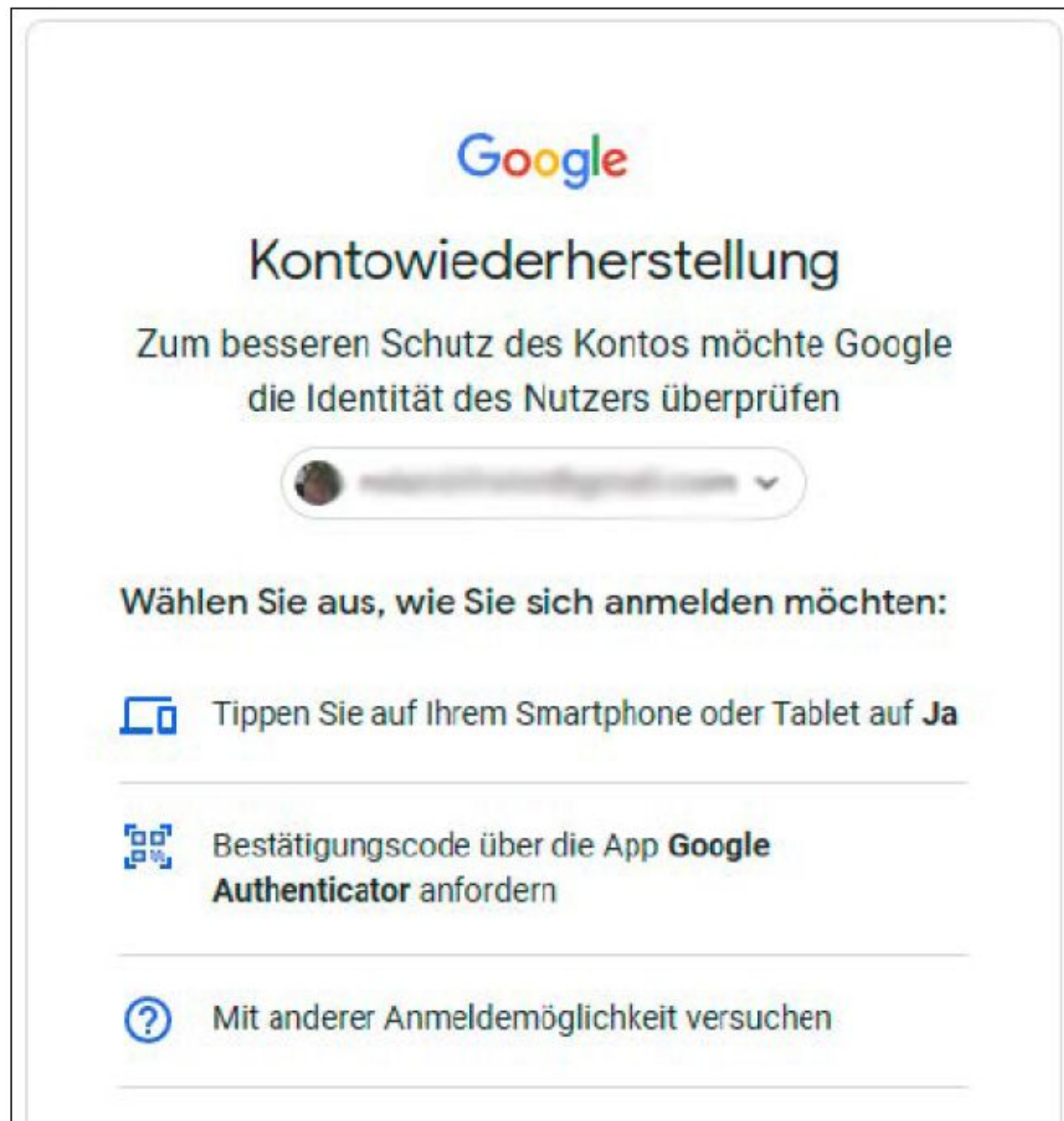
SO SCHÜTZEN SIE IHRE ONLINEKONTEN

- Um den Zugriff auf Bank- und andere Konten abzusichern, empfiehlt das BSI folgende Maßnahmen:**
1. Verwenden Sie starke Passwörter, die aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen. Sie sollten mindestens 16 Zeichen lang sein. Notieren Sie sich die Passwörter auf einem Blatt Papier oder speichern Sie sie in einem Passwortmanager, den Sie ebenfalls mit einem langen Passwort und einer Zwei-Faktor-Authentisierung absichern.
 2. Nutzen Sie bei allen Websites, die das anbieten, eine Zwei-Faktor-Authentisierung oder eine Anmeldung per Passkey.
 3. Wenn der zweite Faktor eine Bestätigung per Smartphone-App ist, laden Sie die Software ausschließlich aus dem Google Play Store beziehungsweise dem Apple App Store herunter.
 4. Halten Sie Ihre Bankverbindung geheim und seien Sie vorsichtig bei der Eingabe von Kontodaten bei dubiosen Online-shops.
 5. Benutzen Sie fürs Onlinebanking nur Ihre eigenen Geräte. Betreiben Sie kein Onlinebanking über ein öffentliches WLAN.
 6. Klicken Sie nicht unüberlegt auf Links in einer E-Mail. Denken Sie außerdem daran, dass Banken Sie niemals nach Ihren Zugangsdaten zum Onlinebanking, nach Ihrer PIN oder TAN fragen. Falls das geschieht, kommt die Anfrage immer von einem Betrüger.
 7. Definieren Sie für das Onlinebanking ein tägliches Überweisungslimit.

8. Steuern Sie die Website Ihrer Bank immer nur durch Eingabe der Webadresse auf Ihrer Tastatur oder über einen Favoriten in Ihrem Browser an.
9. Installieren Sie verfügbare Updates für Windows, Ihre Anwendungen und Ihre Smartphone-Apps immer sofort. Achten Sie darauf, dass unter Windows das Antivirenprogramm aktiviert ist.



Amazon und viele andere Onlineshops und Webdienste bieten eine Zwei-Faktor-Authentisierung für eine sichere Anmeldung an.



Gmail und andere Maildienste bieten automatisierte Verfahren an, mit denen Sie wieder Zugriff auf Ihr E-Mail-Konto erlangen.

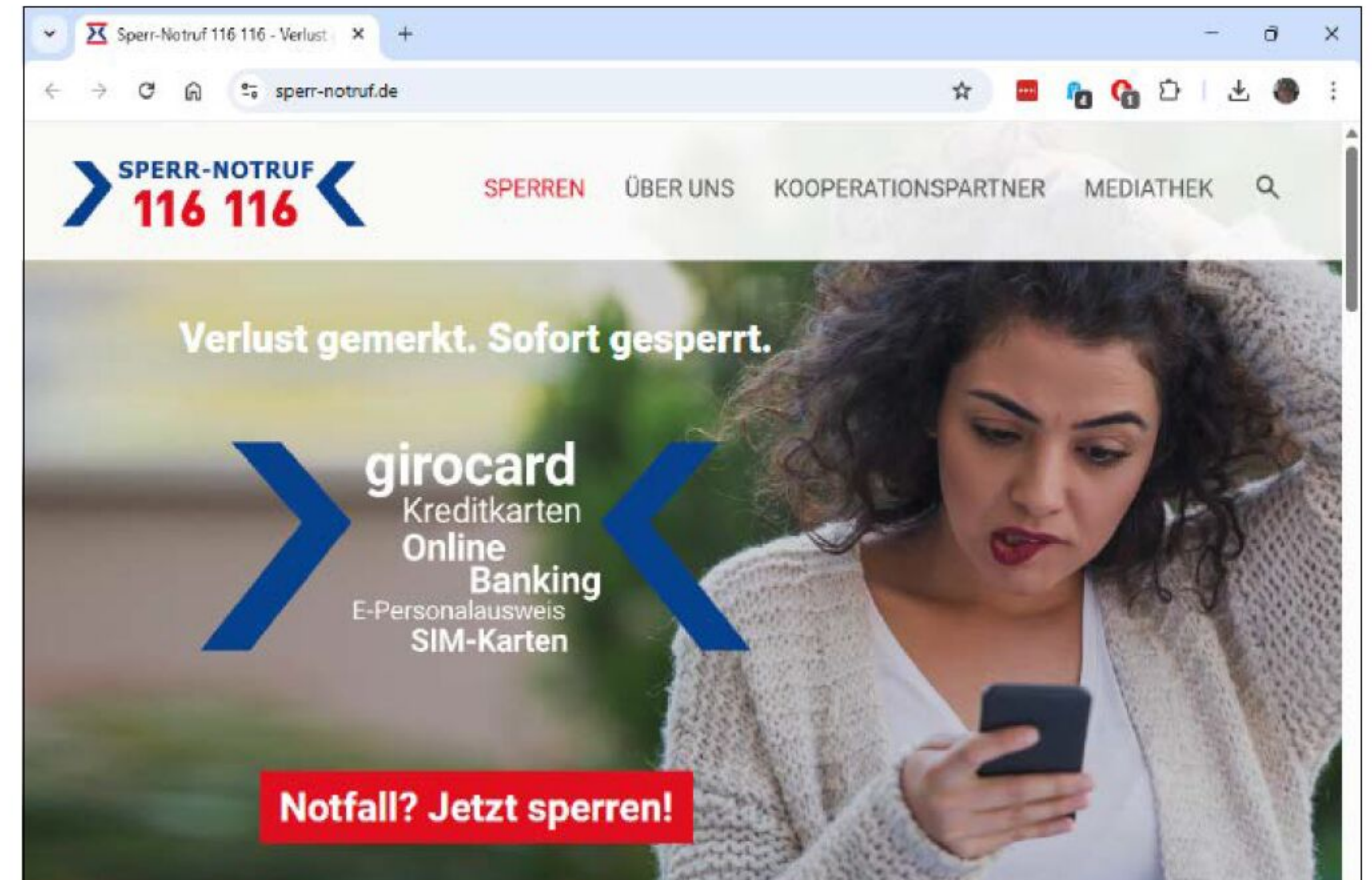
So handeln Sie bei einer Vireninfektion Ihres Rechners

Anzeichen für die Infektion mit einem Schadprogramm sind unter anderem spürbare Geschwindigkeitseinbußen, nicht mehr erreichbare Funktionen und von Ihrem Gerät verschickte Spamnachrichten an die Kontakte aus Ihrem Adressbuch. Ransomware meldet sich zudem automatisch mit einer Zahlungsaufforderung.

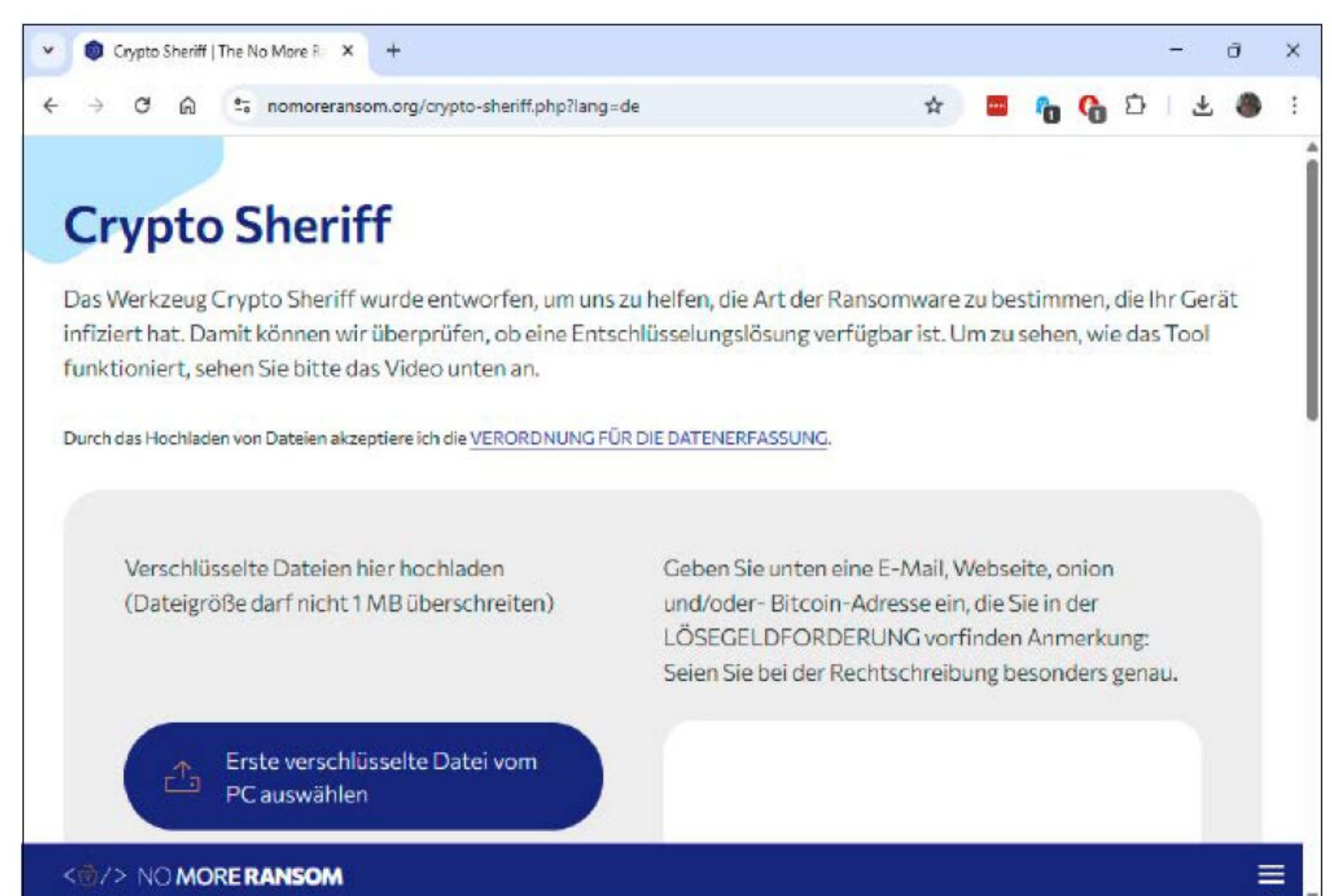
Wenn Ihr Rechner von einem Virus befallen ist, sollten Sie sofort die Netzwerkverbindungen kappen, um eine weitere Ausbreitung und den Abfluss von Daten zu verhindern. Danach führen Sie mit Ihrem Antivirenprogramm einen gründlichen Scan durch. Doch selbst wenn die Software angibt, dass alle Schadprogramme entfernt wurden, empfiehlt es sich, Windows von Grund auf neu zu installieren. Ein Smartphone oder Tablet sollten Sie auf die Werkseinstellungen zurücksetzen. Anschließend sollten Sie zunächst das Mailprogramm wieder einrichten, um andere Passwörter ändern zu können.

Für den Fall eines Ransomware-Angriffs empfiehlt das BSI, kein Lösegeld zu zahlen. Denn es ist nicht gesagt, dass die Kriminellen danach tatsächlich eine Anleitung schicken, wie Sie wieder Zugriff auf Ihre Daten bekommen. Sehen Sie stattdessen auf www.nomoreransom.org nach, ob es dort ein Entschlüsselungstool für die Ransomware gibt. Die Website bietet auch Anleitungen für die Tools. Außerdem sollten Sie bei der Polizei Anzeige erstatten. Schließlich sollten Sie auch in diesem Fall die SSD Ihres PCs formatieren und Windows neu aufsetzen.

Über den Notruf 116 116 können Sie nicht nur den Onlinezugriff auf Ihr Konto sperren. Sie können unter dieser Nummer unter anderem auch den Verlust von Giro-, Kredit- und SIM-Karten melden.



Auf der Website Nomoreransom.org finden Sie mit dem Crypto Sheriff einen Assistenten, der Ihnen bei der Identifizierung der Ransomware hilft, die Ihren Computer befallen hat.



Um Datenverlusten durch Ransomware vorzubeugen, legen Sie regelmäßig Backups Ihrer wichtigen Daten an. Am besten

nutzen Sie dazu ein externes Laufwerk oder einen USB-Stick, die Sie nach der Sicherung wieder von Ihrem Rechner abziehen. ■

BSI-TIPPS ZUR KONFIGURATION VON MICROSOFT OFFICE



Vergangenen September hat das BSI neue Empfehlungen für die Konfiguration der Version 2024 von Microsoft Office bereitgestellt. Die sieben PDF-Dokumente beschreiben, wie Administratoren Word, Excel, Powerpoint, Outlook, Access, Visio und das Officepaket insgesamt nach den Maßstäben eines möglichst hohen Sicherheitsniveaus konfigurieren. Die Dokumente enthalten Empfehlungen für die Einstellungen der Gruppenrichtlinien von Microsoft Office und richten sich damit vor allem an Administratoren in mittleren und großen Unternehmen. Aber auch private Anwender und kleinere Firmen können davon profitieren.

So rät das BSI beispielsweise, die Einstellungen der Gruppenrichtlinien immer explizit auf „Aktiviert“ oder „Deaktiviert“ zu setzen. Denn die Voreinstellung „Nicht konfiguriert“ könnte durch Sicherheitspatches ihre Bedeutung ändern. Weiterhin sollte der Benutzer beim Zugriff auf Clouddienste die automatische Anmeldung bei Onedrive und Office deaktivieren und er sollte bei Dokumenten aus dem Internet die Ausführung von Makros abschalten. Bei Outlook sollte die Synchronisation der Daten mit sozialen Netzwerken abgeschaltet werden.

Die BSI-Empfehlungen stehen unter der Adresse <https://tinyurl.com/49w3erbh> kostenlos zum Download im PDF-Format bereit.



© bsi.bund.de

Die offiziellen Tipps: Sicher online bezahlen

Jedes Verfahren zum Bezahlen beim Onlineshopping hat Vor- und Nachteile. Das Bundesamt für Sicherheit in der Informationstechnik ordnet das jeweilige Risiko ein. Wir ergänzen die offizielle Analyse mit Hinweisen der Verbraucherzentralen und weiteren Tipps.

VON PETER STELZEL-MORAWIETZ

Das Einkaufen im Internet ist bequem, praktisch und zeitsparend. Zudem bieten Onlineshops eine viel größere Auswahl als

„Bei Unstimmigkeiten leichtfertig eine Lastschrift oder Ähnliches zurückzuziehen schafft in aller Regel nur zusätzliche Probleme.“

die Geschäfte vor Ort, sofern es diese überhaupt noch gibt. Doch während man im lokalen Handel die Ware nach dem Bezahlen sofort mitnimmt, gibt es diese Gleichzeitigkeit im E-Commerce nicht. Einer der beiden Vertragspartner, Kunde oder Händler, geht in Vorleistung und trägt damit das Risiko, dass der andere unter Umständen nicht zahlt beziehungsweise liefert. In vielen Fällen müssen Verbraucher bei ihren Onlinebestellungen zahlen, bevor ein Händler Artikel versendet. Bei seriösen Shops klappt das meist problemlos, und der Kunde erhält seine bestellte Ware. Was aber, wenn ein Kauf nicht wie vereinbart funktioniert? Die Konfliktpunkte sind vielfältig und reichen aus Verbrauchersicht

von nicht eingehaltenen Lieferterminen bis zu falschen oder defekten Produkten. Ohne hier auf die Rechte und Pflichten beider Parteien einzugehen, entzündet sich im Anschluss in zahlreichen Fällen auch ein Streit ums liebe Geld. Als Kunde ist man dann unter Umständen mit der Frage konfrontiert, wie man bereits bezahltes Geld zurückerhält.

Das kommt, wie so häufig bei rechtlichen Streitfragen, darauf an. Vor allem hängt es davon ab, wie der vereinbarte Kaufpreis beglichen wurde. Denn die meisten Geschäfte im Internet bieten mehrere Zahlungsmöglichkeiten an, die sich hinsichtlich Sicherheit, Käuferschutz und Komfort zum Teil deutlich unterscheiden. Der vor-

liegende Ratgeber erläutert, welche Methoden besonders sicher sind, welche mit einem erhöhten Risiko verbunden sind, und welche man bei unsicheren Geschäften auf keinen Fall wählen sollte.

BSI rät: Vorsicht bei Vorkasse, Rechnung ist besonders sicher

Dass es im Detail kompliziert wird, zeigt bereits ein schneller Blick in die schier endlosen AGBs und Nutzungsbedingungen von Zahlungsdienstleistern wie Paypal, Kreditkartenunternehmen und Banken: Das Kleingedruckte können juristische Laien weder komplett lesen noch verstehen.

Da kommen die kurzen Zusammenfassungen der häufigsten Bezahlverfahren durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) gerade recht. Auf acht Schaubildern erläutert die Behörde Vor- und Nachteile von Kreditkarte, Sofortüberweisung (inzwischen Klarna), Vorkasse, Nachnahme, Rechnung, Lastschrift, Smartphone-Bezahlsystemen und Onlinediensten wie Paypal (<https://tinyurl.com/y4uyzd3u>). Dabei weist das BSI auch auf Gefahren beispielsweise durch Phishing hin.

Das Wichtigste sind die beiden folgenden Ratschläge der Behörde: Wo immer das Bezahlen per Rechnung möglich ist, birgt diese Option das geringste Risiko. Schließlich begleicht man die Rechnung erst nach Erhalt der Ware. Allerdings sollte man rechtzeitig ans Überweisen denken und darf die meist per E-Mail zugeschickte Rechnung nicht vergessen. Sonst werden schnell ein paar Euro Mahngebühren fällig.

Dazu ein Tipp: Immer mehr Rechnungen enthalten einen QR-Code, der alle wichtigen Daten für die Überweisung enthält: den Empfänger mit IBAN und BIC, den Zahlungsbetrag sowie den Verwendungszweck, also beispielsweise die Kunden- oder Rechnungsnummer. Bei solchen Rechnungen machen Sie vom QR-Code in der PDF-Datei einen Screenshot, schneiden den Ausschnitt passend zu und speichern ihn als Bilddatei ab. Am Windows-PC ist das mit Paint schnell erledigt. Wenn Sie dieses Bild im Onlinebanking über die Funktion „QR-Code Überweisung“ einlesen, werden alle Daten automatisch ausgefüllt. Sie können sich beim Eintippen von IBAN und den übrigen Angaben also nicht vertun.

Der zweite Rat des BSI lautet: Vorsicht bei Vorkasse! Diese Zahlungsmethode sollten Sie nur nutzen, wenn Sie den Onlinehändler

Kreditkarte

Zahlungsmittel, bei dem Sie die Zahlung durch das Eingeben Ihrer Kartendaten beim Onlineshop freigeben und sich über das 3D-Secure-Verfahren authentisieren.



- + Registrierung bei der Bank, kein weiteres Nutzerkonto nötig
- + Betrug wird erschwert, da Zwei-Faktor-Authentisierung (3D-Secure) erfolgt
- + Rückbuchungen von betrügerischen Transaktionen leicht möglich
- Eingabe der sensiblen Kartendaten bei jedem Einkauf
- Gefahr von Phishing-Angriffen

© Bundesamt für Sicherheit in der Informationstechnik

bsi.bund.de

So wie für die Kreditkarte stellt das Bundesamt für Sicherheit in der Informationstechnik das Wichtigste auch für andere Bezahloptionen beim Onlineshopping übersichtlich zusammen.

FAKESHOPS SICHER ERKENNEN



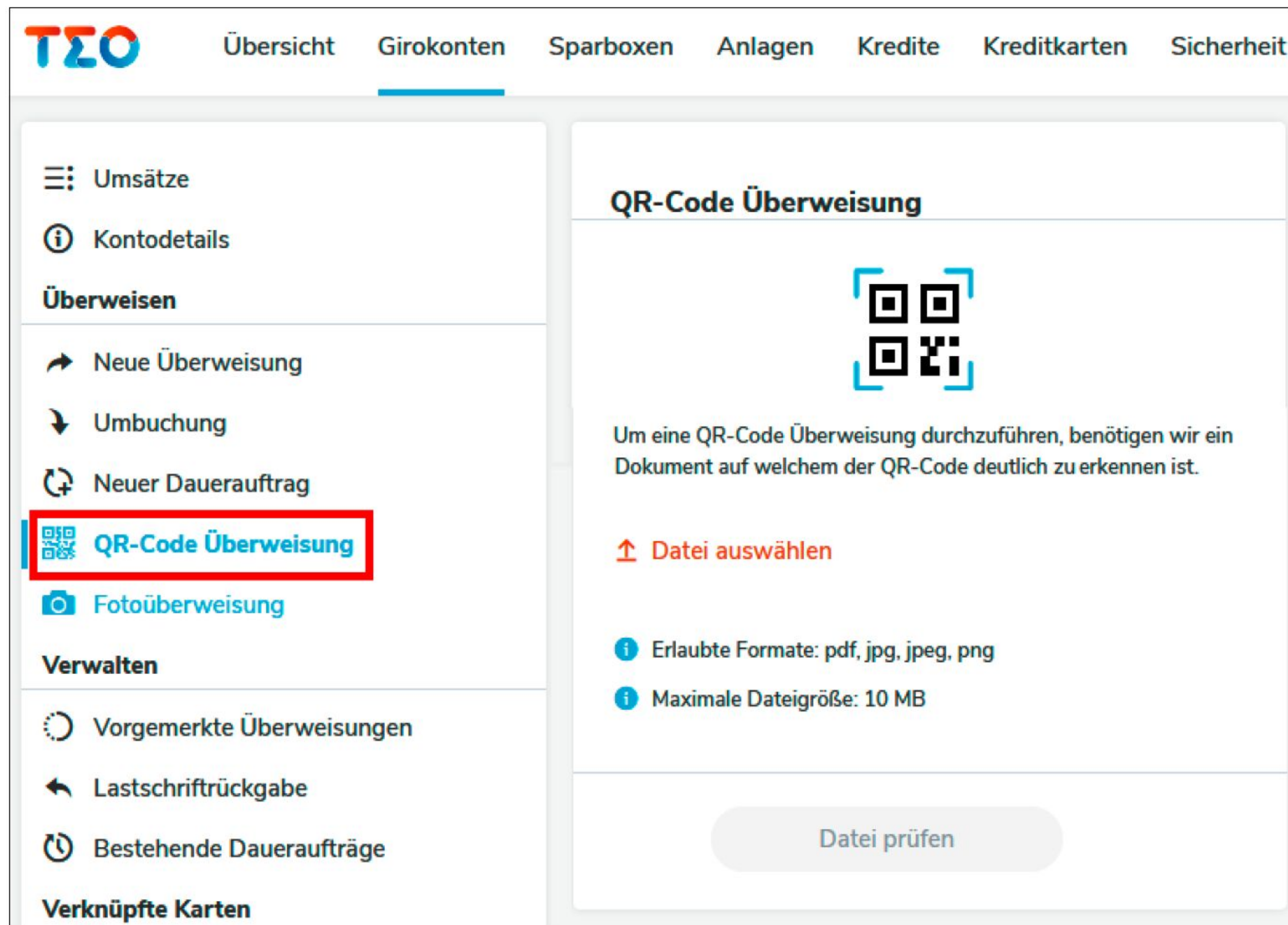
Wenn ein Onlineshop mit besonderen Schnäppchen wirbt oder gezielt Produkte anbietet, die anderswo gerade nicht erhältlich und lieferbar sind, ist besondere Vorsicht geboten. Denn bei dem vermeintlichen Händler könnte es sich um einen Fakeshop handeln. Also um einen Betrüger, der gar keine Ware hat und liefert, sondern nur auf das Geld seiner „Kunden“ aus ist.

Glücklicherweise lassen sich viele Fakeshops mittlerweile recht sicher erkennen. Zum einen über den „Fakeshop-Finder“ der Verbraucherzentralen (www.verbraucherzentrale.de/fakeshopfinder). Die Webseite zeigt in Sekundenschnelle, was Sie sonst mühsam selbst prüfen müssten: Stimmen die Angaben im Impressum, ist die Steuer-ID gültig, existiert der Eintrag im Handelsregister, wie lange gibt es die Webdomain bereits, sind die Prüfsiegel echt, und so weiter. Das alles erledigt der Fakeshop-Finder nach Eingabe der Shop-URL automatisch.

Typisch für Fakeshops ist zum Zweiten, dass sie bis zum letzten Bestellschritt mehrere Zahlungsweisen anbieten, dann aber plötzlich doch nur Vorkasse per Überweisung zur Verfügung steht. Mit dieser Bezahlvariante aber wäre Ihr Geld bei einem Fakeshop unwiderruflich weg! Unseren ausführlichen Ratgeber zum Thema lesen Sie unter www.pcwelt.de/1198323.

Heizel-schneller.com:

Eine schöne URL, jedoch ein Händler, der nicht existiert, wie der Check des Fakeshop-Finders der Verbraucherzentralen zeigt.



Rechnungen mit aufgedrucktem QR-Code lassen sich besonders bequem bezahlen, sämtliche Angaben zum Überweisen im Onlinebanking werden automatisch ausgefüllt.

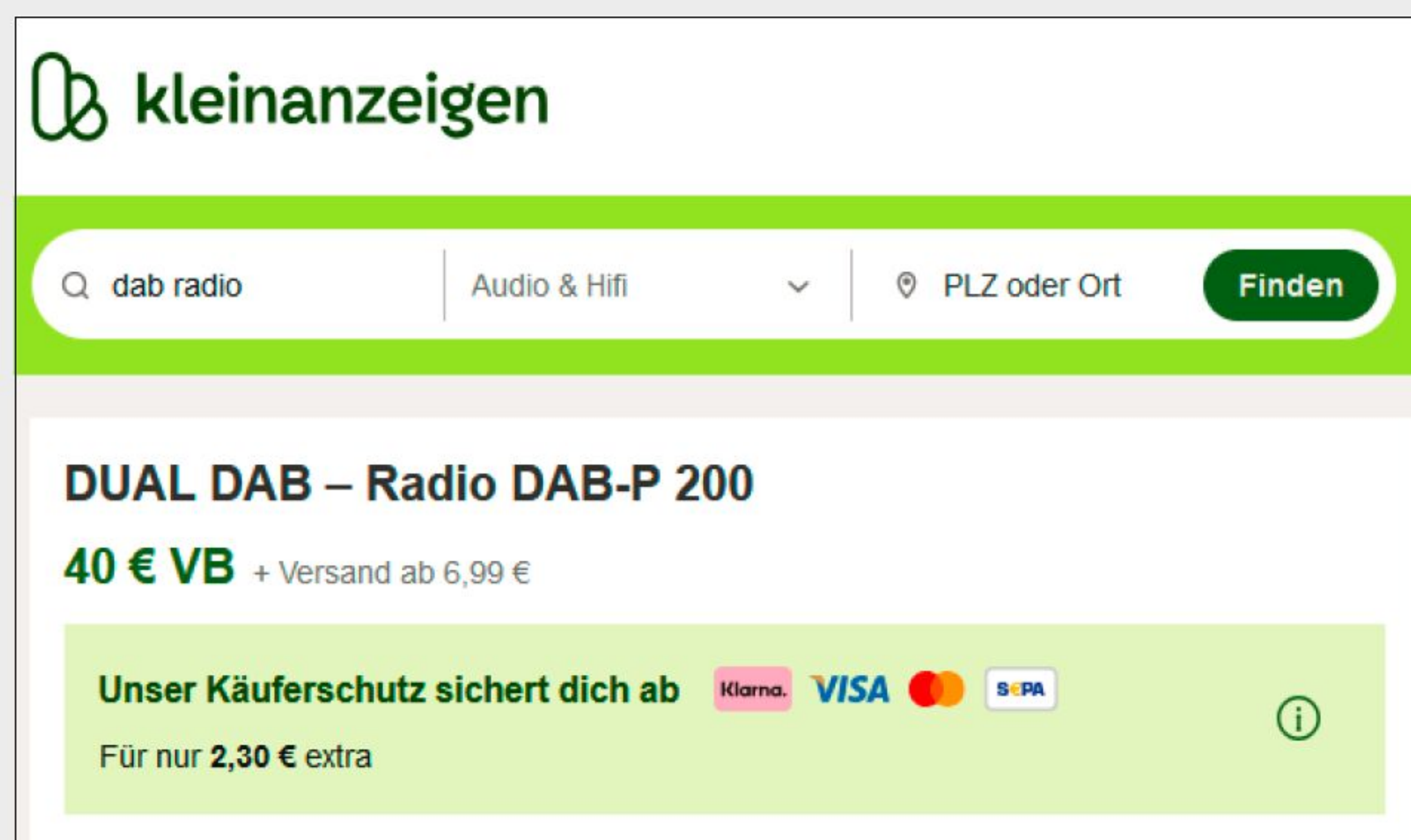
SICHER BEZAHLEN BEI PRIVATVERKÄUFEN

Die Frage, wie man Bezahlung und Versand privater Käufe und Verkäufe absichert, stellt sich auf Verkaufsplattformen wie Ebay, Kleinanzeigen.de, Vinted und Co. Denn auf vielen dieser Portale lassen sich Sachen anbieten, ohne dass die Identität der Beteiligten überprüft wird. Das macht das Verkaufen zwar besonders einfach, ruft gleichzeitig jedoch Betrüger auf den Plan.

Um die Abwicklung über das Internet auch beim Verschicken verlässlich zu machen, bieten immer mehr dieser Plattformen einen Käuferschutz: Gegen Zahlung einer Gebühr sichert der Portalbetreiber den Handel ab. Kleinanzeigen.de beispielsweise verlangt eine Pauschale von 50 Cent plus 4,5 Prozent des Verkaufspreises. Bei einem Verkaufspreis von 50 Euro muss der Käufer demnach 2,75 Euro extra zahlen. Voraussetzung für die Nutzung der häufig „Sicher bezahlen“ genannten Option ist allerdings, dass sich Käufer und Verkäufer über eine einmalige Identitätsprüfung authentifizieren.

Auch der Bezahlendienst Paypal sichert einen privaten Handel mit der Variante „Artikel oder Dienstleistung bezahlen“ gegen Gebühr ab. Die alternative Option „Geld an Freunde senden“ ist zwar kostenlos, das Geld im Betrugsfall jedoch weg.

Viele Internetverkaufsportale bieten gegen Gebühr die Möglichkeit, den Versand nach dem Bezahlen abzusichern. Für den Käuferschutz muss man sich einmalig registrieren.



kennen. Denn selbst ausgeführte Überweisungen lassen sich kaum rückgängig machen. Ein Risiko besteht insbesondere auch bei sogenannten Fakeshops, also (vermeintlichen) Onlinehändlern, die es tatsächlich gar nicht gibt. Während seriöse Händler in aller Regel mindestens eine alternative Zahlungsmethode anbieten, ist das bei Fakeshops nicht der Fall. Mehr zu diesem Thema lesen Sie im Kasten „Fakeshops sicher erkennen“.

Blättern Sie die Onlinebildergalerie mit den Zusammenfassungen des BSI einmal durch, der Text darunter enthält weitere Informationen zu den einzelnen Bezahlverfahren. Tipps, besonders Wichtiges und Vorsichtshinweise werden hier hervorgehoben. Deutlich ausführlicher ist die Broschüre „Sicher zahlen im E-Commerce“ mit FAQ, rechtlichen und technischen Hintergründen und vielem mehr (<https://tinyurl.com/yjz6j3wk>).

Verbraucherzentrale-Info zu Klarna und Barzahlung bei Abholung

Eine weitere empfehlenswerte Übersicht zu Onlinezahlungen bietet die Verbraucherzentrale NRW unter <https://tinyurl.com/2s4z7885>. Dort sehen Sie – ähnlich wie beim BSI – zu jeder Bezahloption eine kurze Beschreibung, ihre Vor- und Nachteile sowie weitere Hinweise und Tipps. Hervorzuheben ist hier die explizite Beschreibung der populären Bezahlendienstleister Klarna und Paypal.

Das Wichtigste zu diesen beiden Diensten sowie zur zunehmend verbreiteten Möglichkeit, online bestellte Ware im Geschäft abzuholen und dort zu bezahlen, fassen wir kurz zusammen. Oder wissen Sie auf Anhieb, ob es sich bei der Abholvariante um einen Onlinekauf mit zweiwöchigem Widerrufsrecht oder doch um einen Vor-Ort-Kauf handelt?

Klarna: Der schwedische Zahlungsdienst Klarna bietet Rechnungsbau, Ratenzahlung und Sofortüberweisung. Man kann also entscheiden, wie man bezahlen möchte. Hierzu ist ein Onlineaccount bei Klarna inklusive eines weiteren Passworts notwendig. Vor Betrug durch eine mögliche Accountübernahme schützt die in der EU inzwischen obligatorische Zwei-Faktor-Authentifizierung. Datenschützer kritisieren, dass Klarna die Kontenbewegungen der Kunden analysiere. Der Zahlungsdienstleister weist dies jedoch zurück.

Paypal: Der internationale Zahlungsabwickler ist auch deshalb so verbreitet, weil er einfach und zuverlässig funktioniert. Man loggt sich am Schluss des Bestellprozesses mit seinen Paypal-Zugangsdaten ein und zahlt, optional auch mittels Lastschrift oder Ratenzahlung. Paypal garantiert einen Käuferschutz für den Fall, dass bei der Lieferung etwas schiefgeht. Vor Betrug durch mögliche Accountübernahme schützt auch hier die Zwei-Faktor-Authentifizierung.

Bezahlung bei Abholung: Immer mehr Onlineshops mit Filialnetz bieten die Möglichkeit, im Internet bestellte Ware im Laden abzuholen und erst vor Ort zu bezahlen. So spart man mögliche Versandkosten und erhält die Ware zudem häufig schneller als über den Postweg. Beim Abholen zahlt man wie gewohnt an der Ladenkasse. Das 14-tägige Widerrufsrecht für Onlineeinkäufe gilt auch hier – es sei denn, man hat die Ware über das Internet nur unverbindlich reserviert.

Ergänzt wird die Übersicht der Verbraucherzentralen durch weitere Hinweise, unter anderem zu Gebühren. So dürfen Händler für die gängigen Bezahlverfahren Giro- und Kreditkarten, Überweisungen sowie Lastschriften keinerlei Gebühren verlangen. Anders verhält es sich bei Klarna oder Paypal, weil diese Dienste für die Onlineshops zusätzliche Leistungen wie etwa eine Bonitätsprüfung übernehmen. Weitere Infos zu Paypal und Klarna inklusive Käufer-schutz gibt es bei der Verbraucherzentrale Niedersachsen unter <https://tinyurl.com/4z34any9>.

Fazit: Stets abwägen, welche der Bezahloptionen am besten passt

Welche Bezahloption für Sie erste Wahl ist, müssen Sie letztlich selbst entscheiden. Die Rechnung ist die sicherste Variante, weil Sie erst bezahlen müssen, nachdem Sie die Ware erhalten haben. Auf der anderen Seite muss man ans Bezahlen denken und die Überweisungen zudem manuell ausführen. Wer es bequemer mag und ohnehin vorwiegend bei seinen angestammten Onlineshops kauft, wählt besser Kreditkarte oder Lastschrift/Bankeinzug.

Die völlig freie Wahl zwischen allen Varianten besteht meist ohnehin nicht, kaum ein Händler bietet sämtliche Bezahlverfahren an. Dann muss man eine der zur Verfügung stehenden Optionen wählen oder zu einem anderen Onlineshop wechseln. ■

verbraucherzentrale
Beratung
Bildung
Politik
Shop
Marktbeobachtung
Beschwerde einreichen

Bezahlen beim Online-Shopping: Vor- und Nachteile von Bezahl Diensten

Klarna

Zahlungszeitpunkt: nach Erhalt der Ware bei Rechnungskauf oder Ratenzahlung, vor Erhalt der Ware bei Sofortüberweisung

Wie zahlen Sie?
Klarna bietet den Kauf auf Rechnung, per Sofortüberweisung und per Ratenzahlung an.

Vorteile

- Die Ware wird schnell versendet.
- Sie können relativ flexibel entscheiden, wie Sie die Ware bezahlen möchten.

Nachteile

- Wenn Betrüger:innen Ihr Passwort bekommen, können sie, ohne Ihre Bankdaten zu kennen, einkaufen.
- Ratenzahlung wird als Kredit gewertet und kann sich negativ auf den Schufa-Eintrag auswirken.

Das haben andere Verbraucher:innen berichtet

- Verbraucher:innen berichten teils, dass sie beim Abschluss der Bestellung mit Klarna **versehentlich statt eines Rechnungskaufs, in eine Ratenzahlung gelangt sind**. Beides wird vom Anbieter im Zahlungsprozess als Option angeboten.

Achten Sie immer darauf, welche Optionen Sie angewählt haben. Kontaktieren Sie notfalls den Anbieter, um in eine andere Zahlungsmodalität zu wechseln.

- Betrüger:innen konnten mit dem Klarna-Passwort ungehindert bei Online-Shops einkaufen.

*Geben Sie Ihr Passwort nicht weiter, achten Sie auch auf unsere **Tipps zur Passwortsicherheit**.*

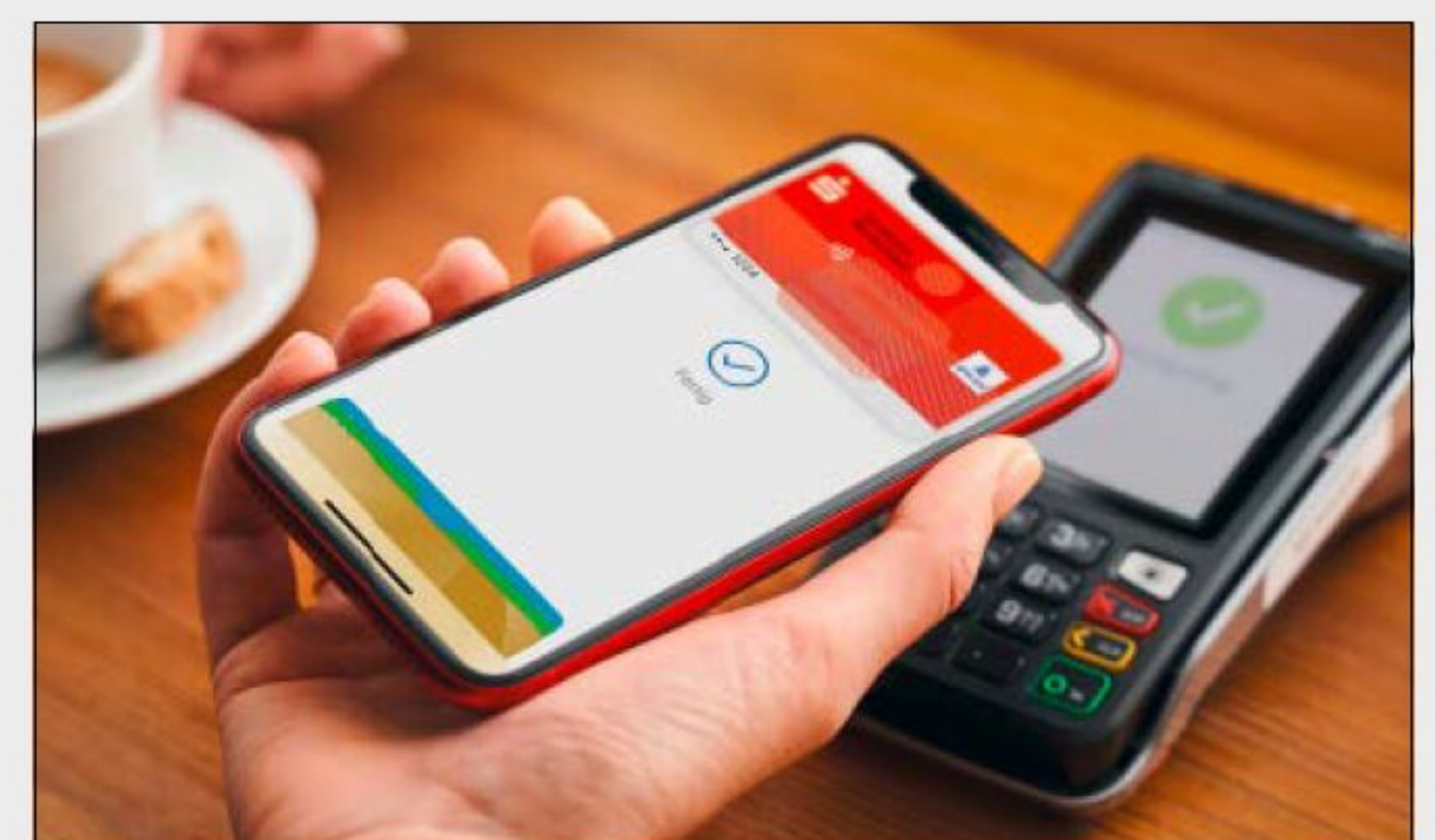
Wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) informieren auch die Verbraucherzentralen im Internet über die Vor- und Nachteile sowie mögliche Risiken, hier für den Bezahl Dienstleister Klarna.

SICHER MOBIL BEZAHLEN



Auch zum Bezahlen mit dem Smartphone gibt das Bundesamt für Sicherheit in der Informationstechnik Tipps. Das sollten Sie beim „Mobile Payment“ beachten:

- Installieren Sie die Bezahl-App nur über vertrauenswürdige Quellen, also aus einem bekannten Appstore. Automatische Updates stellen sicher, dass Sie stets die neueste App-Version nutzen.
- Verwenden Sie kein gerootetes beziehungsweise jailbreaktes Smartphone für Mobile Payment. Halten Sie auch das Betriebssystem Ihres Mobilgeräts immer auf dem aktuellen Stand.
- Verwenden Sie die Bildschirmsperre Ihres Gerätes mit PIN, Passwort, Fingerabdruck (Touch-ID) oder Gesichtserkennung (Face-ID).
- Machen Sie in der Bezahl-App nur die unbedingt erforderlichen Angaben, freiwillige Angaben erleichtern das Erstellen von Nutzerprofilen. Deaktivieren Sie zudem nicht benötigte Zusatzfunktionen in der App.
- Richten Sie wenn möglich eine automatische Sperre der App ein, die bei wiederholter Falscheingabe des Anmeldepassworts oder einer TAN weitere Eingabeversuche stoppt.
- Lassen Sie bei Verlust des Smartphones unverzüglich Ihre SIM-Karte und alle Zugänge zu Ihren hinterlegten Bankkonten und -karten sperren.
- Überprüfen Sie regelmäßig alle Kontobewegungen und informieren Sie Ihre Bank, wenn Ihnen etwas auffällig erscheint.



Bezahlen mit dem Smartphone ist inzwischen weitverbreitet. Einige grundlegende Dinge sollte man jedoch beachten, damit „Mobile Payment“ auch sicher ist.



Vorsicht: Neue KI-Tricks beim Phishing

Kriminelle greifen zunehmend auf KI-Tools zurück, um ihre Phishing-Mails zu perfektionieren. Nicht nur die Texte sind KI-generiert, auch die Absenderadressen werden von der KI auf den Empfänger zugeschnitten. Und angehängte PC-Viren erzeugt die KI ebenfalls.

VON ROLAND FREIST

Im Februar 2025 warnten mehrere Medien vor einer neuen Bedrohung, die sich gegen Nutzer von Googles E-Mail-Dienst Gmail richtete. Angreifer verwendeten KI-Technik, um Phishing-Mails zu perfektionieren und überzeugender wirken zu lassen. Dazu sammelte die KI im Internet frei verfügbare Daten aus sozialen Netzwerken, von Websites und Onlineforen und formulierte anhand dieser Informationen eine täuschend echt aussehende E-Mail, die vorgab, von einem Bekannten, Familienmitglied oder Vorgesetzten zu stam-

men. Mehr noch: Damit die Nachricht auch tatsächlich täuschend echt aussah, generierte die KI auch gleich noch passende Domains als Absender für die Mails. Die Masche wurde „Deepfish“ getauft – ein Kofferwort aus den Begriffen Deep Learning und Phishing.

Auch wenn die anfangs erwähnte Meldung einige Fragen aufwirft – etwa warum insbesondere Gmail-Nutzer von dem Deepfish-Angriff betroffen waren –, macht sie doch eine Entwicklung deutlich, mit der Experten schon länger gerechnet hatten. Kriminelle Gruppen nutzen zunehmend KI-Werkzeuge, um ihre Angriffe zu perfektionieren.

Mit KI erzeugte Domains

Einer der Schwachpunkte herkömmlicher Phishing-Attacken war immer schon die Absenderadresse. Die meisten Phishing-Mails lassen sich einfach über den Absender identifizieren. Wenn etwa eine Nachricht von einem Streamingdienst wie Netflix oder Disney+ mit einer Adresse wie

andy@brandbot.com versehen ist, handelt es sich mit Sicherheit um eine Fälschung – ganz gleich, wie perfekt die sonstige Aufmachung auch sein mag. In der KI-unterstützten Variante eines Phishing-Angriffs kommen hingegen neuartige Algorithmen zum Einsatz, die eine an den Text der E-Mail angepasste Absenderadresse mit einer passenden URL erzeugen.

Wie wirksam diese Algorithmen sein können, untersuchte eine Forschungsgruppe um Alejandro Correa Bahnsen bei der US-Firma Cyxtera Technologies, einem Betreiber von Rechenzentren. Sie entwickelten einen Algorithmus namens Deepfish, der darauf trainiert wurde, passende URLs für Phishing-Attacken vorzuschlagen. Dazu fütterten sie ein neuronales Netzwerk mit mehr als einer Million URLs, die in der Vergangenheit für das Phishing per E-Mail eingerichtet wurden, und trainierten damit ihren Algorithmus. Dabei gaben sie zwei unterschiedliche Profile für die Akteure hinter der Phishing-Attacke vor.

„Künstliche Intelligenz erstellt täuschend echte Phishing-Mails.“

Mit den per KI erzeugten Adressen erreichten sie bei dem einen Profil eine Effizienzsteigerung der Angriffe von 0,69 auf 20,9 Prozent, bei dem anderen von 4,91 auf 36,28 Prozent. Ihre Ergebnisse veröffentlichten sie in einer englischsprachigen Studie, die sich unter der Adresse <https://tinyurl.com/27xzmtve> kostenlos herunterladen lässt.

Während Deepphish ursprünglich lediglich den bei Cyxtera entwickelten Algorithmus bezeichnete, wird er heute in den meisten Fällen ganz allgemein für KI-gestützte Phishing-Angriffe benutzt.

Wie eine Deepphish-Attacke abläuft

Deepphish-Angriffe folgen einem einheitlichen Muster. In einem ersten Schritt wird das soziale Umfeld der Zielperson erforscht: Wo lebt sie, wo arbeitet sie, wie heißen die Mitglieder ihrer Familie, ihre Freunde, ihre Kollegen und Vorgesetzten? Wie lauten deren E-Mail-Adressen, wie nah stehen sie der Zielperson? Als Quellen nutzt die KI soziale Netzwerke und Onlineforen, aber auch die von Hackern veröffentlichten Daten aus Einbrüchen in Firmennetzwerke und Websites. Je mehr Daten auf diese Weise zusammenkommen, desto präziser kann die Phishing-Mail auf das Opfer zugeschnitten werden.

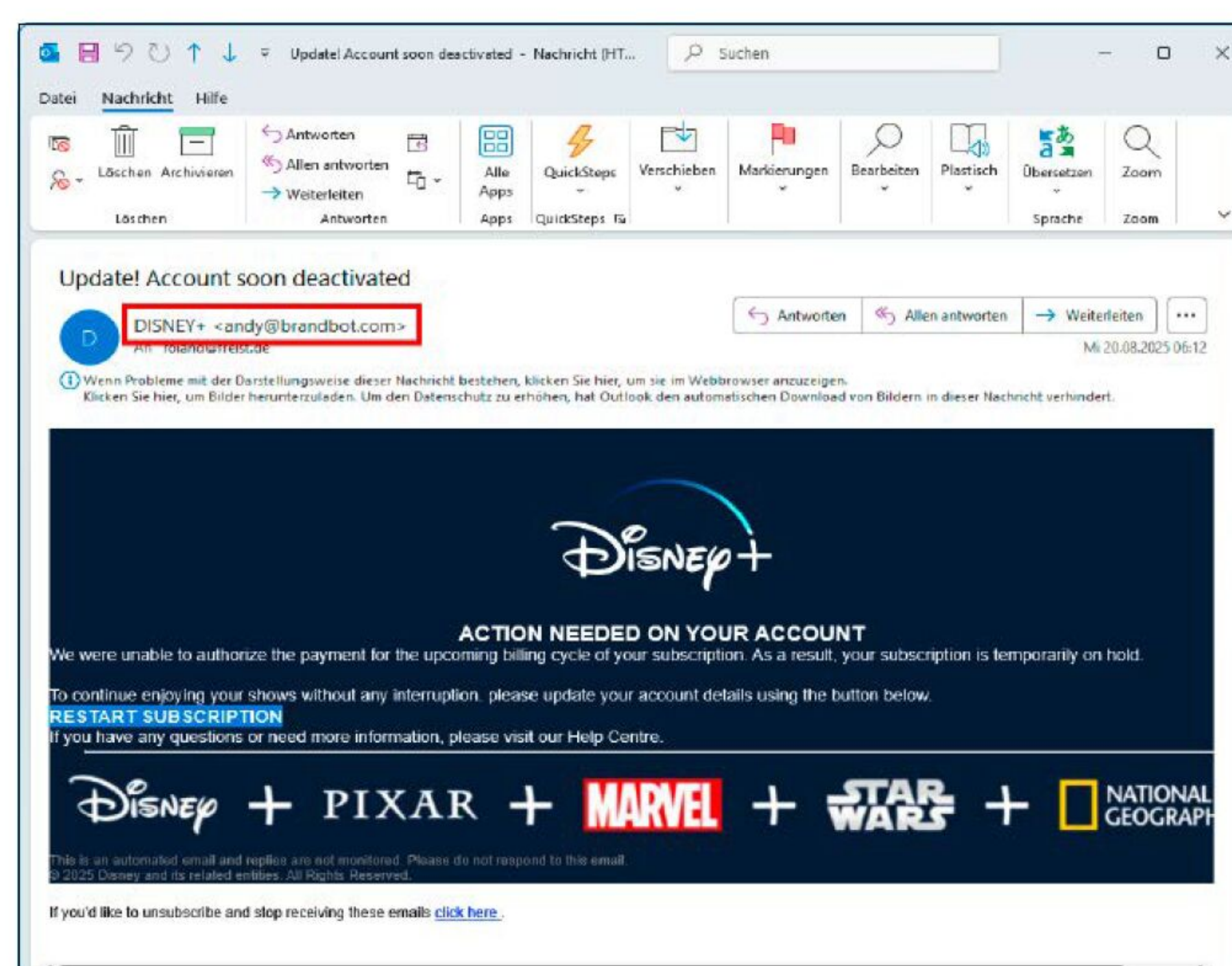
Es folgt die Anmeldung einer passenden Domain und die Generierung einer Absenderadresse mit einem Algorithmus wie Deepphish. Anschließend schreibt die KI den Text der Mail. Mit den gesammelten Informationen erzeugt sie eine passende Betreffzeile, eine auf den Empfänger abgestimmte Anrede sowie einen Inhalt, der fehlerfrei formuliert ist und tatsächlich von dem angeblichen Absender geschrieben sein könnte. Aufgrund der präzisen Personalisierung wirkt die Nachricht erheblich glaubwürdiger als eine übliche Phishing-Mail.

Was aber wollen die Kriminellen mit ihren Deepphish-Attacken erreichen? Sie wollen mit ihren Fälschungen so viel Vertrauen erwecken, dass der Empfänger bereit ist, auf einen Dateianhang oder einen eingebetteten Link zu klicken. Alles Weitere geschieht automatisch: Der Dateianhang lädt dann meist eine Schadsoftware nach und installiert sie. Der Link dagegen führt auf eine ebenfalls gefälschte Website, auf der beispielsweise Kreditkartendaten oder Anmeldeinformationen für einen Streamingdienst abgefragt werden.

Auch www.pcwelt.de berichtete im Februar 2025 über eine von KI unterstützte Phishing-Attacke auf Gmail-Benutzer.



Phishing-Mails lassen sich häufig an den Absenderadressen erkennen. Wenn wie in diesem Fall eine angeblich von Disney+ stammende Nachricht von andy@brandbot.com kommt, stimmt etwas nicht.



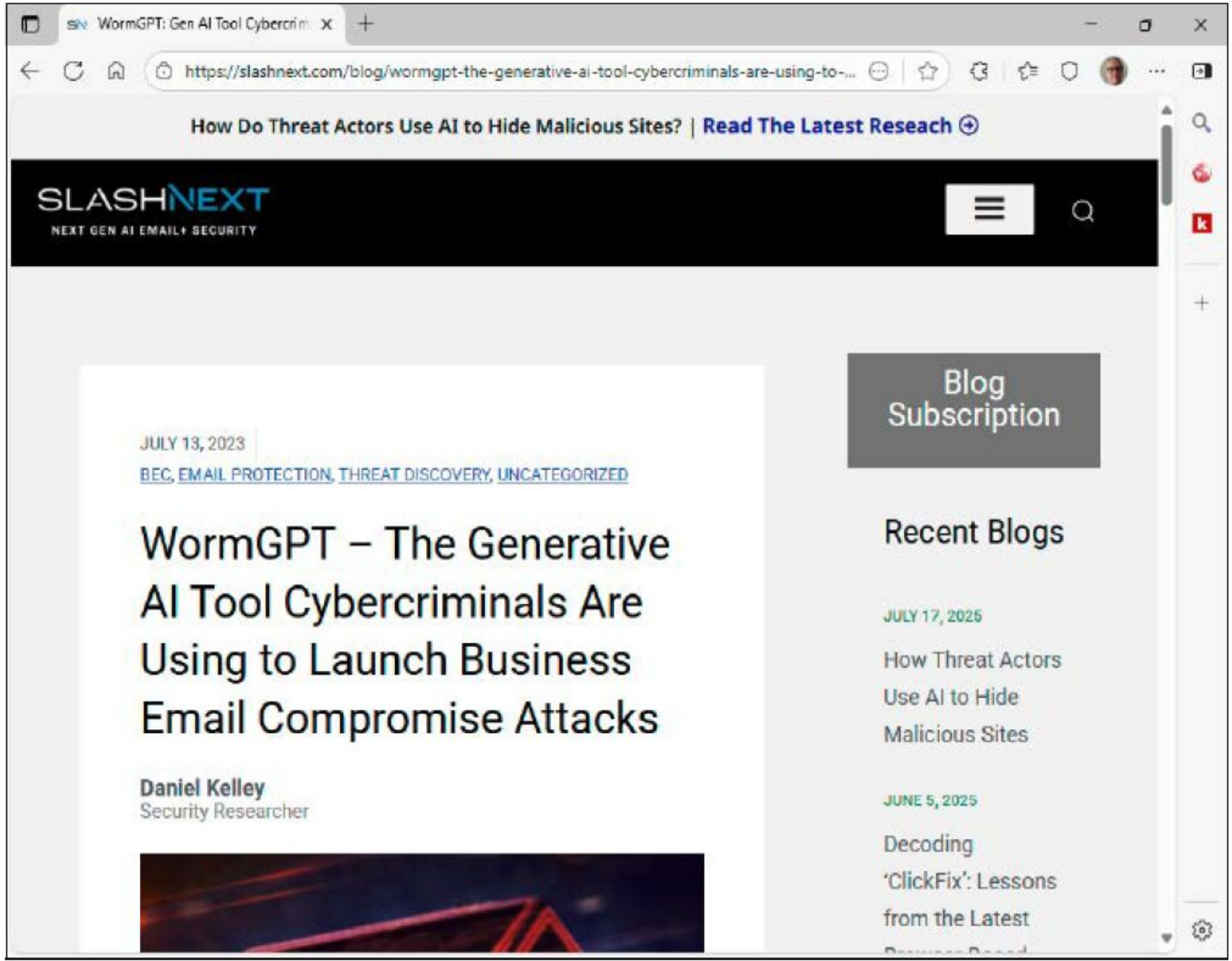
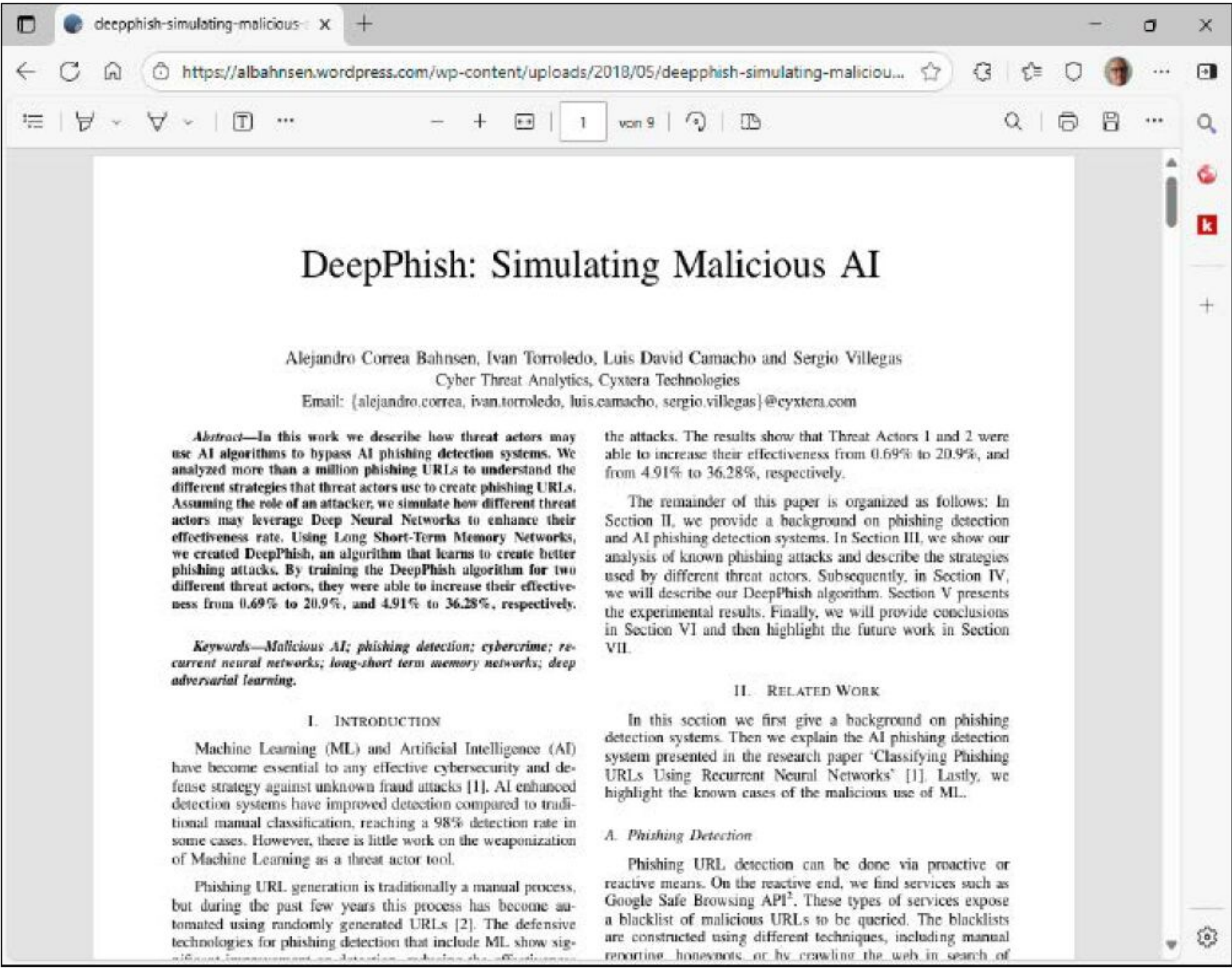
KI-gestützte Phishing-Mails

Der Deepphish-Algorithmus ist allerdings erst der Anfang. Mittlerweile existiert eine ganze Reihe von Tools, die den Kriminellen die gesamte Arbeit beim Formulieren von Phishing-Nachrichten abnehmen. Die Programme heißen FraudGPT, WormGPT oder GhostGPT. Sie formulieren Phishing-Mails, die sich gezielt gegen einzelne Personen oder bestimmte Unternehmen richten. Der Benutzer kann diese Programme beispielsweise anweisen, eine E-Mail im Stil von Netflix mit einer Aufforderung zur Eingabe von Kontodaten auf einer gefälschten Website zu erzeugen. Oder er kann sich Fragen beantworten lassen wie etwa „Wie hacke ich ein WLAN-Passwort?“. Oder er gibt der KI die Anweisung, einen Software-Keylogger zu programmieren, der sämtliche Tastatureingaben auf einem Computer übers Internet an eine Serveradresse weiterleitet.

ChatGPT und andere Large Language Models (LLMs) besitzen eingebaute Filter, so dass sie auf solche und ähnliche Anfragen keine Antwort geben. Da ChatGPT seinen Code nicht offenlegt, lässt sich daran auch nichts ändern. Allerdings ist es mit Anleitungen aus dem Darknet möglich, über bestimmte Prompt-Folgen LLMs wie ChatGPT so zu verwirren, dass sie anschließend bereit sind, ihre eingebauten Filter zu missachten. Parallel dazu sind einige kriminelle Gruppen auf LLMs aus der Open-Source-Szene ausgewichen und haben dort die entsprechenden Filter entfernt.

KI erzeugt Schadprogramme

Wie weit die Möglichkeiten KI-generierter Schadprogramme bereits gehen, demonstriert die Website Stopwatch AI (<https://stopwatcha.io>). Sie zeigt, wie man mit KI in drei einfachen Schritten eine Malware program-



Für eine Studie erforschten Mitarbeiter der Firma Cyxtera, wie sich durch die Auswahl einer mit KI generierten Absenderadresse die Erfolgsquote bei Phishing-Mails erhöhen lässt.

Hacking-Tools wie WormGPT nutzen KI, um überzeugend aussehende und formulierte Phishing-Mails zu erzeugen. Sie zielen in den meisten Fällen auf bestimmte Personen oder Unternehmen ab.

mieren kann, die ganz gezielt den Schutzschirm der großen Antivirentools unterläuft. Im ersten Schritt namens „Choose Platform“ wählt man das Betriebssystem des Computers, den man angreifen will. Zur Auswahl stehen Mac, Windows, Linux, AWS (Amazon

Web Services, der Clouddienst von Amazon), Google Cloud und Microsoft Azure, der professionelle Clouddienst von Microsoft. Der zweite Schritt heißt „Choose Defense“ und bietet neun Antivirentools an, darunter den Microsoft Defender, Eset Endpoint Pro-

tection Advanced, McAfee Endpoint Security, Symantec Endpoint Security und Kaspersky Endpoint Security for Business. Im dritten Schritt „Choose Attack“ gibt man an, welche Art von Virus man erzeugen will. Die Auswahl reicht von Adware und Spyware über Ransomware und Keylogging bis hin zu Data Exfiltration, also zum Datenklau. Nach dem Klick auf eine Angriffsform verlangt Stopwatch AI nach den Log-in-Daten. Eine Registrierung bei der Site ist mit einem Google-, Github- und einem Microsoft-Konto möglich. Sobald die Anmeldung erledigt ist, beginnt die KI mit der Programmierung der gewünschten Malware. Um die Site benutzen zu dürfen, muss der Benutzer den Nutzungsbedingungen zustimmen, die einen Angriff gegen andere Systeme ausschließen. Denn Stopwatch AI ist lediglich zum Studium der Malware-Entwicklung mit KI gedacht. Und: Sämtliche Projekte werden dem jeweiligen Benutzer zugeordnet und gespeichert.

AN DIESEN MERKMALEN ERKENNEN SIE KI-GENERIERTE PHISHING-MAILS



Werfen Sie bei eingehenden E-Mails immer einen Blick auf die Absenderadresse und überlegen Sie, ob sie plausibel ist. Achten Sie darüber hinaus auf folgende Merkmale:

- Werden Sie vorsichtig bei E-Mails von Personen, mit denen Sie normalerweise nicht in Kontakt stehen oder von denen Sie längere Zeit nichts gehört haben. Das gilt vor allem dann, wenn diese Nachrichten ungewöhnliche Bitten oder Anfragen an Sie richten.
- Fahren Sie mit der Maus über enthaltene Links und überprüfen Sie, wohin sie führen. Passt die Adresse nicht zum Absender der E-Mail oder zum Text der Nachricht, handelt es sich häufig um einen Betrugsversuch.
- Keine Bank, kein Streamingdienst und keine Behörde fragt jemals Ihr Passwort ab oder will per E-Mail Ihre Kontodaten wissen.
- Werden Sie misstrauisch bei E-Mails, die Sie unter Zeitdruck setzen oder eine hohe Dringlichkeit behaupten.

POP-Kontoeinstellungen
roland@freist.de

Allgemeine Einstellungen

Ihr Name

Kontoname

Beispiel: "Geschäftlich-" oder "Microsoft-Konto"

Antwortadresse

Organisation

E-Mail-Einstellungen

☒ Eine Kopie der Nachrichten auf dem Server belassen

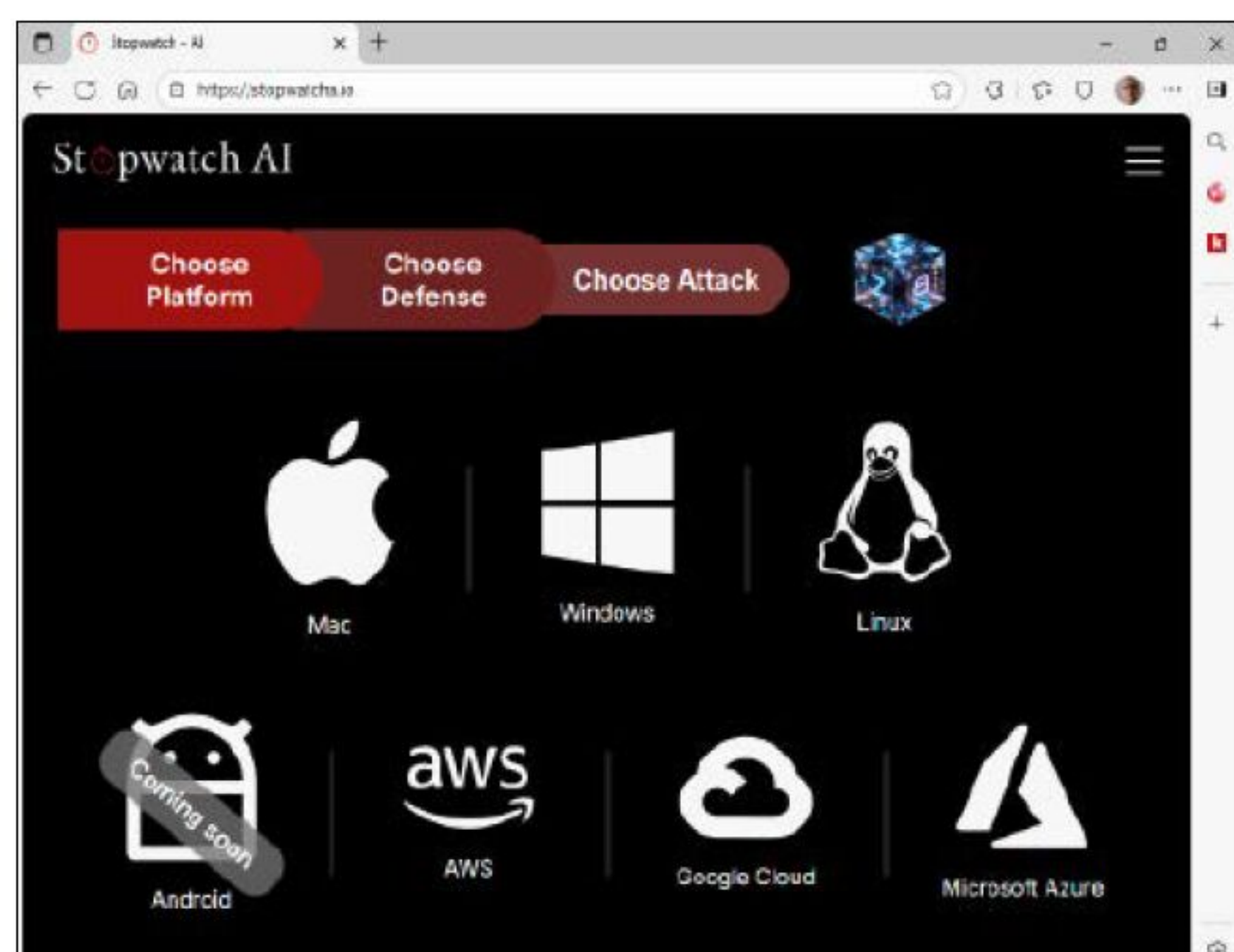
☒ Vom Server entfernen nach Tagen entfernen

☐ Vom Server entfernen, wenn aus "Gelöschte Elemente" gelöscht

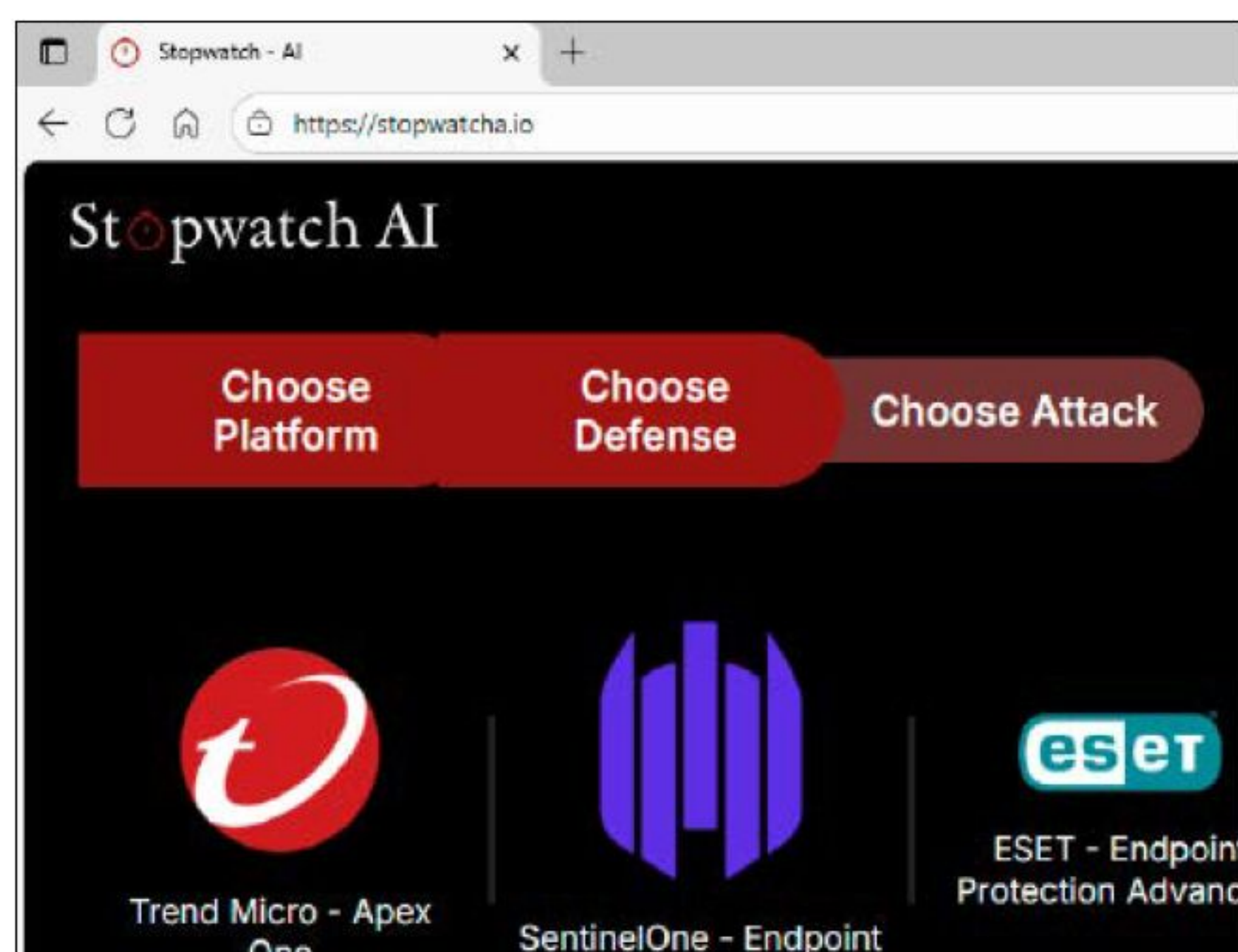
In den Kontoeinstellungen von E-Mail-Programmen lassen sich in vielen Fällen der angezeigte Name sowie die Antwortadresse ändern. Die Domain des Absenders ist allerdings fest.

Mit KI Antivirentools austricksen

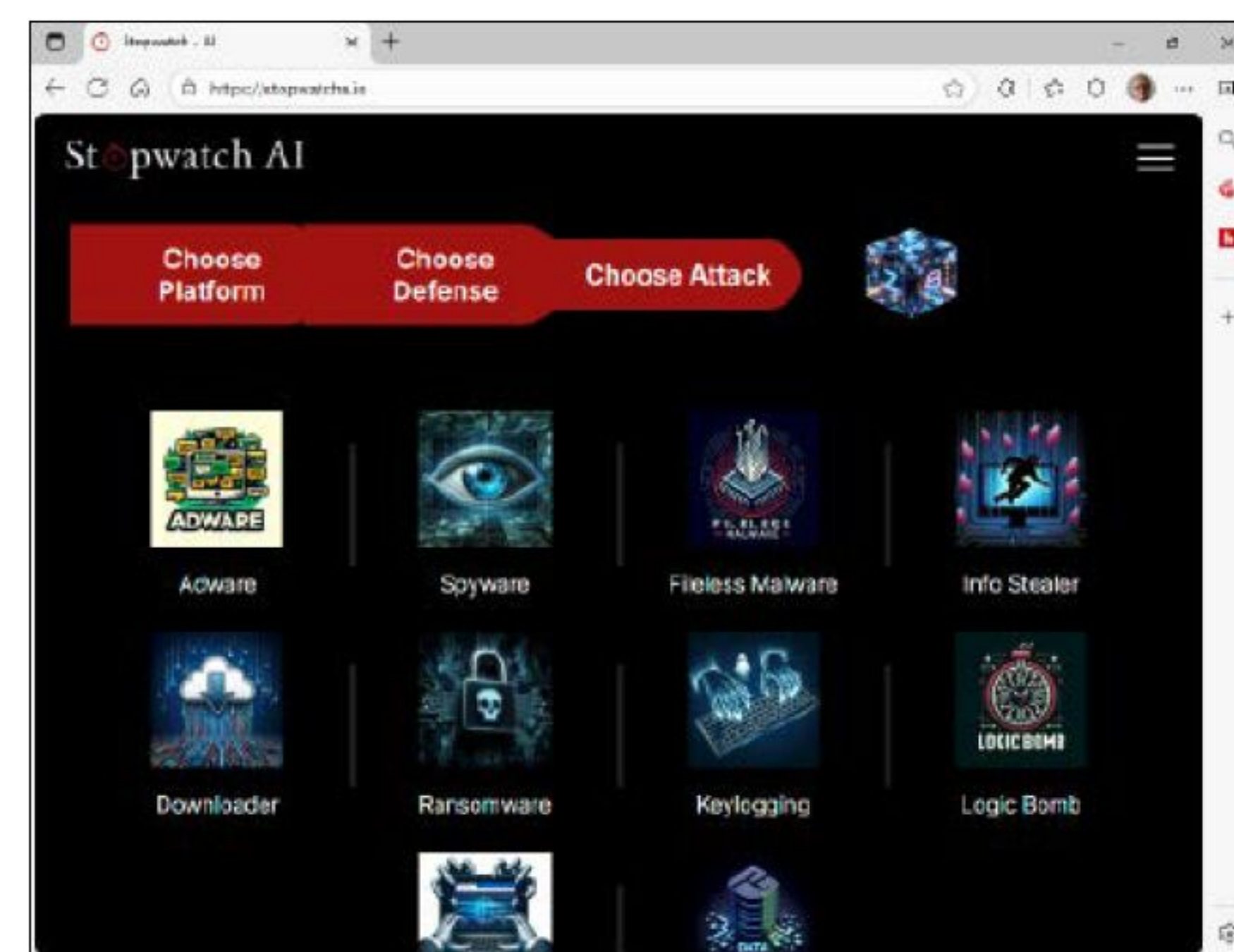
Jedes Antivirenprogramm lädt jeden Tag mindestens einmal die neuesten Virendefinitionen vom Server des Herstellers herunter. Sie beschreiben die Eigenschaften der in den letzten Stunden neu entdeckten Malware-Varianten, sodass die Software auf den Rechnern der Anwender die Schadprogramme zuverlässig erkennen kann. Dieser Schutzschirm ist jedoch immer löchriger geworden. Grund: Bereits seit Jahrzehnten kursieren im Darknet – aber



Die Website Stopwatch AI demonstriert, wie sich mithilfe von KI-Tools in wenigen Handgriffen eine Schadsoftware programmieren lässt. Am Anfang steht die Auswahl des Betriebssystems, das angegriffen werden soll.



Im zweiten Schritt wählt der Benutzer bei Stopwatch AI das Antivirenprogramm aus, dessen Schwächen er mit seinem Malware-Angriff ausnutzen will. Auch der Microsoft Defender ist hier aufgelistet.

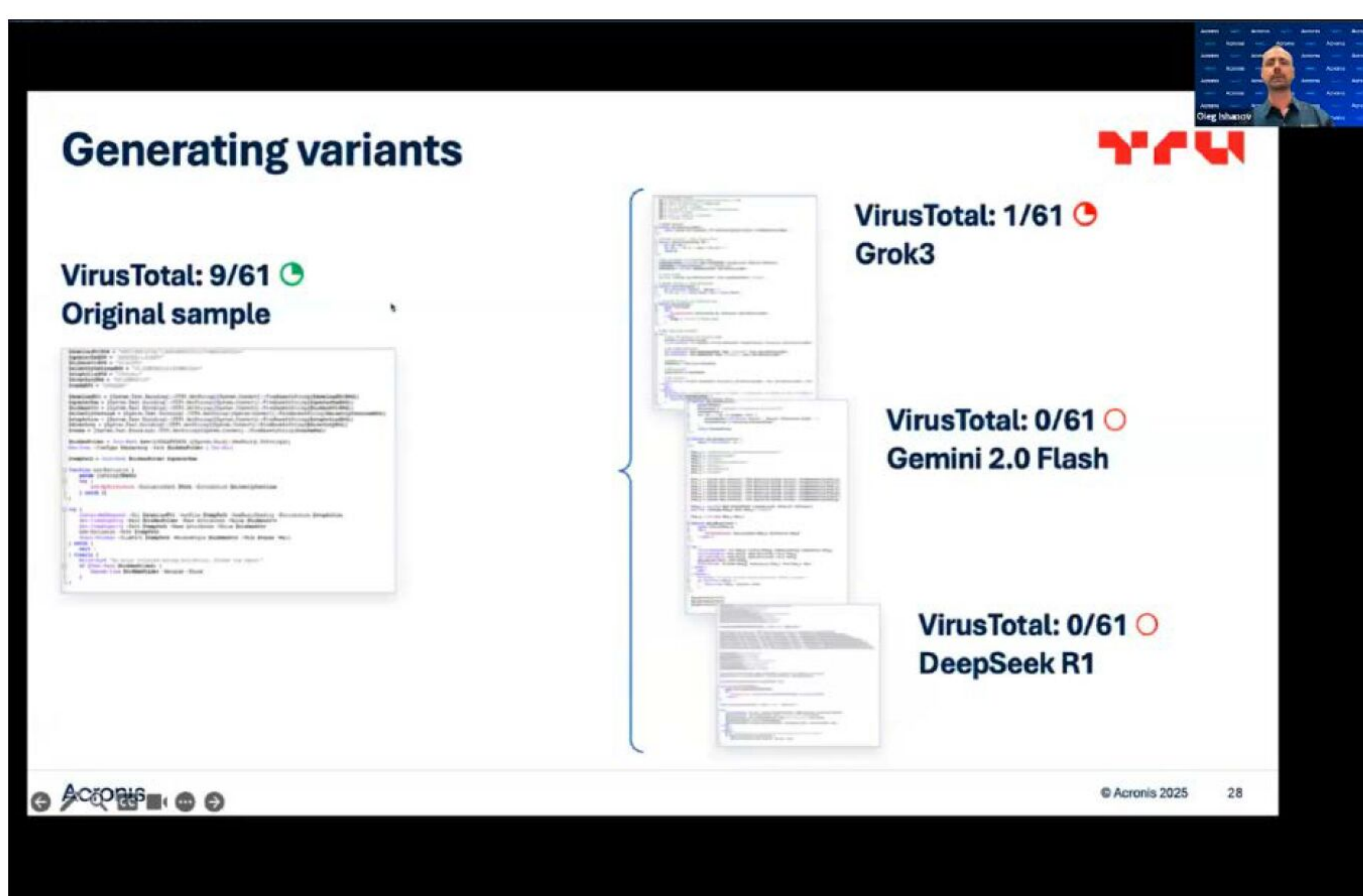


Stopwatch AI bietet zehn verschiedene Malware-Arten an, vom Keylogger bis hin zur Ransomware. Für die Umsetzung der gewählten Schadsoftware muss sich der Benutzer registrieren.

nicht nur dort – Virenbaukästen, die es Hobbyprogrammierern auch ohne KI erlauben, funktionierende Malware zu erzeugen. Viele dieser Schadprogramme sind einfach nur minimal veränderte Varianten bereits altbekannter Viren. Der Autor muss oft nur die Signatur ändern, damit seine Malware als neuer Virus gezählt wird. Nur so ist es zu erklären, dass die Antivirenhersteller pro Tag 560.000 neue Schädlinge melden.

Im KI-Zeitalter hat die Produktion von Malware-Varianten eine neue Qualität bekommen. Denn die Security-Hersteller hatten ihren Antivirenprogrammen beigebracht, die Varianten bereits bekannter Schadsoftware zu erkennen und zu isolieren. Mit KI-Unterstützung ist es nun möglich, eine bestehende Malware gezielt so zu manipulieren, dass sie von den Virenwächtern nicht mehr erkannt wird.

Der Toolhersteller Acronis demonstrierte das in einer Präsentation an einem Malware-Sample, das er bei Googles Erkennungsdienst Virustotal (www.virustotal.com) hochgeladen hatte. Während es anfangs noch von neun der dort eingesetzten Antivirenprogramme als Schädling erkannt wurde, konnte nach der Überarbeitung durch die KI von Grok3 nur noch ein Virenwächter die Schadsoftware als solche identifizieren. Als die Forscher den Code des Samples durch Gemini 2.0 Flash und Deepseek R1 bearbeiten ließen, wurde der Virus anschließend von keinem der Programme bei Virustotal mehr erkannt. Immerhin: Die heuristischen und verhaltensbasierten Methoden der Antivirenprogramme funktionieren auch bei Schadsoftware, deren Code mithilfe von KI verändert wurde. ■



Je nachdem, welche KI-Software eingesetzt wird, kann der Hacker bestehende Schadprogramme so manipulieren, dass sie bei Virustotal nahezu oder sogar komplett unentdeckt bleiben.

E-MAIL-SPOOFING



Das Fälschen von E-Mail-Adressen, das sogenannte E-Mail-Spoofing, kommt heute kaum noch vor. Seit 2014 wurden nach und nach die Authentifizierungs-Verfahren SPF, DKIM und DMARC als Standards definiert und anschließend von den E-Mail-Providern eingesetzt. Seither ist es nicht mehr möglich, die Angabe der Domain in einer E-Mail-Adresse zu fälschen. Bei einer Adresse wie *magazin@pcwelt.de* ist die Domain beispielsweise *pcwelt.de*. Sind die genannten Authentifizierungs-Verfahren bei einem Provider deaktiviert, so werden diese Mails beim Empfänger normalerweise als Spam aussortiert.

Spoofing-Versuche gibt es trotzdem noch. So lässt sich in vielen E-Mail-Clients der Absendername ändern, im klassischen Outlook etwa über „Datei → Kontoeinstellungen → Kontoeinstellungen → Ändern → Ihr Name“. Die Angabe der E-Mail-Adresse bleibt davon jedoch unberührt. Bei Hacker-Attacken wird an gleicher Stelle teilweise die Antwortadresse geändert. Auf diese Weise gehen alle Antworten auf die versendeten Mails an die Adresse des Hackers. Ein anderer Trick ist, eine ähnlich aussehende Domain zu verwenden, etwa *magazin@pswelt.de*.

Betrug bei Kleinanzeigen

Die populäre Plattform für private Angebote zieht auch Kriminelle an. Sie haben mehrere Tricks und Maschinen entwickelt, wie sie Käufer und Verkäufer um ihr Geld oder auch ihre Ware bringen können.

VON ROLAND FREIST

Die Site Kleinanzeigen (www.kleinanzeigen.de) ist bereits seit Jahren ein höchst erfolgreiches Portal für den Kauf und Verkauf von gebrauchten, teilweise auch neuen Waren aller Art. Notebooks, Smartphones, Möbel, Kleidung, Bücher, sogar Autos und Wohnungen – hier wird alles gehandelt. Obwohl es mittlerweile mehr als ein halbes Dutzend Alternativen gibt, zu nennen sind vor allem Quoka, Facebook Marketplace, Shpock oder Markt.de, ist Kleinanzeigen.de der unbestrittene Marktführer und bietet eine riesige Auswahl.

Kein Wunder also, dass sich bereits seit Jahren auch Betrüger für die Site interessieren. Sie haben im Laufe der Zeit eine ganze Reihe von Methoden entwickelt, um sowohl Käufer als auch Verkäufer übers Ohr zu hauen und sie um ihr Geld zu bringen. Die Verbraucherschutzzentralen und



die Polizei berichten immer wieder über neue Betrugsmaschinen. Wir stellen Ihnen einige Beispiele aus den letzten Monaten vor und erklären, wie Sie sie erkennen und die Fallen vermeiden.

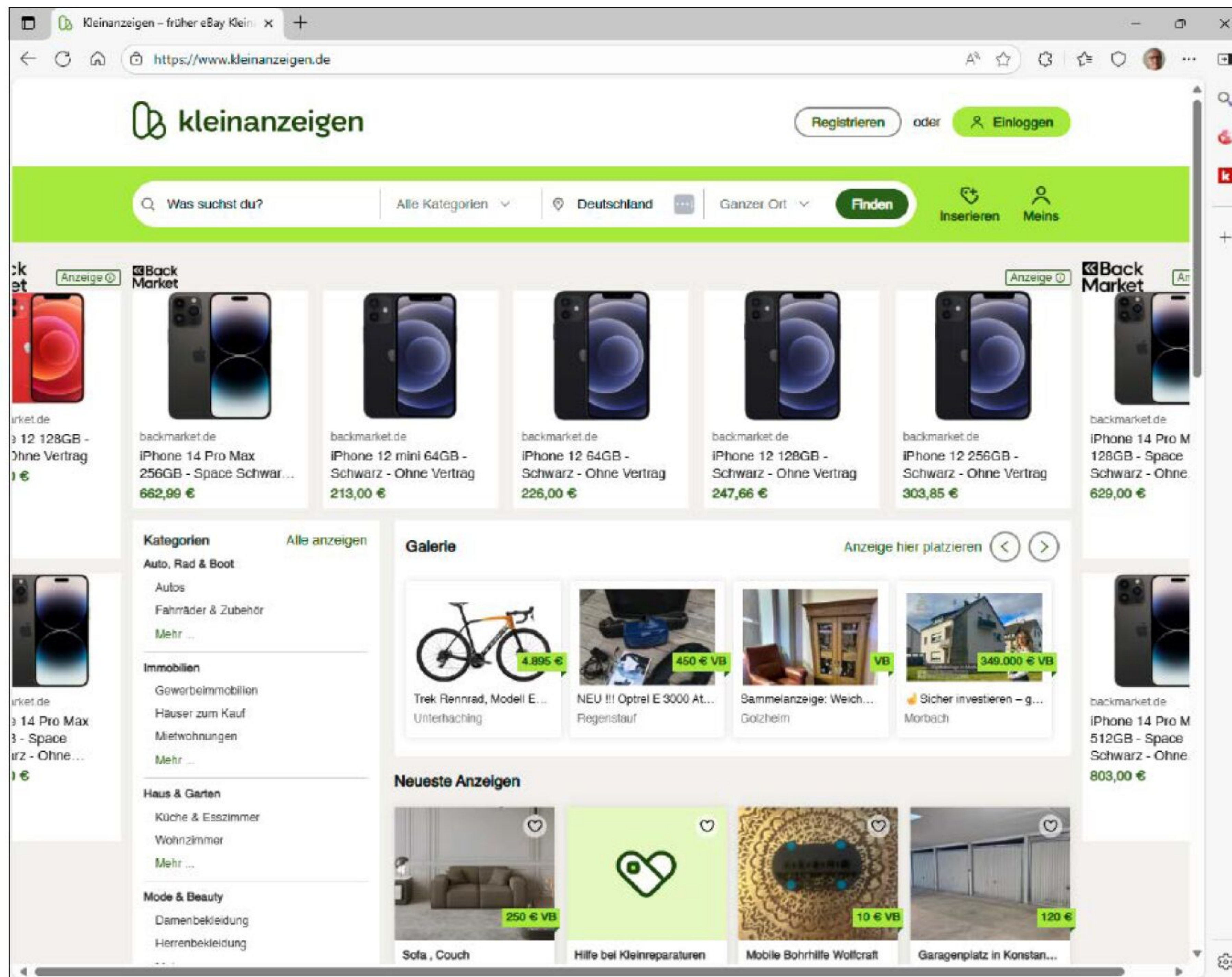
Gefangen in der Support-Schleife

Die Banken beobachten in den letzten Jahren eine Zunahme von Fällen, in denen ihre Kunden bei Verkäufen auf der Kleinanzeigen-Plattform zu Überweisungen auf die Konten von Kriminellen überredet wurden. Der Trick geht folgendermaßen: Stellen Sie sich vor, Sie bieten eine Ware auf Kleinanzeigen an und erhalten eine Whatsapp-Nachricht von einem interessierten Kunden. Er bestellt die Ware und schreibt Ihnen, dass er das Geld bereits auf Ihr Kleinanzeigen-Konto überwiesen habe. Dann fragt er nach, ob Sie schon eine Benachrichtigung von Kleinanzeigen über den Geldeingang erhalten haben. Wenn Sie verneinen, weist Sie der vermeintliche Käufer auf den Chatsupport von Kleinanzeigen. Sie bekommen dann eine Nachricht, die angeblich vom Support von Kleinanzeigen stammt

und das Logo der Plattform zeigt. Darin enthalten ist ein Link in Form eines Buttons. Sobald Sie ihn anklicken, werden Sie auf eine gefälschte Support-Website mit einem Chatprogramm geführt.

Dort wartet ein angeblicher Kleinanzeigen-Mitarbeiter auf Sie. Er behauptet, er brauche die Daten Ihres Bankkontos, um das Problem mit der nicht eingegangenen Überweisung zu klären. Sobald der Betrüger die Daten hat, loggt er sich in Ihr Konto ein und legt eine Überweisung an. Jetzt erklärt er Ihnen, dass er für die Bestätigung der Gültigkeit Ihres Kontos eine TAN von Ihnen benötige. Sie fordern im Browser eine TAN an und schicken sie ihm per Chat. Hat nicht funktioniert, behauptet er, bitte noch mal. Und jedes Mal, wenn Sie ihm wieder eine neue TAN übermitteln, führt er eine Überweisung auf sein eigenes Konto aus. Da Sie selbst auch in Ihr Konto eingeloggt sind, sehen Sie seine Überweisungen. Doch er erklärt Ihnen, das werde alles später korrigiert. Zunächst einmal müsse er das Problem mit der nicht eingegangenen Zahlung lösen.

„Wer auf Kleinanzeigen & Co. handelt, muss äußerst misstrauisch sein. Sonst droht der Trickbetrug.“



Auf dem Portal Kleinanzeigen wird nahezu alles gehandelt, von Smartphones über Fahrräder und Sofas bis hin zu kompletten Häusern. Auch Dienstleistungen werden hier angeboten.

Wichtig: Kein Support wird Sie jemals zur Übermittlung Ihrer Kontodaten plus TAN auffordern. Wenn Sie auf diesen Trick hereingefallen sind, sollten Sie sofort Ihre Bank kontaktieren und versuchen, die Überweisungen zu stoppen und das Geld zurückzuholen. Machen Sie Screenshots vom Chatverlauf und der gefälschten Website, erstatten Sie Anzeige bei der Polizei und legen Sie die Bilder als Beweismaterial vor.

Phishing von Kreditkartendaten

Eine der einfachsten, aber von den Betrügern immer noch genutzten Maschen geht folgendermaßen: Sie bieten einen Artikel auf Kleinanzeigen an. Ein Interessent meldet sich bei Ihnen per Whatsapp oder über einen anderen Messenger und bekundet Interesse an der Ware. Er bietet an, den Kauf über die Methode „Sicher bezahlen“ zu begleichen. Die existiert zwar bei Kleinanzeigen tatsächlich. Der Betrüger hat aber nicht vor, sie auch zu benutzen. Stattdessen soll sein Angebot Sie lediglich in Sicherheit wiegen.

Der angebliche Kaufinteressent gibt nun an, das Geld auf Ihr Kreditkartenkonto überweisen zu wollen. Dazu schickt er Ihnen einen Link zu einer Website, auf der Sie Ihre Kreditkartendaten eingeben sollen. Nachdem das geschehen ist, hören Sie nie

wieder etwas von ihm, und natürlich erhalten Sie auch keine Überweisung. Stattdessen stellen Sie in den Tagen und Wochen danach fest, dass jemand mit Ihrer Kreditkarte Geld abgehoben hat.

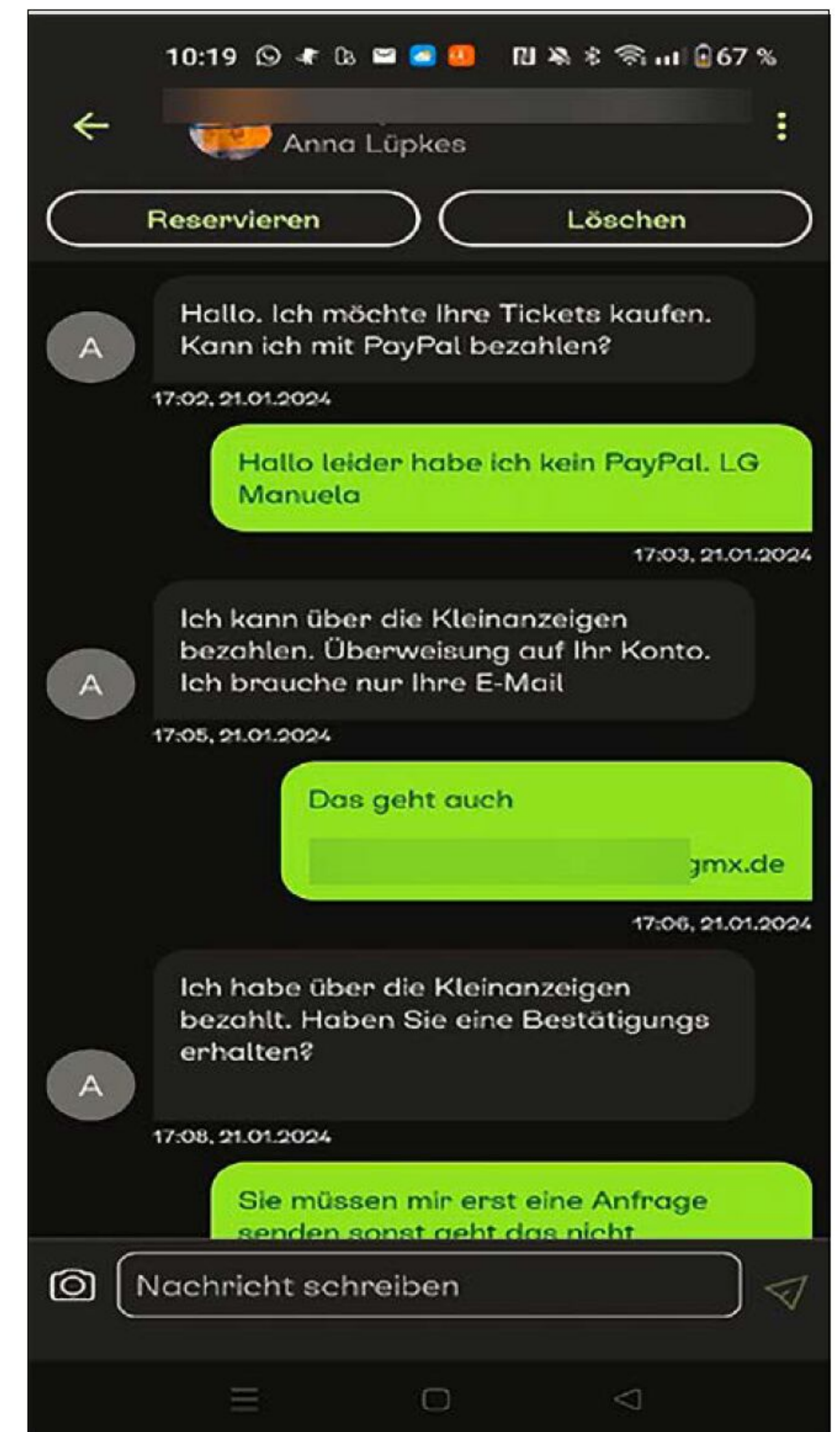
Wichtig: Sie sollten bereits stutzig werden, wenn jemand anbietet, den Verkaufspreis für eine Ware auf Ihr Kreditkartenkonto überweisen zu wollen. Denn für einen Außenstehenden ist das in der Regel nicht möglich. Stattdessen kann er Geld lediglich auf das mit der Karte verknüpfte Referenzkonto überweisen. Normalerweise handelt es sich dabei um ein Girokonto. Wenn also jemand nur nach den Kreditkartendaten fragt, sollten Sie vorsichtig werden und den Verkaufsvorgang lieber abbrechen.

Am besten akzeptieren Sie Zahlungen ausschließlich über den integrierten Nachrichtendienst von Kleinanzeigen und mit der echten Methode „Sicher bezahlen“. Lassen Sie sich nicht dazu überreden, einen Bezahlendienst außerhalb von Kleinanzeigen zu nutzen.

Falls Sie einmal auf diesen oder einen ähnlichen Trick hereingefallen sollten, sperren Sie mithilfe Ihrer Bank sofort Ihre Kreditkarte.

Der Trick mit den Transportkosten

Sie bieten eine etwas größere und sperrige Ware auf Kleinanzeigen an, beispielsweise



Ein angeblicher Kaufinteressent meldet sich bei Ihnen über Whatsapp und bietet an, die Überweisung über das Bezahlssystem von Kleinanzeigen durchzuführen. Es folgen ein Verwirrspiel und ein fieser Trick.

ein Bettgestell, ein teures Fahrrad oder eine alte Kommode. Der Betrüger zeigt Interesse, behauptet aber, derzeit im Ausland zu sein oder kein Auto zu besitzen, um die Ware transportieren zu können. Er will daher eine Spedition beauftragen, die die Ware bei Ihnen abzuholen. Sie sollen die Transportkosten zunächst vorstrecken, er will sie Ihnen dann später zusammen mit dem Kaufpreis überweisen. Für die Begleichung der Transportkosten gibt er Ihnen eine Kontonummer, die angeblich der Spedition gehört, und nennt auch gleich den Betrag. Meist geht es um Summen von 300 bis 400 Euro.

Sie überweisen das Geld und erhalten bald darauf eine E-Mail, die angeblich von einem Bezahlendienst wie Paypal oder auch von einer ausländischen Bank stammt. Darin wird bestätigt, dass der angebliche Käufer bereits eine Überweisung über die Summe aus Kaufpreis plus Transportkosten an Sie freigegeben hat. Diese E-Mail ist jedoch gefälscht. Die Spedition taucht nie bei Ihnen auf, und Ihr Geld ist weg.

Wichtig: Das Verfahren, dass jemand für die Abholung einer Ware eine Spedition



Über einen Link werden Sie zu einem gefälschten Chat geleitet, wo ein angeblicher Mitarbeiter von Kleinanzeigen auf Sie wartet. Dort sollen Sie Ihre Kontodaten und eine TAN eingeben.

organisiert, die Sie dann erst einmal bezahlen sollen, ist so ungewöhnlich, dass Sie

Kleinanzeigen bietet eine Methode zum sicheren Bezahlen an, bei der Überweisungen automatisch im Hintergrund überwacht werden.



misstrauisch werden sollten. Brechen Sie den Verkauf an dieser Stelle sofort ab.

Der Dreieckstrick

Sehr populär unter Kriminellen ist der Dreieckstrick. Dabei erbeutet der Betrüger anstatt Geld eine Ware, die er anschließend

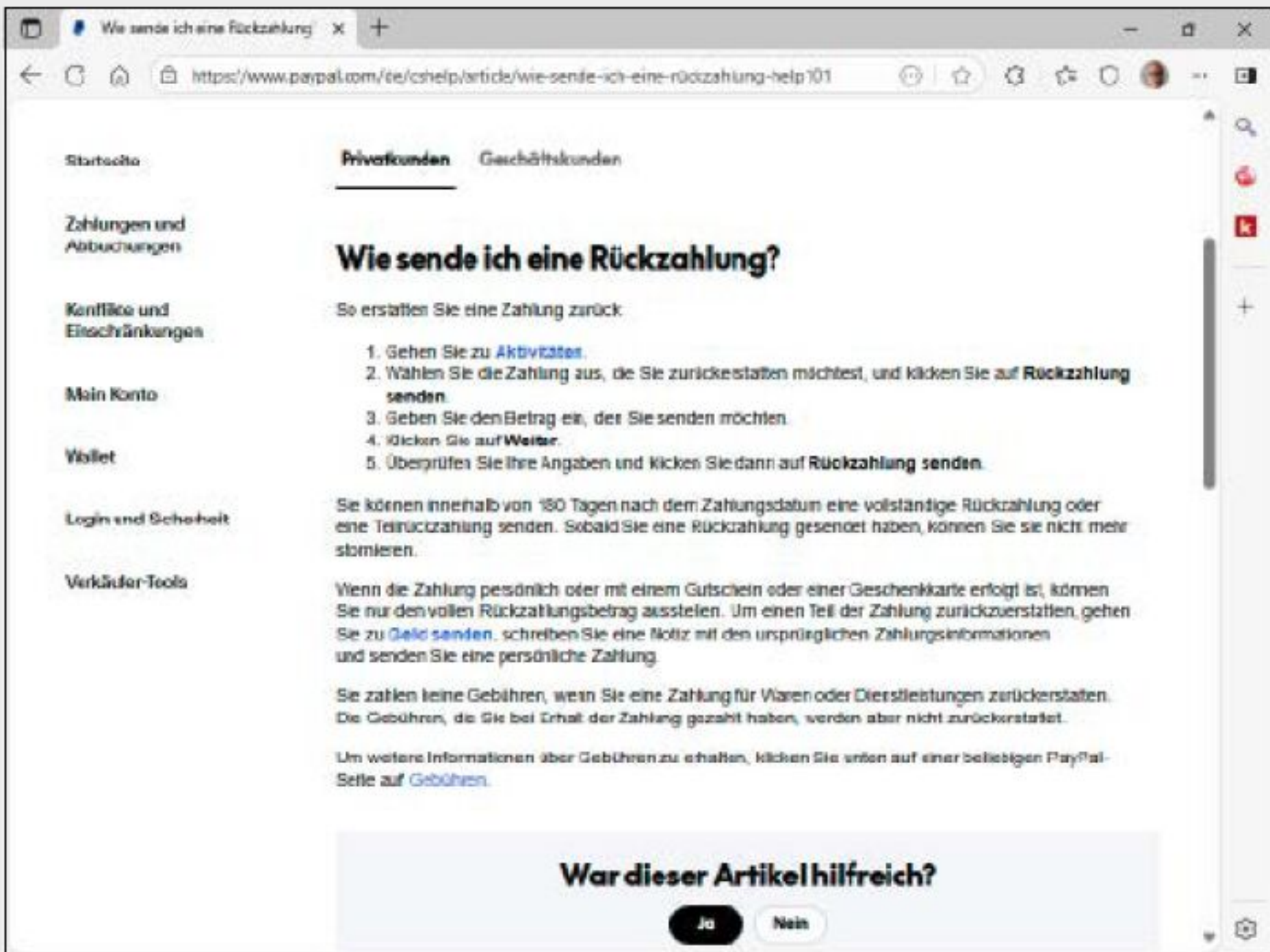
verkaufen kann. Das funktioniert so: Sie haben einen Artikel bei Kleinanzeigen eingestellt. Der Kriminelle meldet sich bei Ihnen und bekundet Interesse an der Ware. Gleichzeitig schaltet er selbst eine Annonce und bietet darin Ihren Artikel an. Sobald sich bei ihm ein Interessent meldet, gibt er

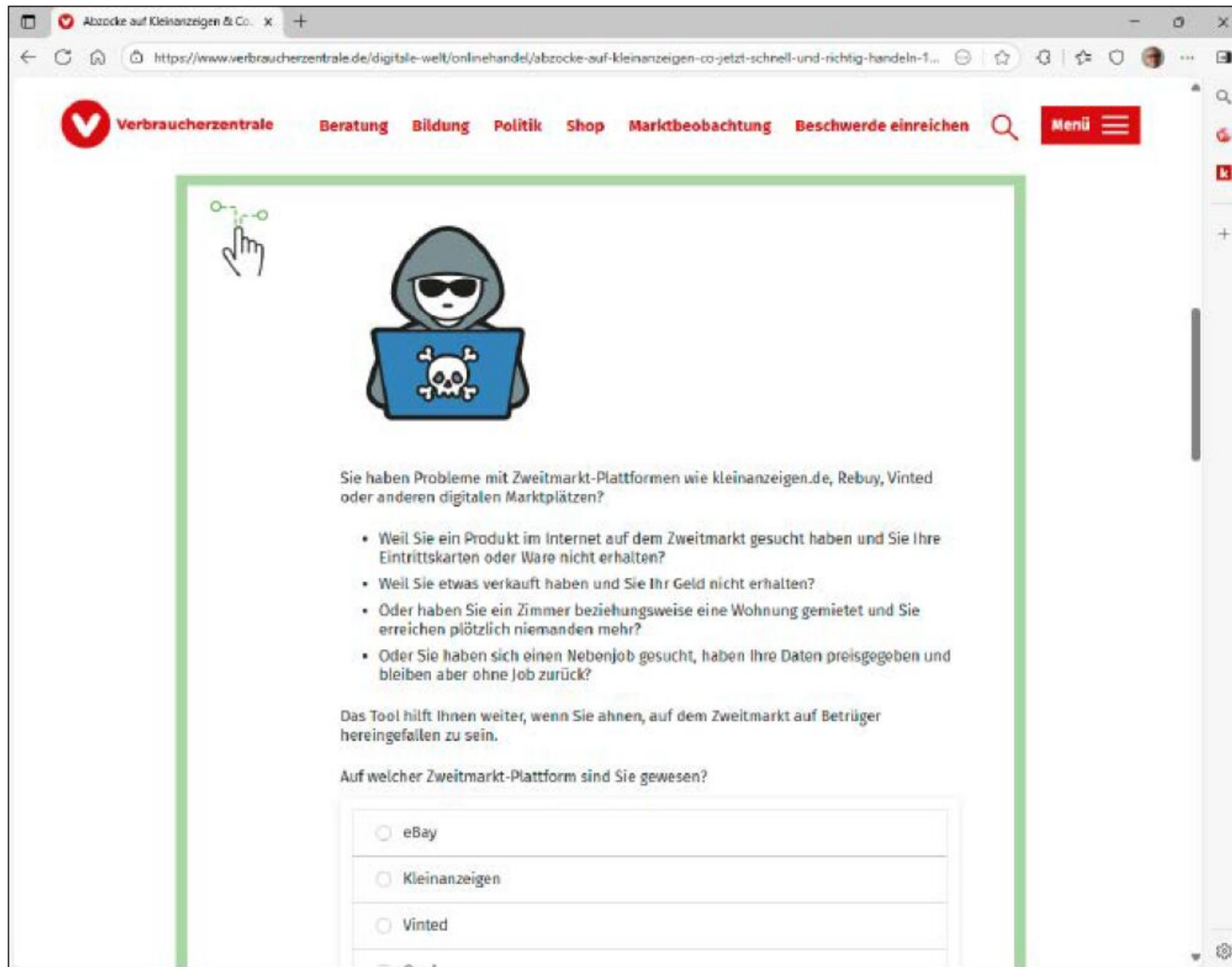
RÜCKÜBERWEISUNG MITHILFE VON PAYPAL

Die Verbraucherzentralen NRW und Rheinland-Pfalz warnen vor einer neuen Betrugsmasche. Dabei bekommen Sie per Paypal unerwartet Geld von einer Ihnen fremden Person überwiesen. Kurz darauf meldet sich der Absender und erzählt Ihnen, dass er Ihnen die Summe irrtümlich geschickt hat. Eigentlich sei das Geld für jemand anderen bestimmt gewesen. Nun bittet er Sie um eine Rücküberweisung per „Freunde und Familie“. Was der Absender nicht sagt: Im Modus „Freunde und Familie“ gibt es keinen Käuferschutz. Sobald Sie das Geld an den Absender zurücküberwiesen haben, bekommen Sie es nicht zurück. Der Betrüger allerdings wendet sich jetzt sofort an Paypal und meldet einen Problemfall. Da der Bezahlendienst einen Käuferschutz umfasst, macht Paypal die Transaktion rückgängig, holt das Geld von Ihrem Konto und überweist es ihm zurück.

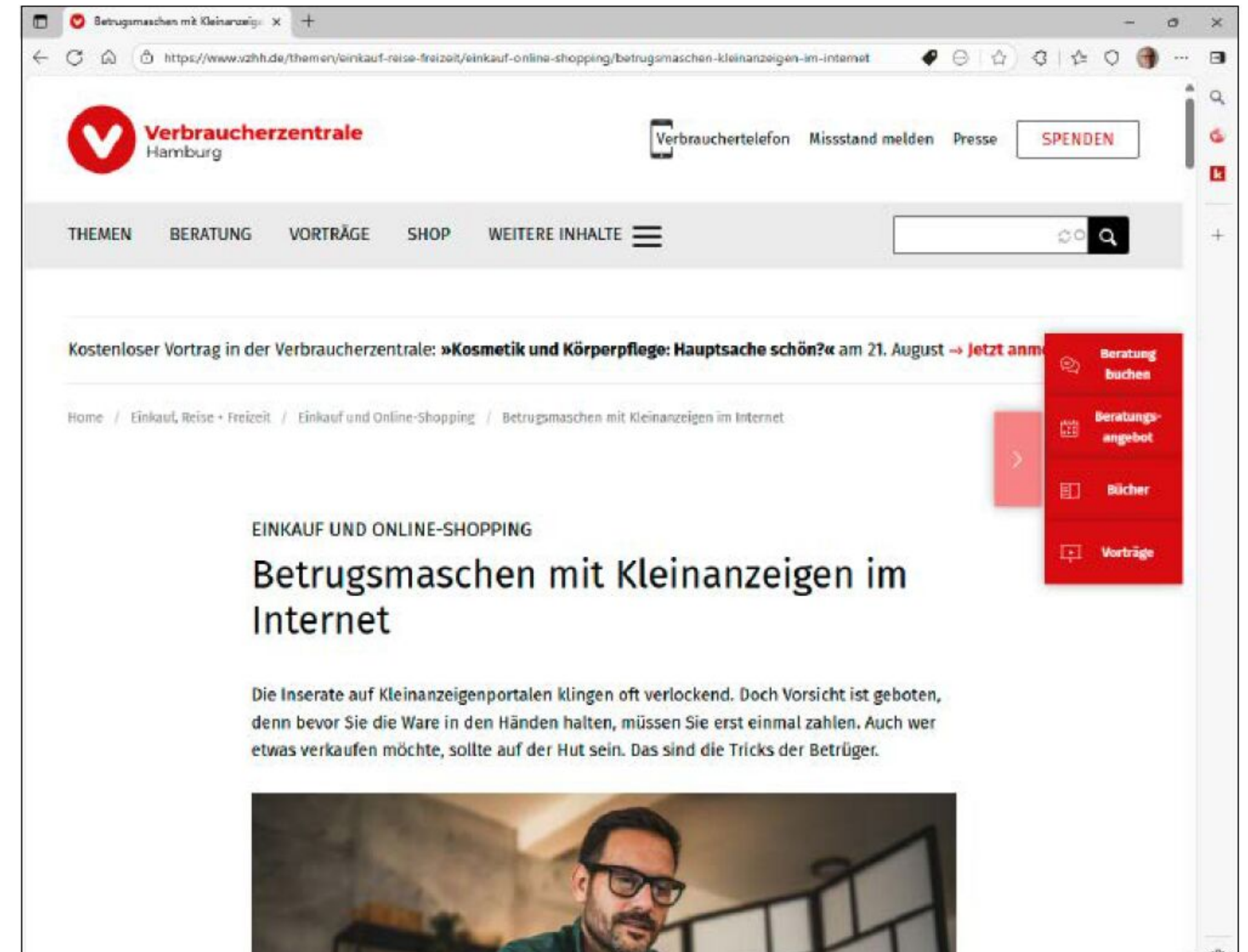
Der Betrüger erhält also zwei Rücküberweisungen, eine von Ihnen und eine von Paypal, und hat damit sein Geld glatt verdoppelt.

Der Bezahlendienst Paypal bietet seinen Kunden einen Käuferschutz, mit dem sie bei ausbleibender Ware ihren überwiesenen Betrag zurückholen können.





Die Verbraucherzentrale bietet auf ihrer Website ein Tool an (<https://tinyurl.com/mr24v8p3>), das Ihnen bei Betrugsfällen auf Verkaufsplattformen weiterhilft.



Die Verbraucherzentrale Hamburg klärt auf Ihrer Website über verschiedene Formen des Betrugs bei Kleinanzeigen-Plattformen auf.

ihm Ihre Kontodaten. Parallel dazu schließt er mit Ihnen den Kauf ab und bittet Sie, ihm die Ware zu schicken. Sie erhalten dann die Bezahlung von der dritten Person, die jedoch vergeblich auf ihre Bestellung wartet und Sie daher eventuell sogar bei Kleinanzeigen als Betrüger meldet.

Um eine solche Situation zu vermeiden, sollten Sie bei Ihren Verkäufen auf Kleinanzeigen niemals Ihre Kontonummer preisgeben. Nutzen Sie stets den Bezahl dienst des Portals, der gegen solche betrügerischen Machenschaften abgesichert ist.

Der Dreieckstrick mit Variante

Bei einer Variante des Dreieckstricks erhält der Betrüger das Geld, der Betrogene muss die Rechnung zwei Mal bezahlen. Das geht so: Der Kriminelle bietet auf Kleinanzeigen eine Ware an, die Sie per Paypal oder Überweisung bezahlen sollen. Damit Sie die Lieferung auch empfangen können, übermitteln Sie ihm Ihre Adresse. Der Betrüger bestellt jetzt das gleiche Produkt bei einem anderen Lieferanten und lässt es an Ihre Adresse schicken. Für die Bezahlung lässt er sich eine Rechnung zuschicken, allerdings an eine falsche E-Mail-Adresse. Für Sie scheint zunächst alles in Ordnung zu sein – Sie haben bezahlt und dafür die gewünschte Ware bekommen. Wenn dann jedoch die Mahnungen des echten Lieferanten bei Ihnen eintrudeln, merken Sie, dass etwas nicht stimmt.

Wichtig: Auch in diesem Fall lautet der Rat, Zahlungen für Waren, die Sie bei Kleinanzeigen gekauft haben, ausschließ-

lich über das Bezahlssystem der Plattform laufen zu lassen. Damit genießen Sie einen

Käuferschutz, der Sie vor Tricks, wie sie oben geschildert wurden, bewahrt. ■

SO KAPERN BETRÜGER BANKKONTEN

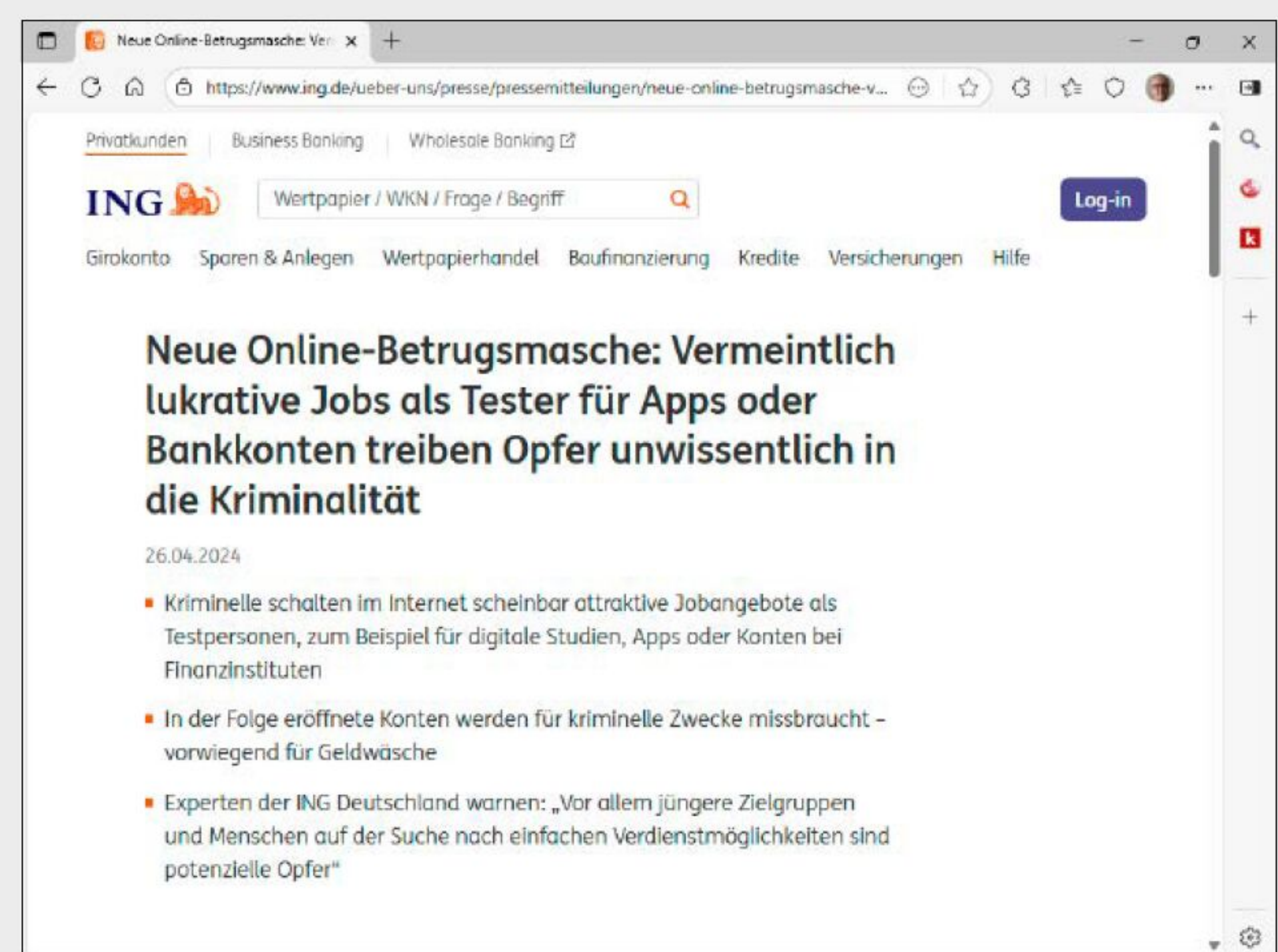


Ein Problem für die Kriminellen ist, wie sie an das erbeutete Geld gelangen.

Sie können es sich ja nicht auf ihr eigenes Konto überweisen lassen und damit ihre Identität preisgeben. Stattdessen greifen sie auf das Konto eines Strohmans zurück, der idealerweise nichts davon weiß.

Sie arbeiten dazu mit falschen Jobangeboten. Die Betrüger schicken Ihnen beispielsweise ein Angebot als gut bezahlter App-Tester für die Software einer Bank. Wenn Sie darauf eingehen, richten sie für Sie im Hintergrund ein Konto ein und schicken Ihnen einen Link zum Video-Ident-Verfahren der Bank. Es handele sich zwar um ein Testkonto, dennoch müssten Sie sich per Video-Ident identifizieren. Auch das sei Teil des Tests. Sobald Ihnen die Bank dann per Post die Kontounterlagen geschickt hat, sollen Sie diese bitte an sie weiterleiten. Danach werde das Konto automatisch gelöscht.

Tatsächlich wird das Konto jedoch nicht gelöscht, sondern wird von den Kriminellen für ihre Geschäfte genutzt – alles unter Ihrem Namen, aber ohne Ihr Wissen. Sie werden dadurch zu einem Finanzagenten und stehen nach der Aufdeckung des Betrugs unter Verdacht, Geldwäsche zu fördern.



Die ING-Bank erklärt auf ihrer Website, wie Kriminelle an Konten anderer Personen gelangen. Über diese Konten führen sie anschließend ihre Geldgeschäfte durch, der Kontoinhaber gerät unter Geldwäscheverdacht.



Passwort geklaut?

Ein riesiges Datenpaket mit 16 Milliarden gestohlenen Passwörtern ist im Internet aufgetaucht. Darin enthalten sind Passwörter zu Konten von Google, Apple, Facebook und anderen Unternehmen. Prüfen Sie jetzt, ob auch Sie betroffen sind, und schützen Sie sich vor Angriffen.

VON ARNE ARNOLD

Fehler passieren. Sie passieren auch Profis. Zum Beispiel einem Profi wie Troy Hunt. Er ist ein weltweit bekannter Sicherheitsexperte und betreibt unter anderem die Website Have I Been Pwned (HIBP) unter <https://haveibeenpwned.com>. Auf dieser Website sind Milliarden gestohlener Log-in-Daten zusammengetragen, sodass Nutzer nachschauen können, ob ihr Passwort betroffen ist. Dazu später mehr. Troy Hunt kennt sich also bestens mit Passwortdiebstahl aus. Und dennoch ist er Opfer eines Phishing-Angriffs geworden. Er betreibt

den Sicherheits-Blog www.troyhunt.com. Tausende haben seinen Newsletter zum Blog abonniert. Hunt versendet die Newsletter über einen Dienst namens Mailchimp. Von diesem Dienst erhielt der Profi Hunt scheinbar eine Nachricht, dass er keine Newsletter mehr versenden könne, da es Beschwerden wegen Spam-Mails gegeben habe. Hunt klickte auf den Link in dieser E-Mail, um den Fall zu klären, und gab seine Anmeldedaten auf einer Website ein, von der er glaubte, sie gehöre zu Mailchimp. Tatsächlich hat er seine Daten jedoch einer Phishing-Website übergeben, ebenso wie kurz darauf ein Einmalpasswort aus der Zwei-Faktor-Authentifizierung. Die Folge: Alle 16.000 Mailadressen seiner Abonnenten sowie weitere Daten fallen den Kriminellen in die Hände. Diese Daten lassen sich etwa für Phishing-Angriffe verwenden. Passwörter waren nicht enthalten. Alle Details zu dem Vorfall erzählt Hunt in diesem lesenswerten Blog-Eintrag: <https://tinyurl.com/3dt9fh4s>. Als Grund für den Reinfluss gibt Hunt Müdigkeit an. Er litt unter Jetlag.

Dieser Phishing-Angriff zeigt, dass auch Sicherheitsexperten Fehler machen, und verdeutlicht, wie in den meisten Fällen große Mengen an Log-in-Daten in die Hände von Kriminellen fallen. Die Angreifer erbeuten sie nicht vom einzelnen Anwender, sondern meist von Internetservern, also aus Datenbanken mit vielen Tausend oder gar Millionen Anmeldedaten.

Milliarden gestohlener Log-in-Daten kursieren im Internet

Der bereits erwähnte Onlinedienst Have I Been Pwned hat rund 15 Milliarden gestohlene Log-in-Daten gesammelt. Doch woher kommen diese Daten?

Der Großteil stammt aus sogenannten Data Breaches, also Datenpannen oder Datenlecks. Hacker verschaffen sich Zugang zu den Servern von Unternehmen und stehlen die dort gespeicherten Log-in-Daten. Betroffen waren beispielsweise die Kunden von Dropbox (2012), Adobe (2013), Ebay (2014) und LinkedIn (2021), insgesamt mehr als 700 Millionen Nutzer. Auch deutsche Firmen und ihre Kunden sind schon

„Mit diesen Tools lässt sich leicht herausfinden, ob Hacker Ihre Passwörter bereits kennen.“

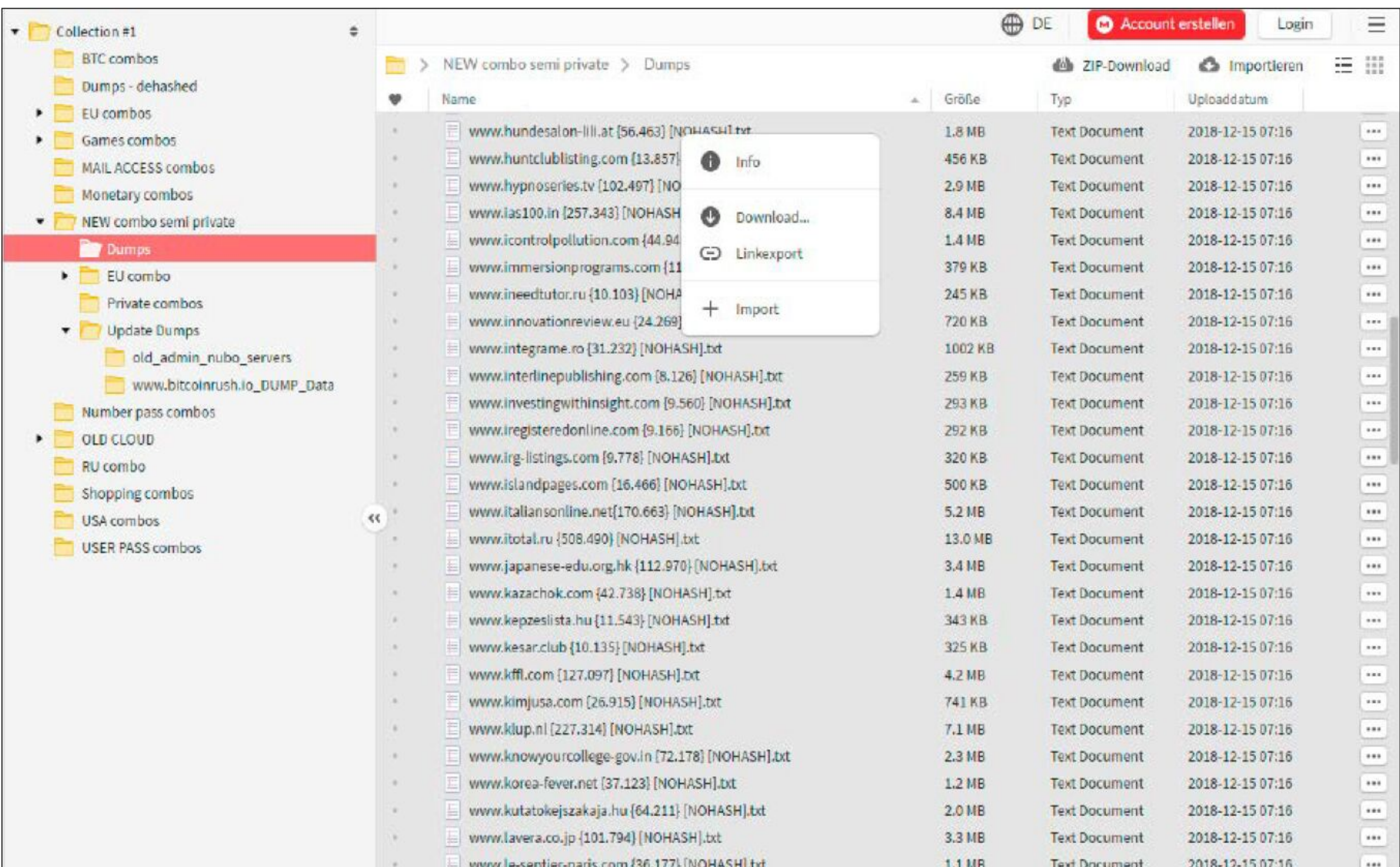
Opfer solcher Angriffe geworden, etwa zwei Hamburger Arztpraxen, denen 2024 rund 100.000 Patientendaten gestohlen wurden, oder der Autovermieter Buchbinder, dem 2020 rund drei Millionen Kundendaten abhanden kamen.

Bei einigen Datenlecks müssen sich die Angreifer nicht einmal in ein Firmennetzwerk hacken. Durch eine fehlerhafte Konfiguration liegen Nutzerdaten oft ungeschützt im Internet, wo sie jeder einsammeln kann, der nach ihnen sucht. Ein kleiner Teil der gestohlenen Daten, die im Internet kursieren, stammt außerdem von Schadcode, sogenannten Info-Stealern. Kriminelle schleusen diese auf die PCs der Anwender, wo der Schadcode persönliche Log-in-Daten stiehlt.

Die Diebe bieten diese Daten anschließend im Dark Web, etwa in Untergrundforen, an. Oft werden die Daten in sogenannte Collections zusammengefasst, die dann Millionen bis Milliarden Einträge enthalten. Das jüngste Datenpaket umfasste 16 Milliarden Einträge. Es sind jedoch etliche Doppler und Daten aus bereits bekannten Datenlecks enthalten, sodass die Zahl der tatsächlich betroffenen Konten geringer ist. Andere Kriminelle nutzen die Datenpakete, um Spam-Mails zu verbreiten oder Phishing-Angriffe zu starten.

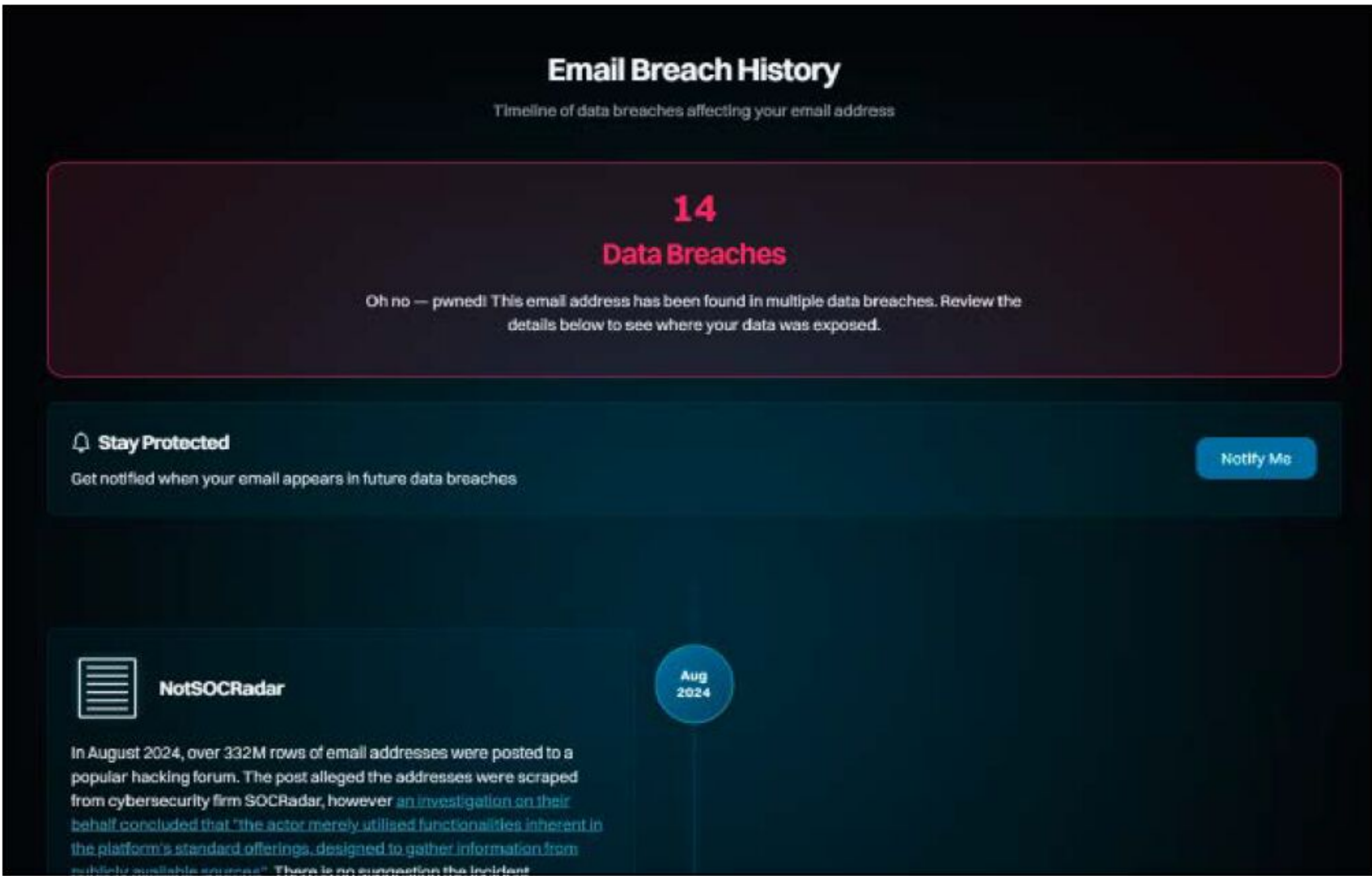
Diese Daten sind bei einem Datenklau betroffen

Die Art der gestohlenen Daten variiert: Sie reicht von simplen Mailadressen und Namen bis hin zu Passwörtern (im Klartext oder gehasht), Kreditkarteninformationen, Postadressen oder sogar medizinischen Befunden. Besonders kritisch wird es, wenn eine Person eindeutig identifiziert werden kann. Denn dann lassen sich diese Daten für Identitätsdiebstahl oder gezielte Phishing-Angriffe verwenden. Entscheidend ist auch, in welcher Form die Daten verloren gehen. Sind Passwörter bei-



Das ist ein Einblick in die „Collection #1“, die 773 Millionen gestohlene Datensätze umfasst und 2019 entdeckt wurde. Mittlerweile gibt es größere Datensammlungen, die aber meist durch Mehrfacheinträge aufgebläht sind.

Der bekannte Dienst Have I Been Pwned (HIBP) listet alle Treffer in seiner Datenbank entlang eines Zeitstrahls auf. Das ist ganz hübsch, aber eigentlich nicht sehr übersichtlich. Details zu gestohlenen Passwörtern liefert HIBP nicht.



spielsweise nur als Hash gespeichert, ist die Gefahr geringer als bei einer unverschlüsselten Speicherung. Dennoch sind auch gehashte Passwörter unter bestimmten Umständen angreifbar. Dafür werden die gestohlenen Daten genutzt Kriminelle holen sich die gestohlenen Log-in-Daten aus Untergrundforen und nutzen

sie, um beispielsweise Spam-Mails zu versenden oder Phishing-Angriffe zu starten. Am häufigsten werden die Daten derzeit jedoch für sogenannte Credential-Stuffing-Angriffe genutzt. Dabei versuchen Angreifer, geleakte Kombinationen aus Benutzernamen und Passwörtern automatisiert bei anderen Onlinediensten einzusetzen. Das funktioniert immer dann, wenn ein Nutzer dasselbe Passwort für mehrere Dienste

IM ÜBERBLICK: SICHERHEITSTOOLS

Name	Beschreibung	Auf	Internet	Preis
Avast Free Antivirus	Antivirentool	Heft-DVD	www.pcwelt.de/article/1135344	Kostenlos
Bitwarden	Passwortmanager	Heft-DVD	www.pcwelt.de/article/1915554	Kostenlos
Cryptomator	Cloudverschlüsselung	Heft-DVD	https://cryptomator.org/de	Kostenlos
Keepass	Passwortmanager	Heft-DVD	www.pcwelt.de/299369	Kostenlos
Malwarebytes Adwcleaner	Adware-Scanner	Heft-DVD	www.pcwelt.de/article/1145757	Kostenlos

Alle Tools sind deutschsprachig.



Collection #2	Dateiname: S(Anti-Duplicates) (Combined 2 Files) (Anti-Duplicates) Split #1.txt Datum: 04.2020 Enthaltene Daten: E-Mail-Adresse, Passwort Passwort: "m...4"
Keine Details bekannt	Dateiname: d1b.de.txt Datum: 08.2023 Enthaltene Daten: E-Mail-Adresse, Passwort Passwort: "m...4"
Collection #2	Dateiname: 168.txt Datum: 04.2020 Enthaltene Daten: E-Mail-Adresse, Passwort Passwort: "m...4"
Collection #4	Dateiname: 1502.txt Datum: 05.2020 Enthaltene Daten: E-Mail-Adresse, Passwort Passwort: "m...4"
Collection #2	Dateiname: 123k.txt Datum: 04.2020 Enthaltene Daten: E-Mail-Adresse, Passwort Passwort: "m...4"
Keine Details bekannt	Dateiname: 839K.txt Datum: 09.2023 Enthaltene Daten: E-Mail-Adresse, Passwort Passwort: "m...4"

Per Mail kommt das Ergebnis des Leak-Checkers der Uni Bonn. Der Checker liefert viele Treffer und verrät Teile der gestohlenen Passwörter.

verwendet. Besitzen die Angreifer beispielsweise die Log-in-Daten aus dem Datenleck des Autovermieters Buchbinder, versuchen sie, sich damit bei Diensten wie Amazon oder Paypal einzuloggen.

So erfahren Sie, ob Sie von einem Datenklau betroffen sind

Grundsätzlich muss der Dienst, dem die Daten gestohlen wurden, seine Kunden informieren. Wichtig ist, dass der Dienst die betroffenen Konten sperrt und seine Kunden auffordert, ein neues Passwort zu vergeben. Problematisch wird es, wenn der Dienst

diesen Pflichten nicht nachkommt – und das ist wohl häufiger der Fall. Deshalb müssen Sie sich auch selbst um das Thema kümmern und mithilfe von sogenannten Leak-Checkern prüfen, ob Ihre Passwörter betroffen sind. Wir stellen die wichtigsten Leak-Checker vor.

Leak-Checker: Prüfen Sie, ob Ihr Passwort betroffen ist!

Es gibt eine ganze Reihe kostenloser Onlinedienste, die gestohlene Log-in-Daten sammeln und es jedem ermöglichen, nach seinen Daten zu suchen. Sie unterscheiden sich im Umfang ihrer Datensammlung und darin, wie viele Informationen sie herausgeben. Es lohnt sich also, mehrere Dienste zu befragen.

Have I Been Pwned: Den bekanntesten Leak-Checker-Dienst erreichen Sie unter <https://haveibeenpwned.com>. Dort geben Sie Ihre Mailadresse ein und klicken auf „Check“. Sollte Ihre Mailadresse bei HIBP bekannt sein, wird das Ergebnis direkt auf der Website angezeigt. Da HIBP alle Passwörter von den übrigen Daten trennt, erfahren Sie nicht, welches Passwort gestohlen wurde. Das ist unproblematisch, wenn HIBP den Onlinedienst anzeigt, von dem Ihre Log-in-Daten gestohlen wurden, etwa Adobe oder Lastpass. Oft wird jedoch eine Collection als Datenquelle genannt. Dann wissen Sie oft nur, dass Ihre Daten in einem Datenleck auftauchen, aber nicht, woher die Daten stammen. Nutzen Sie dann unbedingt den folgenden Dienst, um mehr Informationen zu erhalten.

Nützlich: Sie können bei HIBP Ihre Mailadresse hinterlegen (<https://haveibeenpwned.com/NotifyMe>) und werden informiert, sobald diese in einem neuen Datenleck auftaucht.

Identity Leak-Checker der Uni Bonn:

Um es vorweg zu sagen: Der Leak-Checker der Universität Bonn ist anstrengend. Aber lohnenswert! Er ist anstrengend, weil er meist sehr viele Treffer liefert. Die hohe Zahl entsteht hauptsächlich dadurch, dass der Dienst doppelte Treffer in den vielen Collections nicht aussortiert, sondern sie in jeder einzelnen Collection anzeigt. Das liefert in der Summe deutlich mehr Ergebnisse, die Sie kontrollieren müssen.

Warum es sich dennoch lohnt, diesen Checker zu nutzen: Er liefert auch Hinweise auf das gestohlene Passwort. Zwar werden nur das erste und das letzte Zeichen des Passworts angezeigt, doch das genügt in der Regel, um das Passwort zu identifizieren. Dafür benötigen Sie eine durchsuchbare Liste mit Ihren Passwörtern. Sollte sich Ihr Passwortmanager nicht nach einem Passwort durchsuchen lassen, nutzen Sie dessen Exportfunktion, um eine Liste im CSV-Format zu erhalten. Sortieren Sie die Liste anschließend in der Spalte der Passwörter alphabetisch. So finden Sie das teilweise angezeigte Passwort. Denken Sie anschließend daran, die Liste zuverlässig zu löschen, damit Ihre Log-in-Daten nicht im Klartext auf Ihrem Computer gespeichert bleiben.

HPI Identity Leak Checker: Auch die Log-in-Datenbank des Hasso-Plattner-Instituts (<https://sec.hpi.de/ilc>) enthält viele der im Internet kursierenden Datenlecks. Die Trefferliste ist übersichtlich aufbereitet und enthält viele Informationen. Das Passwort wird nicht angezeigt.

Google Dark Web Report: Wer ein Google-Konto nutzt, sollte auch den Dark Web Report des Suchmaschinenriesen nutzen. Er zeigt bei einem Treffer die ersten drei Zeichen des gestohlenen Passworts an. Sie aktivieren ihn in Ihrem Google-Konto (<https://myaccount.google.com>) unter „Sicherheit → Dark Web Report“.

Kostenpflichtige Dienste: Die oben genannten kostenlosen Dienste liefern einen guten Überblick darüber, welche Ihrer Daten im Dark Web aufgetaucht sind. Es gibt jedoch auch kommerzielle Anbieter, die behaupten, sie seien schneller dabei, Ihre Log-in-Daten in neu

TIPPS GEGEN DEN PASSWORTDIEBSTAHL

1. Verschiedene Passwörter nutzen

Jedes Konto, jeder Dienst bekommt ein eigenes Passwort. So ist im Falle eines Passwortdiebstahls wenigstens nur ein Konto bedroht.

2. Lange Passwörter nutzen

Angreifer können einfache Passwörter wie 12345678 erraten.

3. Zwei-Faktor-Authentifizierung (2FA) einsetzen

Wenn ein Konto mit einem zweiten Faktor, etwa einem Einmalpasswort, geschützt ist, bleibt Ihr Konto auch nach dem Passwortdiebstahl sicher.

4. Passkeys verwenden (sind sicher vor Phishing)

Passkeys werden oft als 2FA angeboten. Gegenüber anderen 2FA-Methoden haben sie den Vorteil, dass sie sicher vor Phishing sind. Ein Einmalpasswort lässt sich dagegen entwerfen.

5. Auf Phishing-Angriffe achten

Tipps gegen Phishing finden Sie in den ausführlichen Ratgebern unter www.pcwelt.de/2571095 und www.pcwelt.de/1184128.

aufgetauchten Datenpaketen im Untergrund zu finden. Zusätzlich überwachen sie auch andere Bereiche des Internets, etwa Youtube, auf Identitätsmissbrauch. Außerdem ergänzen die Anbieter ihre Produkte um Serviceleistungen. Meist handelt es sich dabei um eine Hotline, unter der Sie im Notfall anrufen können, um sich nach einem Datendiebstahl beraten zu lassen.

Die meisten dieser Dienste stammen von Antivirenherstellern wie F-Secure (www.f-secure.com/de/id-protection) oder Bitdefender (<https://www.bitdefender.com/de-de/consumer/digital-identity-protection>). Beide Dienste kosten je 70 Euro pro Jahr. Diese Protection-Dienste sind auch in den Internet-Sicherheitspaketen der beiden Hersteller enthalten. Auch andere Sicherheitshersteller wie Norton (<https://de.norton.com>), G Data (www.gdata.de) oder McAfee (www.mcafee.com) bieten diese Funktion. Sie müssen dann aber stets zu den teuersten und damit am besten ausgestatteten Versionen der Suites greifen, um den Identitätsschutz zu erhalten.

Datenleck gefunden? Keine Panik, wenn Ihre Daten betroffen sind

Wenn ein Leak-Checker bei Ihrer Mailadresse Alarm schlägt, ist das in der Regel kein Grund zur Panik. Wenn nur Ihre Mailadresse und Ihr Passwort bei einem der großen Datendiebstähle, etwa bei Adobe, Sony, Facebook & Co., ins Internet gelangt sind, dann haben Sie von diesen Diensten bereits vor langer Zeit die Aufforderung erhalten, sich ein neues Passwort zuzulegen. Da Sie für jeden Dienst ein eigenes Passwort nutzen, kann ein Angreifer mit diesen Daten nicht viel anfangen. Heikel wird es jedoch, wenn weitere persönliche Daten, wie etwa Ihre Postadresse, gestohlen wurden. Denn dann kann es zu einem Identitätsdiebstahl kommen, bei dem Kriminelle Waren und Dienstleistungen auf Ihre Rechnung bestellen. Sollten Sie jemals Rechnungen für Waren erhalten, die Sie nicht bestellt haben, müssen Sie die Polizei einschalten und der Rechnung widersprechen, bevor ein Inkassounternehmen anrückt und die Situation eskaliert. Ebenfalls heikel ist die Situation, wenn der Datendiebstahl erst vor Kurzem stattgefunden hat. Folgen Sie dann unseren Tipps (siehe Kasten „Erste Hilfe bei Passwortdiebstahl“). ■

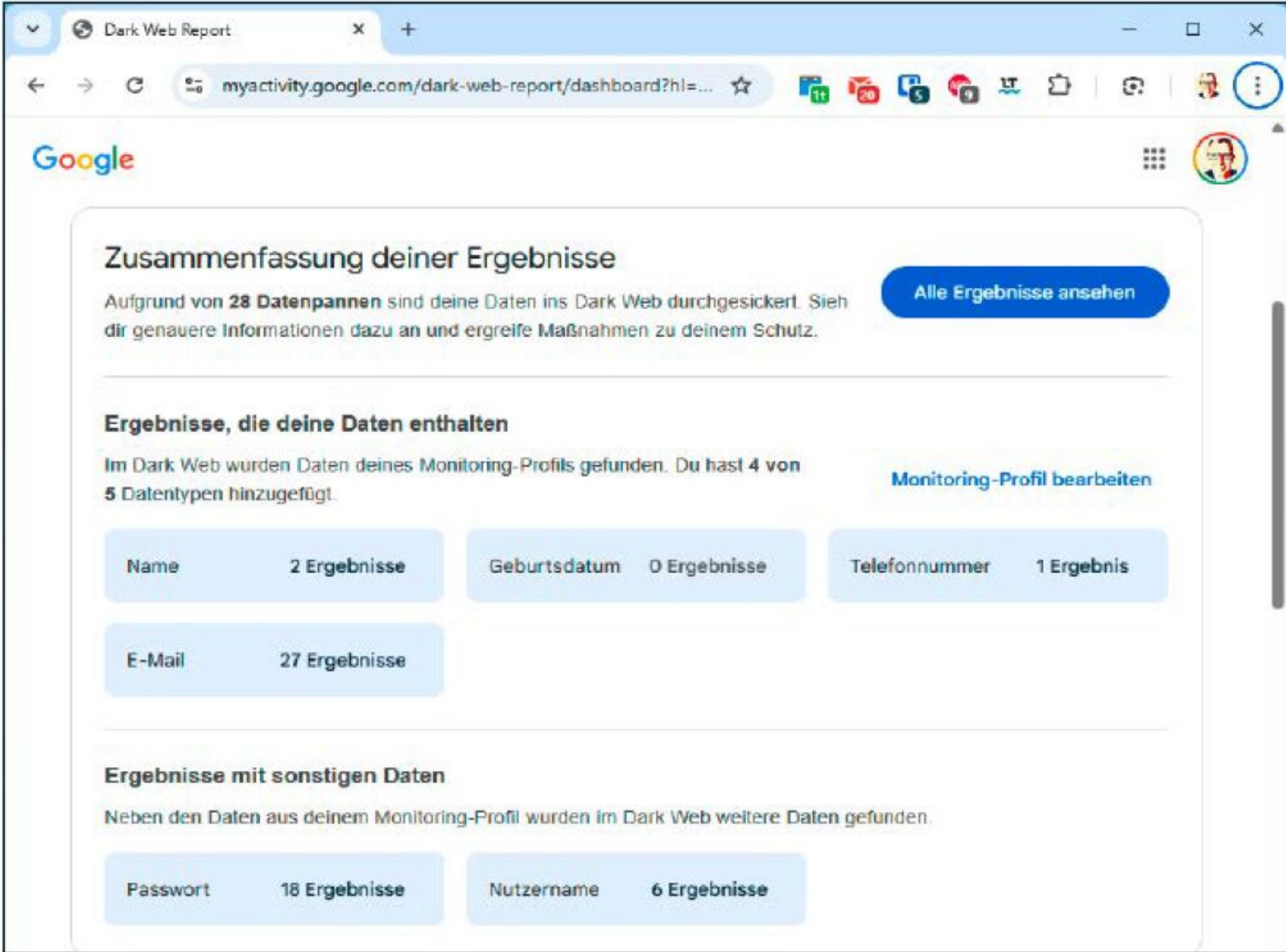
Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse [redacted] taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf. Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozialversicherungs-nr.	IP-Adresse
naz.api	Jan. 2024	✓	19.687.911	Betroffen	-	-	-	-	-	-	-	-
Dieser Leak enthält Identitätsdaten, die von der Domain naz.api entwendet wurden.												
DFB.de	Apr. 2023		2.696.183	Betroffen	-	-	-	-	-	-	-	-
Dieser Leak enthält Identitätsdaten, die von der Domain DFB.de entwendet wurden.												
gravatar.com	Dez. 2021	✓	60.497.906	-	-	-	-	-	-	-	-	-
Dieser Leak enthält Identitätsdaten, die von der Domain gravatar.com entwendet wurden.												
younow.com	Feb. 2019	✓	18.133.902	-	Betroffen	-	-	-	-	-	-	Betroffen
Combolist	Jan. 2019		1.247.433.080	Betroffen	-	-	-	-	-	-	-	-
Der Ursprung der Daten ist unklar. Auch ist nicht bekannt, wie alt die Daten sind bzw. wo genau diese erlangt wurden. Vermutlich handelt es sich aber um eine Zusammenstellung zahlreicher älterer Leaks und Daten aus Privatsphäre-Kampagnen.												
Unknown (Collection #1-#5)	Jan. 2019		2.191.498.885	Betroffen	-	-	-	-	-	-	-	-
Dieser Datensatz wurde im Januar 2019 veröffentlicht und enthält riesige Listen von Zugangsdaten unbekannter Herkunft, ältere Leaks und kleinere Datenbankabzüge.												
500px.com	Jul. 2018	✓	14.866.850	Betroffen	-	-	-	-	-	-	-	-
psmbianco.com (Combolist)	Apr. 2018		479.496.221	Betroffen	-	-	-	-	-	-	-	-
myfitnesspal.com	Feb. 2018	✓	143.425.495	Betroffen	-	-	-	-	-	-	-	-
Unknown (Anti-Public Combolist Jan. 2017)	Jan. 2017		948.385.599	Betroffen	-	-	-	-	-	-	-	-
Combolist	Jul. 2016		2.995.133	Betroffen	-	-	-	-	-	-	-	-
Combolist	Jul. 2016		19.351.766	Betroffen	-	-	-	-	-	-	-	-

Die Ergebnisse des HPI Identity Leak Checkers erhalten Sie per Mail. Die Darstellung ist übersichtlich, enthält aber keine Hinweise darauf, welches Passwort genau betroffen ist.

Für Nutzer von Google Chrome: Wer seine Passwörter in dem Browser Chrome speichert, kann den „Dark Web Report“ von Google nutzen. Dahinter verbirgt sich ein Leak-Checker für gestohlene Passwörter, der die Fundstellen übersichtlich anzeigt.



ERSTE HILFE BEI PASSWORTDIEBSTAHL

+

Wenn ein Leak-Checker meldet, dass Ihr Passwort im Internet kursiert, müssen Sie handeln.

1. Ändern Sie das Passwort beim betreffenden Dienst. Wird als Quelle des Diebstahls nur eine „Collection“ genannt, finden Sie heraus, zu welchem Konto das Passwort passt.

2. Sind die Log-in-Daten Ihres Onlinebankings betroffen, kontrollieren Sie die Umsätze Ihres Bankkontos und nutzen Sie den kostenfreien Sperr-Notruf 116 116.

3. Kappen Sie alle Zugangsberechtigungen, falls der Dienst diese Funktion bietet. Bei Google geht das etwa unter <https://myaccount.google.com> über „Sicherheit > Meine Geräte“.

4. Aktivieren Sie eine Zwei-Faktor-Authentifizierung, am besten per Passkey.

5. Informieren Sie den betroffenen Dienst.

6. Überprüfen Sie, ob Einstellungen im betroffenen Konto verändert wurden.

7. Kontrollieren Sie, welche Daten ein Angreifer in dem Konto ausspähen konnte.

PC-WELT SONDERHEFT XXL 3/2026

185

Abzocke per Briefpost

Phishing per E-Mail wird immer besser erkannt. Kriminelle Banden versuchen es daher verstärkt mit Briefen und ausgedruckten QR-Codes, die sie per Post verschicken oder in der Stadt verteilen.

VON ROLAND FREIST

Phishing-Mails überfluten nach wie vor die E-Mail-Postfächer von Privatpersonen und Unternehmen. Die kriminellen Banden, die dahinterstecken, haben es auf Zugangsdaten für Bankkonten, Streamingdienste oder Onlineshops abgesehen und gehen bei den Raubzügen immer professioneller vor. Mittlerweile kommen KI-Chatbots zum Einsatz, die für die Phishing-Mails gut formulierte, fehlerfreie Texte schreiben.

Obwohl die Zahl der Phishing-Angriffe zunimmt, wird es für die Kriminellen immer schwieriger, an die begehrten Zugangsdaten zu gelangen. Das ist ein Erfolg der Aufklärungskampagnen von Verbraucherzentralen, Polizei, Banken und auch des Bundesamts für Sicherheit in der Informationstechnik (BSI). Viele Menschen wissen nun, was eine Phishing-Mail ist, wie man

„Betrug bei Immobilienbörse: Wer den 30.000-Euro-Kredit zahlen muss, ist nach wie vor ungeklärt.“



© Mit Material von contrastwerkstatt, MarkRademaker – AdobeStock

sie erkennt und wie Phishing funktioniert. Sie sind gewarnt und folgen Vorsichtsmaßnahmen wie etwa, dass man die Absenderadresse einer Mail sorgfältig prüfen und nicht einfach auf enthaltene Links klicken sollte. Mittlerweile weichen die Betrüger daher auf das Phishing per Briefpost aus. Es gibt bereits mehrere Beispiele, in denen Phishing-Links nicht mehr per E-Mail, SMS oder Whatsapp kamen, sondern als ausgedruckte QR-Codes im Briefkasten lagen.

Phishing per gedrucktem QR-Code und Briefpost

Um potenzielle Opfer auf ihre Webseiten zu locken, verwenden Kriminelle gerne QR-Codes. Denn diese haben für sie den Vorteil, dass man ohne technische Hilfsmittel nicht

erkennen kann, zu welcher Webadresse der Code führt. Man nennt diese Form des Betrugs Quishing, das Wort leitet sich ab aus „QR-Code“ und „Phishing“.

Zunächst tauchten die betrügerischen QR-Codes in E-Mails auf. Den Kriminellen gelang es damit in vielen Fällen, die Schutzfunktionen von E-Mail-Programmen zu unterlaufen. Im vergangenen Jahr registrierten Polizei und Verbraucherschützer jedoch eine zunehmende Zahl von QR-Codes, die auf anderen Wegen verteilt wurden.

So meldete sich im August 2024 eine Frau beim Phishing-Radar der Verbraucherzentrale NRW und reichte einen Brief ein, der laut Absender von der Commerzbank stammte. Darin wurde sie aufgefordert, das Photo-TAN-Verfahren zur Sicherung ihrer

Bankgeschäfte zu aktualisieren. Außerdem enthielt der Brief einen prominent platzierten QR-Code, der sie angeblich direkt zur notwendigen Reaktivierung des Photo-TAN-Verfahrens führen würde. Da die Frau jedoch keine Kundin der Commerzbank ist, wurde sie misstrauisch. Die Verbraucherzentrale stellte dann fest, dass der Link im QR-Code auf eine von Kriminellen betriebene Webseite verwies.

Natürlich stammte der Brief nicht von der Commerzbank, sondern wurde von einer kriminellen Bande verschickt. Mittlerweile sind mehrere solcher Aussendungen bekannt geworden. Sie tarnen sich nicht nur mit dem Logo der Commerzbank, sondern erreichen die Empfänger auch im Namen anderer Banken.

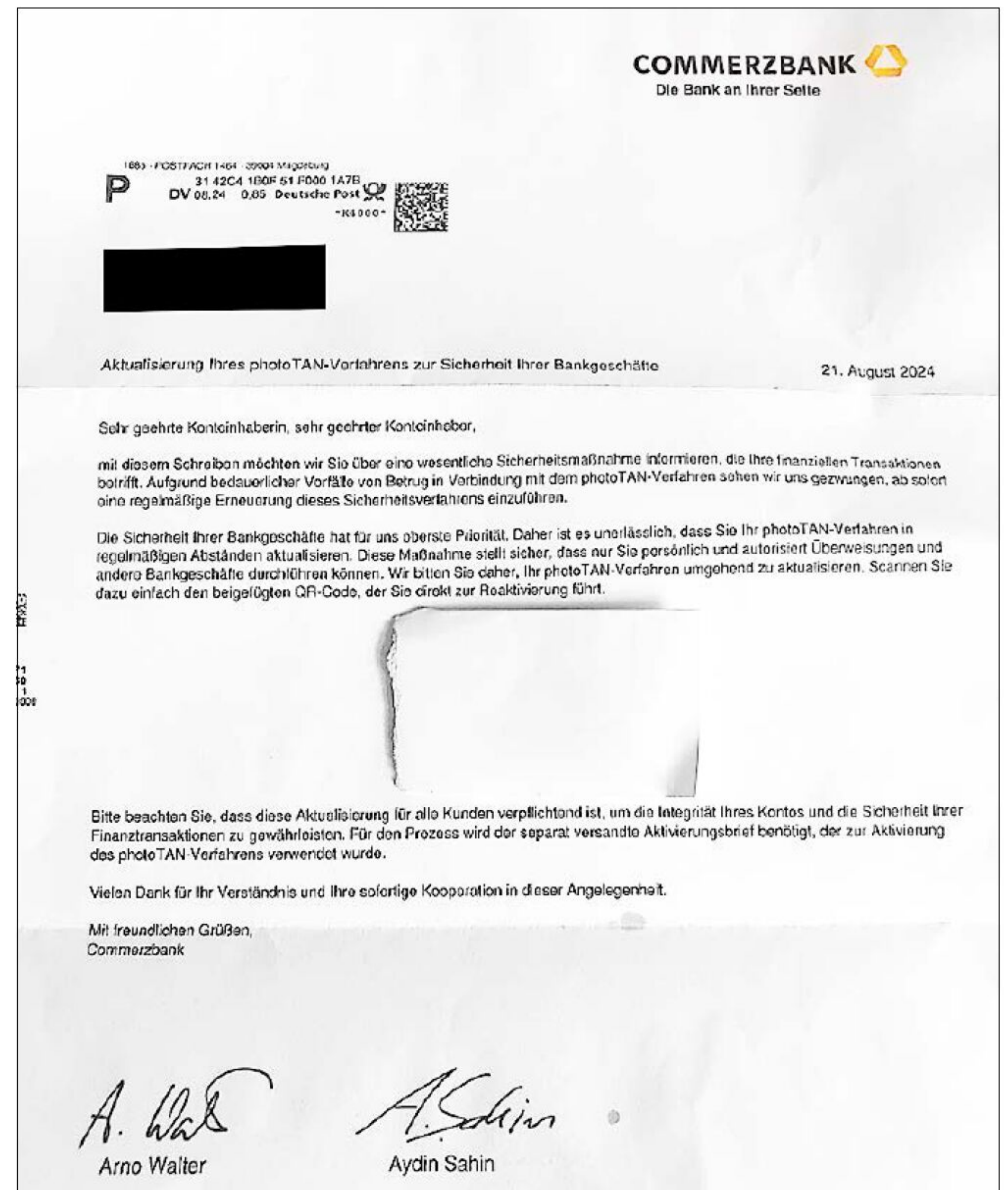
Betrug mit gefälschten Immobilienanzeigen

Mit einem besonders raffinierten Trick ergatterten Betrüger einen Kredit über 30.000 Euro, den jetzt vermutlich ihre Opfer abbezahlen müssen. Alles begann ganz harmlos mit einem Inserat bei Immoscout24, das in Berlin-Tiergarten eine Dreizimmerwohnung für 900 Euro Miete anbot – für Berliner Verhältnisse ein sehr günstiger Mietpreis. Der Anbieter verlangte in dem Inserat von den Interessenten diverse Unterlagen, darunter auch Gehaltsabrechnungen und Bankdaten.

Ein junges Paar beschloss, sich für die Wohnung zu bewerben, und reichte die geforderten Unterlagen ein. Vorsichtshalber überprüften sie die Domain der E-Mail-Adresse des Anbieters. Sie verwies auf die Website eines seriösen Immobilienmaklers. Es schien alles in Ordnung zu sein. Eines hatten sie jedoch übersehen. In der echten Website-Adresse wird der Name des Maklers zusammengeschrieben, in der E-Mail-Adresse stand jedoch zwischen Vor- und Nachnamen ein Bindestrich. Außerdem hatten die Betrüger vorgesorgt: Gab man die Webadresse mit Bindestrich ein, wurde man automatisch auf die Seite des echten Maklers weitergeleitet. Da alles zu stimmen schien, schickte das Paar seine Unterlagen daraufhin an die E-Mail-Adresse des angeblichen Maklers.

Einige Stunden später sperrte Immoscout24 die Anzeige. Das Paar erstattete Anzeige bei der Polizei und erhielt eine Vorgangsnummer. Der Fall schien damit für das Paar erledigt.

Der Quishing-Brief, wie er von den Betrügern verschickt wurde. Das Foto stammt von der Empfängerin, die ihn an die Verbraucherzentrale weiterleitete. Der QR-Code in der Mitte ist abgedeckt.



Auf ihrer Website warnt die Commerzbank vor Briefen mit einem gefälschten QR-Code.



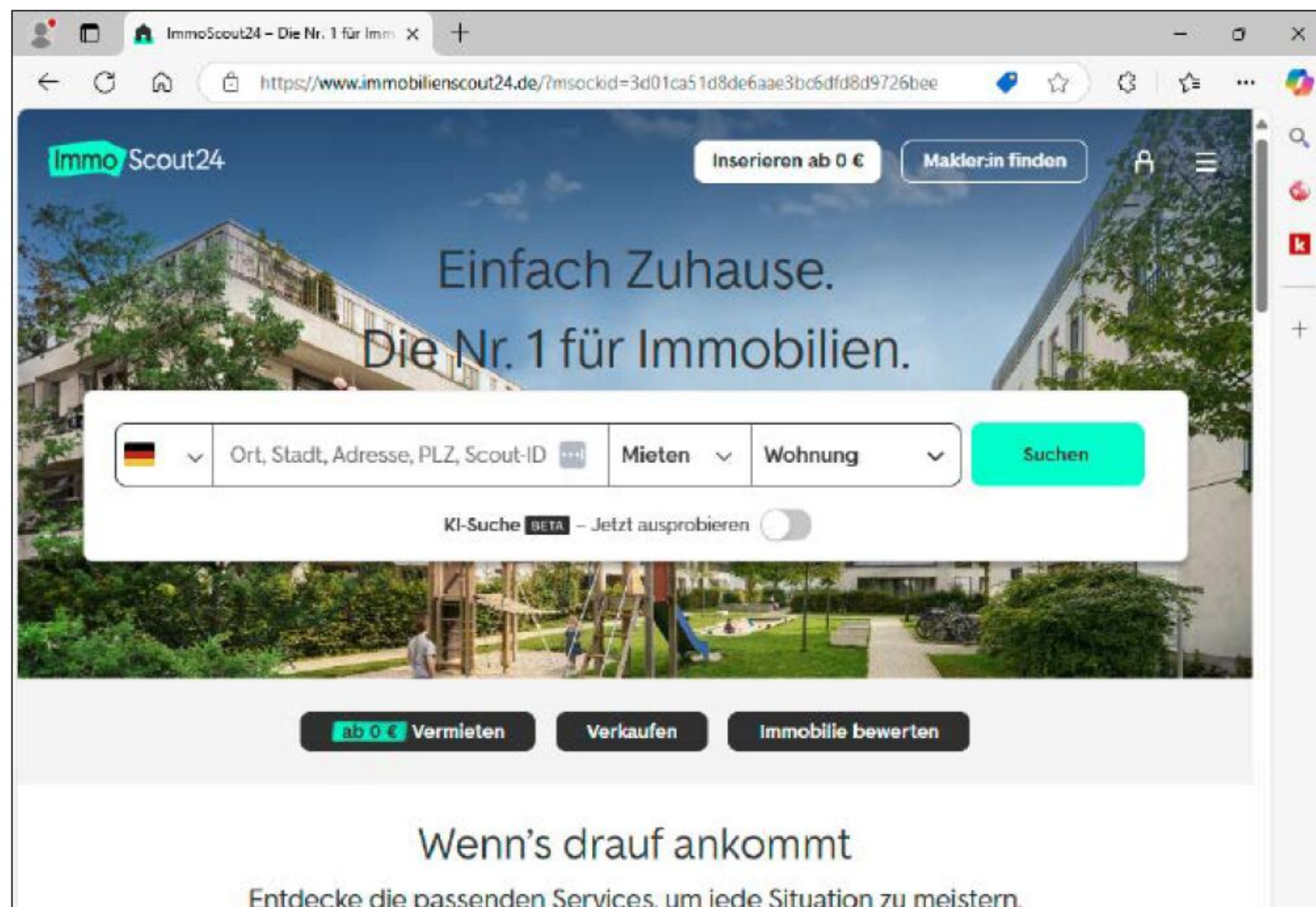
Kredit unter Vorspiegelung einer falschen Identität

Einige Wochen später bekamen sie jedoch Post von ihrer Bank. Sie forderte eine Verifizierung für ein bereits seit Jahren bestehendes Konto an. Das Paar bestätigte seine Identität per Postident-Verfahren. Ohne es zu wissen, genehmigte es damit einen Kredit über 30.000 Euro mit einer Laufzeit von fünf Jahren. In dieser Zeit sollten sie nun monatlich 532 Euro abbezahlen.

Das Paar wandte sich daraufhin an seine Bank und verwies auf die bereits erstattete Anzeige bei der Polizei. Die Bank zeigte sich

zunächst wenig kooperativ, willigte dann jedoch ein, die Ratenzahlungen vorerst zu pausieren. Anhand von Schufa-Auszügen stellte das Paar später fest, dass die Betrüger noch bei 13 weiteren Banken versucht hatten, in ihrem Namen einen Kredit über 30.000 Euro zu bekommen.

Der echte Immobilienmakler wiederum erklärte, dass sich noch weitere Betroffene bei ihm gemeldet hätten. Immoscout24 schließlich verwies das Paar lediglich an die Polizei und gab ansonsten den Hinweis, dass Bewerber ihre Unterlagen nicht per Mail an den Makler oder Vermieter, son-



Betrüger nutzten das Immobilienportal Immoscout24, um an die Bankdaten eines jungen Paares zu gelangen und damit einen Kredit von 30.000 Euro zu beantragen.

der immer nur ausgedruckt an sie schicken sollten. Der Anbieter bekäme dann eine Bestätigung, dass die Unterlagen vollständig seien, könnte sie aber zunächst nicht einsehen.

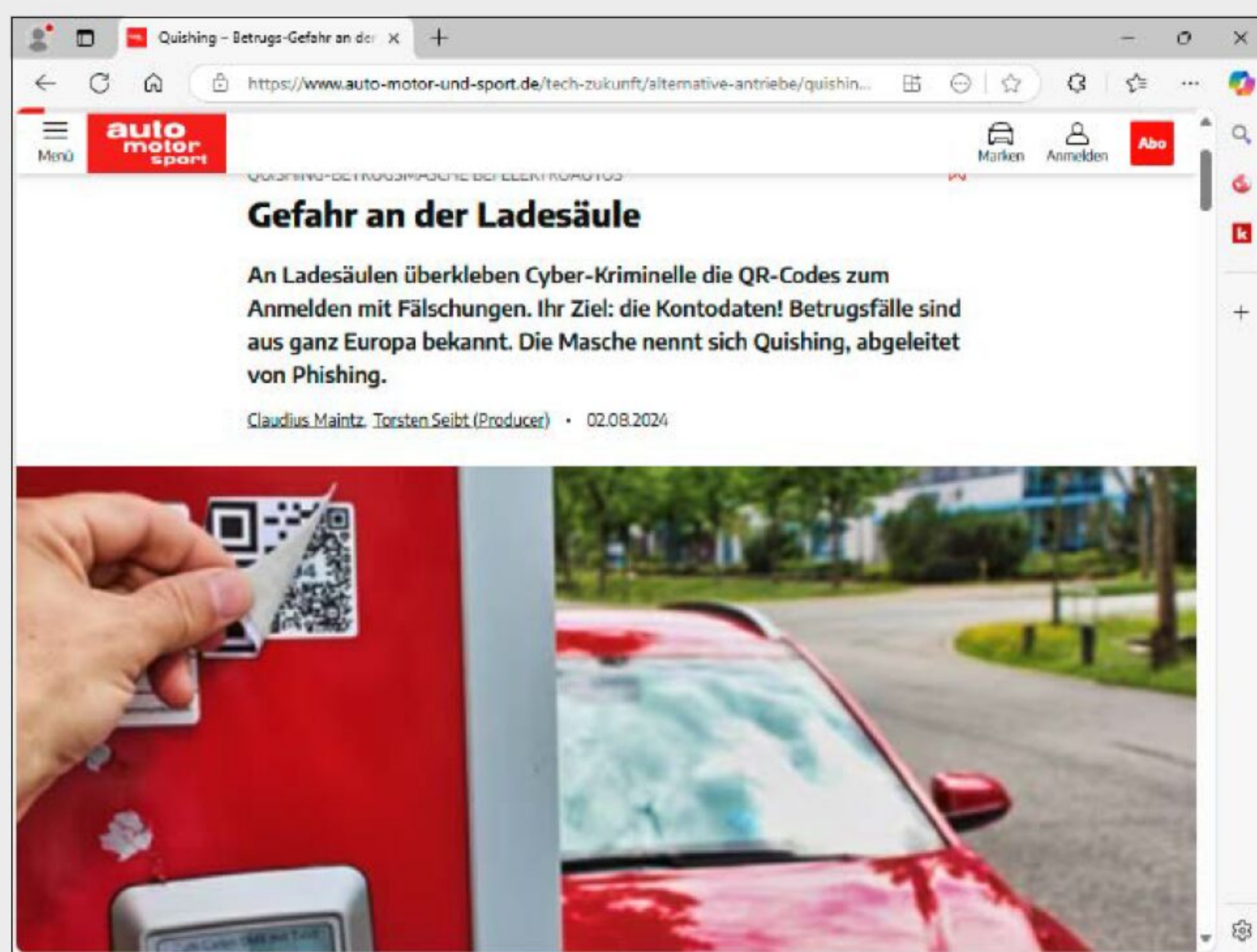
Wer den 30.000-Euro-Kredit letztlich bezahlen muss, ist nach wie vor ungeklärt.

1N Telecom begrüßt neue Kunden – ohne Vertragsabschluss

Die Verbraucherzentralen führen derzeit mehrere Prozesse gegen die Düsseldorfer Telekommunikationsfirma 1N Telecom. Das Unternehmen hat in den vergangenen Monaten Schreiben an Privatpersonen ge-

QUISHING-ATTACKEN AN ÖFFENTLICHEN PLÄTZEN

In der zweiten Jahreshälfte 2024 wurden mehrere Fälle bekannt, in denen Kriminelle die QR-Codes an Ladesäulen für E-Autos überklebt hatten. Die neuen Codes führten zu gefälschten Zahlungssites, wo die Benutzer der Ladesäulen ihre Kreditkartendaten eingeben sollten. Der ADAC rät daher, keine überklebten QR-Codes zu scannen. In den meisten Fällen benötigen die Benutzer keinen Code, sondern können den Ladestrom über eine App oder die Karte eines anderen Anbieters bezahlen. Sollte dennoch einmal das Einlesen eines QR-Codes notwendig sein, sollten die Benutzer ihn möglichst auf dem Display der Ladesäule scannen.



Die Zeitschrift Auto Motor Sport berichtet über Fälle aus ganz Europa, in denen Kriminelle die Benutzer von Ladesäulen mit gefälschten QR-Codes auf betrügerische Websites gelotst haben.

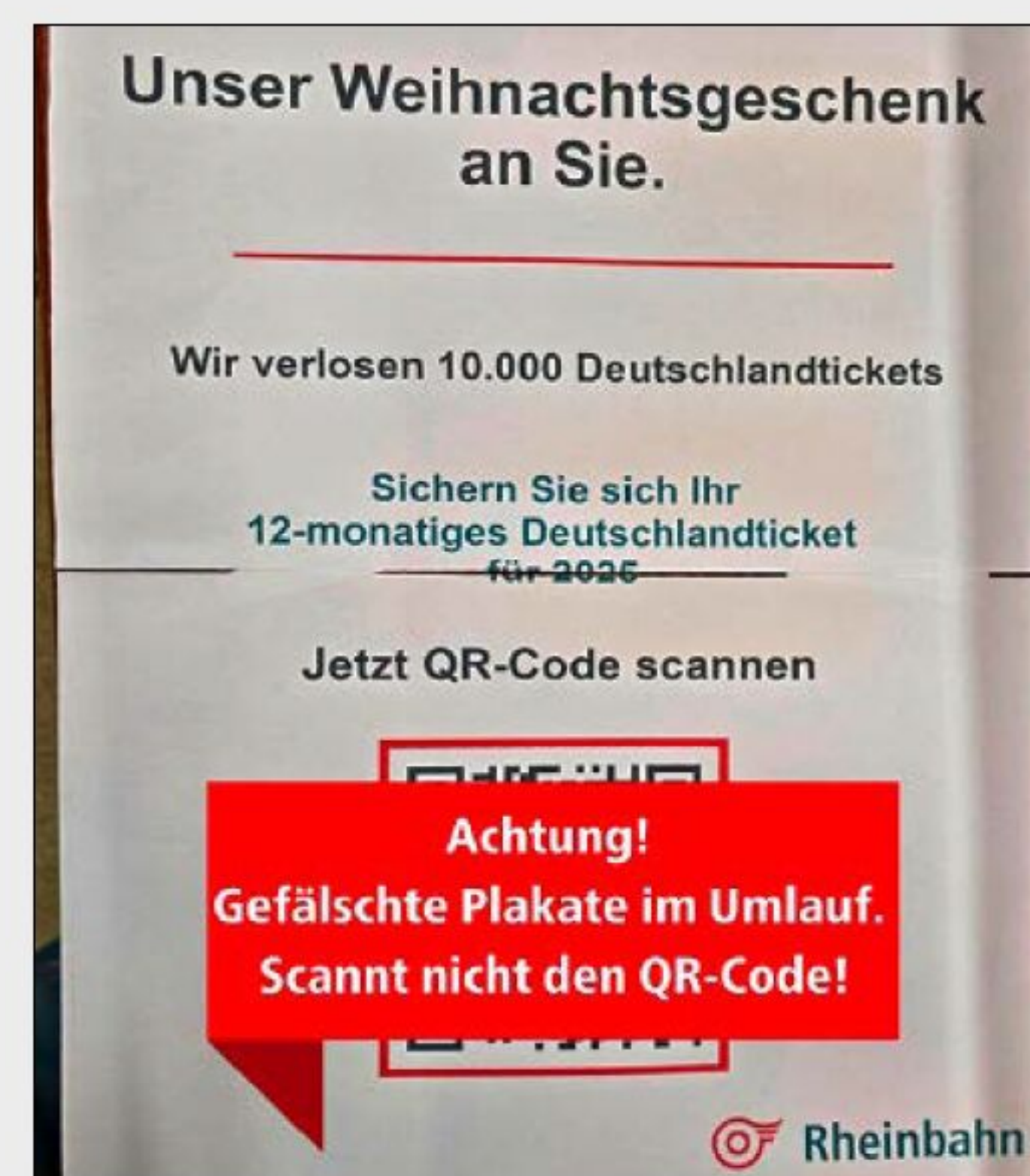
Ebenfalls überklebt wurden im November 2024 die QR-Codes an Parkscheinautomaten in Hannover. Angeblich sollte der Link zur Firma Easypark führen, tatsächlich aber öffnete er eine gefälschte Webseite. Auch hier wurde versucht, Kreditkartendaten abzugreifen. Schließlich versuchten es Kriminelle auch bei Strafzetteln mit Quishing. In einigen Städten klemmt

die Polizei Falschparkern einen Zettel mit einem QR-Code unter den Scheibenwischer, über den die Fahrer eine Seite erreichen, wo sie die Strafe direkt bezahlen können. Kriminelle fälschten diese Zettel und verteilten sie ihrerseits an parkende Fahrzeuge. Verbraucherschützer empfehlen, mit verdächtigen Strafzetteln sofort zur Polizei zu gehen und den Sachverhalt dort zu klären.

Im Dezember 2024 warnte die Düsseldorfer Rheinbahn vor gefälschten Plakaten in ihren Bussen und Straßenbahnen. Sie waren mit dem Logo des Verkehrsunternehmens versehen und kündigten eine Verlosung von Deutschlandtickets an. Um an der Verlosung teilzunehmen, müsse man den abgedruckten QR-Code scannen. Wer das tat, gelangte zu einer Seite, die natürlich nicht von der Rheinbahn ins Netz gestellt worden war. Dort sollte man Name, Anschrift, E-Mail-Adresse und Telefonnummer eingeben. Die Verbraucherschutzzentrale vermutet, dass die Daten entweder verkauft werden oder als Basis für Identitätsdiebstähle mit anschließendem Betrug dienen.



Die Stadt Hannover warnt vor gefälschten QR-Codes an Parkscheinautomaten. Betrüger wollen auf diese Weise persönliche Daten abgreifen.



Die Plakate in den Verkehrsmitteln der Düsseldorfer Rheinbahn waren amateurhaft gestaltet und bestanden einfach nur aus zwei aneinandergeklebten DIN-A4-Blättern.

schickt und sie dazu aufgefordert, den Vertrag bei ihrem aktuellen Telefonanbieter zu kündigen und 1N Telecom einen Portierungsauftrag zum Übertragen der Rufnummer zu erteilen. Wer dieser Aufforderung nicht folgte, bekam einige Monate später einen weiteren Brief mit einer Schadenersatzforderung in dreistelliger Höhe. 1N Telecom begründet die Forderung damit, dass die angeschriebene Person ihrem alten Telefonanbieter bisher keinen Auftrag zum Wechsel erteilt habe und 1N Telecom daher den bestehenden Vertrag nun vorzeitig beenden müsse.

Wohlgemerkt: Die angeschriebene Person hatte nicht unterschrieben und die Briefe von 1N Telecom einfach nur ignoriert.

1N Telecom: Irreführende Werbung mit IBAN-Trick

In anderen Fällen verschickte 1N Telecom Briefe mit Werbung für seinen DSL-Tarif. Darin stand, dass der Adressat in das beiliegende Formular lediglich seine IBAN eintragen und unterschreiben müsse. Dann würde automatisch der Vertrag mit dem bestehenden Anbieter gekündigt und eine Portierung der Rufnummer in die Wege geleitet.

Betroffene meldeten sich daraufhin bei den Verbraucherzentralen und gaben an, dass sie den Brief für ein Schreiben der Deutschen Telekom gehalten hätten. Er sei ihnen so vorgekommen wie ein Angebot für einen Wechsel in einen günstigeren Tarif. Sie hätten jedoch nie vorgehabt, zu einem anderen Telekommunikations-Anbieter zu gehen.

Wer keinen Vertrag mit 1N Telecom abgeschlossen hat, soll laut den Verbraucherzentralen die Forderungen der Firma nicht bezahlen. Stattdessen solle er einen Nachweis über den Vertragsabschluss anfordern, aber gleichzeitig vorsichtshalber Widerspruch einlegen.

Außerdem solle er beim Datenschutzbeauftragten von 1N Telecom Auskunft verlangen, auf welcher Rechtsgrundlage das Unternehmen ihn angeschrieben hat. Laut Datenschutzgrundverordnung (DSGVO) Paragraph 12 muss 1N Telecom ihm „unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags“ Auskunft erteilen. Die Verbraucherzentralen halten unter dem Link <https://tinyurl.com/3vm3zbas> entsprechende Musterbriefe für Betroffene bereit. ■

Die Firma 1N Telecom stellt Rechnungen aus, wenn jemand bei seinem bisherigen Telefonanbieter keinen Wechselauftrag einreicht – auch wenn er nie einen Vertrag unterschrieben hat.

1N Telecom verunsicherte in der Vergangenheit Privatpersonen mit Angeboten zum Anbieterwechsel. Unklar ist, woher die Firma die Adressen bekam.



SO SCHÜTZEN SIE SICH VOR QUISHING

- **Benutzen Sie nur QR-Code-Scanner**, die zunächst die Adresse anzeigen und nicht sofort die im Code verschlüsselte Seite aufrufen. Die meisten Kamera-Apps der Smartphones arbeiten heute so, aber auch der Großteil der Scanner im Google Play Store und im App Store von Apple.
- **Achten Sie bei den Internetadressen** genau auf die Schreibweise, vor allem auf Binde- und Schrägstriche und kleine Schreibfehler. Überlegen Sie sich auch, ob eine Adresse plausibel ist. Wenn etwa Ihre Heimatstadt eine ausländische Domain benutzt, stimmt etwas nicht. Ganz generell gilt: Kommt Ihnen etwas verdächtig vor, sollten Sie dem Link nicht folgen.
- **Wenn Sie einen ungewöhnlichen oder verdächtigen Brief** Ihrer Bank oder eines anderen Unternehmens erhalten, rufen Sie beim Absender an. Verwenden Sie dabei nicht die im Brief angegebene Telefonnummer, sondern suchen Sie die Nummer auf der Website im Internet heraus. Banken kommunizieren mit ihren Kunden heute vornehmlich über ein Onlinepostfach. Sehen Sie nach, ob es dort Benachrichtigungen gibt, die sich auf den Brief beziehen.
- **Sehen Sie bei Ladesäulen** und Parkscheinautomaten nach, ob der QR-Code überklebt wurde. Falls ja, scannen Sie ihn nicht.

Eigene Daten vor KI-Nutzung schützen

Im Kampf um die Vorherrschaft auf dem KI-Markt nehmen die Hersteller oft keine Rücksicht auf das Urheberrecht. Doch es gibt Mittel und Wege, wie Anwender ihre Daten vor dem Zugriff der KI-Unternehmen schützen können.



© Mit Material von Benjamin Haas - AdobeStock

VON ROLAND FREIST

Künstliche Intelligenz beruht auf Daten. Auf je mehr Daten die KI-Modelle zurückgreifen können, desto besser fallen die Ergebnisse bei Abfragen aus. Die großen Chatbot-Entwickler wie Open AI, Meta, Google und Microsoft sammeln daher alles an Daten ein, was ihre Crawler im Web nur finden können. Texte, Bilder, Videos aller Art, alles wandert in ihre Rechenzentren.

Denn die Antworten der KI-Chatbots basieren auf Wahrscheinlichkeitsrechnung: Die KI berechnet, welche Antwort die höchste Wahrscheinlichkeit aufweist, und arbeitet auch bei der Formulierung mit Wahrscheinlichkeiten, indem sie Wortaneinanderreihungen aus dem Internet zu Trainingszwecken übernimmt. Je mehr Inhalte die KI-Crawler zusammentragen, desto umfangreicher wird der Wissensschatz der KI, und desto präziser und besser formuliert werden ihre Antworten.

„Mit diesen Tipps erfährt die KI weniger über Sie.“

Und wie fast immer, wenn eine neue Technik für Furore sorgt, kümmern sich die Unternehmen erst einmal um die Entwicklung und den Ausbau ihrer Marktanteile. Das Rechtliche folgt später. Die Produzenten der Webinhalte gehen deshalb bislang leer aus. Denn obwohl die KI-Modelle ohne fremde Inhalte nicht funktionieren würden, weigern sich die dahinterstehenden Firmen meist, für die Nutzung von Texten im Internet zu bezahlen. Mittlerweile haben mehrere Zeitungen, Zeitschriften und Verlage gegen diese Praxis geklagt. Endgültige Urteile sind jedoch noch nicht ergangen.

Klage gegen den Facebook-Mutterkonzern

Mitte 2025 ging der Eilantrag der Verbraucherzentrale NRW gegen den Facebook-Mutterkonzern Meta durch die Presse. Das Unternehmen hatte angekündigt, ab dem 27. Mai 2025 sämtliche Daten der Facebook- und Instagram-Nutzer für das Training seiner Meta-KI zu verwenden. Dazu zählen laut Meta die Posts, Fotos und Videos der Nutzer sowie die Kommentare unter anderen Einträgen und Reaktionen wie Likes. Voraussetzung ist, dass diese Inhalte öffentlich sind, also nicht über die Profileinstellungen der Dienste für Außenstehende gesperrt sind.

Außerdem will der Konzern ausschließlich auf Daten von Personen mit einem Mindestalter von 18 Jahren zugreifen.

Doch der Eilantrag scheiterte. Das Verwaltungsgericht Köln verwies auf die Einschätzung der irischen Datenschutzbehörde, die in der EU für Meta zuständig ist. Der Behörde zufolge ist die Datensammlung mit EU-Recht vereinbar.

Bis zum 26. Mai konnten die Nutzer von Facebook und Instagram noch mit einem Einspruch die Verwendung ihrer bereits vorhandenen Daten verhindern. Wer allerdings diese Frist versäumte und keinen Einspruch erhob, dessen Daten sind inzwischen in dem riesigen neuronalen Netz der KI aufgegangen. Persönliche Datensätze im Nachhinein wieder daraus zu entfernen ist unmöglich. Sie können jedoch trotzdem Einspruch einlegen und auf diese Weise zumindest die Nutzung der Daten verhindern, die Sie in Zukunft bei den beiden Diensten eingeben. Bei Facebook finden Sie das entsprechende Formular nach einem Log-in unter <https://tinyurl.com/3k9u4cxj>, bei Instagram unter <https://tinyurl.com/4z6nwezu>.

Der Messenger Whatsapp, der ebenfalls zu Meta gehört, ist von der Datensammlung nicht betroffen. Die Chats in diesem Dienst

sind Ende-zu-Ende verschlüsselt, das Unternehmen hat also keinen Zugriff auf die Inhalte. Lediglich die Nachrichten, die direkt an „Meta AI“ geschickt werden, können von der Firma ausgewertet und verwendet werden.

Das in der App angezeigte Symbol „Meta AI fragen“, der blau-violette Kreis, lässt sich nicht deaktivieren oder entfernen. Solange Sie es jedoch nicht antippen und die Funktion benutzen, erhält die KI auch auf diesem Weg keine Daten von Ihnen.

Andere Social-Media-Daten schützen

Aber nicht nur die Dienste von Meta greifen Ihre Postings und andere persönliche Daten ab. Auch X, ehemals Twitter, behält sich vor, die veröffentlichten Beiträge zum Training zu verwenden, in diesem Fall für den Chatbot Grok von xAI. Sie können dieser Nutzung jedoch widersprechen. Klicken Sie dazu im X-Menü auf „Mehr → Einstellungen und Datenschutz → Datenschutz und Sicherheit → Grok und unabhängige Kooperationspartner“ und löschen Sie das Häkchen bei „Erlauben, dass deine öffentlichen Daten sowie deine Interaktionen, Eingaben und Ergebnisse bei Grok und xAI für Training und Feinabstimmung herangezogen werden“. Die beiden anderen Optionen an dieser Stelle sind in der Voreinstellung inaktiv und sollten es auch bleiben.

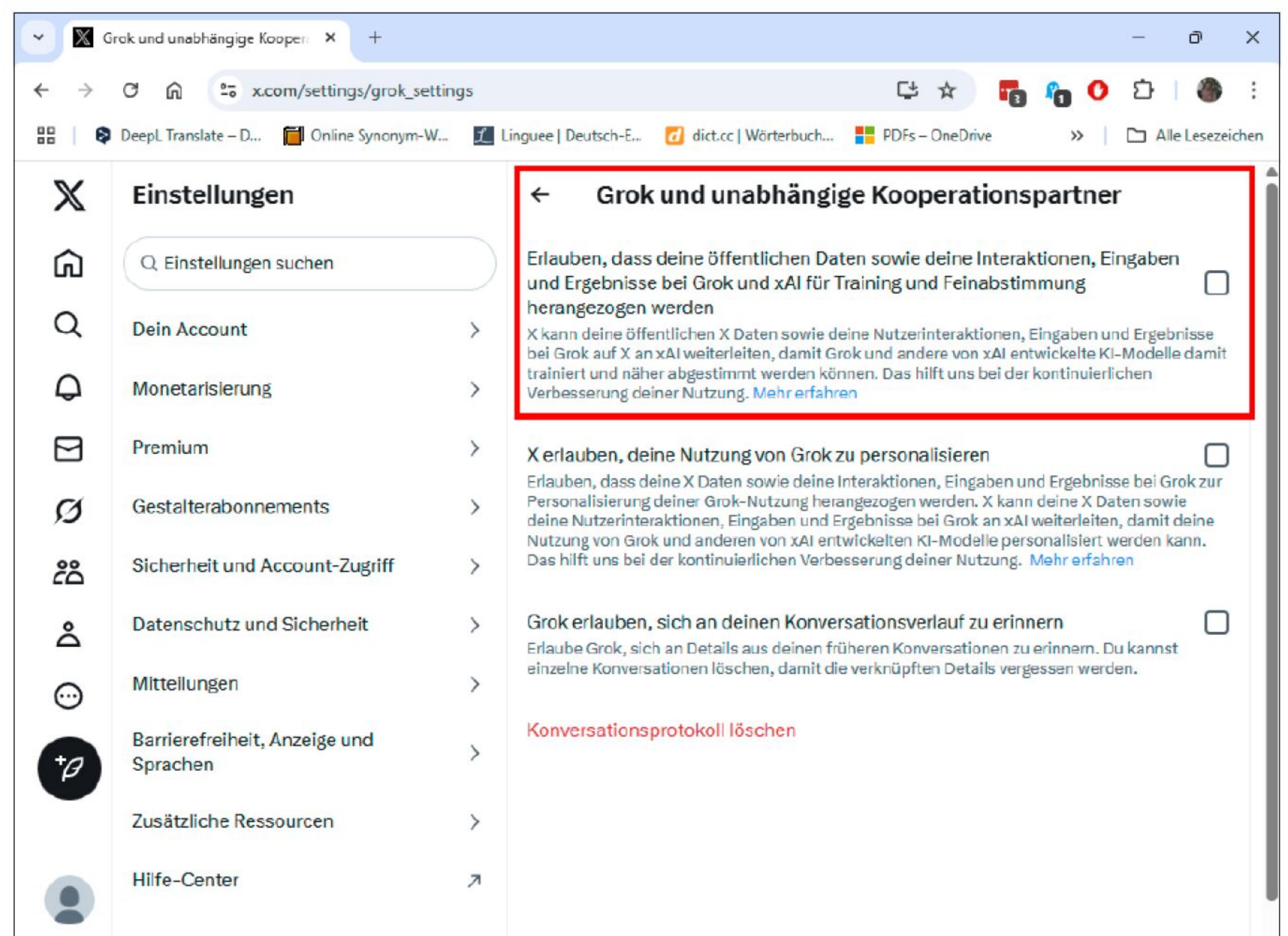
Das soziale Netzwerk LinkedIn gibt an, dass es die Daten seiner Mitglieder so wenig wie möglich verwendet. Wenn Sie oben in der Menüleiste auf Ihr Profilbild klicken und „Einstellungen und Datenschutz → Datenschutz“ aufrufen, finden Sie dort die Option „Daten zur Verbesserung generativer KI“. Nach einem Klick erfahren Sie jedoch, dass LinkedIn die generative KI in Ihrer Region nicht mit Nutzerdaten schult. Und: Wenn Sie diese Seite ein zweites Mal ansteuern wollen, ist sie plötzlich verschwunden. Erst nachdem Sie sich aus- und wieder eingeloggt haben, taucht sie wieder auf.

Tiktok verwendet KI, um die Videofeeds auf den Benutzer zuzuschneiden. Außerdem nutzt Bytedance, die Firma hinter Tiktok, die Daten für das Training ihrer KI-Modelle. Wie und in welchem Umfang das geschieht, ist unbekannt. Eine Möglichkeit zum Einspruch besteht in der aktuellen Tiktok-App nicht.

Ähnlich bei Youtube: Der Videodienst benutzt KI für personalisierte Videoempfeh-



Facebook hat genauso wie Instagram ein Formular online gestellt, mit dem die Benutzer die Verwendung ihrer Daten für das Training der Meta AI verbieten können.



Auch in X können Sie den Gebrauch Ihrer Daten für das Training von Chatbots unterbinden. In diesem Fall geht es um Grok von der Firma xAI. Achten Sie darauf, dass das entsprechende Kontrollkästchen leer ist.

lungen, das Erzeugen von Untertiteln und die Erkennung von Urheberrechtsverstößen. Für das Training greift Google auf Methoden des maschinellen Lernens zurück. Eine Widerspruchsmöglichkeit gegen die Verwendung persönlicher Daten gibt es nicht. Sie können Ihre Videos lediglich privat oder nicht gelistet hochladen. Dadurch

sinkt die Wahrscheinlichkeit, dass sie in den KI-Modellen aufgehen.

Eigene Website-Inhalte vor ChatGPT & Co. schützen

ChatGPT und die anderen KI-Modelle sammeln im Internet alle Inhalte ein, derer sie habhaft werden können. Dazu gehören



Einstellung nicht verfügbar

Diese Einstellung ist an Ihrem Standort nicht verfügbar, da wir die generative KI nicht schulen, Inhalte mithilfe von Mitgliederdaten aus Ihrer Region zu erstellen.

[Mehr erfahren](#)

[Zu den Einstellungen](#)

[Zur Startseite](#)

Linkedin gibt an, dass es in Deutschland keine Daten zur Verbesserung generativer KI sammelt.

auch die Inhalte privater Websites. Wenn Sie nicht wollen, dass die KI-Modelle auch Ihre Webinhalte in ihre Indexe aufnehmen, haben Sie folgende Möglichkeiten:

- Nehmen Sie die Crawler der KI-Modelle in die „robots.txt“ auf. Diese Datei wird im Stammverzeichnis einer Website abgelegt und diente ursprünglich dazu, den Crawler

openai.com/gptbot.json

Quelltextformatierung

```
{
  "creationTime": "2025-05-22T11:51:00.000000",
  "prefixes": [
    {
      "ipv4Prefix": "52.230.152.0/24"
    },
    {
      "ipv4Prefix": "20.171.206.0/24"
    },
    {
      "ipv4Prefix": "20.171.207.0/24"
    },
    {
      "ipv4Prefix": "4.227.36.0/25"
    },
    {
      "ipv4Prefix": "20.125.66.80/28"
    },
    {
      "ipv4Prefix": "172.182.204.0/24"
    },
    {
      "ipv4Prefix": "172.182.214.0/24"
    },
    {
      "ipv4Prefix": "172.182.215.0/24"
    }
  ]
}
```

Open AI veröffentlicht im Web die IPv4-Adressen der Webcrawler, mit denen die Firma nach Trainingsmaterial für ihre KI-Projekte sucht.

lern der Suchmaschinen zu sagen, welche Teile einer Website sie in ihren Index übernehmen dürfen und welche nicht. Mittler-

weile können Sie über die „robots.txt“ auch die Crawler der KI-Modelle ansprechen und ihnen die Nutzung der Website-Inhalte verbieten. Das sieht dann so aus:

User-agent: ChatGPT-User
Disallow: /

User-agent: GPTBot
Disallow: /

User-agent: Google-Extended
Disallow: /

User-agent: anthropic-ai
Disallow: /

User-Agent: PerplexityBot
Disallow: /

User-Agent: Applebot-Extended
Disallow: /

Beachten Sie, dass zwischen den einzelnen Einträgen jeweils eine Leerzeile stehen muss. Erwarten Sie sich insgesamt jedoch nicht zu viel von dieser Maßnahme. Denn einige Crawler sind so programmiert, dass sie die „robots.txt“ ganz einfach ignorieren.


KI-ANFRAGEN MASKIEREN

Wenn Sie einen Chatbot bitten, eine Bewerbung für Sie zu schreiben oder etwa auch einen Brief an eine Versicherung aufzusetzen, erfährt die KI notwendigerweise viele private Details über Sie. Um das zu verhindern, hat der Entwickler Frank Börncke ein kleines Open-Source-Tool geschrieben, das die privaten Daten, die Sie per Prompt an den Chatbot übergeben, automatisch durch frei wählbare, erfundene Angaben ersetzt. So können Sie beispielsweise Ihren Namen und Ihre Adresse durch einen anderen Namen und eine andere Adresse überschreiben lassen. Aber auch Telefonnummern, E-Mail-Adressen, Kreditkarten- und Kontonummern lassen sich auf diese Weise vor der KI geheim halten. Zunächst definieren Sie in Private Prompts (www.privateprompts.org, kostenlos, Deutsch) – so heißt die Software – die Angaben, die anstatt Ihres echten Namens, der Adresse et cetera an den Chatbot übergeben werden sollen. Anschließend schreiben Sie Ihren Prompt und klicken auf den Button „Mask“. Das Programm sucht und ersetzt nun automatisch alle persönlichen Angaben in der Anfrage. Danach kopieren Sie den Text und fügen ihn in den Chatbot Ihrer Wahl ein. Die Antwort der KI kopieren Sie wiederum in Private Prompts, klicken auf „Unmask“ und erhalten eine Bewerbung oder ein Schreiben an die Versicherung mit Ihren echten Daten.

Neben dieser Grundfunktion stellt Private Prompts auch einen Prompt-Manager zur Verfügung, mit dem Sie häufig wiederkehrende Prompts speichern und verwalten können.

Private Prompts

File Edit View Window Navigation Help



PRIVATE PROMPTS PROMPT MANAGER PRIVACY REGELN SYSTEM EINSTELLUNGEN

Private Prompts - Schütze Deine Daten

Originaler Prompt

Schreibe eine freundliche Bewerbung für Roland Fraist

Maskierter Prompt

Schreibe eine freundliche Bewerbung für Gerd Schmidt

Geben Sie Ihr Prompt ein

MARK MASK UNMASK

Mit der Open-Source-Software Private Prompts können Sie Ihre Anfragen an die KI-Chatbots maskieren, also mit falschen persönlichen Daten abschicken.

- Sicherer ist die Sperre der IP-Adressbereiche der Webcrawler. Leider gibt lediglich Open AI die zugehörigen IPv4-Adressen bekannt. Sie finden sie unter <https://openai.com/gptbot.json>.
- Führen Sie für Ihre Website ein Rate Limiting ein. Damit setzen Sie eine Grenze für Anfragen, die von ein und derselben Quelle stammen.

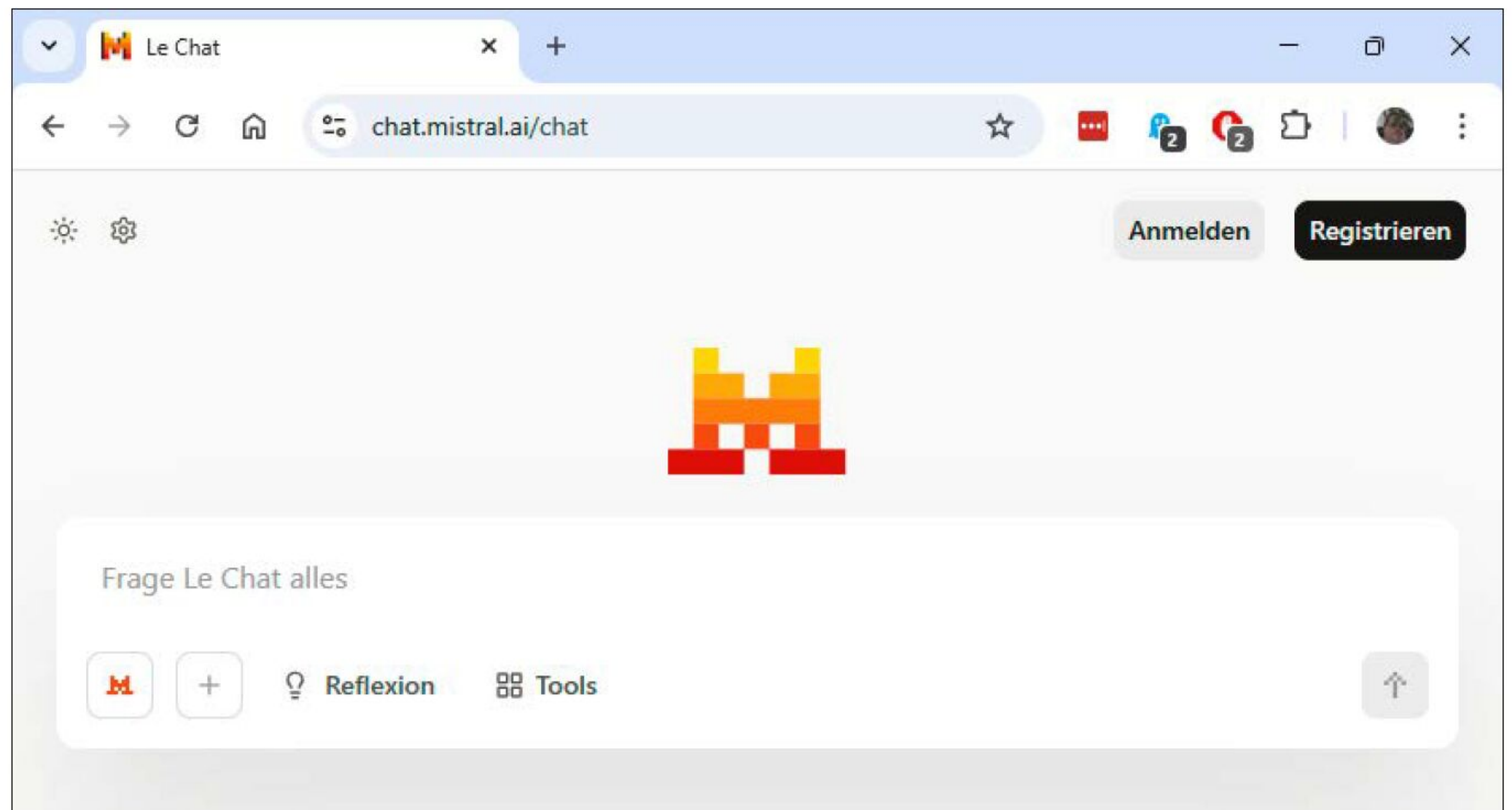
Die Texte der Anfragen schützen

Neben den Inhalten der Websites greifen die Chatbots auch die Texte der Anfragen ab, die sie von den Nutzern bekommen. Das lässt sich zwar nicht verhindern, Sie können jedoch dafür sorgen, dass die KIs daraus keine personalisierten Profile generieren. Die wichtigste Maßnahme ist, kein Konto bei den KI-Modellen einzurichten. Anfragen ohne vorherige Registrierung lassen gleich mehrere Chatbots zu, unter anderem ChatGPT (<https://chatgpt.com>), Perplexity (www.perplexity.ai), Meta AI (www.meta.ai), und Le Chat (<https://chat.mistral.ai/chat>). Außerdem sollten Sie die Chatbots immer nur im Incognito- beziehungsweise Inprivate-Modus Ihres Browsers nutzen.

Datenschutz bei Microsoft Copilot

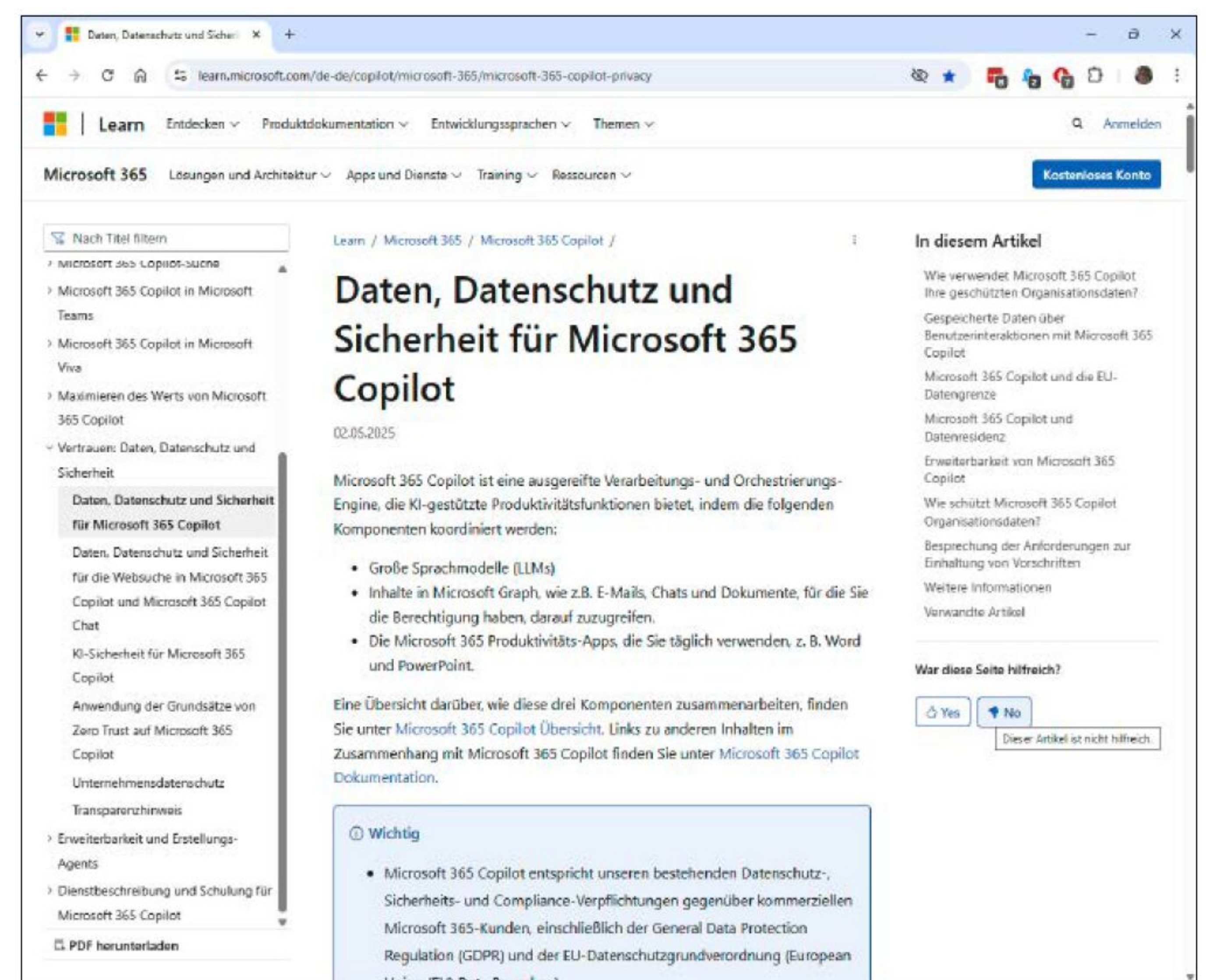
Die von Microsoft entwickelte KI Copilot ist direkt in die Büroanwendungen Word, Excel, Powerpoint et cetera integriert und kann Ihnen unter anderem beim Schreiben von Texten oder beim Beantworten von E-Mails helfen. Dazu ist es natürlich erforderlich, dass Copilot Texte und E-Mails liest und den Inhalt verarbeitet. Insbesondere bei geschäftlicher Korrespondenz ist es jedoch häufig Firmenrichtlinie, dass die Dokumente vertraulich bleiben und das Haus nicht verlassen dürfen.

Microsoft ist sich dieses Problems offensichtlich bewusst. So findet man auf der Website einen langen Artikel (<https://tinyurl.com/eujpa9fx>), der sich mit dem Datenschutz in Copilot befasst. Dort erklärt das Unternehmen, dass es zwar den Aktivitätsverlauf speichert, also die an Copilot gestellten Fragen und Aufgaben sowie die daraufhin erfolgten Antworten. Diese Daten werden jedoch laut Microsoft verschlüsselt und auf keinen Fall für das Training von Large Language Models (LLMs) verwendet. Außerdem verließen sie niemals das Gebiet der EU und unterlägen damit den Regelungen der europäischen Datenschutzgesetze. ■



Viele KI-Chatbots lassen sich auch ohne vorherige Registrierung nutzen, der Anwender bleibt anonym. Dazu gehört unter anderem auch Le Chat von Mistral AI.

Microsoft versichert in einem langen Beitrag auf seiner Website, dass die Fragen an Copilot und die erzeugten Antworten nicht zum Training von KI-Modellen verwendet werden.



WAS META MIT IHREN DATEN MACHT



Meta verwendet Ihre Daten bei Facebook und Instagram zum Trainieren seiner KI-Modelle. Doch was genau wird mit den Daten trainiert?

- Die Texte und Kommentare, die Sie in den Diensten eingegeben haben, dienen zum Verbessern des Sprachgebrauchs. Die KI lernt dadurch beispielsweise, sinnvolle, grammatisch korrekte Sätze zu bilden. Darüber hinaus wird sie jedoch auch darin geschult, Emotionen und Stimmungen zu erkennen und sowohl positive wie auch negative Gefühle aus einem Text abzulesen.
- Mit den Daten zu Ihrem Verhalten und Ihren Interaktionen mit anderen Nutzern ergänzt Meta Ihr Profil bei den Diensten. Ziel ist es, Ihre Nutzungsgewohnheiten zu erfassen, Ihr Verhalten vorhersagen zu können und mehr über Ihre Interessen zu erfahren. Damit will das Unternehmen Ihnen besser auf Ihre Person zugeschnittene Inhalte und Werbung einblenden können.
- Die bei Facebook und Instagram hochgeladenen Fotos und Videos schließlich dienen als Trainingsmaterial, um die Gesichtserkennung zu verbessern. Außerdem werden damit die Funktionen für die Bilderstellung der KI-Modelle optimiert.

IMPRESSUM

Anschrift



IDG Tech Media GmbH

Georg-Brauchle-Ring 23, 80992 München
Telefon: 089/36086-0
E-Mail Magazin: magazin@pcwelt.de
E-Mail pcwelt.de: online@pcwelt.de
Internet: www.pcwelt.de

Chefredakteur:

Sebastian Hirsch (v.i.S.d.P.)

VP DACH Sales:

Verena Yimen
E-Mail:
verena.yimen@foundryco.com

Druck: Mayr Miesbach GmbH,
Am Windfeld 15, 83714 Miesbach

Herstellung: Pia Küsters

WEITERE INFORMATIONEN

Redaktion Magazin

IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München
E-Mail: magazin@pcwelt.de

Chefredakteur:

Sebastian Hirsch
(verantwortlich für den redaktionellen Inhalt)

Stellvertretender Chefredakteur:

Thomas Rau (tr)
Chef vom Dienst:
Andrea Kirchmeier (ak)

Hardware & Testcenter:

Verena Ottmann (vo),
Ines Walke-Chomjakov (iwc)

Software & Praxis:

Arne Arnold (afa),
Peter Stelzel-Morawietz (psm)

Freie Mitarbeit Redaktion:

Marlene Buschbeck-Idlachemi, Thorsten Eggeling, Roland Freist, Andreas Hitzig, Michael Seemann, Daniel Wolski, Steffen Zellfelder

Freie Mitarbeit Layout:

Alex Dankesreiter, Andreas Förth

Freie Mitarbeit digitale Medien:

Ralf Buchner

Titelgestaltung:

Schulz-Hamparian, Editorial Design /
Thomas Lutz

Bildnachweis:

© AdobeStock – guteksk7, yun visual /
Anbieter, sofern nicht anders angegeben

Redaktion pcwelt.de

E-Mail: online@pcwelt.de

Chefredakteur:

Panagiotis Kolokythas (pk), (verantwortlich
für den redaktionellen Inhalt)

Redaktion:

Hans-Christian Dirscherl (hc), Daniel
Geßner (dg), Jérémie Kaiser (jk), Laura
Pippig (lp), Michael Schmelzle (ms),
Kris Wallburg (kw)

Head of New Media Growth & Partnerships:

Dennis Steimels (ds)

Video Producer B2C:

Christian Seliger

PC-WELT bei Facebook:

www.facebook.com/pcwelt

PC-WELT bei Twitter:

<http://twitter.com/pcwelt>

PC-WELT bei TikTok:

www.tiktok.com/@pcwelt.de

PC-WELT bei Youtube:

www.youtube.com/pcwelt.de

Einsendungen:

Für unverlangt eingesandte Beiträge sowie
Hard- und Software übernehmen wir keine
Haftung. Eine Rücksendegarantie geben wir
nicht. Wir behalten uns das Recht vor,
Beiträge auch auf anderen Medien, etwa
auf DVD oder online, zu veröffentlichen.

Copyright:

Das Urheberrecht für angenommene und
veröffentlichte Manuskripte liegt bei der IDG
Tech Media GmbH. Eine Verwertung der
urheberrechtlich geschützten Beiträge und
Abbildungen, insbesondere durch Vervielfältigung und/oder Verbreitung, ist ohne
vorherige schriftliche Zustimmung der IDG
Tech Media GmbH unzulässig und strafbar,
soweit sich aus dem Urheberrechtsgesetz
nichts anderes ergibt. Eine Einspeicherung
und/oder Verarbeitung der auch in elektro-

nischer Form vertriebenen Beiträge in
Datensysteme ist ohne Zustimmung der IDG
Tech Media GmbH unzulässig.

Haftung:

Eine Haftung für die Richtigkeit der Beiträge
können Redaktion und IDG Tech Media
GmbH trotz sorgfältiger Prüfung nicht
übernehmen. Die Veröffentlichungen in PC-
WELT erfolgen ohne Berücksichtigung eines
eventuellen Patentschutzes. Auch werden
Warennamen ohne Gewährleistung einer
freien Verwendung benutzt.

Anzeigen

Anzeigenabteilung:

Tel. 089/36086-0,
E-Mail-Adresse für Anzeigen:
germanysalesteam@foundryco.com

VP DACH Sales

Verena Yimen
+49 (0)174 188 66 32
verena.yimen@foundryco.com

Senior Sales Manager Consumer DACH

Saskia van der Kraaij
+49 (0)172 3254 197
saskia.vanderkraaij@foundryco.com

Senior Sales Manager Consumer

Bastian Wehner
+49 (0)174 85 38 245
bastian.wehner@foundryco.com

Digitale Anzeigenannahme – Datentransfer:

Zentrale E-Mail-Adresse:
anzeigendispo@foundryco.com

Digitale Anzeigenannahme – Ansprechpartner: Pia Küsters (-257),
E-Mail: pia.kuesters@foundryco.com

Anzeigenpreise:

Es gilt die Anzeigenpreisliste 37
(1.1.2020).

Bankverbindung:

Account Name: IDG TECH MEDIA GMBH
Account Number: 21875017
Account Currency: EUR
Bank Name: Bank of America,
N.A. London branch
IBAN: DE21500109000021875017
Branch Swift Address: BOFADEFX
Anschrift für Anzeigen: siehe
Anschrift IDG Tech Media GmbH

Erfüllungsort, Gerichtsstand: München

Verlagsrepräsentanten für Anzeigen in ausländischen Publikationen

Europa: Wolf Peter Lauck
+49 (0)176 3159 2152
peter.lauck@foundryco.com

Vertrieb

Vertrieb Handelsauflage:

MZV GmbH & Co. KG, Ohmstr. 1,
85716 Unterschleißheim,
Tel. 089/31906-0, Fax 089/31906-113
E-Mail: info@mzv.de
Internet: www.mzv.de

Druck: Mayr Miesbach GmbH,
Am Windfeld 15, 83714 Miesbach

Anschrift

IDG Tech Media GmbH

Georg-Brauchle-Ring 23,
80992 München
Tel. 089/36086-0
E-Mail Magazin: magazin@pcwelt.de,
E-Mail pcwelt.de: online@pcwelt.de,
Internet: www.pcwelt.de

Geschäftsführer:

Maria Savidou
Veröffentlichung gemäß § 8, Absatz 3
des Gesetzes über die Presse vom
8.10.1949

Gründer:

Patrick J. McGovern (1937 – 2014)

ISSN 2193-9225



PC-WELT-LESER-SERVICE

Haben Sie PC-Probleme?

Besuchen Sie einfach unser Forum im
Internet unter www.pcwelt.de/forum, und
schildern Sie dort Ihr Anliegen. Häufig
kennen andere PC-WELT-Leser die Lösung
für Ihr Problem!

Kontakt zur Redaktion

Wir haben E-Mail-Adressen für Sie
eingesetzt, falls Sie uns etwas mitteilen
wollen. Allgemeine Leserbriefe und
Anregungen zum Heft: magazin@pcwelt.de

PC-WELT-Kundenservice: Fragen zu
Bestellungen (Abonnement, Einzelhefte),
zum bestehenden Abonnement / Premium-
Abonnement, Umtausch defekter
Datenträger, Änderung persönlicher Daten
(Anschrift, E-Mail-Adresse, Zahlungsweise,
Bankverbindung) bitte an

**DataM-Services GmbH,
PC-WELT-Kundenservice,
Postfach 9161, 97091 Würzburg,
E-Mail:** idg-techmedia@datam-services.de
Tel: 0931/4170-177, **Fax:** 0931/4170-
497, Servicezeiten: 8 bis 17 Uhr
(an Werktagen Montag bis Freitag)

Jetzt
am
Kiosk!

Sonderheft
für nur
12,90 €

Erweiterte
Neuaufgabe mit
228 Seiten!



Bestellen unter
www.pcwelt.de/linuxwelt-xxl oder per Telefon: 0931/4170-177 oder ganz einfach:



1. Formular ausfüllen



2. Foto machen



3. Foto an idg-techmedia@datam-services.de

Ja, ich bestelle das LinuxWelt SH XXL 1/26 Tipps-Handbuch für nur 12,90 €.

Zzgl. Versandkosten (innerhalb Deutschland 3,- €, außerhalb 4,- €)

BESTELLEN	Vorname / Name			
	Straße / Nr.			
	PLZ / Ort			
	Telefon / Handy		Geburts- tag	TT MM JJJJ
	E-Mail			

BEZAHLEN	<input type="radio"/> Ich bezahle bequem per Bankeinzug. <input type="radio"/> Ich erwarte Ihre Rechnung.
	Geldinstitut
	IBAN
	BIC
	Datum / Unterschrift des neuen Lesers

PCWELT

Die beste Software 2026

Jetzt
am
Kiosk!

Sonderheft
für nur
9,90€

Auf DVD im Heft:
235 Programme
kostenlos!



Bestellen unter
www.pcwelt.de/pcwelt-sonderheft oder per Telefon: 0931/4170-177 oder ganz einfach:



1. Formular ausfüllen



2. Foto machen



3. Foto an idg-techmedia@datam-services.de

Ja, ich bestelle das PC-WELT SH 2/26 Die beste Software 2026 für nur 9,90 €.

Zzgl. Versandkosten (innerhalb Deutschland 3,- €, außerhalb 4,- €)

BESTELLEN	Vorname / Name			
	Straße / Nr.			
	PLZ / Ort			
	Telefon / Handy		Geburts- tag	TT MM JJJJ
	E-Mail			

BEZAHLEN	<input type="radio"/> Ich bezahle bequem per Bankeinzug.	<input type="radio"/> Ich erwarte Ihre Rechnung.
	Geldinstitut	
	IBAN	
	BIC	
	Datum / Unterschrift des neuen Lesers	