

SICHERHEIT

ALLES, WAS SIE ZUM SCHUTZ VON PC, NOTEBOOK UND SMARTPHONE BRAUCHEN

DIE LETZTE NOTFALL- DVD

• RETTEN • REPARIEREN
• SCHÜTZEN • PRÜFEN



8 SECURITY- SUITEN IM TEST

Antiviren-Programme im Labor-Check. Plus: Avast One **gratis** auf Heft-DVD!



EBAY, AMAZON, PAYPAL SICHER SHOPPEN

So schützen Sie sich vor Betrug und Abzocke beim Online-Shopping



EINBRUCH- SCHUTZ

Überwachungskameras im Test und Sicherheits-Tipps zur Urlaubszeit

**GESAMT-
WERT**
260 EURO

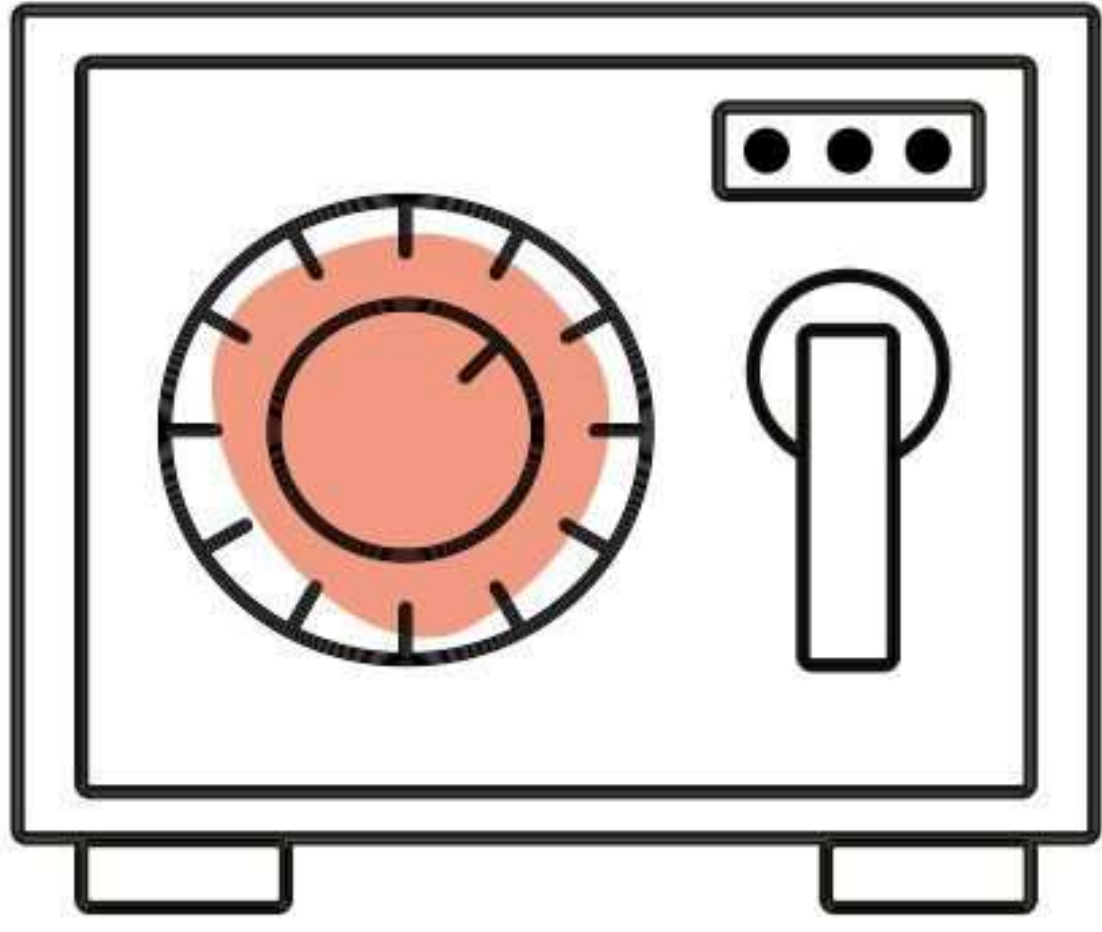
DAS GROSSE SOFTWARE PAKET

15 Vollversionen für mehr Sicherheit an PC, Mac und Handy

INFO-
Programm
gemäß
§ 14
JuSchG



Dein Cyber-Schutz: Tresor



Avast One

Hurra, Ihr Smart-Scan ist abgeschlossen!

Wir empfehlen, regelmäßig einen Smart-Scan auszuführen, um sicher und privat zu bleiben.

Fertig

Computer Bild

„BESTER IM PRAXISTEST“

Avast One

NOTE **2,0**

Ausgabe 6/2022
8 PRODUKTE IM VERGLEICH

Avast One

13:58

Willkommen bei Avast One

Lassen Sie uns Ihren ersten Smart-Scan ausführen

Finden und entfernen Sie Sicherheitsbedrohungen und verbessern Sie Ihre Privatsphäre mit diesem optimierten Scan.

Smart-Scan ausführen

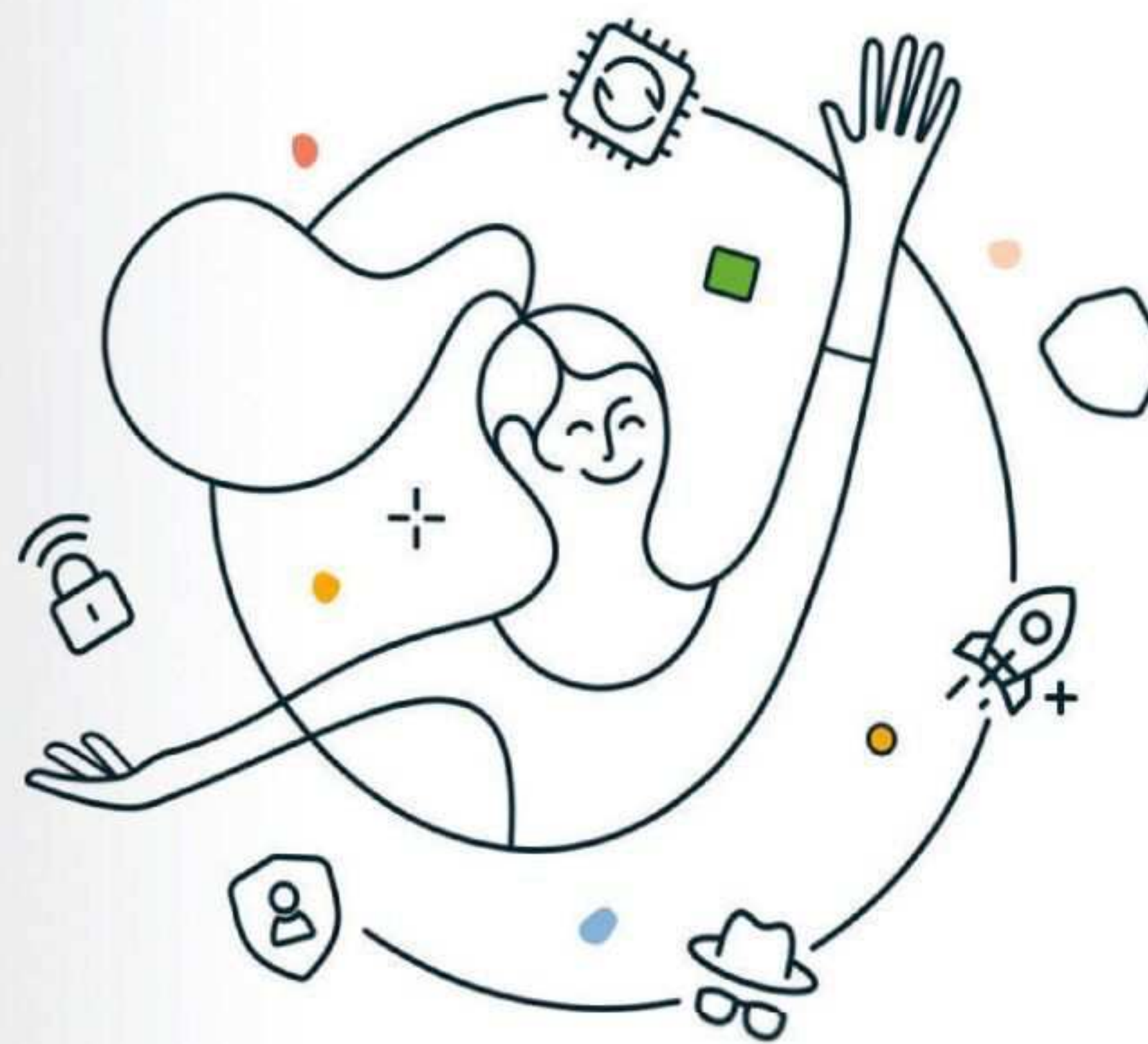
Das dauert nur einen Moment

Start Entdecken Profil



One

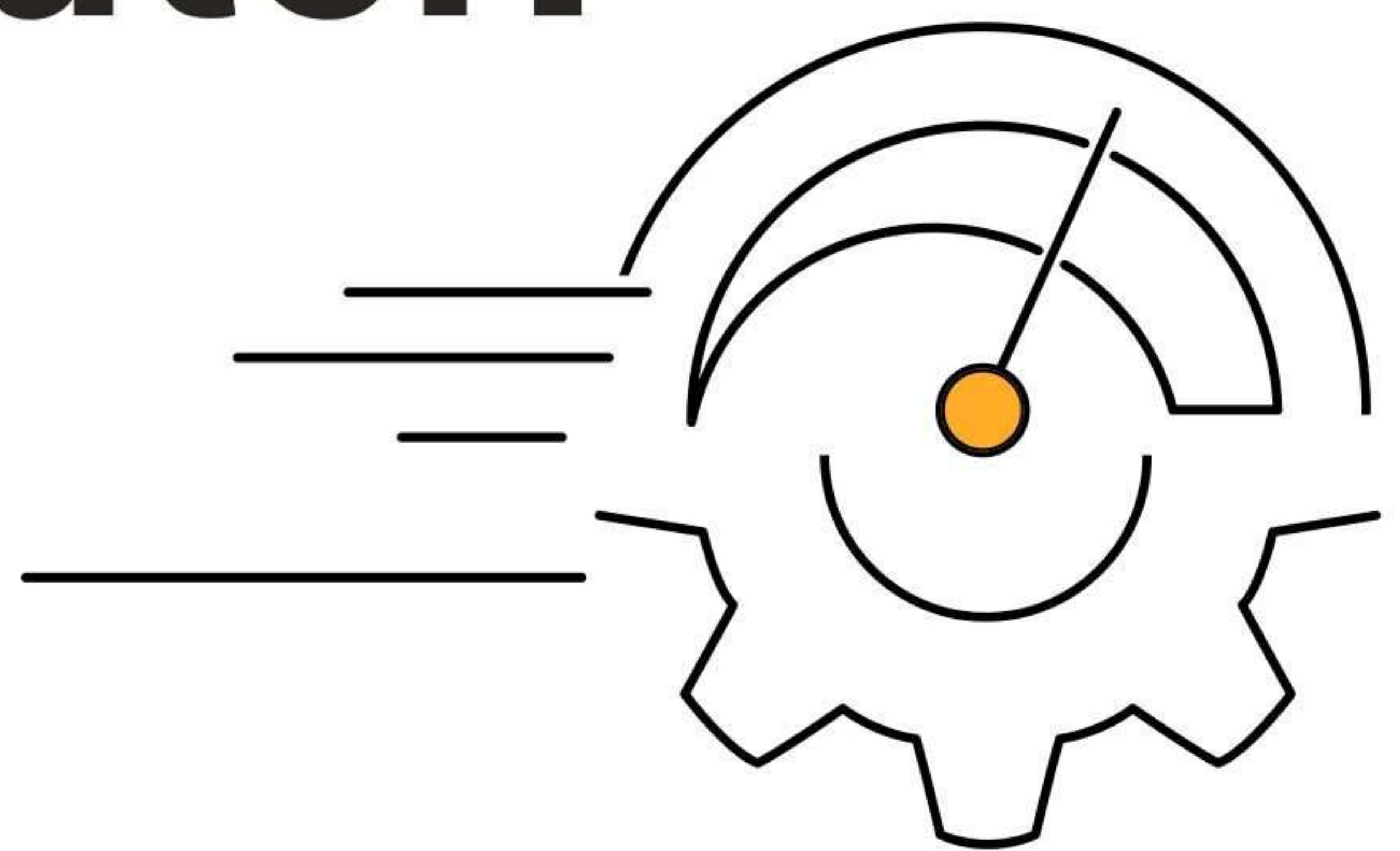
Proaktiver, starker Schutz
für dein digitales Leben.



Nur für
kurze Zeit*
26,28 €
statt ~~89,99 €~~
avast.com/cobi

One

Dein Computer: Turbo



Sicherheit, Privatsphäre & Performance in One.



Wir schützen die digitale Freiheit für alle.

* Das Angebot ist gültig bis zum **30.09.2022** über den angegebenen Link und beinhaltet Avast One Individual für das erste Jahr als Download für bis zu 5 Endgeräte (PC, Mac, Android und iPhone/iPad). Es können zusätzliche Kosten für den Download durch den jeweiligen Internetanbieter entstehen. 2022 Copyright Avast Deutschland GmbH

Limitiertes Angebot: Samsung Tablet gratis zum Jahresabo!

The central graphic features a large, tilted image of a **Computer BILD** magazine cover. The cover includes the title 'Computer BILD', the price '5,90 EURO', and several headlines: 'test Wer ist der Android-King? Die besten Smartphones im knallharten Wettkampf', 'news Schluss mit Passwort-Stress Report: Apple, Microsoft, Google & Co. wollen das Einloggen vereinfachen.', and 'aktionen'. A large hand is shown holding a magnifying glass over the magazine. To the right of the magazine is a yellow circular callout for the **Samsung Galaxy Tab A7 Lite** with features: 'Android 11', '8,7 Zoll', and 'Dolby Surround Sound'. Below the magazine is a red circular callout for 'Anti-Schnüffel-Tipps für iOS & Android'. In the foreground, a **Samsung Galaxy Tab A7 Lite Wi-Fi** tablet is displayed, showing a colorful abstract background. The Samsung logo is visible below the tablet.

Ihre Vorteile:

- 12 Monate von Trends, Tipps & Testberichten profitieren
- ein Top-Film zum Streamen in jeder Ausgabe
- Kostenloser Versand
- **Samsung Galaxy Tab A7**
- **gratis als Prämie**

Jetzt bestellen: computerbild.de/abo/tablet ☎ 0800 / 12 45 60 8

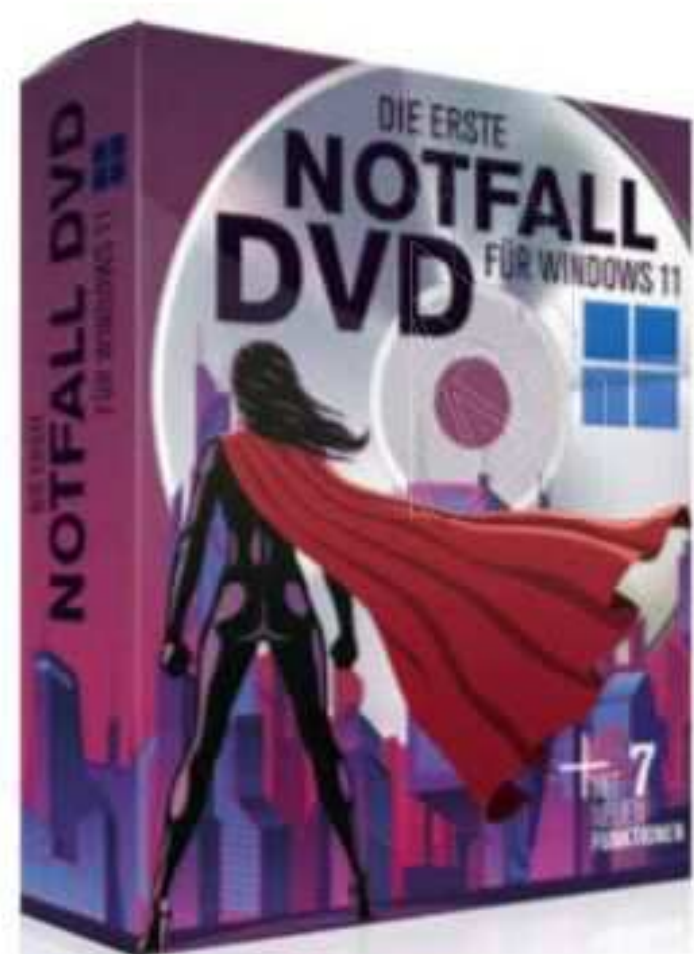
- 12 Monate **COMPUTER BILD** mit **DVD** zum Kioskpreis von nur 5,90 € pro Ausgabe
- Bestellnummer | 10169537

Computer
BILD

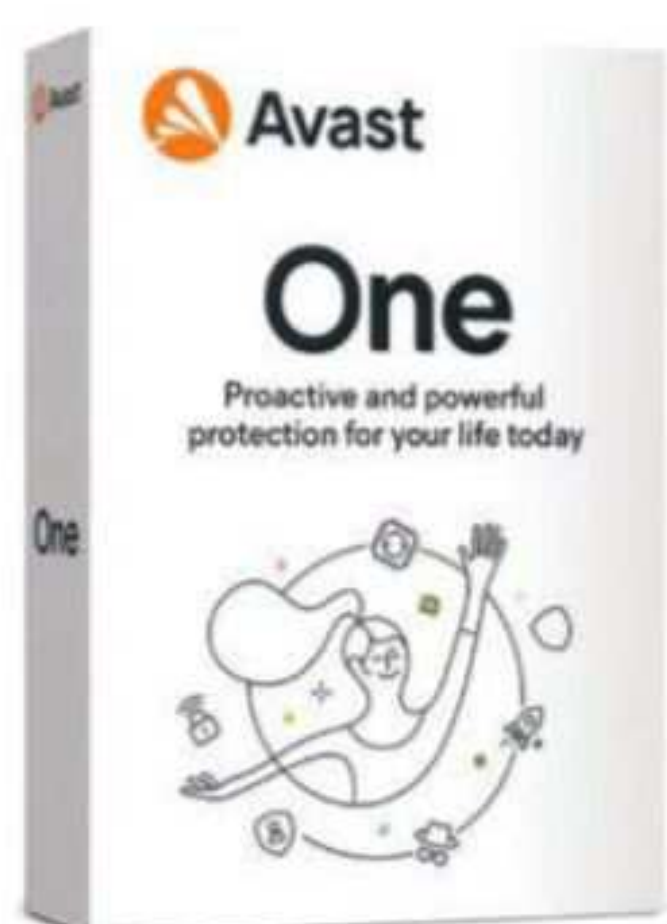


Marco Häntsch
Ressortleiter
Sonderpublikationen

HIGHLIGHTS AUF HEFT- DVD:



Notfall-DVD Vol. 17
Die Letzte ist die Beste!
Die Notfall-DVD 17 ist die perfekte Hilfe bei allen PC-Problemen – jetzt mit sieben neuen Funktionen.



Avast Premium Security
Erstklassiger Virenschutz gratis für PC und Handy. Nutzen Sie die Vollversion bis zum 22. April 2023 ohne Einschränkungen.



Hacker-Tools
Nur wer die Tricks der Hacker kennt, ist dagegen gefeit – mit dieser DVD schützen Sie Ihren PC und Ihre Daten.

Vertrauen war gestern, Sicherheit geht jetzt vor!

Während die russische Armee die Ukraine angreift, wird das Internet zum digitalen Schlachtfeld um Daten und Zugriffsrechte. Mit dem Krieg ist nicht nur die Hoffnung in die Berechenbarkeit der russischen Politik verloren gegangen. Auch Dienstleister und Software-Anbieter verlieren an Vertrauen, wenn sie mit dem brutalen Regime in Verbindung stehen könnten. So warnte das BSI öffentlich sogar vor der Nutzung der über Jahrzehnte untadeligen Antiviren-Software Kaspersky. Und plötzlich werden Datenleitungen in Putins Reich unerwartet zum Risiko. Das Sicherheitsunternehmen Appvisory hat im Auftrag von COMPUTER BILD untersucht, ob auch Apps entsprechende Verbindungen zu russischen Servern aufbauen. Zum Politikum werden zunehmend auch chinesische Tech-Unternehmen wie Huawei. Sie stehen weiter unter Verdacht, die Unterdrückung der uigurischen Volksgruppe technisch zu unterstützen.

Es reicht also nicht mehr, blind auf namhafte Unternehmen zu vertrauen. Sie müssen genauer hinsehen und sich informieren, welche Sicherheitsvorkehrungen Sie jetzt brauchen. Dabei möchte Ihnen COMPUTER BILD helfen: online unter computerbild.de, alle zwei Wochen mit einem neuen Heft am Kiosk und mit diesem Sonderheft, das Ihnen ein wertvolles Software-Paket und zahlreiche Hintergrundinfos zum Thema liefert.



Noch mehr News und Downloads zum Thema Sicherheit gibt es auf computerbild.de.



Fotos: iStock, Hersteller; Montage: COMPUTER BILD

**AKTUELLE
SICHERHEITS-
NEWS ONLINE!**



**Computer
Bild**

QR-CODE
SCANNEN UND
LINK FOLGEN.



[computerbild.de/
sicherheitscenter](https://computerbild.de/sicherheitscenter)

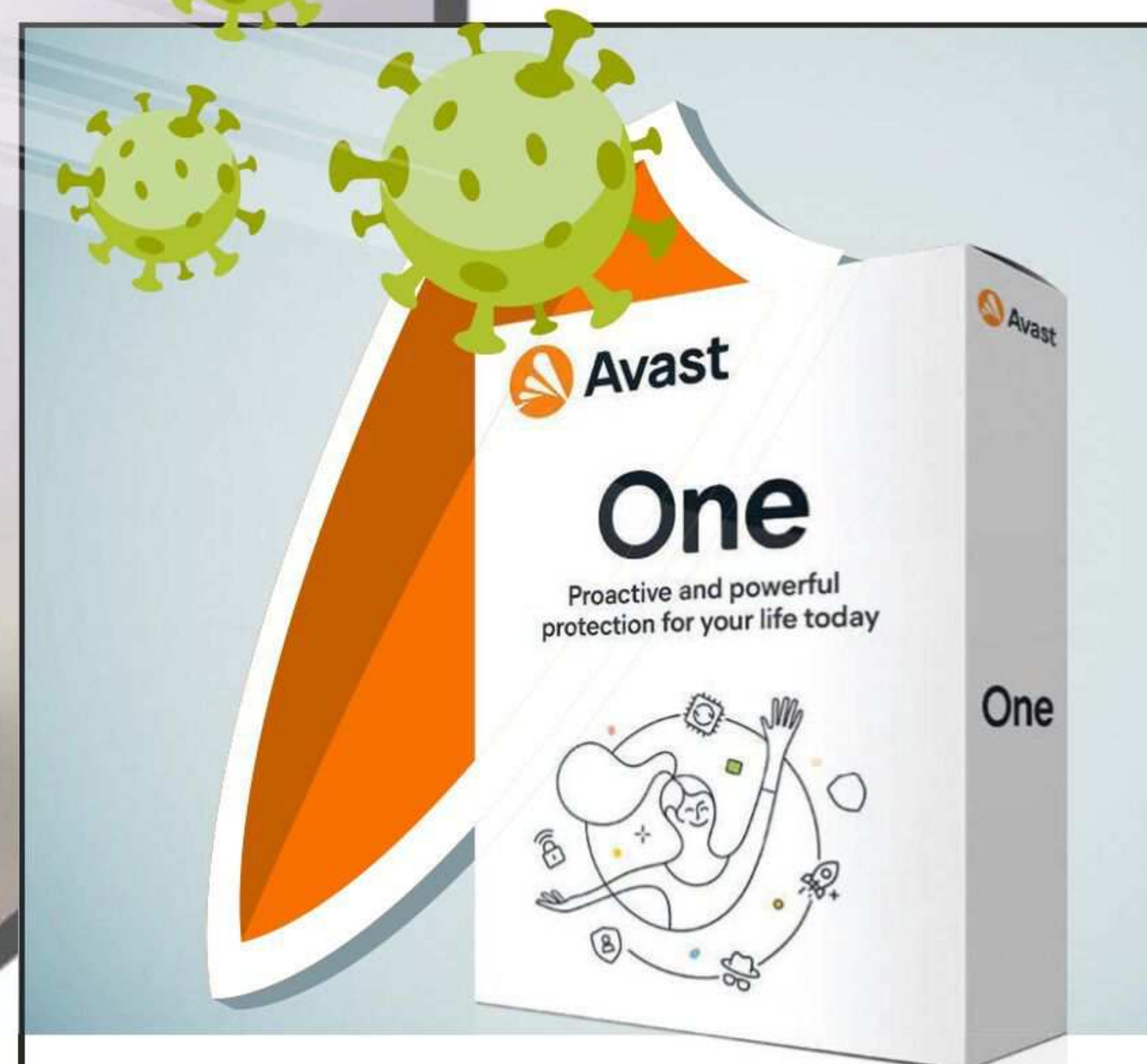
DIE LETZTE NOTFALL- DVD



Zum letzten Mal präsentiert COMPUTER BILD die Notfall-DVD. Hier gibt's noch mal das volle Programm: Die Version 17 ist die perfekte Hilfe bei allen PC-Problemen wie Abstürzen oder anderem Windows-Ärger. **Seite 30**

EINBRUCH- SCHUTZ

Eine smarte Überwachungskamera bringt mehr Sicherheit und Komfort. COMPUTER BILD hat acht Modelle getestet und erklärt, wie Sie die am besten installieren und einrichten. **Seite 100**



PRAXISTEST-SIEGER

ABWEHRSCHIRM

Viren, Trojaner, Malware: Wer sich ins Internet wagt, lebt gefährlich. Mit der Security-Suite Avast One erhalten Sie für PC, Mac und Smartphone exklusiven Top-Schutz bis zum 21. April 2023 zum Nulltarif. **Seite 66**



IHR WINDOWS- RETTER

Windows zickt oder will gar nicht mehr? Mit dem genialen Windows-Retter von der Heft-DVD versetzen Sie PC oder Notebook einfach in den Zustand vor dem Problem, als wäre es nicht aufgetreten. **Seite 86**

HACKER-DVD

GUTE TOOLS, BÖSE TOOLS

Wer die Tricks der Hacker kennt, kann sich besser gegen ihre Angriffe wehren. Mit den Tools von der DVD schützen Sie Ihre Daten noch besser.

Seite 76



SICHERHEITS-PAKET

Mit diesen 15 kostenlosen Vollversionen auf Heft-DVD oder zum Downloaden sorgen Sie für mehr Sicherheit auf PC, Mac und Smartphone.

Seite 58



SICHERHEITS-CENTER

Hört Putin mit?

Haben wir russische Wanzen auf unseren Smartphones? 8

Angriff auf Microsoft

Hackergruppe verbreitet Microsoft-Programmcode im Internet 10

Großer Betrug mit kleinen Anzeigen

Auf Ebay Kleinanzeigen wollen Betrüger an Ihr Geld 12

„Kinder haben bei Facebook nichts verloren“

Interview mit dem neuen Hamburger Datenschutzbeauftragten 14

Kampf gegen Hassrede im Netz

Neue Hebel gegen Hetze in sozialen Netzwerken 16

Die Sache mit den Cookies

Neues Recht soll den lästigen Cookie-Bannern ein Ende bereiten ... 18

Emotet ist zurück!

Das gefährlichste Virus der Welt greift wieder an 20

Betrug mit Amazon-Anrufen

Kriminelle geben sich am Telefon als Amazon-Mitarbeiter aus 22

Cybersicherheit in Zahlen

So gefährlich ist das Internet in Deutschland 24

Das Ende des Passworts

Google, Apple und Microsoft arbeiten an einer cleveren Alternative .. 26

Tipps zum sicheren Online-Shopping

COMPUTER BILD erklärt, wie die Ware Sie sicher erreicht 28

SOFTWARE

Die letzte Notfall-DVD

Der ultimative Helfer bei PC-Problemen mit neuen Funktionen 30

Steganos Privacy Suite 22: Vollversion gratis

Mit diesen Tools sichern Sie Passwörter, Daten und Anonymität 48

Ascomp Guardian Of Data

Verschlüsseln Sie Ihre sensiblen Daten auf dem Computer 50

Filewhopper

Daten verschlüsselt per Cloud-Dienst verschicken 51

Safe Erase

Löschen Sie Daten unwiederbringlich 51

Werbeanrufblocker von Tellows

Schluss mit nervigen Werbeanrufen auf dem Handy! 52

Cryptomator

Speichern Sie wichtige Dokumente verschlüsselt in der Cloud 54

Der große Security-Suiten-Test

COMPUTER BILD hat acht Schutzpakete geprüft 58

Avast-One-Vollversion

Gratis: Virenschutz bis zum 21. April 2023 vom Praxistest-Sieger 66

Hacker-Tools

Nur wer die Tricks der Hacker kennt, ist gegen sie gefeit 76

Das unzerstörbare Windows

Machen Sie Windows-Probleme einfach ungeschehen 86

Avast One Mobile

Die Top-Security-Suite für Ihr Smartphone 94

Acebit Password Depot

All Ihre Passwörter an einem sicheren Ort 96

Abelssoft EasyBackup

Sichern Sie Ihre Daten mit wenigen Klicks 97

Salfeld Kindersicherung

Schützen Sie Ihren Nachwuchs vor Mobbing im Internet 98

All-In-One Key Finder Pro Personal Edition

Mit diesem Tool geht kein Lizenzschlüssel mehr verloren 99

Secuperts Anti-Spy CBE

80 Schnüffelfunktionen von Windows 10 einfach abschalten 99

SPECIAL

Vergleichstest Überwachungskameras

Was leisten die smarten Wächter, und was kosten sie? 100

SERVICE

Outro / Impressum 108

HÖRT PUT

Nicht immer ist eine potenzielle Gefahr offensichtlich. Sicherheitsforscher schlagen Alarm: Haben wir russische Wanzen auf unseren Smartphones?

Kein Ende in Sicht für den Kriegshorror in der Ukraine. Und immer klarer wird: Die demokratische Welt muss sich wohl dauerhaft an einen Konflikt mit Putins Russland gewöhnen. Das hat auch Konsequenzen für unseren Umgang mit Technik. Das russische Sicherheitsunternehmen Kaspersky bekam das bereits zu spüren: Nach Warnungen des BSI (Bundesamt für Sicherheit in der Informationstechnologie), Putins Machtapparat könnte Druck ausüben und das Virenschutzprogramm am Ende zur Waffe machen, steht Kaspersky in Deutschland wirtschaftlich mit dem Rücken zur Wand.

Doch nicht immer ist eine potenzielle Gefahr so offensichtlich. Möglicherweise nämlich tragen wir gleich mehrere Bedrohungen mit uns herum, ohne es zu ahnen – direkt auf unseren Smartphones! COMPUTER BILD hakt nach.

Feind in der Hosentasche?

Klar, einen russischen Hersteller von Smartphones gibt es nicht, und weder Android noch iOS funktionieren – zumindest in Deutschland – direkt nach Moskau. Schauen wir aber auf einzelne Apps, dann zeigt sich ein anderes Bild. Im Auftrag von COMPUTER BILD hat das Security-Unternehmen Appvisory die wichtigsten und bekanntesten Apps in den Stores von Apple und Google unter die Lupe genommen und überprüft, ob die jeweilige Apps mit russischen Servern Kontakt aufbauen.

Und in der Tat: Das Ergebnis sorgt zumindest punktuell für

Stirnrunzeln. Die Experten fanden unzählige Apps, bei denen ein Datenversand nachgewiesen werden konnte. Und vielfach laufen die Informationen an einer ganz zentralen Stelle zusammen: bei Yandex.

Der russische IT-Gigant

Soziales Netzwerk, Suchmaschine, Bezahl dienst, Browser und vieles mehr: Wenn es ums Internet geht, dann läuft in Russland nichts ohne den Riesenkonzern Yandex. Hierzulande fast unbekannt, ist der IT-Gigant seit über 30 Jahren aktiv und ein international gehandeltes Aktienunternehmen. Wie bei vielen russischen Unternehmen hat auch hier die Regierung bei wesentlichen Dingen ein Wörtchen mitzureden. Vor einigen Jahren wurde bekannt, dass der Konzern Informationen über Spenden an den Oppositionellen Alexei Nawalny an den russischen Geheimdienst FSB weitergegeben hat.

Eben jenes Unternehmen bietet ein sogenanntes SDK mit dem Namen „AppMetrica“ an, das App-Entwickler häufig verwenden. Dahinter steckt eine Art Baukasten, mit dem sich Apps schneller erstellen lassen. Das ist nicht weiter ungewöhnlich, auch Unternehmen wie Google stellen solche Baukästen bereit. Sie sind so beliebt, weil sie kostenlos sind – im Gegenzug erhalten die Mega-Konzerne allerdings Zugriff auf bestimmte Daten.

Und dieser Zugriff, so fürchten Experten, könnte gefährlich werden. Denn die Informationen, die

„Die Angst vor russischen IT-Angriffen ist groß. Aber ebenso berechtigt.“

Dirk General-Kuchel
Chefredakteur

IN MIT?



über viele (westliche) Nutzer anfallen, können am Ende für Spionage genutzt werden.

Wo das Problem liegt

AppMetrica ist in vielen Apps eingebaut. Der US-Sicherheitsforscher Zach Edwards schätzt auf seinem Twitter-Account eine Zahl von über 50 000 Apps. Damit dürfte es viele Millionen Menschen geben, die potenziell ausgeforscht werden könnten – und zwar ohne dass sie es merken.

Zwar fragen Apps bei der Installation nach Berechtigungen, denen der Nutzer zustimmen muss. Aber die Begehrlichkeiten der SDKs sind möglicherweise auch den App-Entwicklern gar nicht bekannt – oder egal. Yandex selbst gibt an, lediglich Gerätetyp, IP-Adresse und Informationen über das genutzte Netzwerk zu sammeln, und zwar anonymisiert.

Westliche Sicherheitsforscher gehen aber davon aus, dass sich auch aus solchen Daten Rückschlüsse auf konkrete Personen ergeben. Wer Zugriff auf solche Daten hat, könnte gezielt nach Menschen in politischen, militärischen oder wirtschaftlichen Schaltstellen suchen. Wie die Financial Times berichtete, sind auch US-Politiker sehr besorgt. Senator Ron Wyden warf Google und Apple als Betreiber der App-Stores vor, nicht genug gegen die Yandex-Software zu tun.

Besonders beunruhigend: Sicherheitsexpertin Cher Scarlett spricht in der Financial Times von 21 VPN-Apps, in die das Yandex-SDK innerhalb des vergangenen

Monats erst eingebaut worden sei. Aufgrund dieser Gerüchte nahmen sich die Experten von Appvisory im Auftrag von COMPUTER BILD auch die wichtigsten VPN-Anbieter vor, die in Deutschland relevant sind. Hier konnten keine Hinweise auf Verbindungen nach Russland gefunden werden – eine Ausnahme war allerdings OperaVPN.

Der App-Check

Insgesamt prüften die Appvisory-Experten rund 33 000 iOS- und etwa 13 000 Android-Apps. Dabei zeigte sich: Bei Apple hatten 7 Prozent der untersuchten Apps zumindest die Möglichkeit einer Verbindung mit russischen Servern – aber nicht ausschließlich mit denen von Yandex. Bei Android waren es knapp unter 6 Prozent. Wirklich genutzt wurde die Verbindung dann aber nur von jeweils weniger als 2 Prozent.

Unter den untersuchten Apps, die tatsächlich Verbindungen aufbauten, waren beliebte Spiele aus der „Cut the Rope“-Reihe, der

icq- und der Viber-Messenger, eine App der Modekette H&M, Alibaba, Drohnen-Apps von DJI, „Geheimer Ordner – Photo Vault“, „Visitenkarten Scanner“ und „Audi Service“. Da der Datenstrom aber meist verschlüsselt ist, lässt sich kaum genau sagen, welche Dateien fließen.

App-Stores in der Pflicht

Die Aufregung um Yandex ist bei genauerem Hinsehen also berechtigt, aber kein Grund zur Panik. Vor allem aber bleibt ein ungutes Gefühl, dass die Nutzer zu wenig Kontrolle über das haben, was die SDKs auf den Smartphones tun. Die App-Stores liefern da einfach nicht genug Informationen. Apple und Google sind hier eindeutig in der Pflicht. [dgk]



Beliebtes Tool für viele App-Entwickler: AppMetrica von der russischen Firma Yandex könnte sich zur Gefahr entwickeln.

DAS SAGT DER EXPERTE



Sebastian Wolters
CEO Appvisory

COMPUTER BILD: Eine böseartige App auf dem Smartphone – wie gefährlich ist das wirklich?

Sebastian Wolters: Die Gefahr ist absolut real. Wir sehen, dass Apps zunehmend als Einfallstor für Spionage und Cybercrime genutzt werden – leider wird dieser offensichtliche Fakt weiterhin unterschätzt.

In der angespannten Situation mit Russland ändert sich das Bewusstsein jetzt – hoffentlich dauerhaft. Der Konflikt zeigt einmal mehr, wie wichtig der bewusste Umgang mit digitalen Sicherheitsrisiken ist.

Sind Apps mit Russland-Verbindungen nicht sehr selten?

Wir waren bei der Untersuchung überrascht, wie viele Apps aus den gängigen Apple- und Android-App-Stores Verbindungen nach Russland aufbauen oder zumindest die technische Möglichkeit dazu im Code geschaffen haben. Was da passiert, können wir nicht sagen, wir sehen aber die Möglichkeit einer Gefahr. Und diese Sorge teilen unsere Kunden offenbar. Wir sehen, dass Unternehmen momentan verstärkt dazu tendieren, Apps mit Datenverbindungen nach Russland von ihren Firmengeräten zu entfernen oder im Idealfall gar nicht erst zu installieren.

ANGRIFF AUF MICROSOFT

Programmcodes von Microsoft wurden offen im Internet verbreitet. Dahinter steckt die berüchtigte Lapsus\$-Gruppe. COMPUTER BILD erklärt die Hintergründe.

Cyber-Angriffe auf die IT-Infrastruktur gehören für Tech-Giganten wie Microsoft, Google oder Amazon zum Alltag. Dass sie auch erfolgreich sind, ist dagegen eher eine Seltenheit – aber wenn's doch mal passiert, dann ist die Verunsicherung groß. Schließlich geht's nicht nur um die Firmen selbst, sondern oft um die bange Frage, ob auch die vielen Millionen Kunden der Unternehmen betroffen sind. So auch vor einiger Zeit, als bekannt wurde, dass eine Hackergruppe mit dem Na-

men Lapsus\$ Daten von Microsoft entwendet hat. COMPUTER BILD erklärt, was passiert ist, wen es betrifft und was über die ominöse Cyber-Bande Lapsus\$ bekannt ist.

Das ist passiert

Die ersten Hinweise auf ihren „Erfolg“ gab die Hackergruppe auf ihrem von zigtausend Abonnenten gelesenen Telegram-Kanal: Dort behaupteten die Cyber-Kriminellen, sie hätten den Programmcodes von Bing, Cortana und weiteren Microsoft-Projekten

in ihren Händen und würden ihn demnächst veröffentlichen. Zunächst gab es nur einen Screenshot, der offenbar aus einer internen Gruppe von Microsoft-Mitarbeitern stammte. Doch schon einen Tag später stand tatsächlich eine 9 Gigabyte große Datei parat, die nach Angaben von bleepingcomputer.com fast 40 Gigabyte Programmcodes in komprimierter Form enthielt. Schließlich bestätigte auch Microsoft den Datendiebstahl. Und der Konzern beeilte sich zu betonen:

Die betroffenen Projektdaten stammen von webbasierten Angeboten. Code aus Windows oder Office etwa ist zumindest bisher nicht veröffentlicht worden.

Bleibt es dabei, können sich Windows- und Office-Nutzer also entspannen, denn eine unmittelbare Gefahr besteht zumindest bei dieser Software nicht.

Gefahr aus anderer Quelle?

Microsoft war aber nicht das einzige Ziel der Bande. Schon in den Monaten zuvor hatte sie nicht we-

niger bekannte Namen auf der Opferliste. So steckte Lapsus\$ hinter Hacks bei Samsung, Nvidia und Vodafone. Auch dort entwendeten die Hacker Daten – immer mit dem Ziel der Erpressung. Wer nicht zahlt, der muss damit rechnen, dass Firmengeheimnisse oder Kundendaten an die Öffentlichkeit gelangen.

Ein Verbrauchern weniger bekanntes Opfer: Okta. Das Unternehmen gehört zu den Schwerge- wichten bei der Absicherung von Kunden-Log-Ins. Der Dienstleister kümmert sich laut eigener Websei- te in Deutschland zum Beispiel um das Identitätsmanagement beim Versicherungsunternehmen HDI und ist auch für die Bestelldienst- Firma Delivery Hero tätig.

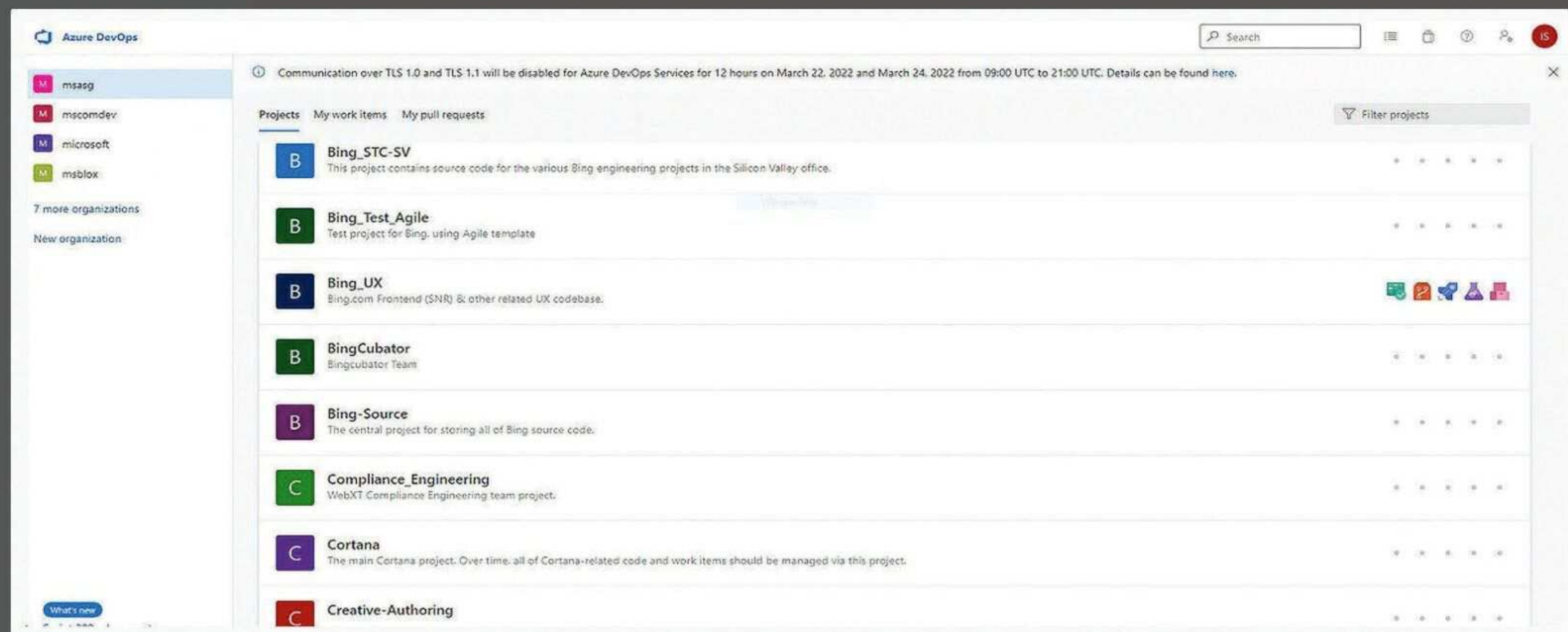
International gehören Peloton, Sonos, aber auch T-Mobile USA zu den Kunden. Lapsus\$ behauptete, seine Finger tief in den Systemen von Okta gehabt zu haben – mit weitreichendem Zugriff auf die Daten. Wäre das wahr, so hätte das vermutlich einen Security-Super- Gau bedeutet.

Okta hat den Fall detailliert unter- sucht und sagt, dass die Behauptungen der Gruppe nicht den Tatsa- chen entsprechen. Die Bande ha- be keinen Zugriff gehabt, sondern nur Screenshots auf dem Rechner eines Service-Technikers gemacht.

Wer ist Lapsus\$?

Mittlerweile wird immer klarer: Es geht der Lapsus\$-Gruppe vor al- lem um Aufmerksamkeit und viel Wind. Experten vermuten, dass die Gruppe technisch nicht so ver- siert ist wie zunächst gedacht. Sie arbeite wohl eher mit Bestechung und dem Aufkauf vertraulicher Daten. Schon mehrfach war aufge- fallen, dass die Gruppe im Inter- net neue Handlanger rekrutierte. Die, so die „Stellenbeschreibung“ von Lapsus\$, sollten möglichst In- sider sein und Zugriffsdaten lie- fern – Verrat gegen Geld also. Rund 20 000 Dollar „Honorar“ pro Woche sollen angeboten worden sein. Aber auch mit den üblichen kriminellen Methoden wie Pass- wortklau über Phishing gelangen die Hacker an Zugänge.

Microsoft vermutet in einem Blog-Beitrag, dass diese Strategie auch das Eindringen in die inter-



Dieses Bild postete die Hackergruppe bei Telegram zum Beweis ihres erfolgrei- chen Angriffs auf Microsoft.

LAPSUS\$

Forwarded from LAPSUS\$

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

If you are not sure if you are needed then send a DM and we will respond!!!!

If you are not a employee here but have access such as VPN or VDI then we are still interested!!

Kollege gesucht: Mit „Stellengesuchen“ wie diesem hat die Bande Handlanger für ihre Erpressungsversuche rekrutiert.

nen Foren des US-Softwarekon- zerns ermöglicht hat. Am Ende, so Microsoft, habe „unsere Untersu- chung lediglich ein einziges kom- promittiertes Konto entdecken können“ und das habe nur über begrenzte Zugriffsrechte verfügt. Kundendaten, so das Unterneh- men, seien nicht betroffen.

Wer aber steckt nun hinter der Gruppe und sorgt für so viel Sturm im Wasserglas? Inzwischen kamen erstaunliche Details ans Tages- licht: Nicht nur Microsoft äußerte sich verwundert darüber, dass die Mitglieder der Gruppe kaum Mühe darauf verwendeten, ihre Spuren zu beseitigen. Das hatte Folgen: Wenige Tage nach dem Angriff auf

Microsoft verhaftete die Londoner Polizei sieben mutmaßliche Mit- glieder der Bande.

Unglaublich: Das jüngste Mit- glied soll laut BBC News erst 16 Jahre alt sein und angeblich ein ergaunertes Vermögen von 14 Mil- lionen US-Dollar in Bitcoin ange- häuft haben. Der Teenager könnte der Kopf der Bande sein.

Auch die anderen verhafteten mutmaßlichen Mitglieder sind nicht älter als 21 Jahre. Ob diese „Jugendbande“ wirklich der Kern der Lapsus\$-Gruppe ist? Der zum Redaktionsschluss noch laufende Gerichtsprozess in London wird vermutlich mehr Aufschluss darü- ber bringen. [dgk]



„Offenbar muss man kein IT-Experte sein, um große Konzerne schwer zu treffen.“

Dirk General-Kuchel
Chefredakteur

GROSSER BET

Auf **Ebay Kleinanzeigen** wollen **Betrüger** nur Ihr Bestes: Ihr Geld. COMPUTER BILD zeigt **drei aktuelle Maschen** und wie Sie sich davor schützen.

Wer im Internet einkauft, muss sich vor Betrügern in Acht nehmen. Mit immer neuen Maschen und schmutzigen Tricks versuchen Gangster, Ihnen online Ihr Geld oder auch sensible Daten abzuknöpfen. Gern gesehene Opfer sind die Nutzer der Plattform Ebay Kleinanzeigen.

Ebay Kleinanzeigen im Fokus

Immer wieder warnen sogar die Landeskriminalämter vor den raffinierten Betrügereien der Gauner. Oft betreffen die Maschen nicht nur Käufer, sondern auch Verkäufer. Doch Nutzer sind dem nicht schutzlos ausgeliefert. Im Gespräch mit COMPUTER BILD

verrät Jöran Rieß, der Leiter des „Trust and Safety“-Teams von Ebay Kleinanzeigen, worauf Nutzer beim Ein- und Verkaufen auf der Plattform achten sollten.

Das fängt schon mit einem ganz einfachen Grundsatz an. „Wenn etwas zu gut aussieht, um wahr zu sein, dann kann es auch nicht

wahr sein. Zu 99 Prozent handelt es sich dann um Betrug“, verrät Rieß. Nutzer sollten sich also auf der Jagd nach einer neuen PlayStation 5 nicht von traumhaft günstigen Preisen blenden lassen.

Hier zeigt COMPUTER BILD drei fiese Tricks und gibt Hilfestellung bei der Erkennung. [me]



MASCHE 1: DIE FALSCHER SPEDITION

Diese Methode taucht immer wieder in verschiedenen Varianten auf. Die Masche: Der Betrüger interessiert sich für ein sperriges Produkt, etwa ein Möbelstück, ein Klavier oder ein Boot. Selbst abholen will er es aber nicht. Die Gründe dafür sind vielfältig: Mal lebt der Interessent im Ausland, mal fehlt der fahrbare Untersatz. Eine Lösung hat der betrügerische Käufer aber parat: Den Transport wird eine Spedition übernehmen, die er beauftragt. Die Kosten soll allerdings zunächst der Verkäufer übernehmen, gerne per Überweisung. Die Bankdaten liefert der Käufer. Als zusätzlichen Beweis für die „Seriosität“ der Aktion erhält der Verkäufer die E-Mail eines Bezahlendienstes wie PayPal. Sie soll beweisen, dass der Käufer den fälligen Betrag inklusive Transportkosten eingezahlt hat und freigeben wird, sobald der Verkäufer die Spedition bezahlt. Am Ende ist das Geld natürlich weg, und das Sperrgut bleibt an Ort und Stelle. Eine Spedition hat es genauso wenig gegeben wie das Interesse des möglichen Käufers. Die Mail war gefälscht.

Die Lösung: Nutzer sollten an dieser Stelle skeptisch sein und sich fragen, wie wahrscheinlich es ist, dass ein vermeintlicher Interessent aus dem Ausland zum Beispiel einen Ikea-Schrank aus Deutschland kaufen und für viel Geld importieren möchte. Außerdem ist es nicht sehr logisch, dass der Käufer die Spedition zwar mit der Abholung beauftragt, aber nicht selbst bezahlt. Nutzer sollten in jedem Fall darauf bestehen, dass der Käufer die Ware selbst abholt oder für die Transportkosten aufkommt. Geld sollten Sie auf keinen Fall überweisen. Jöran Rieß hat für solche Fälle einen einfachen Grundsatz: „Jemand, der etwas Sperriges abholen möchte, kommt auch selbst vorbei“, sagt er. Sollte ein Käufer auf ein dubioses Verfahren bestehen, sehen Sie vom Verkauf ab.

KEINE
CHANCE
FÜR FIESE
BETRÜGER

ebay
Kleinanzeigen

RUG MIT KLEINEN ANZEIGEN



MASCHE 2: SICHERE ZAHLUNG

Vor dieser fiesen Masche warnte zuletzt sogar die Polizei Berlin: Die Verbrecher kontaktieren den Anbieter einer Ware zunächst per WhatsApp oder einem anderen Messenger und bekunden Interesse an einem Artikel. Anschließend geben sie an, den Kauf per „Sichere Bezahlung“ abwickeln zu wollen – das klingt vertrauenerweckend, denn die Funktion gibt es bei Ebay Kleinanzeigen wirklich. Als Verkäufer erhalten Sie nun einen offiziell aussehenden Link. Auf der entsprechenden Webseite sollen Sie Ihre Kreditkartendaten eingeben. Geld gibt es im Anschluss nicht, aber die Daten für Ihre Kreditkarte sind Sie los.

Die Lösung: Sollten Sie auf die Masche hereingefallen sein, lassen Sie Ihre Kreditkarte umgehend sperren. Den Angaben der Polizei Berlin zufolge nutzen die Betrüger die Daten, um Geld abzuheben. Das geschieht überwiegend im Ausland. Um sich vor einem Betrug zu schützen, wickeln Sie Verkäufe nach Möglichkeit über den integrierten Nachrichtendienst von Ebay Kleinanzeigen ab. Der wird automatisiert beobachtet und meldet verdächtige Begriffe an die Mitarbeiter, die dann wiederum finstere Gesellen aus dem Verkehr ziehen. Zusätzlich sollten Sie davon absehen, Ihre Telefonnummer in der Anzeige abzubilden, um gar nicht erst per

WhatsApp oder über andere Messenger kontaktiert zu werden. „Wir wollen unsere Nutzer stärker dafür sensibilisieren, ihre Mobilnummer nicht einzustellen, in dem wir sie darauf hinweisen, dass sie ein weiteres Tor für Betrugsmaschen darstellt“, erklärt Jöran Rieß. Außerdem sollte Sie die Erwähnung der Kreditkarte stutzig machen. Das sagt auch der Experte: „Kein Mensch kann eine Zahlung auf seine Kreditkarte empfangen.“ Im Idealfall greifen Sie bei der Zahlungsabwicklung auf die echte Funktion für sichere Bezahlung zurück. Dann sind sowohl Käufer als auch Verkäufer im Betrugsfall durch Ebay Kleinanzeigen geschützt.



MASCHE 3: DER DREIECKSTRICK

Bei dieser Methode kopiert ein Betrüger Ihre Anzeige und täuscht gleichzeitig Interesse an Ihrem Artikel vor. Bezahlen will er per Überweisung. Schicken Sie ihm Ihre Bankdaten, leitet er diese an einen Interessenten für das Fake-Inserat weiter. Der Dritte bezahlt, ohne es zu wissen, an Sie, Sie schicken Ihren Artikel jedoch an den Betrüger. Besonders perfide: Weil der unwissende Dritte kein Produkt erhält, ist die Chance groß, dass er Sie als Betrüger bei Ebay Kleinanzeigen meldet, obwohl Sie nach bestem Wissen gehandelt haben.

Die Lösung: Geben Sie Ihre Bankdaten nicht an andere Nutzer weiter. Ebay Kleinanzeigen bietet mittlerweile selbst eine Bezahlmethode an. Die schützt Verkäufer unter anderem vor der Offenlegung ihrer Kontodaten und vor Rückbuchungen durch Kreditkartenzahlungen. „Überweisung ist eine der unsichersten Bezahlmethoden und nur geeignet, wenn man den Empfänger gut kennt“, rät auch Jöran Rieß. Nebenbei bietet Ebay Kleinan-

gen auf diesem Wege noch einen Käuferschutz. Erhalten Käufer keine Ware, erstattet das Partnerunternehmen Online Payment Platform den Kaufbetrag. Außerdem können Sie den Käuferschutz einschalten, wenn Sie einen gefälschten Artikel erhalten oder das Produkt stark von der Beschreibung abweicht. Kommt Ihnen etwas komisch vor, können Sie auch schon vor der Transaktion aktiv werden und die verdächtige Anzeige melden. Handelt es sich tatsächlich um Betrug, wird das Nutzerkonto des Ganoven auf Ebay Kleinanzeigen gesperrt.

Fotos: iStock; Montage: COMPUTER BILD



DAS BSI WARNT VOR KASPERSKY

Umstieg empfohlen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor der Nutzung der Antiviren-Software des russischen Herstellers Kaspersky. Auslöser dafür ist der Krieg in der Ukraine. Die von russischer Seite ausgesprochenen Drohungen gegen die NATO, die EU und die Bundesrepublik seien mit einem erheblichen Risiko eines IT-Angriffs verbunden, heißt es in der BSI-Pressemeldung.

Russische Software-Anbieter könnten Angriffe entweder selbst durchführen, dazu gezwungen werden oder Opfer einer Cyberattacke und ohne eigene Kenntnisse ausspioniert werden. Besonders gefährdet sind laut BSI Unternehmen und Behörden mit besonderen Sicherheitsinteressen und Betreiber kritischer Infrastrukturen.

Der Bundesverband für den Schutz Kritischer Infrastruktur (BSKI) teilte mit, er werde die Mitgliedschaft Kasperskys nach der Warnung ruhen lassen. Auch COMPUTER BILD nimmt die Warnung ernst und bietet bis auf Weiteres keine Kaspersky-Produkte mehr zum Download an. Wenn Sie als Kaspersky-Nutzer auf ein anderes Produkt umsteigen wollen: Im Test in Heft 6/2022 hat COMPUTER BILD Schutzprogramme getestet. Alle Infos unter www.cobi.de/42103



„KINDER HABEN BEI FACEBOOK NICHTS VERLOREN“

Thomas Fuchs ist neuer Hamburger **Datenschutzbeauftragter**. Im Exklusivinterview verrät er, was er von **Facebook** hält und welche **Herausforderungen** auf uns zukommen.

COMPUTER BILD: Herr Fuchs, in Ihren Zuständigkeitsbereich fallen die Überwachung von Facebook mit seinen Diensten WhatsApp und Instagram sowie Google, da beide Unternehmen ihren Deutschland-Sitz in Hamburg haben. Wie intensiv beschäftigt sich Ihre Behörde mit den Konzernen?

Thomas Fuchs: Wir stellen bis zu acht Mitarbeiterinnen und Mitarbeiter dafür ab. Die beschäftigen sich überwiegend mit Unter-

nehmen wie Facebook und Google. Das sind rund 20 Prozent unseres Teams.

In den 1980er-Jahren gab es in der Bundesrepublik einen Riesenaufschrei wegen der damaligen Volkszählung. Heute geben wir praktisch einen Großteil unseres Privatlebens freiwillig in sozialen Netzen preis. Wie beurteilen Sie unser aller Nutzerverhalten, wenn Sie an Dienste wie Facebook oder WhatsApp denken?

Im Vergleich zu den 80er-Jahren hat sich unsere Welt grundlegend verändert; das kann man nicht mehr miteinander vergleichen. Die Digitalisierung der Gesellschaft lässt sich nicht aufhalten und bietet ja auch zahlreiche Vorteile. Aber ich gebe Ihnen recht: Viele Bürgerinnen und Bürger gehen heute zu sorglos mit Diensten wie Facebook um, wenn es um den Schutz ihrer persönlichen Daten geht.

Stichwort persönliche Daten: Vor allem Facebook versucht immer wieder, durch neue Techniken oder die Verschmelzung von Diensten an noch mehr Daten zu kommen. Und die Datenschützer müssen immer neu reagieren. Das erinnert an ein Katz-und-Maus-Spiel...

Entscheidend ist, wer am Ende die Oberhand behält. Ein gutes Beispiel ist die jetzt gerade beschlossene Abschaffung der automatischen Gesichtserkennung bei Facebook. Mein Vorgänger hat diese Technik schon 2012 für Deutschland untersagt; jetzt ist sie weltweit vom Tisch. Es lohnt sich also, als Datenschutzbehörde und als Bürger permanent

Druck auf die Unternehmen auszuüben.

In den USA wird immer wieder über eine Zerschlagung von Facebook diskutiert. Wäre das denn wirklich ein probates Mittel, um den Konzern in Zukunft auch datenschutzrechtlich besser kontrollieren zu können?

Ehrlich gesagt überzeugt mich eine mögliche Zerschlagung nicht wirklich. Das ist eine Pseudodebatte, die suggeriert, dass wir damit sofort Probleme wie Hate Speech, Fake News oder Jugendschutz bei Facebook lösen könnten. Eine Zerschlagung würde das Ganze nur noch mehr fragmentieren. Stattdessen plädiere ich für eine strenge Regulierung.

Nutzen Sie selbst Google und Facebook?

Die Google-Suche ist ja in den meisten Fällen praktisch, die nutze ich schon. Bei Facebook sieht das anders aus. Dort bin ich nicht. Zum einen, weil es mich persönlich nicht sonderlich inter-



News-Ressortleiter Rainer Schuldt (rechts) traf Thomas Fuchs in seinem Büro – mit Blick auf den Michel, eines der Wahrzeichen Hamburgs.



Die Chancen der Digitalisierung nutzen und dabei auf den Datenschutz achten: So versteht Thomas Fuchs seine Aufgabe.

HAMBURGS NEUER DATEN- SCHÜTZER



Thomas Fuchs wurde am 23. Juli 1965 in Hamburg geboren.

Er ist Sohn der SPD-Politiker Anke Fuchs und Andreas Fuchs, besuchte Schulen in Frankfurt und Bonn. Danach leistete er Zivildienst und absolvierte eine Ausbildung zum Bankkaufmann.

Fuchs studierte Rechtswissenschaften, Philosophie und Europäisches Recht, legte 1993 das erste Staatsexamen ab. 1995 bestand er das zweite Staatsexamen und arbeitete freiberuflich als Rechtsanwalt.

1996 trat Thomas Fuchs in den Staatsdienst der Freien und Hansestadt Hamburg. Dort war er als Rundfunkreferent der Länder und von 1999 bis 2001 als persönlicher Referent von Wirtschaftssenator Thomas Mirow tätig. Danach war er Leiter der Präsidialabteilung der Behörde für Wissenschaft und Forschung (2001 bis 2004) sowie der Abteilung Theater, Musik und Bibliotheken in der Kulturbehörde (2004 bis 2007). Zudem saß er seit 2005 im Vorstand der Stiftung Elbphilharmonie.

Ab 2008 leitete Thomas Fuchs als Direktor die Medienanstalt Hamburg/Schleswig-Holstein in Norderstedt. Am 18. August 2021 wurde Fuchs von der Hamburgischen Bürgerschaft zum Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit gewählt und trat das Amt am 1. November 2021 an.

Thomas Fuchs ist verheiratet und Vater von zwei Töchtern. Er lebt in Hamburg.

essiert, zum anderen wegen Datenschutzbedenken.

Was würden Sie Eltern empfehlen, wenn es um die Nutzung von sozialen Netzen geht?

Meine Töchter sind zwar schon volljährig, aber ich hätte ihnen den Umgang mit Facebook & Co. bis zu einem bestimmten Alter untersagt. Ich bin dafür, dass man damit bis zum 13. Lebensjahr warten sollte – und dass die Eltern auch danach die Nutzung kritisch begleiten. Übrigens halte ich auch das Posieren von Eltern mit ihren kleinen Kindern bei Facebook oder Instagram für hochproblematisch und rate davon ab.

Sie sind seit dem 1. November 2021 im Amt. Was, glauben Sie, werden die Themenschwerpunk-

te sein, mit denen Sie sich als Datenschutzbeauftragter beschäftigen müssen?

Der gesamte Beschäftigtendatenschutz ist ein großes Thema, Stichwort: zunehmendes Home-Office. Aber hier haben wir zum Glück die DSGVO, die den Datenschutz in diesem Bereich schon deutlich verbessert hat. Außerdem will die Ampelkoalition die Digitalisierung der staatlichen Dienstleistungen vorantreiben. Hier ist Deutschland noch zu rückständig, und hier gibt es – auch für die Datenschützer – noch viel zu tun, etwa bei digitalen Behördengängen oder bei der elektronischen Gesundheitskarte.

Und wie sieht es aus Ihrer Sicht mit der Digitalisierung der Ver-

kehrsinfrastruktur bei uns in Deutschland aus?

Das ist ein wichtiges Thema. Zum Beispiel können maßgeschneiderte Kfz-Versicherungen durch das Aufzeichnen von Fahrdaten etwas Positives sein, dagegen ist vom Ansatz her nichts zu sagen. Auch hier werden wir auf die strikte Einhaltung des Datenschutzes achten.

Sie erwähnten, dass Sie nicht bei Facebook sind. Nutzen Sie überhaupt irgendwelche sozialen Netze oder Messenger?

Wenn, dann bin ich auf Twitter unterwegs. Bei WhatsApp habe ich mich wegen der engen Verknüpfung mit Facebook wieder abgemeldet. Ich nutze stattdessen Signal.

Fotos: iStock, Bildwerkstatt Nienstedten; Montage: COMPUTER BILD



Neue Maßnahmen sollen Hass und Hetze in sozialen Netzwerken eindämmen. Doch zum Start hakt es gewaltig.

Seit dem 1. Oktober 2017 gilt in Deutschland das sogenannte Netzwerkdurchsetzungsgesetz (NetzDG). Es soll dabei helfen, wirksam gegen die Verbreitung von Hass, Rassismus, Antisemitismus, Morddrohungen und Aufrufen zu Gewalttaten vorzugehen – auch, wenn sie gegen staatliche Institutionen gerichtet sind.

Das wirkt offenbar bei den Netz-Trollen: Einer aktuellen Studie zufolge hat die Zahl der Hass-Posts auf Twitter abgenommen. Dennoch bleiben soziale Netzwerke ein Nährboden für rechtswidrige Äußerungen. Auch aus diesem Grund hat der Gesetzgeber das NetzDG erweitert. Jetzt ist es in der neuen Fassung in Kraft gesetzt. Es sieht unter anderem vor, dass soziale Netzwerke wie Facebook, Twitter und TikTok rechtswidrige Posts, die auf ihren Plattformen publiziert werden, an eine neue Stelle melden müssen. Diese „Zentrale Meldestelle für strafbare Inhalte im Internet“ (ZMI) ist beim Bundeskriminalamt (BKA) angesiedelt und soll

mit rund 200 Beamtinnen und Beamten besetzt werden. Und auf die könnte in Zukunft viel Arbeit zukommen: Das BKA rechnet damit, dass aufgrund des geänderten NetzDG rund 250 000 Meldungen jährlich bei der ZMI eingehen. Laut einem Sprecher der Behörde gehe man davon aus, dass circa 150 000 Meldungen dann auch tatsächlich in ein Strafverfahren münden.

Gegenwind für die ZMI

Ob diese gewaltige Zahl allerdings wirklich erreicht wird, ist äußerst zweifelhaft. Denn vorerst dürfte wohl kaum etwas passieren: Nach Verabschiedung des NetzDG im vergangenen Jahr legten Facebook und Google (Muttergesellschaft von YouTube) sofort gemeinsam Beschwerde ein.

Beide Unternehmen weigern sich, jede mögliche Rechtsverletzung an die ZMI zu melden. Sie begründen das mit einem unverhältnismäßig großen Aufwand, der nicht zu stemmen sei. Außerdem, so ein Google-Sprecher, sei

man nicht bereit, personenbezogene Nutzerdaten einfach so weiterzuleiten. Vielmehr solle die Weitergabe nur nach einer ausführlichen Prüfung durch ein Gericht und eine richterliche Bestätigung verpflichtend sein.

Die Verfahren laufen noch. Deshalb entschied das Bundesjustizministerium im August 2021, bis zur Entscheidung über die Beschwerden auf eine Meldungspflicht zu verzichten.

Im neuen Jahr zogen zwei weitere Unternehmen nach: TikTok und Twitter. Eine Woche vor Inkrafttreten des neuen NetzDG reichte TikTok eine von Facebook und Google unabhängige Klage beim Verwaltungsgericht Köln ein. Der Plattform geht es dabei nicht nur um die Pflicht, von sich aus rechtswidrige Inhalte zu löschen. Zusätzlich ist man nicht bereit, binnen 24 Stunden auf Nutzermeldungen über mögliche Verstöße zu reagieren; das sieht das NetzDG vor. Außerdem glaubt TikTok seine Integrität in Gefahr: Wenn Nutzer sich nicht mehr si-

cher sein könnten, dass ihre Privatsphäre geschützt sei, hätte das negative Auswirkungen auf das Unternehmen. Dass solche Bedenken ausgerechnet von einem chinesischen Netzwerk kommen, ist bemerkenswert.

Ende Januar zog Twitter nach – ebenfalls mit einer eigenen Klage vor dem Verwaltungsgericht Köln. Nach Auffassung des Kurznachrichtendienstes werde durch die proaktive Weitergabe von Daten in die Grundrechte der Bürger eingegriffen.

Wann eine rechtskräftige Entscheidung über die Beschwerden fällt, steht bislang nicht fest. Dazu kommt, dass das ZMI viele der geplanten 200 Stellen noch nicht besetzen konnte.

ZMI – ein zahnlöser Tiger?

Bis zum endgültigen Entscheid sind der ZMI also die Hände gebunden. Dennoch will die neue Behörde nicht untätig sein. Seit dem 1. Februar unterstützen die Ermittler bis auf Weiteres unter anderem die „Zentralstelle zur Be-



WEITERE SICHER- HEITS-NEWS



Unsichere Kundendaten

Wegen einer Sicherheitslücke bei einem Schnittstellen-Dienstleister waren die Kundendaten großer Online-Marktplätze über drei Jahre lang frei im Netz zugänglich. Betroffen sind Plattformen von Otto, Kaufland, Media Markt und andere.

Der Fehler ist mittlerweile behoben, betroffene Kundinnen und Kunden wurden aber bislang nicht informiert. Und von denen gibt es einige: Mehr als eine Million Datensätze von rund 700 000 Nutzerinnen und Nutzern gelangten über die undichte Stelle ins Netz.

Unter den Daten befanden sich Mail- und Postadressen sowie Bestellinformationen, Telefonnummern und sogar Zahlungsdaten wie Bankverbindungen. Die Plattformbetreiber – etwa Kaufland – erklärten, dass sie mit ihren Marktplätzen nur als Vermittler zwischen Kunden und Händlern auftreten würden und nicht für die Speicherung und Absicherung der Kundendaten zuständig seien. Der Landesdatenschutzbeauftragte von Baden-Württemberg bezeichnet es als schwerwiegenden und skandalösen Vorgang, dass die Unternehmen betroffene Kunden bis heute nicht über das Datenleck informiert haben. Ein Schweizer IT-Experte bestätigte gegenüber dem ARD-Magazin Plusminus, dass die Daten in den Händen von Cyberkriminellen ideale Voraussetzungen böten, um Phishing-Angriffe oder Identitätsdiebstahl durchzuführen. Ob die Informationen im Darknet gelandet sind, sei aufgrund der langen Zeitspanne des Leaks nicht nachvollziehbar.

kämpfung der Internetkriminalität“ (ZIT), die bei der Generalstaatsanwaltschaft Frankfurt am Main angesiedelt ist. Außerdem sollen die Meldungen der „REspect!“-Initiative der Jugendstiftung im Demokratiezentrum Baden-Württemberg ans BKA weitergeleitet werden.

Aber auch diese Aufgaben kann das ZMI wohl nur mit angezogener Handbremse wahrnehmen: Da Facebook, Google & Co. keine Daten an die ZMI weitergeben, fehlen den Beamten unter anderem die IP-Adressen, mit denen sich der Urheber eines rechtswidrigen Posts schnell identifizieren ließe.

Telegram verweigert sich

Noch schwieriger sieht es beim Messengerdienst Telegram aus. Der hat sich bislang jeglicher Diskussion mit dem BKA entzogen. Das von Russen gegründete Unternehmen sitzt mittlerweile in Dubai (Vereinigte Arabische Emirate). Und es will offenbar nichts gegen rechtswidrige Umtriebe in Deutschland unterneh-

men. Auf die Frage, wie Nutzer illegale Inhalte löschen könnten, heißt es in den AGB: „Alle Telegram- und Gruppenchats sind die Privatsache der jeweiligen Nutzer. Wir bearbeiten keine diesbezüglichen Anfragen.“ Nur öffentlich einsehbare Inhalte, nicht aber die Posts in einer geschlossenen Gruppe, lassen sich melden. Mit anderen Worten: Wer sich in Telegram-Gruppen wie auch immer äußert, dem droht keine Verfolgung.

Taskforce gegen Radikale

Folge: Der Messenger ist zur bevorzugten Plattform von Radikalen aufgestiegen. Sie unterwandern unter anderem Telegram-Gruppen, in denen sich zum Beispiel Corona-Impfgegner organisieren. Der Ton, so Verfassungsschützer, werde dort immer rauer; Rechtsradikale beherrschen zunehmend die Gruppen und stacheln die Protestler an.

„Die Pandemie hat dazu beigetragen, dass sich Menschen auf Telegram radikalisierten, andere bedrohen oder sogar Mordaufrufe

veröffentlichen“, bestätigt BKA-Präsident Holger Münch. Deshalb wurde eine Telegram-Taskforce ins Leben gerufen. Deren Aufgabe ist es, in Telegram-Gruppen Tatverdächtige zu identifizieren und strafrechtlich zu verfolgen. Dies, so das BKA, geschehe in enger Abstimmung mit den Polizeibehörden der Bundesländer und der ZIT. Dabei hoffen die Beamten auch auf eine Zusammenarbeit mit dem Messenger: „Wir schauen bei Fällen politisch motivierter Kriminalität genau hin, wie gut Telegram bei ‚Löschungsanregungen‘ und Bestandsdatenabfragen kooperiert“, so das BKA. Allerdings werde man auch dann Maßnahmen ergreifen, wenn Telegram sich weiter verweigert.

Zuletzt regte Bundesinnenministerin Nancy Faeser (SPD) an, Telegram EU-weit aus dem Play Store (Android) und dem App Store (iOS) zu verbannen. Neue Verordnungen, die schon bald in der EU in Kraft treten könnten, würden für solche Entscheidungen die Basis liefern. [rs]

Fotos: iStock; Montage: COMPUTER BILD

Die Sache mit den DOCKIES



Ein neues Gesetz sollte den täglichen Umgang mit Cookie-Bannern ändern. **Doch die Revolution muss noch warten.**



Viele Gesetze beschäftigen sich direkt mit den Auswirkungen des Internets auf unser Leben. Ende 2021 traten gleich mehrere in Kraft – vorrangig zum Schutz der Privatsphäre. Doch bis das Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) im Alltag wirken kann, wird noch einige Zeit ins Land gehen. Die Änderungen betreffen vor allem die altbekannten „Cookies“.

1 WAS SIND COOKIES?

Jeder kennt sie, aber nur wenige wissen, was genau sie tun. Im Prinzip sind Cookies nur kleine Textdateien. Sie werden von Internetseiten im Speicher Ihres Smartphones oder Computers „verkrümelt“. Besuchen Sie diese Internetseite später erneut, dann werden sie als wiederkehrender Besucher erkannt. Das hat den Vorteil, dass etwa ein Warenkorb in einem Shop noch immer die Produkte enthält, die Sie dort hineingelegt haben. Oder Sie sind dann noch mit Ihrem Benutzerkonto angemeldet und müssen nicht erneut Ihre Daten angeben.

2 WAS BRINGEN DIE BANNER?

Die Hinweise auf die Cookies sind da, weil die europäischen Gesetzgeber für mehr Transparenz bei den Nutzern sorgen wollten. Im Alltag ist daraus eine lästige Prozedur geworden, die viele Klicks erfordert. Unter anderem kann man sich anzeigen lassen, welche Unternehmen bei einem Besuch der Website Informationen ablegen oder abrufen dürfen. Das sind oft Dutzende von Firmen, von denen man noch nie gehört hat. In den meisten Fällen kann man dann seine Einwilligung generell oder teilweise entziehen und dann die Website trotzdem anschauen. Es kann aber sein, dass dann bestimmte Inhalte nicht funktionieren.

Weil fast alle Websites Cookies verwenden, müssen auch alle darauf hinweisen. Die meisten Nutzer sind davon nur noch genervt, viele ersparen sich die ständige

Klick-Orgie und haben sich längst daran gewöhnt, einfach auf „Alle akzeptieren“ zu klicken.

3 SIND COOKIES GEFÄHRLICH?

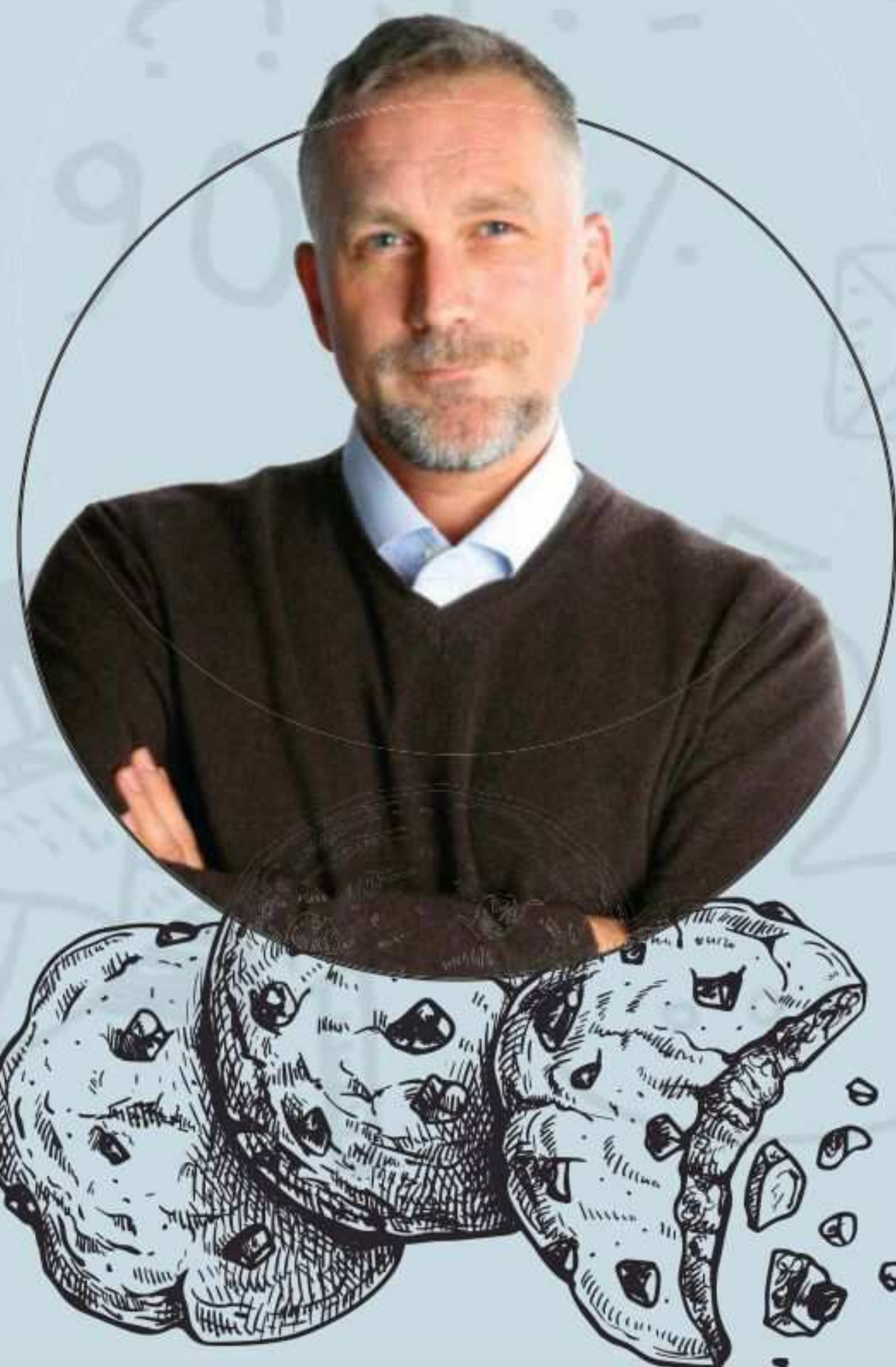
Zunächst einmal ist ein Cookie nicht schädlich. Aber: Nicht nur die besuchten Seiten setzen Cookies, sondern auch Werbenetzwerke und Analyseunternehmen, die sich dafür interessieren, welche Ziele die Nutzer ansteuern. Sogenannte Tracking-Cookies sorgen dafür, dass Sie auf Seite A nach einer Jeans schauen und auf Seite B selbst Tage später noch Anzeigen für Jeans sehen. Das Werbeunternehmen weiß also genau, was einen Nutzer interessiert. Auf eine ganz konkrete Person, zum Beispiel Eva Müller in der Hauptstraße 4, lässt sich das aber nicht eingrenzen. Zumindest nicht nur anhand von Cookies.

4 WAS KANN ICH DAGEGEN TUN?

Jeder Browser hat eine Funktion, mit der Sie die Cookies löschen können, in den Einstellungen von Chrome etwa zu finden unter „Datenschutz und Sicherheit“ und „Browserdaten löschen“. Allerdings gibt es andere Methoden,

„Der Umgang mit Cookies wird sich fundamental wandeln.“

Dirk General-Kuchel
Chefredakteur



einen Besucher wiederzuerkennen – auch ohne Cookies. Das sogenannte Browser Fingerprinting ermöglicht das durch die Kombination verschiedener technischer Informationen von Bildschirmauflösung, installierten Erweiterungen oder Betriebssystem. Das können Nutzer nur mit Zusatz-Software wie zum Beispiel „Anti Browser Spy“ unterbinden (www.cobi.de/11436).

5 WAS IST NUN ANDERS?

Unglaublich, aber: im Prinzip nichts. Denn die EU-Vorgaben sind schon mehr als zehn Jahre alt, der deutsche Gesetzgeber hat sie nur nie korrekt umgesetzt. Daher gab es diverse Rechtsverfahren. Die Cookie-Banner, die Sie schon kennen, haben die Seitenbetreiber schon in der Erwartung eingerichtet, dass die Vorgabe kommt.

Banner wird es also auch in Zukunft geben. Nichts Neues also? Doch, denn schon bald könnten wir uns alle mit den sogenannten PIMs beschäftigen.

6 WAS SIND PIMs?

Auch der Gesetzgeber weiß, wie lästig die Cookie-Banner sind. Deswegen soll es eine Alternative geben: das sogenannte Personal Information Management. Im PIM soll der Nutzer einmalig angeben, was er akzeptieren und was er blockieren will. Aufgerufene Seiten würden diese Informationen dann zur Kenntnis nehmen und sich an die Vorgaben halten.

PIM könnte etwa eine Einstellung im Handy sein, wo man die Vorgaben einträgt. Die könnten aber auch in einem zentralen Portal gespeichert sein, dessen Benutzerkonto dann auch zur Anmeldung auf anderen Seiten gilt und die Einstellungen dorthin übergibt. Aber: Noch fehlt eine entsprechende Verordnung, die genau regelt, wie so ein PIM gestaltet werden kann. Im Herbst soll es nun voraussichtlich soweit sein. Bis dahin heißt es: weiter die Banner wegeklicken. [dgg]

EMOTET IST ZURÜCK!

Das gefährlichste Virus der Welt ist ein Wiedergänger – schon besiegt geglaubt, kam es mächtig zurück. Das müssen Sie wissen.

Emotet ist ein Programm gewordenen Albtraum. Davon wissen vor allem Mitarbeiter an Krankenhäusern, Universitäten und Gerichten zu berichten, denn solche Institutionen attackiert das Virus besonders häufig. Emotet gehört zur Klasse der Ransomware – solche Erpresserprogramme befallen Computer, um alle erreichbaren Dateien zu verschlüsseln. Dann geht nichts mehr. Opfer können nur Lösegeld an die Erpresser zahlen und hoffen, dass das Gegengift kommt.

Verrückt: Eigentlich war das alles längst bekannt und die Gefahr gebannt. Doch dann kam Emotet zurück und startet noch immer täglich viele Tausend Angriffe! Was ist da los?

Was genau macht Emotet?

Emotet ist eine extrem gefährliche Erpressersoftware. Sie hat es im Gegensatz zu vielen anderen verwandten Schädlingen nicht auf die Dokumente und Fotos von Privatanutzern abgesehen. Stattdessen dient sie dem Ziel, komplette Infrastrukturen von Unternehmen lahmzulegen und für die Entschlüsselung mehrere

Millionen Euro Lösegeld zu fordern.

Emotet kommt als Office-Dokument im Anhang einer Mail. Öffnet es der Empfänger, nutzt Emotet sogenannte Makros und die in vielen Betriebssystemen eingebaute Power Shell, um den eigentlichen Schädling herunterzuladen, das System unbrauchbar zu machen und sich auf andere Geräte im Netzwerk weiterzubreiten (siehe Grafik unten).

Die Phishing-Mails, mit denen Emotet in ein System gelangt, sind keineswegs übliche Massenschreiben in schlechtem Deutsch mit kryptischen Absendern. Die Mails stammen von echten Absen-

dern, mit denen es zuvor bereits Kontakt gab, sie beziehen sich auf die vorherige Konversation und sind auch für Experten nicht immer als Betrug zu erkennen.

Emotet kann alles

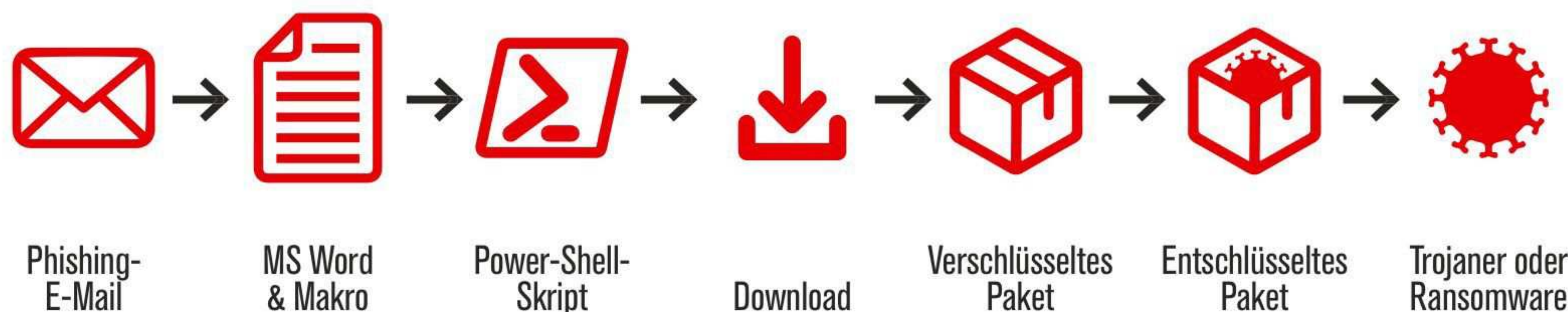
Neben der Professionalität der Spam-Angriffe ist Emotet durch seine Vielfältigkeit so gefährlich. „Emotet ist ein Access Broker, er öffnet die Tür für fast jede beliebige Verwertungsstrategie durch Kriminelle. Am Ende steht irgendwann Ransomware. Was dazwischen passiert, bekommen die meisten Opfer gar nicht mit“, erklärt Dr. Tilman Frosch, Geschäftsführer von G Data Advanced Ana-

lytics. Zudem erkennen viele Schutzprogramme neue Emotet-Varianten erst nach Tagen. Das renommierte Testinstitut AV-Test hat das in einer Grafik festgehalten (siehe Grafik rechts): Erst eine Woche nach dem Auftauchen einer neuen Variante hatten 90 Prozent der Schutzprogramme das Virus erkannt und blockiert – in den ersten 24 Stunden schaffen das nur knapp 30 Prozent!

Emotet war schon zerschlagen

In einer internationalen Großaktion mit Europol, BKA und weiteren Strafverfolgungsbehörden gelang es Anfang 2021, Emotet zu zerschlagen – jedenfalls dachte

ABLAUF EINER EMOTET-INFESTION



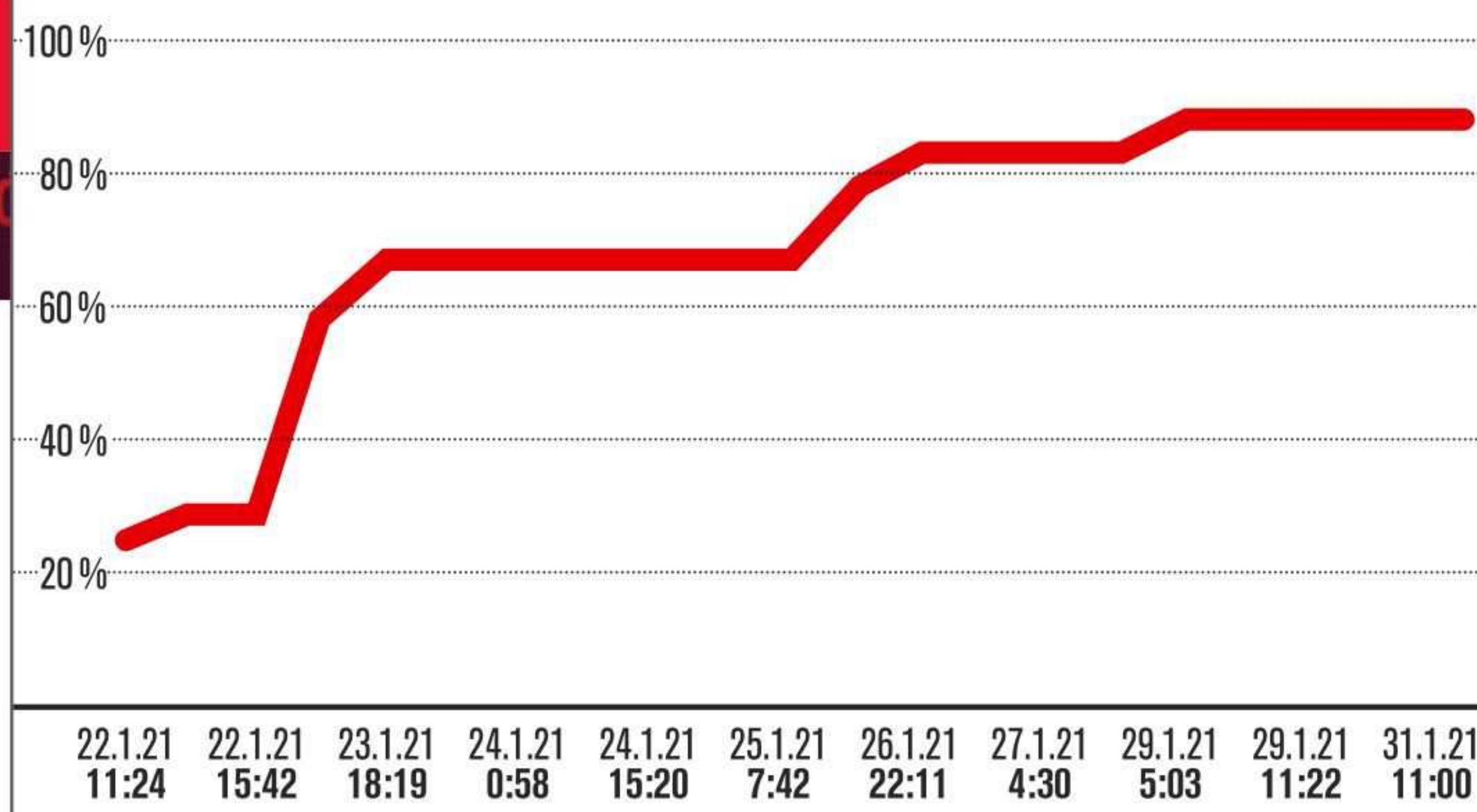
Quelle: AV-Test Institut

„Emotet öffnet die Tür für nahezu jede beliebige Verwertungsstrategie durch Kriminelle.“

Dr. Tilman Frosch
Geschäftsführer G Data Advanced Analytics



VIRENERKENNUNG NEUER VARIANTEN



Quelle: AV-Test Institut

man das. Große Teile der Infrastruktur der Hacker wurden in den Niederlanden beschlagnahmt und unschädlich gemacht. Hintermänner, darunter mindestens ein Administrator, wurden in der Ukraine verhaftet, Gold, Bargeld und PCs sichergestellt. Die Schadsoftware verschwand, und es gab vorerst keine weiteren Angriffe.

Emotet ist zurück

Doch am 14. November 2021 registrierten die Systeme von G Data bei einem Kunden die Schadsoftware Trickbot, die wiederum eine weitere Malware nachlud. Und eben die erkannten die Systeme des Unternehmens als Emotet. Experten anderer Sicherheitsfirmen bestätigten die Analyse, der gefürchtete Schädling war zurück und nutzt nun lediglich ein neues „Beiboot“, um auf die Systeme der Nutzer zu gelangen.

Top-Virus 2022

Seitdem machte sich Emotet weltweit breit – zwar nicht mehr so stark wie zu seinen Hochzeiten, aber dennoch gilt er noch immer als der am stärksten verbreitete Schädling des Jahres 2022. Unter-

nehmen und Nutzer sollten sich daher unbedingt auf erneute Angriffswellen der Horror-Malware vorbereiten.

Das müssen Sie jetzt tun!

Emotet ist vor allem für Unternehmen eine Gefahr. Ist das Firmennetzwerk erst mal infiziert, erfordert seine Rettung extremen Aufwand und horrenden Kosten. Um Angriffe zu vereiteln, müssen Unternehmen also Mitarbeiter sowie Administratoren schulen und die Systeme sichern. Das kostet zwar Geld, aber: „Jeder Euro, den ein Unternehmen in die Abwehr von Cyberangriffen steckt, spart 10 Euro beim Aufräumen eines Angriffs“, sagt Experte Dr. Frosch.

Mitarbeiter sollten vorsichtig sein, schließlich will keiner für einen Totalausfall des Unterneh-

mensnetzwerks verantwortlich sein. Prüfen Sie daher vor allem E-Mail-Anhänge ganz genau: Verlangt das Dokument den Einsatz von Makros, fragen Sie lieber telefonisch beim Absender nach, ob er es wirklich geschickt hat. Solche Makros sind nämlich in vielen Excel-Tabellen oder Word-Dokumenten enthalten und führen Befehle aus. Die können aber auch Schaden anrichten.

Schutz für zu Hause

Antivirus-Programme schützen zwar meist, aber mittlerweile hat auch Office-Hersteller Microsoft reagiert und blockiert standardmäßig die Ausführung von Makros, wenn Sie in einem Dokument stecken, das aus dem Internet kam. Seither lässt die Verbreitung von Emotet leicht nach. [av]

BEKANNTE EMOTET-OPFER

■ Im Juni 2014 tauchte die Schadsoftware Emotet erstmals auf und infizierte die Systeme von Kunden deutscher und österreichischer Banken.

■ Im November 2018 traf es das Klinikum Fürstentfeldbruck. Das Krankenhaus schaltete alle 450 Rechner im Haus ab und meldete sich bei der Rettungsleitstelle ab.

■ Im Mai 2019 infizierte Emotet die PCs der Heise Gruppe und legte die Redaktion vorerst lahm.

■ Im September 2019 war das Kammergericht Berlin durch eine Emotet-Attacke quasi handlungsunfähig. Ein Gutachten riet zum kompletten Neuaufsetzen der IT-Infrastruktur.

■ Im August 2020 erwischte es den Fuhrpark-Service der Bundeswehr, der teilweise auch den Fahrdienst des Deutschen Bundestags stellt.

Fotos: iStock; Montage: COMPUTER BILD

BETRUG M amazon-ANRUF

Der Betrug per Telefon nimmt immer mehr zu. Neue Masche: Kriminelle rufen an und geben sich als **Mitarbeiter von Amazon** aus. Das Ziel sind Ihre Daten und Log-ins – und damit Ihr Bankkonto!



Über **9500** verdächtige Telefonnummern wurden 2021 durch Tellows-Nutzer gemeldet. Viele davon sind nur wenige Tage aktiv.

Quelle: https://www.tellows.de/s/analyse_de/amazon

Stellen Sie sich vor, Sie bestellen etwas bei Amazon. Ein paar Stunden später klingelt das Telefon. Am anderen Ende meldet sich ein Amazon-Mitarbeiter und fragt, ob Sie einen bestimmten Artikel wirklich bestellt haben. Danach fragt er nach einigen persönlichen Daten, die angeblich im System fehlen. Und weil ja alles in Ordnung sein soll, rücken Sie die Daten raus. Klingt ganz normal für Sie? Vorsicht!

Denn am Apparat ist wahrscheinlich ein hinterlistiger Betrüger.

Betrug mit Fake-Support

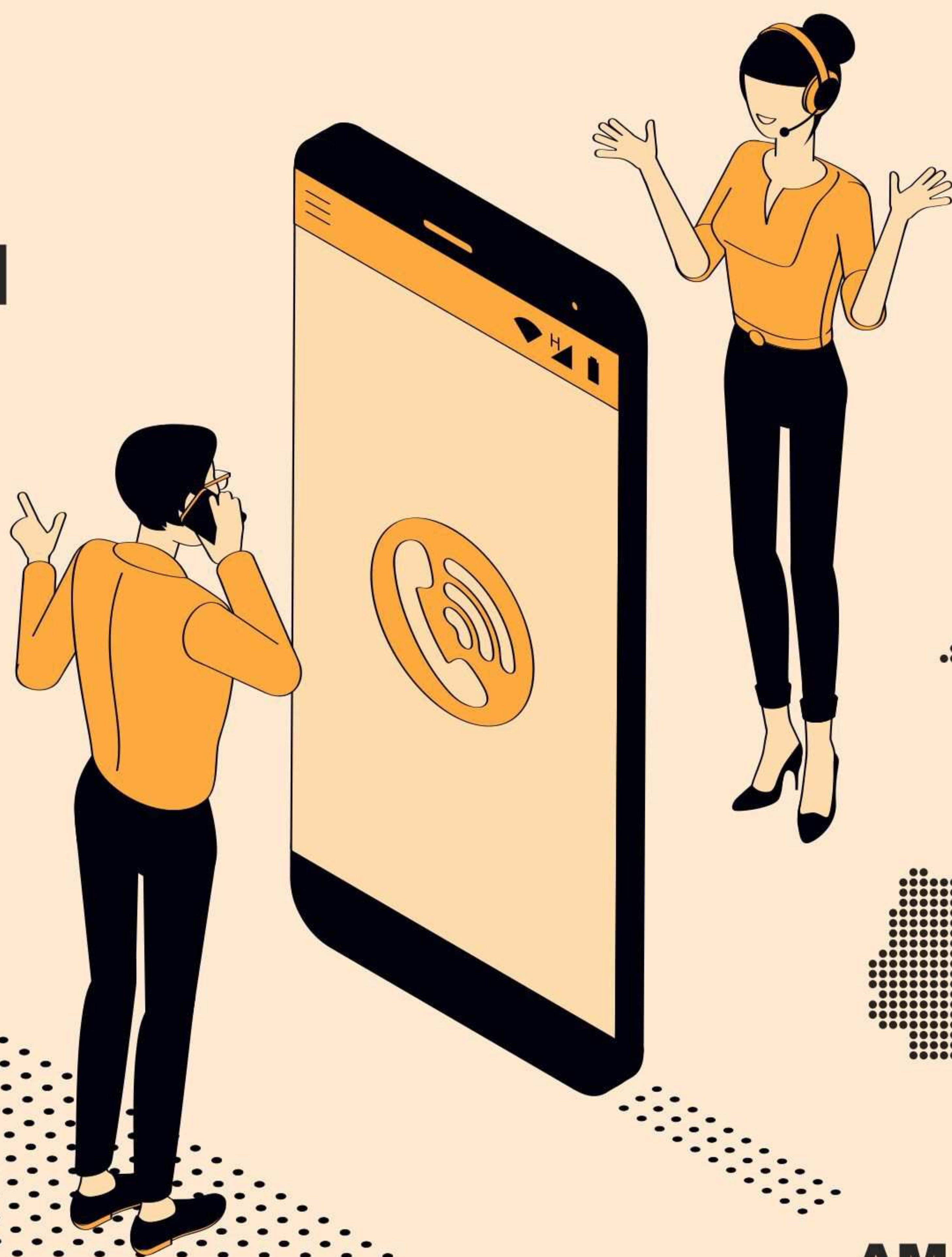
Derzeit häufen sich solche Anrufe, die Masche scheint also gewinnträchtig zu sein für die Kriminellen. Meist sind sie auf Kreditkarten- oder andere Zahlungsdaten aus, mit denen die Angreifer auf Kosten ihrer Opfer shoppen wollen. Wie gravierend das Problem ist, zeigt eine schockierende aktuelle Studie der Anti-Telefonterror-Community Tellows: Demnach ist bei weniger als der Hälfte der Anrufe tatsächlich ein Amazon-Mitarbeiter am Apparat. In gut 16 Prozent der Fälle versuchten dagegen Callcenter, den Gesprächspartnern eine Amazon-Kreditkarte anzu-drehen. Das ist nicht direkt gefährlich, aber nervig. Doch unglaubliche 37 Prozent der Anrufe sind schlicht Betrugsversuche!

Fake-Anrufe im Vormarsch

Die Initiatoren von Tellows haben das Aufkommen solcher Anrufe über das vergangene Jahr beobachtet und ausgewertet. Ihr Ergebnis: Der Anteil von Betrugsanrufen nimmt ständig zu. Besonders in der Vorweih-



IT EN



nachtszeit verzeichneten die Experten einen deutlichen Anstieg.

Doch wie kommen die Anrufer eigentlich an die Telefonnummern? Die meisten stammen aus einem Datenleck bei Facebook. Dadurch sind dem US-Konzern auch Telefonnummern der Nutzer abhandengekommen. Kriminelle missbrauchen sie aktuell massiv für betrügerische SMS mit Meldungen zu angeblich verpassten Anrufen oder fehlgeschlagenen Paketzustellungen. Wer darauf klickt, landet auf Phishing-Seiten.

Amazon ruft nur auf Wunsch an
Amazon selbst ruft Kunden nur an, wenn sie es wollen und den Prozess selbst gestartet haben. Zum Beispiel, wenn es ein Problem mit einer Bestellung gibt. Außerdem rufen Fahrer des Amazon-Lieferdienstes hin und wieder an, wenn Schwierigkeiten oder Unklarheiten bei der Lieferung bestehen. Aber: In beiden Fällen verlangt niemand von Ihnen, dass Sie erklären, wer Sie sind. Und niemand fragt Sie nach Kontodaten oder Passwörtern.

Kriminell mit großen Namen
Die Verbrecher geben sich übrigens nicht nur als Amazon-Mitar-

beiter aus. Für Ihre Betrugsversuche missbrauchen sie auch den Konzernriesen Microsoft und Telefonanbieter wie Vodafone.

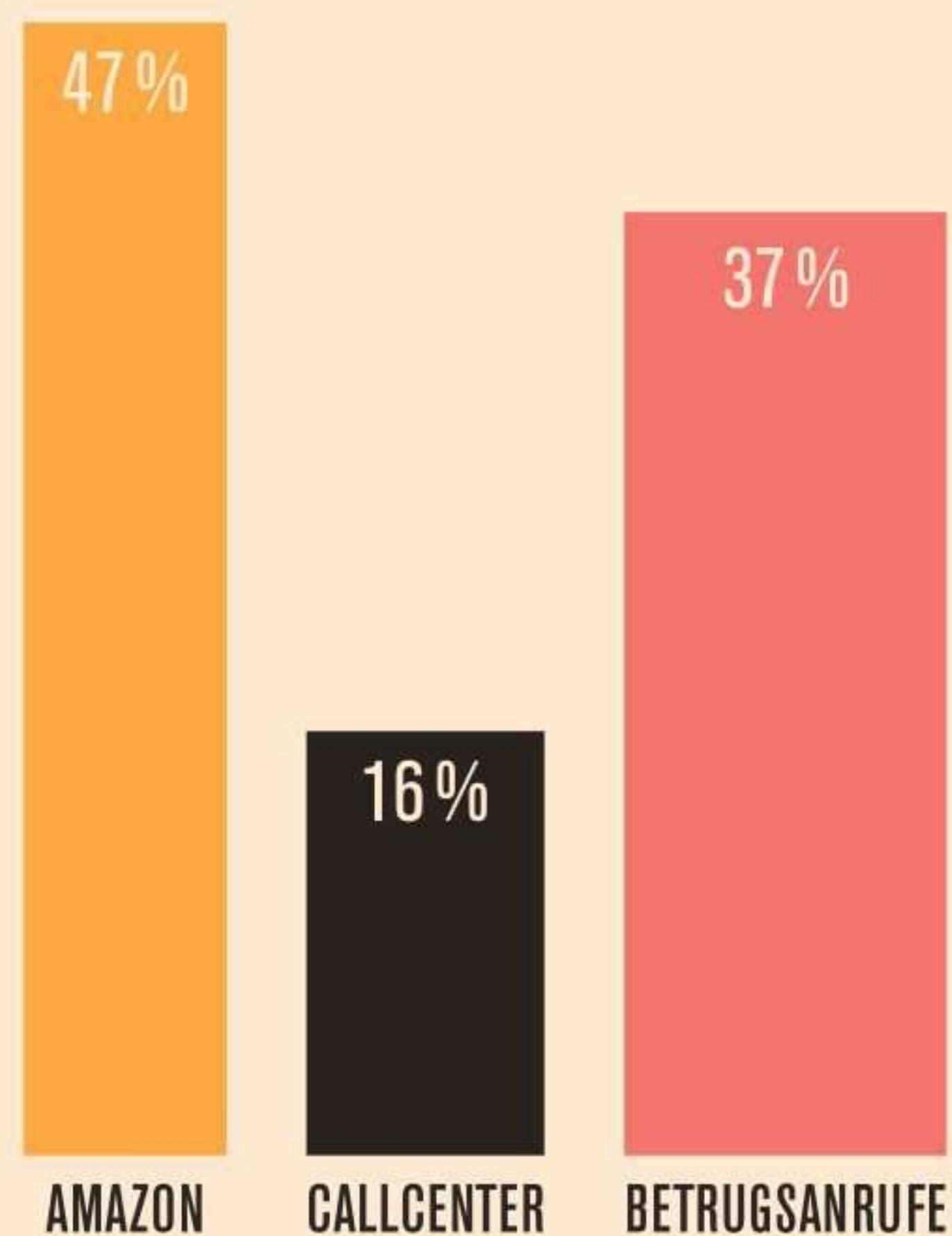
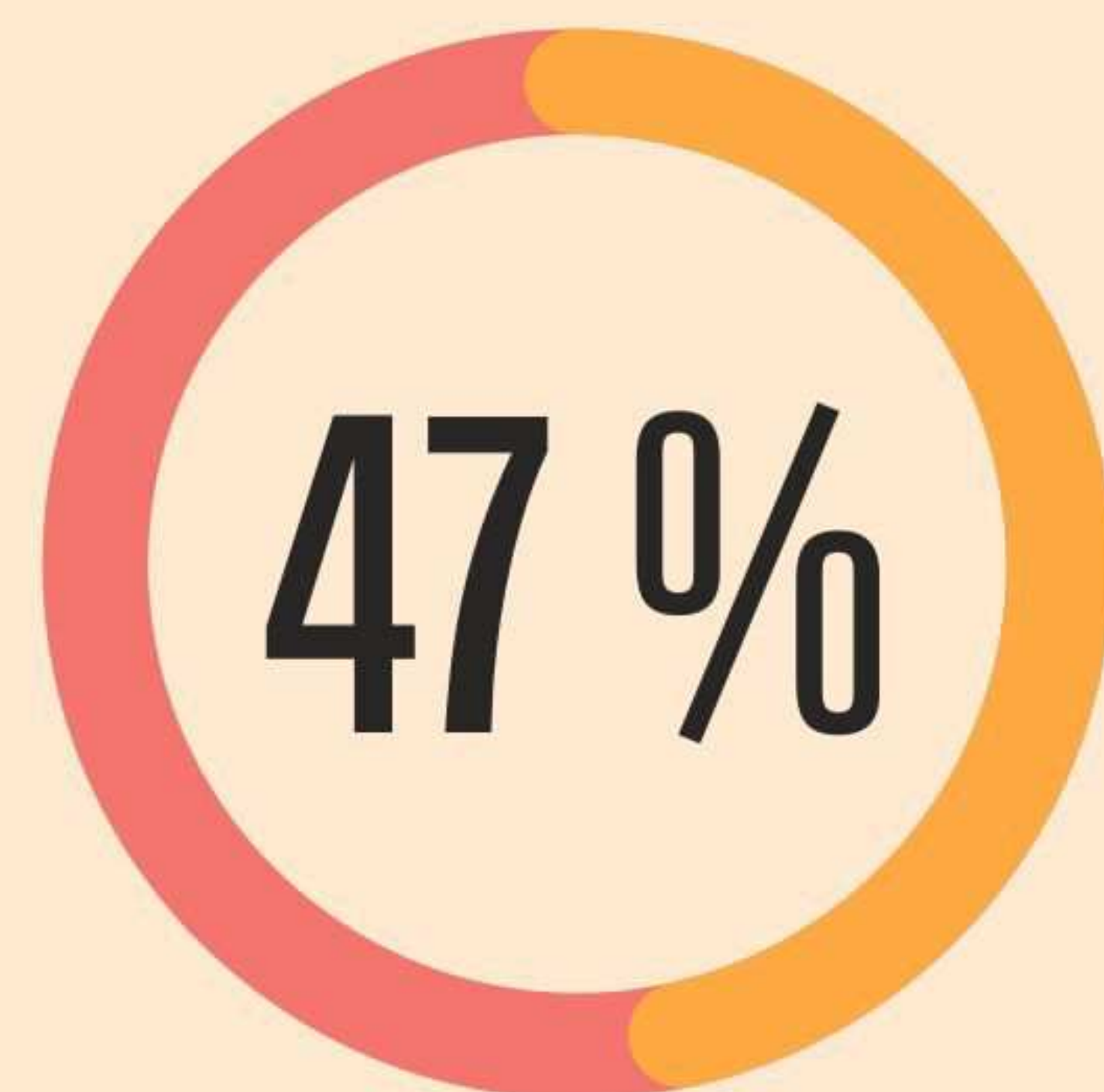
Immer wieder versuchen angebliche Mitarbeiter von Microsoft, Sie zur Installation einer Fernwartungssoftware zu überreden. Wenn Sie das tun und Ihren Zugang freigeben, installieren die Betrüger Schadsoftware und nehmen Fotos und Dokumente in Geiselhaft. Freigegeben werden die Daten nur gegen Lösegeld. Legen Sie lieber auf, statt sich auf Diskussionen einzulassen! Schauen Sie im Internet nach der richtigen Nummer des Kundensupports, und melden Sie sich dort.

Schutz vor Spam-Anrufen

Solche Anrufe vermeiden Sie mit Anruffiltern wie dem von Tellows (siehe Seite 52). Die filtern unseriöse und nervige Anrufer direkt raus. Zudem können Sie Ihr Smartphone so einstellen, dass nur gespeicherte Kontakte Sie anrufen dürfen. Eine Anleitung dazu finden Sie unter **www.cobi.de/42035**. Wollen Sie diese Funktion nutzen, sollten Sie aber wichtige Support-Rufnummern ebenfalls speichern – für den Fall, dass mal ein echter Support-Anruf kommt. [av]

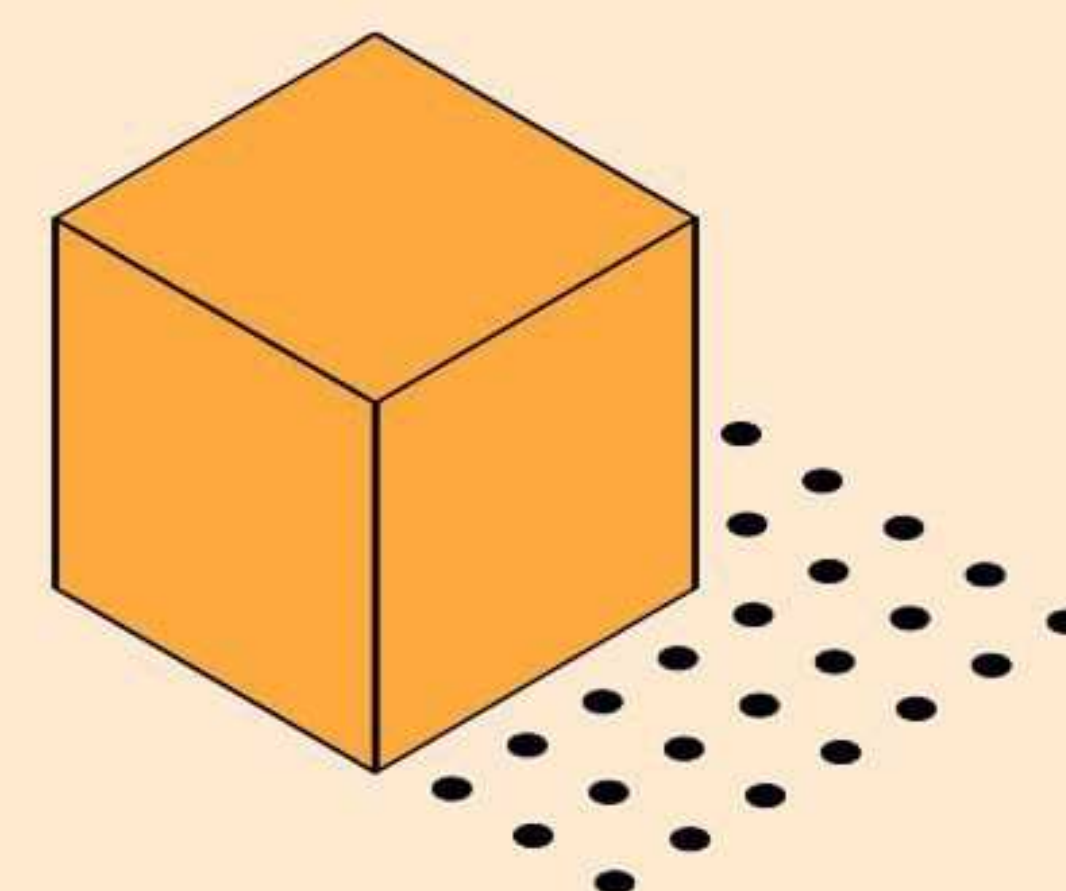
AMAZON nur bei jedem zweiten Anruf dran

Lediglich in 47 Prozent der Fällen ist wirklich ein Amazon-Mitarbeiter dran, wenn der Anrufer das behauptet. Seien Sie also skeptisch!



53 % der Anrufe sind **NICHT ECHT**

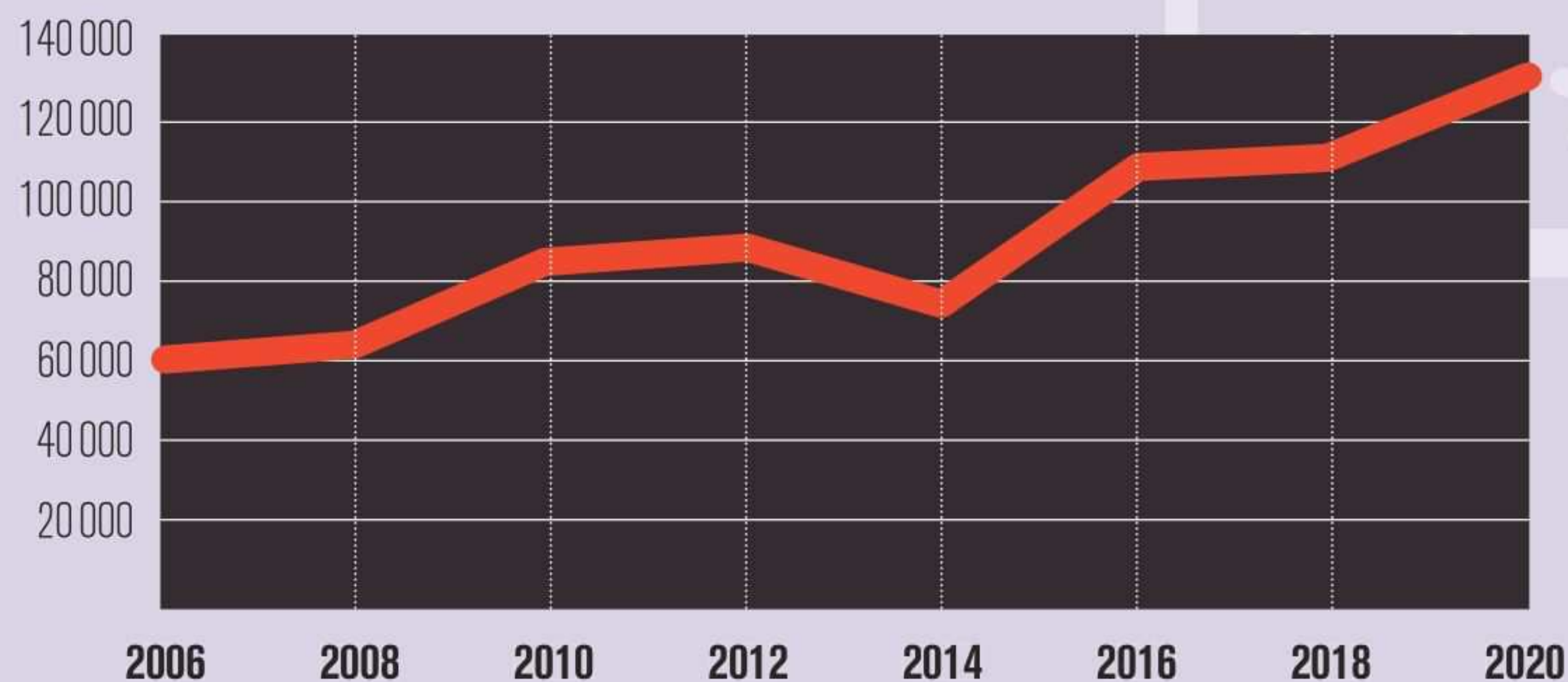
Krasse Zahlen: Ein Großteil der Anrufe sind unverlangte Werbung oder schlicht Betrug.



„Betrugsversuche per Telefon nehmen kräftig zu – passen Sie auf!“

Andy Voß
Redakteur

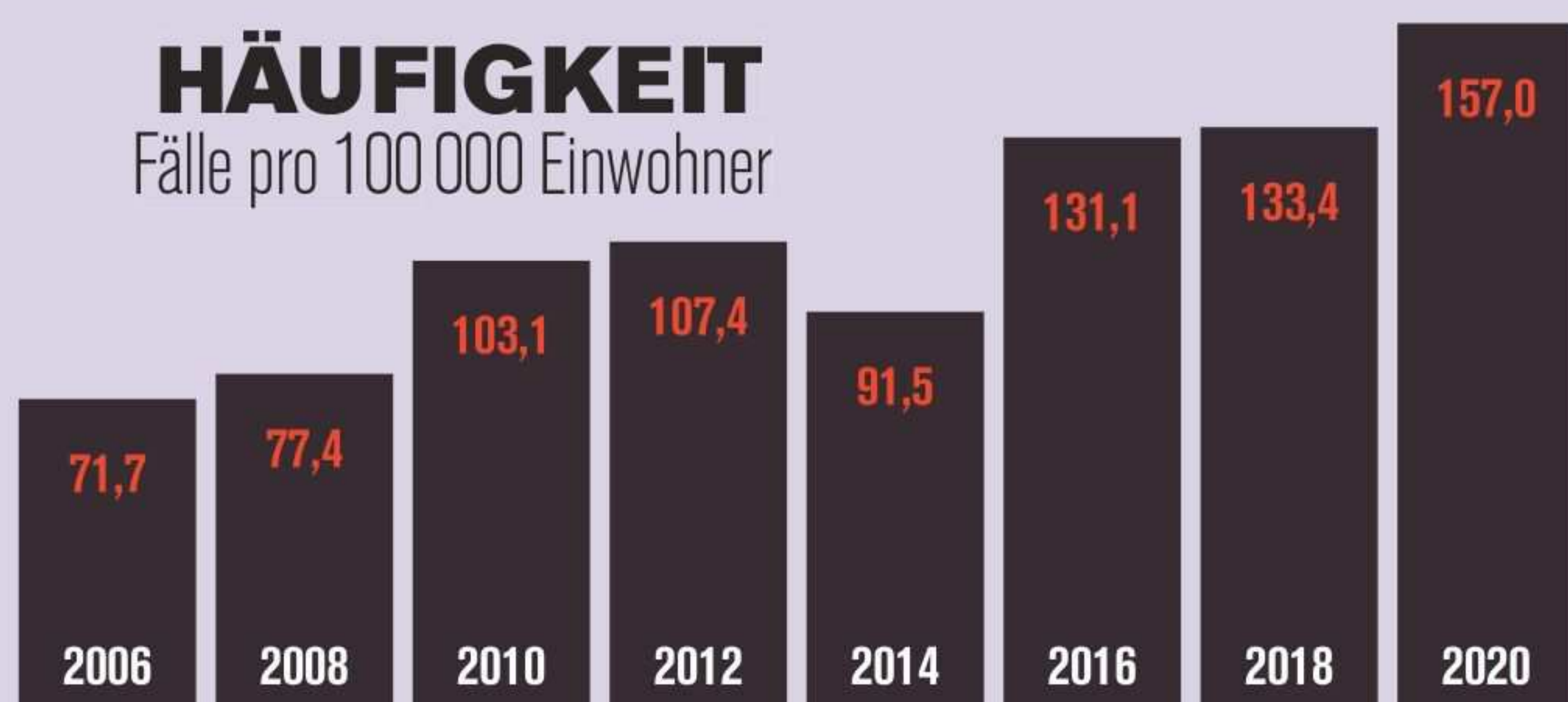
ZAHL DER ERFASSTEN FÄLLE



Die Zahl der erfassten Online-Straftaten steigt stetig: Das heißt aber nicht nur, dass die Bedrohung steigt. Es melden sich auch mehr Opfer.

HÄUFIGKEIT

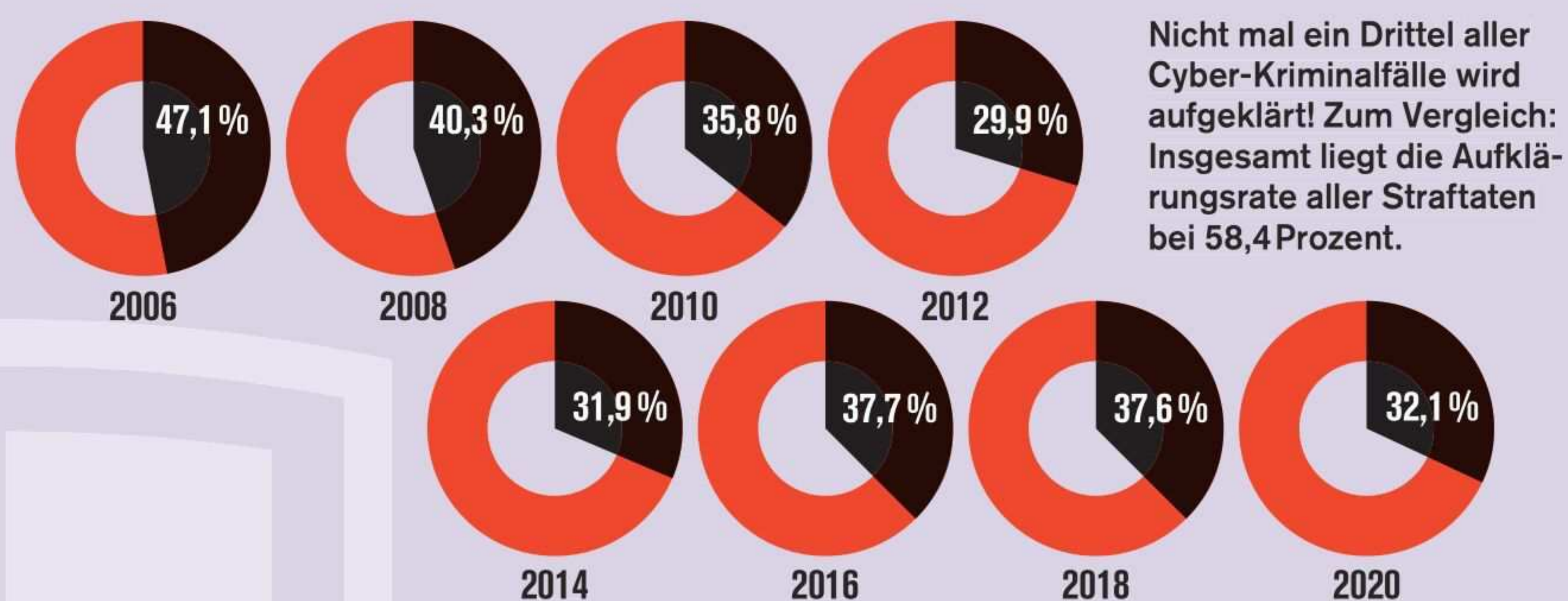
Fälle pro 100 000 Einwohner



Mehr als 150 Deutsche pro 100 000 Einwohner waren 2020 Opfer von Cyberkriminalität. Das sind 50 Prozent mehr als noch vor 10 Jahren!

AUFKLÄRUNGSQUOTE

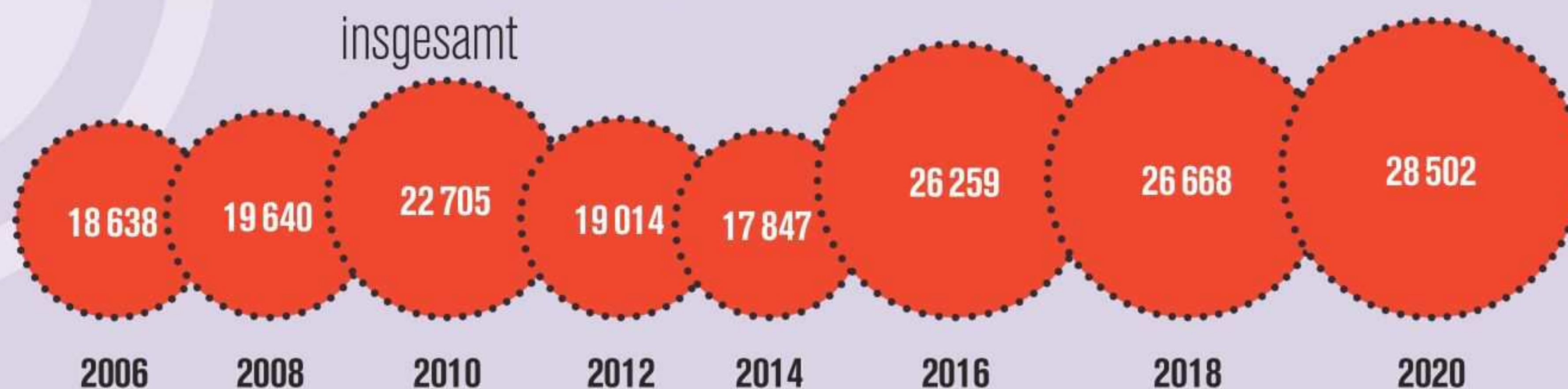
im Fall von Online-Straftaten



Nicht mal ein Drittel aller Cyber-Kriminalfälle wird aufgeklärt! Zum Vergleich: Insgesamt liegt die Aufklärungsrate aller Straftaten bei 58,4 Prozent.

TATVERDÄCHTIGE

insgesamt



Es gibt nicht nur immer mehr Opfer, sondern auch immer mehr Verdächtige und Täter. Im Darknet gibt es sogar Bausätze für Malware zu kaufen – Vorwissen unnötig!

CYB SICHER IN ZAH

So gefährlich ist das Internet in Deutschland

Das Internet macht Spaß, ist Shopping-Meile, und es verbindet uns. Aber im Netz lauern auch Gefahren – Milliarden Schädlinge und massenhaft Abzocker warten dort auf ihre Opfer. Wer sich nicht schützt, merkt oft zu spät, dass etwas nicht stimmt. Viel zu viele Nutzer gehen noch mit der „Mir passiert schon nichts“-Einstellung ins Internet. Wie falsch das ist, zeigt COMPUTER BILD auf dieser Doppelseite mit erschreckenden Statistiken.

Die Gefahr wird unterschätzt

Laut Lagebericht „Digitalbarometer 2021“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) kennen zwei Drittel aller Deutschen die Gefahren im Internet. Trotzdem ergreifen nur 62 Prozent Maßnahmen, und die

WAREN SIE SCHON EINMAL OPFER EINER PHISHING-MAIL?

ER-HEIT LEN

meisten beschränken sich auf die Installation eines Schutzprogramms. Sichere Passwörter oder eine Zwei-Faktor-Authentifizierung nutzen nur 60 beziehungsweise 40 Prozent.

Mehr Fälle, weniger Aufklärung

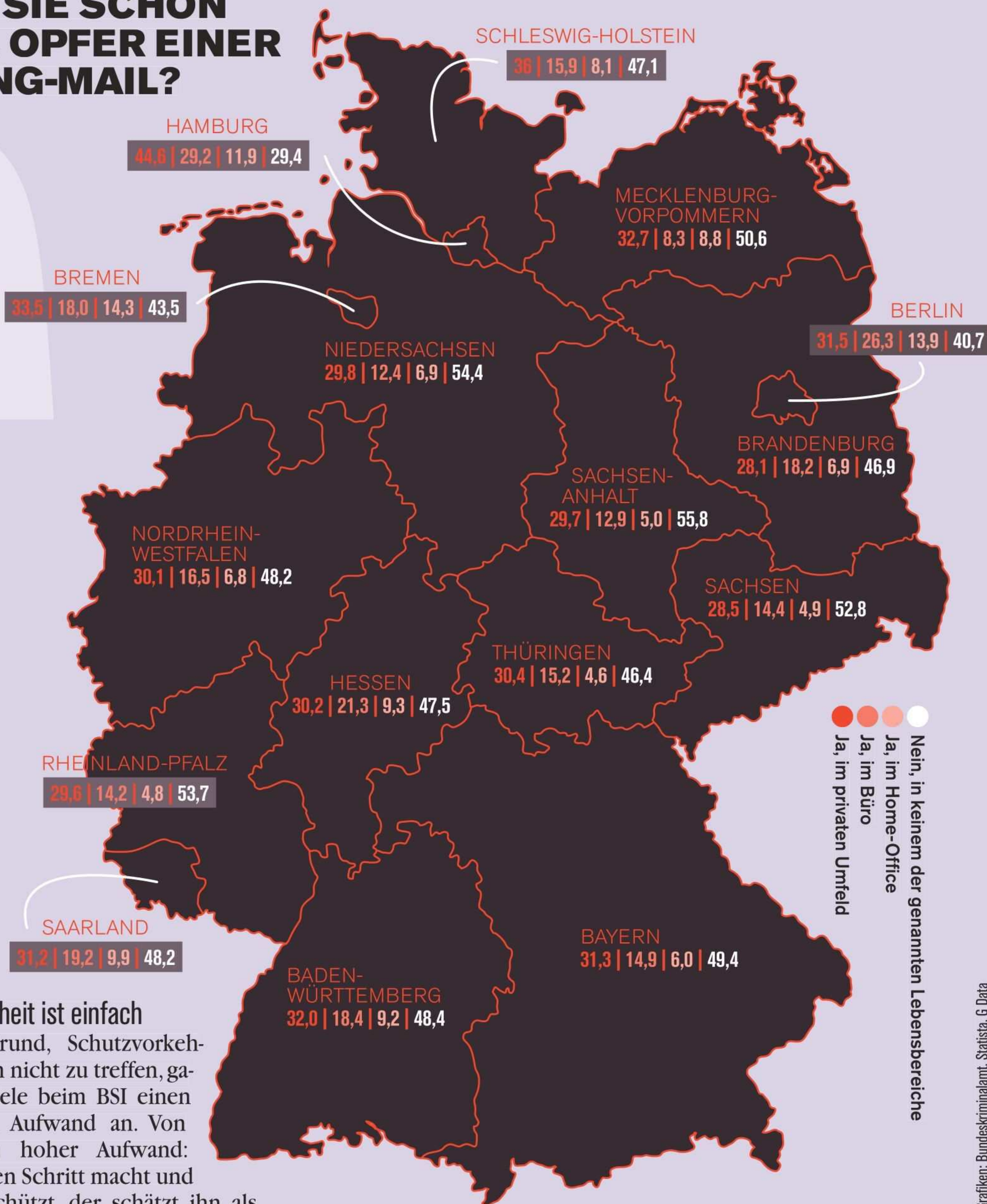
Wohin diese Nachlässigkeit führt, sehen Sie in den Grafiken aus dem Magazin „Cybersicherheit in Zahlen“ von G Data und „brand eins“. Die Vorfälle nehmen demnach stark zu: 2020 gab es 157 Cyber-Straftaten pro 100 000 Einwohner, Tendenz steigend. Die häufigste Straftat ist dabei der Fremdzugriff auf Online-Konten, 31 Prozent aller Deutschen sind betroffen). Straftäter fühlen sich ermutigt, denn die Aufklärungsquote nimmt weiter ab: Ließ sich 2006 noch fast jeder zweite Fall lösen, war es 2020 nur noch knapp ein Drittel – die Kriminellen finden immer ausgeklügelte Wege, um anonym zu bleiben. Wer einen finanziellen Schaden durch Hacker erleidet, bleibt somit oft darauf sitzen.

Sicherheit ist einfach

Als Grund, Schutzvorkehrungen nicht zu treffen, gaben viele beim BSI einen hohen Aufwand an. Von wegen hoher Aufwand: Wer den Schritt macht und sich schützt, der schätzt ihn als recht gering ein. Denn Sicherheit ist wirklich einfach: Installieren Sie ein Schutzpaket wie die G Data Internet Security oder die Avast Premium Security von der Heft-DVD (siehe rechts), und nutzen Sie die Zusatzfunktionen wie Passwortmanager und Update-Tools. Zudem sollten Sie für alle wichtigen Log-ins die Zwei-Faktor-Authentifizierung aktivieren. Auch das dauert nur Minuten.

Mehr Sicherheitsinfos

Weitere Infos zum Thema IT-Security sowie Anleitungen und Programme zum Schutz gibt's im Magazin „Cybersicherheit in Zahlen“ (gdata.de/cybersicherheit-in-zahlen) sowie bei COMPUTER BILD auf der Internetseite www.cobi.de/sicherheitscenter/ [av]



RISIKO regional verschieden

Wer Opfer von Phishing-Mails wird, hängt auch vom Wohnort ab: Im Westen ist es gefährlicher, in Hamburg waren 70 Prozent der Einwohner schon mal solchen Betrugsversuchen ausgesetzt.



SCHUTZPAKET GRATIS

Als Käufer dieses Sonderhefts erhalten Sie Avast One gratis und können das Schutzpaket bis zum 21. April 2023 nutzen. Es enthält alle wichtigen Sicherheitsprogramme.

PASSWORT



ADE?

*Passwort-Anmeldungen sind unsicher und nervig.
Google, Apple und Microsoft wollen sie daher
abschaffen – und setzen auf eine clevere Alternative!*

Fotos: iStock; Montage: COMPUTER BILD

Passwörter sind wohl die größte Plage des digitalen Zeitalters. Klar, man sollte für jeden Shop, jeden Dienst und jede App ein eigenes, höchst komplexes Passwort haben und es dann auch regelmäßig wechseln. Doch wer mit Dutzenden Passwörtern jonglieren will, der braucht Passwort-Manager auf all seinen Geräten. In der Praxis ersparen sich viele den Stress und tippen als Passwort einfach „123456“ oder ihren Namen ein. Cyberkriminelle haben damit leichtes Spiel.

Weil die Sicherheit damit auf der Strecke bleibt, will eine Allianz von Google, Apple, Microsoft und Hunderten anderen Unternehmen Passwörter abschaffen und Anmeldungen sicher und komplett stressfrei machen. Mit der FIDO-Anmeldung genügt der Klick auf „Anmelden“ und die Bestätigung auf dem Smartphone.

1 WAS IST FIDO?

FIDO ist die Abkürzung für Fast Identity Online und der Name einer Allianz von Hunderten Unternehmen weltweit, die sicherere Anmeldeverfahren als Alternative zu Passwörtern entwickeln und verbreiten möchte. Diese Allianz gibt es schon seit zehn Jahren, bekannte Mitglieder sind neben Google, Apple und Microsoft zum Beispiel PayPal, Visa, Mastercard, Amazon, Samsung und viele weitere Firmen. Aber auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) gehört zu der Allianz.

Das FIDO-Anmeldeverfahren nutzt Standardverschlüsselungsverfahren in einer nutzerfreundlichen Art und Weise, um sichere

Anmeldungen zu ermöglichen. Der Nutzer teilt einer Website oder einer App nur noch mit, dass er sich anmelden möchte, und bestätigt das biometrisch auf seinem Smartphone. Diese sogenannte Zwei-Faktor-Authentifizierung macht die Eingabe eines Passworts überflüssig.

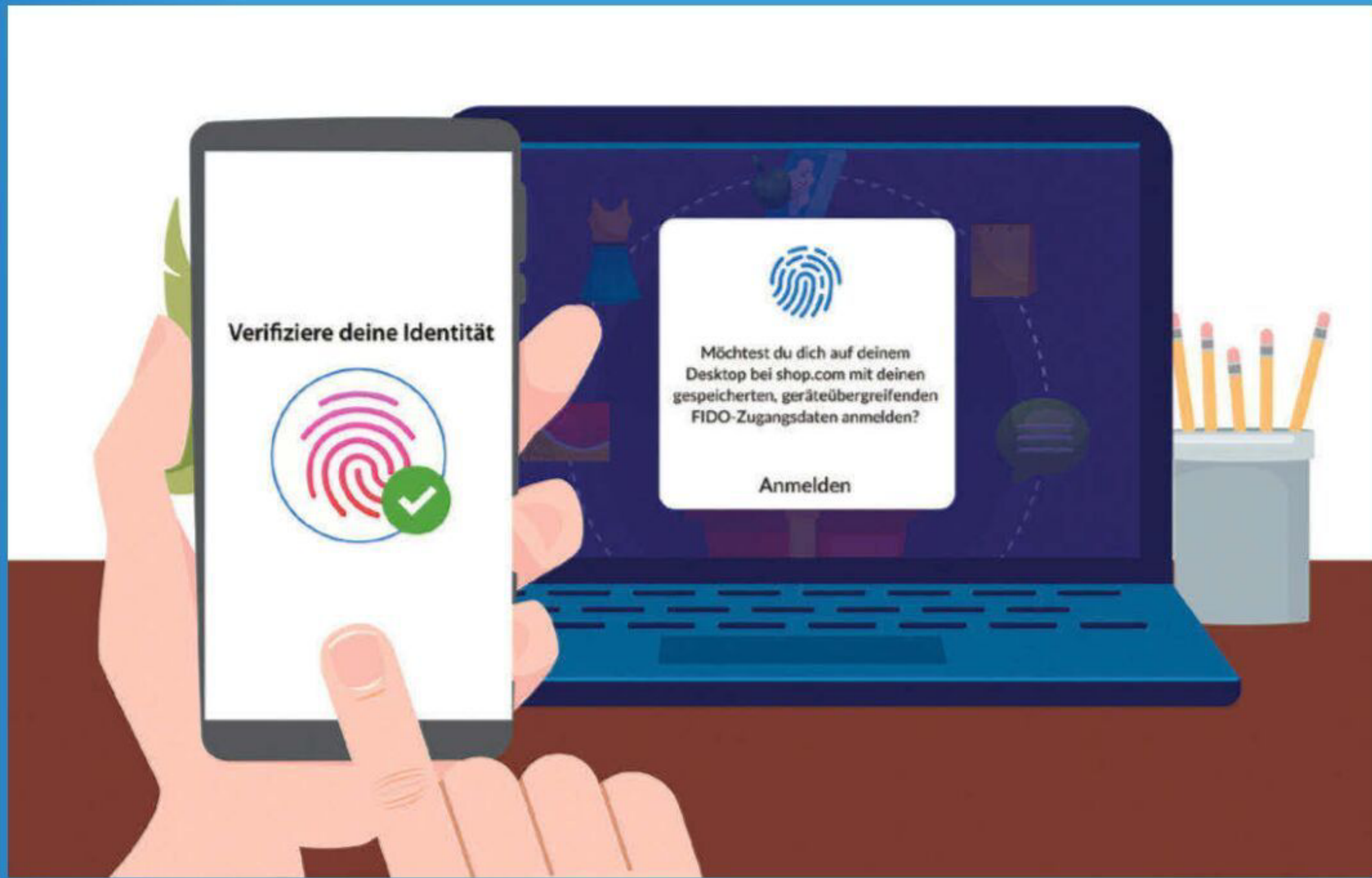
2 WIE FUNKTIONIERT FIDO?

Natürlich funktioniert die einfache Anmeldung per FIDO nur mit Diensten, die diesen Service auch anbieten. Ähnliche Verfahren gibt es bereits von anderen Anbietern, aber dazu benötigen die Nutzer in der Regel eine spezielle Authenticator-App. Das fällt jetzt weg, weil Google, Microsoft und Apple in ihren Betriebssystemen

die Voraussetzungen für die Nutzung von FIDO schaffen. Nutzer und Nutzerinnen registrieren sich wie bisher bei einem Service und tragen alle nötigen Daten ein. Aber statt eines Passworts erzeugt die Seite ein Schlüsselpaar für die „Public Key“-Authentifizierung.

Dieser „öffentliche Schlüssel“ wird auf dem Server gespeichert, der private Schlüssel nur beim Benutzer – und zwar im zum Betriebssystem gehörenden Account bei Google, Apple oder Microsoft.

Will sich der User später anmelden, schickt ihm die Website oder die App eine entsprechende Anfrage nach dem privaten Schlüssel. Der Nutzer erfährt das nur durch eine Bestätigungsabfrage auf seinem Smartphone. Diese Abfrage bestätigt er per Fingerabdruck, PIN oder Face ID, alles Weitere regelt das Betriebssystem im Hintergrund.



Anmelden ohne Passwort: Mit FIDO ist nach dem Klick im Anmeldefenster nur eine Bestätigung auf dem Smartphone nötig.

3 WELCHE VORTEILE HAT FIDO FÜR DIE NUTZER?

■ **Einfach:** Nutzer müssen sich keine Passwörter mehr ausdenken und merken.

■ **Sicher:** Passwörter können nicht mehr gestohlen werden – weder beim Nutzer noch bei Anbietern wie Online-Shops, da eine Anmeldung nur mit beiden Schlüsseln funktioniert. Stiehlt ein Hacker den öffentlichen Schlüssel auf einer Website, fehlt ihm das private Gegenstück. Und der private lässt sich auch nicht aus dem öffentlichen Schlüssel erzeugen. Gelingt einem Hacker der Diebstahl privater Schlüssel, muss er kryptische Zeichenketten erst mal als Schlüssel erkennen. Sollte ihm das tatsächlich gelingen, dann weiß er immer noch nicht, für welche Dienste die Schlüssel sind. Zudem fehlt ihm das zugehörige Smartphone.

■ **Komfortabel:** Klar, schon die kurze Bestätigung per Handy bringt enorm viel Komfort. Aber auch das nervige Umfeld vieler Dienste und Services entfällt komplett, wenn es keine Passwort-vergessen-Funktion oder Bestätigungen per E-Mail mehr geben muss.

4 FUNKTIONIERT FIDO MIT ALLEN GERÄTEN?

Wer sich auf seinem Arbeits-Mac oder Windows-Notebook etwa bei einem Online-Shop angemeldet

hat, der will dort natürlich auch weiterhin mit seinem Android-Smartphone einkaufen können. Die FIDO-Schlüssel werden daher zunächst im Google-, Microsoft- oder Apple-Konto des Kunden gespeichert; bei Bedarf erstellt das Betriebssystem eine Kopie des Schlüssels, um ihn zu den anderen Betriebssystem-Welten zu übertragen.

Beim Wechsel zwischen den Betriebssystemen kann daher eine zusätzliche Bestätigung nötig sein. Der Rest funktioniert dann aber wieder automatisch. Es soll sogar möglich sein, dass sich ein Nutzer etwa auf dem PC eines Freundes auf einer Seite anmeldet: Sein Smartphone wird automatisch per Bluetooth erkannt, und so klappt auch diese Anmeldung per Fingerabdruck.

5 ÜBERNIMMT FIDO BESTEHENDE REGISTRIERUNGEN?

Anbieter, die FIDO unterstützen, wollen Möglichkeiten schaffen, bestehende Konten auf FIDO umzustellen. Wie genau das funktioniert und ob dadurch auch das unsichere Passwort ersetzt wird, hängt vom Anbieter ab.

6 WAS PASSIERT, WENN DAS SMARTPHONE VERLOREN GEHT?

Da die Passkeys in den Nutzerkonten von Apple, Microsoft und Google gespeichert werden, lassen sie sich wiederherstellen,

wenn das Smartphone gestohlen oder beschädigt wurde. Es muss also kein Nutzer befürchten, dass er irgendwann von seinen Konten ausgesperrt wird.

Der Dieb eines Smartphones kann mit den Daten auf dem Handy wiederum gar nichts anfangen, wie Andrew Shikiar, Executive Director bei FIDO, im Interview rechts erklärt.

7 WANN IST DIE FIDO-ANMELDUNG VERFÜGBAR?

Die FIDO-Anmeldung selbst funktioniert bereits, das Drumherum fehlt allerdings noch. So ist beispielsweise die geräteübergreifende Weitergabe noch nicht verfügbar. Google, Apple und Microsoft planen den großen Start für das kommende Jahr – bis Ende 2023 soll alles bereitstehen, um den nervigen Passwörtern endlich Lebewohl zu sagen.

Einige Unternehmen bieten die passwortlose Anmeldung aber auch jetzt schon an. Wer die FIDO-Anmeldung schon mal ausprobieren möchte, kann das auf der Demo-Webseite webauthn.io bereits.

Bis wirklich alle wichtigen Seiten und Anbieter den Zugang per FIDO ermöglichen, vergeht sicherlich noch einige Zeit. Der Gewinn an Sicherheit und Komfort, aber auch die große Zahl der Unternehmen in der FIDO-Allianz sind aber beste Voraussetzungen, dass sich FIDO tatsächlich durchsetzen kann. [av]

„Endlich kümmert sich jemand darum, die nervigen und unsicheren Passwörter zu ersetzen!“

Andy Voß
Redakteur



ZUKUNFT OHNE PASSWÖRTER?



Andrew Shikiar
Executive Director FIDO-Allianz

Wird die FIDO-Anmeldung Passwörter komplett ersetzen oder nur eine Alternative dazu bieten?

Andrew Shikiar: Das entscheidet jeder Anbieter selbst. Beides ist möglich, wobei der Wegfall der Passwort-Anmeldung für mehr Sicherheit sorgt. Wir werden alle unsere Partner mit Richtwerten unterstützen, ab wann es sinnvoll ist, komplett umzustellen.

Das Smartphone wird durch FIDO zum Schlüssel zu allen Accounts. Ist das bei Diebstahl nicht ein Risiko?

Nein. Der Dieb müsste nicht nur das Smartphone entsperren, sondern auch die Biometrie des Besitzers fälschen, also den Fingerabdruck oder das Gesicht des Opfers. Das ist nur bei sehr gezielten Diebstählen überhaupt denkbar und auch dann extrem schwierig.

In der Liste der Partner finden sich auch Banken und Kreditkarten-Anbieter. Planen Sie FIDO auch für andere Zwecke zu nutzen, etwa für Kreditkarten-Zahlungen?

Ja, und das passiert sogar schon. Beispielsweise setzen die spanische Bank BBVA und der deutsche Zahlungsanbieter Pluscard FIDO bereits ein, um Transaktionen zu verifizieren. Der FIDO-Standard bietet eine Menge Potenzial, nicht nur Passwort-Anmeldungen mit einer sicheren, biometrischen Alternative zu ersetzen.

7 TIPPS ZUM SICHEREN ONLINE SHOPPING

SO ERKENNEN
SIE BETRÜGER UND
FAKE-SHOPS



Beim Shoppen im Internet gibt es viele **Gefahren und versteckte Fallen**. COMPUTER BILD erklärt, wie die Ware sicher bei Ihnen ankommt.

Kaufen Sie gerne online ein? Dann aufgepasst! Denn das Shoppen im Netz ist zwar komfortabel und flink erledigt, aber nicht alle Rabatt-Angebote im Internet sind auch wirklich sicher. Cyberkriminelle versuchen zum

Beispiel, mit gefälschten Seiten und Fake-Shops an Ihre Zugangsdaten und Ihr Geld zu kommen. Nur wer auf den Seiten der Shops genau hinschaut, kann das vermeiden und Betrug sofort erkennen.

Worauf Sie bei der digitalen Einkaufstour achten müssen, erklärt COMPUTER BILD auf dieser Doppelseite und gibt Tipps zur zusätzlichen Absicherung. So sind Sie den Betrügern immer einen Schritt voraus. [av]

TIPP 1

IMPRESSUM PRÜFEN

Seriöse Seiten haben ein leicht auffindbares Impressum mit Angaben zu Seiteninhaber, Datenschutzerklärung und allgemeinen Geschäftsbedingungen. Sind die Angaben versteckt oder fehlen sie, steckt mit hoher Wahrscheinlichkeit Betrug dahinter. Kennen Sie die angegebene Firma nicht, googeln Sie den Shop. Bei unseriösen Seiten gibt es häufig bereits Beschwerden in Foren oder Ähnlichem. Prüfen Sie außerdem die Internet-Adresse des Shops. Sind darin Tippfehler enthalten oder folgen beispielsweise „amazon.de“ ein Punkt und eine merkwürdige Zeichenkette, handelt es sich um eine Fälschung. Verlassen Sie in diesem Fall die Seite sofort.

Kontakt | Jobs | Impressum | AGB
Widerrufsbelehrung | Datenschutz

TIPP 2

ZAHLUNGSMETHODEN BEACHTEN

Die meisten Verkäufer im Internet bieten verschiedene Zahlungsmethoden an. Besteht ein Shop auf Bezahlung per Vorkasse, sollten Sie skeptisch werden und nur dann dort bestellen, wenn Sie dem Anbieter vertrauen und ihn – am besten – schon kennen. Am sichersten ist die Nachnahme, in deren Fall Sie dem Postboten bei Lieferung den Kaufpreis des Bestellten zahlen. Aber auch die Zahlung per Lastschrift oder Kreditkarte ist eine gute Option; hier können Sie das Geld im Notfall recht einfach zurückbuchen. Besondere Sicherheit bieten Käuferschutzanbieter wie Amazon oder PayPal (siehe Tipp 3). Zahlen Sie aber nicht mit der Geld-senden-Funktion von PayPal, denn solche Transaktionen sind nur für Freunde und Bekannte gedacht und grundsätzlich nicht abgesichert.





TIPP 3

KÄUFERSCHUTZ

Bei den Käuferschutz-Programmen von Amazon, Ebay und PayPal behält der Zahlungsdienst das Geld so lange, bis die Ware bei Ihnen eingetroffen ist. Erst dann geht es weiter an den Verkäufer. Gibt's Probleme, melden Sie das. Dann bekommen Sie Ihr Geld zurück, sofern es keine andere Lösung gibt. Allerdings gelten die Käuferschutz-Programme meist nur auf bestimmten Seiten oder bei bestimmten Zahlungsmitteln. Informieren Sie sich vorab, ob das für Ihren Einkauf der Fall ist. Falls ja, haben Sie im Betrugsfall sehr gute Karten und bekommen durch den Zahlungsdienst Unterstützung.



Käuferschutz

Falls Ihre berechtigten Bestellungen nicht ankommen oder nicht mit der Angebotsbeschreibung übereinstimmen, wir Ihnen den Preis erstatten.



TIPP 4

PRIVATVERKÄUFE

Besonders bei Amazon Marketplace und Ebay Kleinanzeigen bieten auch Privatpersonen Waren an. Folgendes müssen Sie bei Privatverkäufen beachten:

- Das 14-Tage-Rückgaberecht ist für Privatverkäufer nicht verpflichtend. Zurücksenden bei Nichtgefallen funktioniert daher nicht.
- Ist die Ware defekt (sofern nicht explizit angegeben) oder falsch, muss sie der Verkäufer aber zurücknehmen.
- Prüfen Sie vor dem Kauf, wie andere den Verkäufer bewerteten.
- Zahlen Sie nicht außerhalb der Plattform oder per Geldsendenfunktion, sonst verlieren Sie den Käuferschutz.
- Transportschäden trägt der Verkäufer.

TIPP 5

GÜTESIEGEL CHECKEN

Ein gutes Zeichen für vertrauenswürdige Online-Shops sind Gütesiegel, wie „COMPUTER BILD Top Shop“ (www.cobi.de/topshop). Die bedeuten nämlich, dass unabhängige Dritte die Shops geprüft haben. Doch auch hier ist Vorsicht geboten, zumal Fake-Shops die Siegel oft unberechtigt nutzen. Achten Sie darauf, dass Sie mit einem Klick aufs Siegel per Link auf die Seite des Siegelverleihers gelangen. Kommt Ihnen etwas merkwürdig vor, informieren Sie sich über den Siegelanbieter und prüfen Sie, ob der Online-Shop das Siegel auch wirklich bekommen hat.

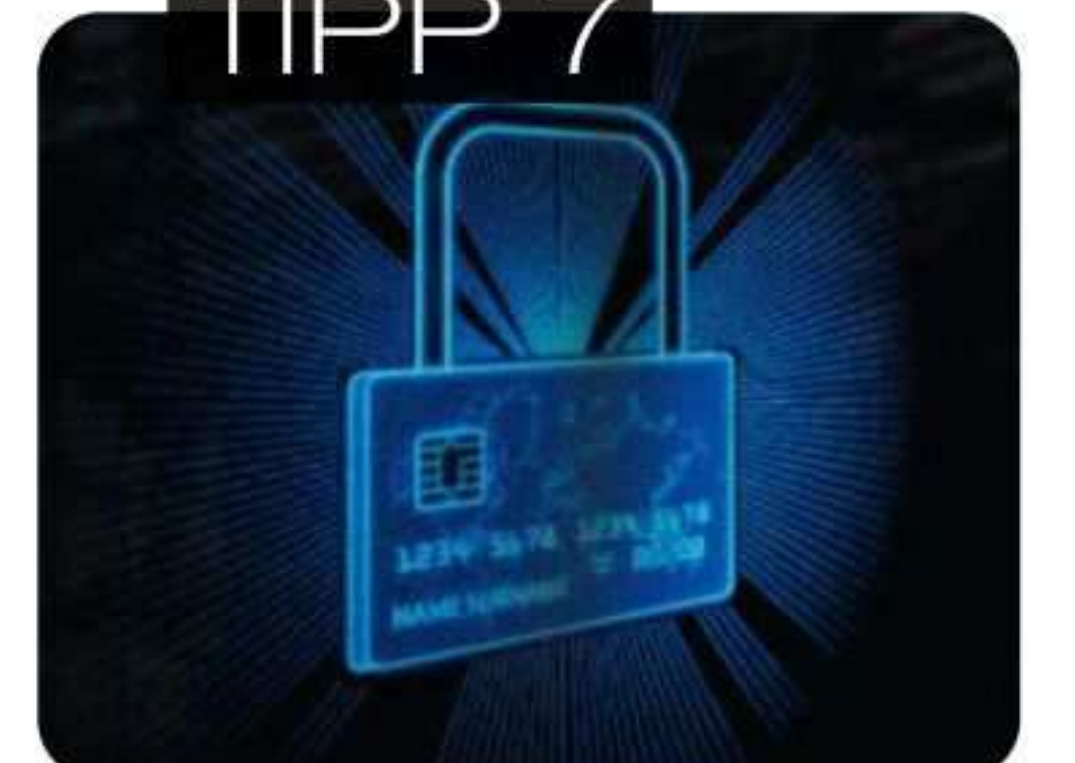
TIPP 6



Sicherheit beachten

Generell gilt beim Online-Shopping: Nutzen Sie kein ungesichertes WLAN, verwenden Sie sichere Passwörter, achten Sie auf HTTPS-Verbindungen, und geben Sie nur die für den Einkauf nötigen Zugangsdaten ein!

TIPP 7



Holen Sie sich Hilfe!

Ist doch einmal etwas schiefgegangen, melden Sie sich bei Ihrer Bank und beim Verbraucherschutz. Dort bekommen Sie Tipps, was Sie tun können und sollten. Der letzte Schritt ist eine Anzeige bei der Polizei.



DIE LETZTE

NOTFALL DVD

Die letzte ist die beste! Die Notfall-DVD 17 ist die perfekte Hilfe bei allen PC-Problemen – jetzt mit sieben neuen Funktionen.

Notfall? Scheibe einlegen! So einfach machte es Ihnen die erste Notfall-CD aus Heft 16/2008, typische PC-Probleme zu lösen. Als Rettungs-CDs noch Sammlungen komplizierter Experten-Programme waren, leitete Sie die COMPUTER BILD-Software per Assistent durch die Problem-

lösung; sie behob automatisch Windows-Fehler, rettete verlorene Dateien oder löschte hartnäckige Viren. 14 Jahre später lässt sich die Notfall-DVD kaum noch verbessern. Version 17 ist daher die letzte Notfall-DVD von COMPUTER BILD. Sie finden sie auf der Heft-DVD und als Download.

Zukunftssichere Version

Neben allgemeinen Verbesserungen wie einem aktuellen Systemkern (Version 5.15) für bessere Hardware-Kompatibilität bietet die Notfall-DVD 17 auch neue Funktionen – siehe nächste Seite. Vor allem hat COMPUTER BILD die letzte Fassung zukunftssicher

gemacht und einen aktuellen Browser sowie einen Gratis-Virens Scanner hinzugefügt. Wie Sie die Notfall-DVD installieren und starten, lesen Sie ab Seite 32.

PC-Probleme beheben

Nach dem Start werden Sie vom übersichtlichen Hauptmenü der



+7 MIT NEUEN FUNKTIONEN

1

Bereit für Windows 11
Die Notfall-DVD 17 arbeitet mit dem neuen Windows, etwa beim Download eines Installationsdatenträgers. **Seite 34**

2

Thunderbird-Retter
Der zeigt notfalls die Postfach-Kennwörter des Mail-Programms an und exportiert dessen Datenbanken. **Seite 37**

3

Firefox-Retter
Auch die im Browser gesicherten Online-Zugangsdaten lassen sich im Notfall jetzt direkt in der Notfall-DVD auflisten. **Seite 37**

4

Virenschutz ClamAV
Der neue Virens Scanner ClamAV ist Open Source und wird daher unbegrenzt mit den nötigen Updates versorgt. **Seite 40**

5

Basis-Sicherheitscheck
Das neue Werkzeug zeigt ungesicherte Passwort-Datenbanken auf der Festplatte und hilft bei der Absicherung. **Seite 41**

6

Firefox 97
Der Mozilla-Browser wurde auf die Version 97 aktualisiert. Er ist updatefähig und damit zukunftssicher. **Seite 46**

7

Neue Anleitungen
Einige QR-Codes in der Notfall-DVD führen jetzt zu Anleitungen im Internet, auch die bleiben somit zukunftssicher.



Notfall-DVD begrüßt, das Sie systematisch durch zahlreiche PC-Probleme führt und diese entweder gleich behebt oder bei der Lösung assistiert. Welche Werkzeuge die Software bietet und wie sie funktionieren, lesen Sie in den ausführlichen Schritt-für-Schritt-Anleitungen ab Seite 34.

Mit Notfall-Arbeitsplatz

Im Expertenmodus finden Sie 70 weitere Profi-Funktionen und den Notfall-Arbeitsplatz. Damit surfen Sie wenn nötig auch ohne Windows im Internet, lesen Ihre E-Mails, bearbeiten Office-Dateien oder hören Musik. Ab Seite 46 erfahren Sie, wie das geht. *[bes]*

„Version 17 ist auch die beste Notfall-DVD, weil alle Tools unbegrenzt laufen.“

Dirk General-Kuchel
Chefredakteur

SO STARTEN SIE DAS NOTFALL-SYSTEM

TIPPS ZUM STARTEN

Starten ohne DVD

Haben Sie kein DVD-Laufwerk? Dann laden Sie die Software bis zum 15. Oktober 2022 von der Webseite **vorteilcenter.de** runter. Dort geben den Vorteilcentercode von der DVD-Hülle ein und klicken auf Eingeben. Nun können Sie die Notfall-DVD herunterladen. Nachdem Sie die Zip-Datei entpackt haben, gibt es zwei Optionen:

■ **DVD brennen:** Nach Einlegen des Rohlings klicken Sie doppelt auf den Ordner **Notfall-DVD**, mit der rechten Maustaste auf **Notfall-DVD, iso**, auf **Datenträgerabbild brennen** und **Brennen**.

■ **Stick erstellen:** Erstellen Sie einen Notfall-Stick, siehe Seite 33.



Abgesicherter Start

Klappt der Start nicht wie rechts beschrieben, probieren Sie im Startmenü die Optionen zum abgesicherten Start durch. Weitere Problemlösungen finden Sie unter **Hilfe zum Start anzeigen**. Dort blättern Sie mit den Tasten **←** und **↓** zeilen- beziehungsweise seitenweise durch den Text. Hinweis: Das Startmenü auf neueren UEFI-PCs (siehe Bild oben) sieht etwas anders aus als auf älteren Geräten mit einem herkömmlichen BIOS.

Sie können den PC direkt von der Heft-DVD starten oder die Notfall-Software zur Vorsorge auf ein Laufwerk installieren.

Wenn der PC spinnt, wichtige Daten verloren scheinen oder ein Virus sein Unwesen treibt, hilft die Notfall-DVD von COMPUTER BILD. Legen Sie dazu einfach die Heft-DVD dieses Sonderhefts ein, und starten Sie den PC neu. Anstelle von Windows erscheint dann der Rettungs-Assi-

stent und behebt die PC-Probleme. Was dabei zu beachten ist, steht unten auf dieser Seite.

Start von Stick oder Festplatte

Gibt es kein akutes Problem, können Sie die Notfall-DVD auch vorsorglich auf ein USB-Laufwerk und sogar neben Windows auf

der PC-Festplatte installieren. Von dort startet die Software erheblich schneller und bietet viele Vorteile. Welche das sind und wie die Installation gelingt, lesen Sie auf der rechten Seite. Tipp: Nutzen Sie alle drei Optionen parallel. Dann sind Sie für jeden Notfall gewappnet. [hes]

NOTFALL-SYSTEM DIREKT VON DVD STARTEN



Voraussetzungen

- DVD-Laufwerk
- mindestens 4 Gigabyte Arbeitsspeicher (RAM)

Empfohlen für

- Soforteinsatz ohne Installation
- gelegentliche Nutzung

1 Datenträger einlegen: Legen Sie die Heft-DVD ins DVD-Laufwerk. Besitzen Sie kein DVD-Laufwerk, beachten Sie den Tipp „Starten ohne DVD“ links auf dieser Seite. Schalten Sie dann den PC ein, oder starten Sie ihn neu.

2 Laufwerk auswählen: Erscheint das Startmenü der Notfall-DVD (1 siehe Randspalte links), wählen Sie **Notfall-DVD 17 starten**, drücken die Eingabetaste und machen direkt mit Schritt 3 weiter. Andernfalls haben Sie zwei Möglichkeiten:

■ **PC mit BIOS:** Um das Bootmenü des PCs zu öffnen, starten Sie ihn neu und drücken mehrmals die Bootmenü-Taste – meist ist es **F8**, **F10** oder **F12**, bei einigen PCs auch **F2**, **F9**, **F11**, **Alt**, **Esc** oder **↵**. Im Bootmenü wählen Sie das CD/DVD-Laufwerk und drücken **↵**.

■ **PC mit UEFI-BIOS:** Hier geht's genauso, es gibt aber einen zweiten Weg: Ist Windows schon gestartet, klicken Sie im Sperrbildschirm oder im Startmenü aufs Ausschalt-Symbol, bei gedrückter **↵**-Taste auf **Neu starten**, gegebenenfalls auf **Trotzdem neu starten, Ein Gerät verwenden** und wählen das DVD-Laufwerk per Klick.

3 Assistenten starten: Bestätigen Sie die Nutzungsbedingungen per Klick auf den Pfeil. Auf Geräten mit zu geringer Bildschirmauflösung ist er möglicherweise nicht zu sehen. Dann verschieben Sie das Fenster bei gedrückter **[Alt]**-Taste, bis der Pfeil erscheint. Ist die Auflösung dagegen zu hoch, öffnet sich das Fenster „Bildschirmeinstellungen“. Dort können Sie eine andere Auflösung wählen und mit **Anwenden** ausprobieren. Sind Sie zufrieden, wählen Sie **Ja** und **Schließen** oder drücken die **[Esc]**-Taste. Erscheint „Windows wurde nicht heruntergefahren“, folgen Sie den Hinweisen auf dem Bildschirm. Danach sehen Sie den Notfall-Assistenten wie im Bild unten. Anleitungen zu allen Funktionen der Notfall-DVD finden Sie auf den folgenden Seiten.

4 Notfall-DVD beenden: Nach einem Klick auf das Ausschalt-Symbol (2) können Sie den PC **Herunterfahren**, mit Windows **Neu starten** oder zu einem anderen Betriebssystem wechseln.



NOTFALL-STICK EINRICHTEN

Übertragen Sie die Notfall-DVD auf ein USB-Laufwerk (ab 4 Gigabyte), startet die Software auch ohne DVD-Laufwerk. Außerdem läuft sie damit schneller und braucht weniger Arbeitsspeicher. Ab 16 Gigabyte Kapazität steht auf dem Stick zudem das separate Laufwerk „Backup-Medium“ für Updates, Downloads und Sicherungen zur Verfügung – auch für Windows. Wich-

tig: Alle Daten auf dem Laufwerk gehen bei der Einrichtung verloren, andere USB-Laufwerke daher bitte vorher abstöpseln! So klappt's:

■ **Mit DVD-Laufwerk:** Öffnen Sie die DVD im Explorer. Klicken Sie doppelt auf den Ordner **Notfall-DVD**, auf **Notfall-DVD auf USB installieren** und **Ja**. Im Fenster „Win32 Disk Imager“ wählen Sie rechts oben den Stick, klicken auf **Schreiben, Yes, OK** und **Beenden**.

■ **Ohne DVD-Laufwerk:** Laden Sie die Software wie im Tipp „Starten ohne DVD“ (Seite 32) herunter. Nach Entpacken der Zip-Datei geht's weiter wie oben. Um den PC vom Stick zu starten, gehen Sie vor wie beim Start von DVD, wählen aber das USB-Laufwerk. Das erkennen Sie an der Modellbezeichnung oder am Namen „Linpus Lite“ auf Lenovo/Medion-Geräten.

Voraussetzungen

- USB-Laufwerk
- Installation nötig
- mindestens 2 Gigabyte Arbeitsspeicher (RAM)

Empfohlen für

- PC ohne DVD-Laufwerk
- mobilen Einsatz
- schnellen Start
- häufige Verwendung

NOTFALL-DVD AUF FESTPLATTE INSTALLIEREN

Möchten Sie die Software auch ohne DVD oder USB-Laufwerk starten, installieren Sie sie neben Windows auf der PC-Festplatte. Das geht so:

1 Programm installieren: Öffnen Sie die Heft-DVD oder die entpackte Zip-Datei im Windows-Explorer. Klicken Sie doppelt auf **Festplatten-Installation, Ja** und **Installieren**. Nach dem Kopiervorgang klicken Sie gegebenenfalls auf **OK** und **Beenden**.

2 Notfall-System starten: Wie Sie die Software starten, hängt davon ab, ob Sie einen Computer mit UEFI-BIOS oder herkömmlichem BIOS haben, siehe Tipp „Abgesicherter Start“ auf Seite 32.

■ **PC mit BIOS:** Entfernen Sie die Notfall-DVD oder den Notfall-Stick vom PC, und starten Sie ihn neu. Im erscheinenden Windows-Start-Manager wählen Sie **COMPUTER BILD Notfall-System** und bestätigen gegebenenfalls mit der **↵**-Taste.

■ **PC mit UEFI-BIOS:** War schon eine ältere Notfall-DVD auf der Festplatte installiert, wurde sie automatisch aktualisiert und lässt sich wie gewohnt starten. Andernfalls starten Sie den PC einmal von der Notfall-DVD oder vom Notfall-Stick, klicken aufs USB-

Symbol **3**, **Installation auf Festplatte**, den Pfeil und **OK**. Nun entfernen Sie die Notfall-DVD oder den Notfall-Stick vom PC und gehen vor wie beim Start von DVD (siehe Seite 32) – anstelle des DVD-Laufwerks wählen Sie aber **COMPUTER BILD Notfall-System**. Wichtig: Folgt eine „Secure Boot“-Fehlermeldung, müssen Sie Secure Boot im BIOS abschalten. Auf der Webseite cobi.de/go/sboot steht, wie das geht.

3 Software löschen: Falls Sie einen PC mit neuem UEFI-BIOS haben, starten Sie das Notfall-System noch mal, klicken auf das USB-Symbol **3**, **Installation auf Festplatte**, den Pfeil und **OK**. In jedem Fall deinstallieren Sie das Programm **COMPUTER BILD Notfall-System** in den Windows-Einstellungen.

Voraussetzungen

- Installation
- 6 Gigabyte Arbeitsspeicher
- 3 Gigabyte Festplattenspeicher

Empfohlen für

- sehr schnellen Start
- häufige Nutzung am selben PC
- Start ohne weiteres Laufwerk

ERSTE SCHRITTE

Bitte geben Sie die folgende PIN an Ihrer Bluetooth-Tastatur ein:

461441

Sobald die Tastatur verbunden ist, können Sie diese hier testen:

✓ OK

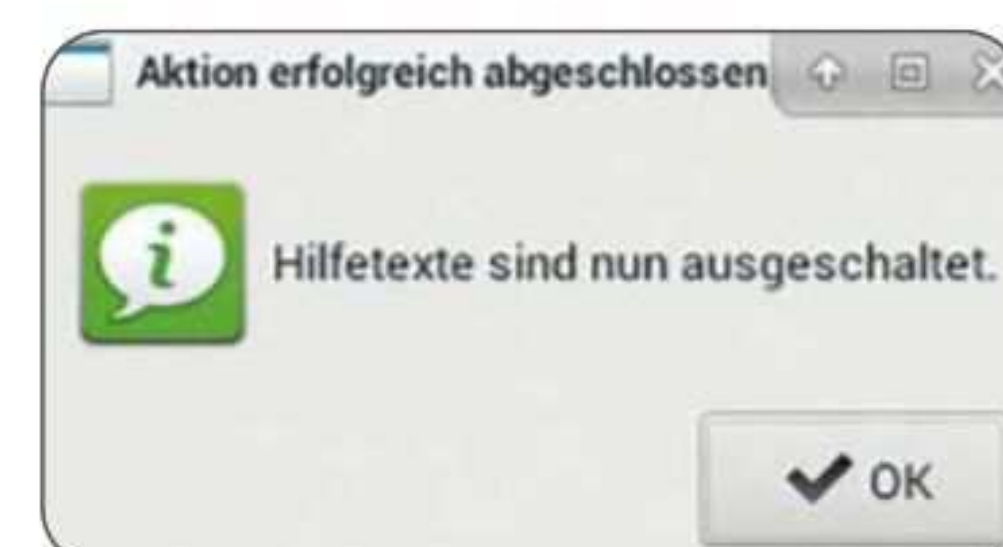
Bluetooth verbinden

Haben Sie eine Bluetooth-Maus/Tastatur, drücken Sie bei der Anzeige der Nutzungsbedingungen einige Sekunden die Kopplungstaste der Maus. Funktioniert sie, drücken Sie die Kopplungstaste der Tastatur, worauf das Fenster oben erscheint. Tippen Sie die angezeigte PIN ein. Drücken Sie **↵**.



WLAN verbinden

Für manche Funktionen braucht die Notfall-DVD eine Internetverbindung. Haben Sie kein Netzkabel, nutzen Sie WLAN. Dazu klicken Sie auf **4**, **Wireless**, in der Liste auf Ihr WLAN und **Connect**, tippen das Kennwort ein und wählen **OK**. Bleibt die Liste leer, klicken Sie auf **ON** und **OFF**, um den Adapter zu initialisieren.



Hilfetexte ausblenden

Zeigen Sie im Menü mit der Maus auf eine Funktion, erscheint daneben ein kurzer Hilfetext. Möchten Sie das nicht, klicken Sie mit der rechten Maustaste auf das Info-Symbol **5** und dann auf **OK**.

BEHEBEN SIE PROBLEME MIT WINDOWS

Spinnt der Computer, machen Sie ihm mit der Notfall-DVD wieder Beine. Wie Sie typische Windows-Probleme lösen, steht hier.

NOCH MEHR HILFE

Windows reparieren -> Wi

Reparaturdatenträger erzeugen

Installationsdatenträger erzeugen

Reparatur-CD brennen

Manche Windows-Probleme behebt nur der Systemreparatur-Datenträger von Microsoft. Haben Sie keinen, klicken Sie auf **Windows reparieren, Windows-DVD erzeugen** und **Reparaturdatenträger erzeugen**. Stellen Sie bei Bedarf eine Internetverbindung her, und folgen Sie den Anweisungen. Für Windows 11 gibt es keinen Reparaturdatenträger, nutzen Sie stattdessen die Setup-DVD.

Setup-DVD brennen

Ist die Reparatur-CD machtlos, hilft nur die Windows-Neuinstallation. Bei Bedarf erzeugt die Notfall-DVD auch den nötigen Setup-Datenträger für Windows 11, 10, 8.1 oder 7. Dazu klicken Sie abweichend auf **Installationsdatenträger erzeugen** und folgen den Anweisungen. Tipp: Der Installationsdatenträger enthält auch die Funktionen des Reparaturdatenträgers.

Anleitungen finden

Brauchen Sie weitere Hilfe? Im Hauptmenü unter **Tipps und Tricks** finden Sie Anleitungen für viele Hardware-, Software- und Netzwerk-Probleme. Soll ein Freund per Fernwartung helfen, nutzen Sie TeamViewer, siehe Seite 47.



WINDOWS REPARIEREN



Windows reparieren



Daten wiederherstellen



Dateien reparieren



Daten sichern

Last und Hitzetest wird durchgeführt

Der Last- und Hitzetest für Arbeitsspeicher, Prozessor und Festplatte wird nun durchgeführt. Er kann auf älterer Hardware mehrere Stunden dauern. Sie können den Test jederzeit abbrechen, allerdings bleiben dann möglicherweise Defekte unbemerkt.

ca. 109 Minuten verbleibend

Test abbrechen

Die Funktionsprüfung findet heraus, ob Hardware-Probleme hinter Abstürzen Ihres Computers stecken.

Die Notfall-DVD behebt Windows-Probleme im Nu. Um die passende Reparaturfunktion zu finden, klicken Sie im Hauptmenü auf **Windows reparieren** und wählen die passende Beschreibung:

Computer stürzt ab

Stürzt Windows nach erfolgreichem Start ab, stecken oft Hardware-Probleme wie ein überhitzter Prozessor oder Festplatten-Defekte dahinter. Um die Ursache zu ermitteln, prüft die Notfall-DVD die Bauteile Ihres PCs (siehe Bild oben). Wird dabei etwa der Prozessor zu heiß, gibt sie Tipps zum weiteren Vorgehen. Im Falle eines Festplatten-Defekts leitet der PC-Retter zur Datensicherungs-Funktion weiter, mit der Sie Ihre Dateien in Sicherheit bringen. Wie Sie dazu vorgehen, steht auf Seite 38.

Systemdateien beschädigt

Erscheint beim Windows-Start eine der im Hilfetext genannten Fehlermeldungen? In diesem Fall kann sich Windows nur selbst reparieren. Klicken Sie auf den angezeigten QR-Code, oder scannen Sie ihn mit Ihrem Smartphone, um die passende Anleitung anzuzeigen. Falls Sie gerade kein Internet haben, finden Sie entsprechende PDF-Anleitungen unter **Tipps und Tricks**, siehe Kasten links.

Startbereich der Festplatte beschädigt

Erscheint eine der im Hilfetext genannten Fehlermeldungen, öffnen Sie diese Funktion. Sie haben dann zwei Möglichkeiten:

■ **Fehlender Bootsektor:** Wahrscheinlich ist nur der Startbereich von Windows auf der Festplatte defekt. Klicken Sie hier zunächst auf den Pfeil, behebt die Notfall-DVD das automatisch.

■ **Partition beschädigt:** Hilft das nicht, ist womöglich die Start- oder Systempartition von Windows beschädigt. Mit dieser Funktion bringen Sie das wieder in Ordnung. Folgen Sie den Anweisungen.

Registrierungsdatenbank beschädigt

Wenn Windows startet, statt der Arbeitsoberfläche jedoch ein unbekanntes Programm oder nur eine Farbfläche erscheint, hat wahrscheinlich ein Schädling wie der sogenannte BKA-Trojaner zugeschlagen. Keine Sorge: Mit dieser Funktion stellen Sie den Desktop wieder her. Im Anschluss sollten Sie Ihre Festplatte auf Viren prüfen, siehe Seite 40.

Windows-DVD erzeugen

Lässt sich Windows mit den vorangegangenen Werkzeugen nicht reparieren, versuchen Sie es mit einer Reparatur-CD von Microsoft, oder installieren Sie Windows per Setup-DVD neu. Wie Sie an die Datenträger kommen, steht im Kasten links.

Fehlender Bootsektor

Windows startet nicht, es erscheinen Fehlermeldungen wie "No operating system found", "Kein System gefunden" oder "Please insert a bootable media". Fehlermeldungen wie diese erscheinen, wenn der Startbereich der Festplatte beschädigt ist. Dies kann die Notfall-DVD beheben.

Klicken Sie hier, um den Startbereich der Festplatte zu reparieren.



Typische Windows-Startfehler wie den fehlenden Bootsektor behebt die Notfall-DVD mit nur einem Klick.

Die **COMPUTER BILD SELECTION** von Hama

Perfekte Verbindung

Erleben Sie höchste Flexibilität im Homeoffice!

COMPUTER BILD und **Hama** haben für Sie das beste Zubehör ausgewählt.



USB-C-Docking-Station „Connect2OfficePro“

- ✓ professionelles Arbeiten im Homeoffice
- ✓ USB-C, HDMI (4K), DisplayPort, LAN/Ethernet
- ✓ Multi-Stream-Transport für zwei Monitore

Jetzt bestellen unter
cobi.de/go/docking



in Kooperation mit

hama

Computer
Bild selection

Erhältlich bei vielen Händlern:



SO LÄUFT DIE DATEN-RETTUNG

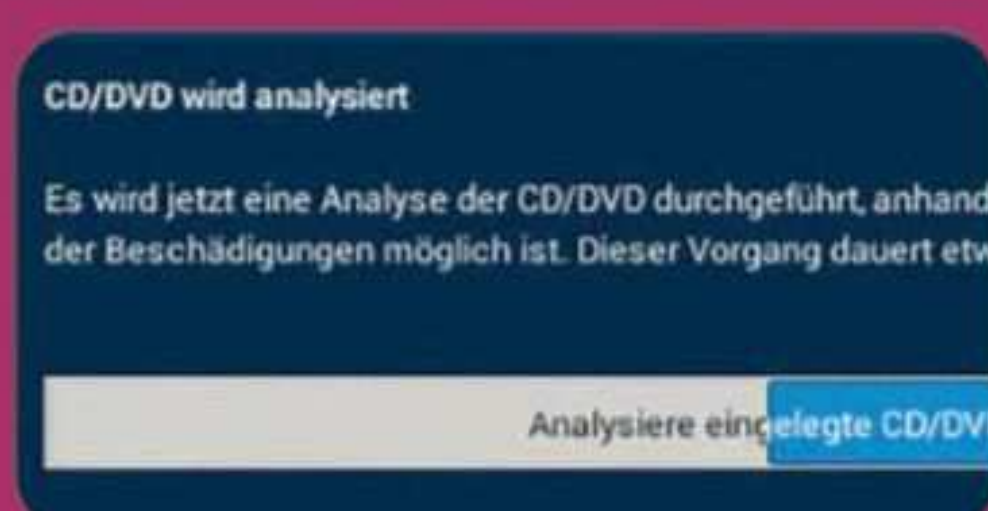
Die Notfall-DVD kann *verlorene und beschädigte Dateien wiederherstellen*. Wie das geht, lesen Sie hier.

KURZ- TIPPS



Datensafe einrichten

Der Notfall-Stick (Seite 33) bietet mit dem Datensafe eine exklusive Schutzfunktion zur Rettung vertraulicher Daten. Nach einem Klick aufs Vorhängeschloss im Hauptmenü legen Sie das Passwort fest (siehe Bild) und wählen **OK**. Nun wird das Laufwerk „Tresor“ auf dem Backup-Medium des Sticks erstellt und geöffnet – das dauert. Ziehen Sie Ihre Dateien von anderen Laufwerken hinein, um sie zu sichern. Um den Safe zu schließen, klicken Sie aufs „offene“ Schloss und **Abbrechen**.



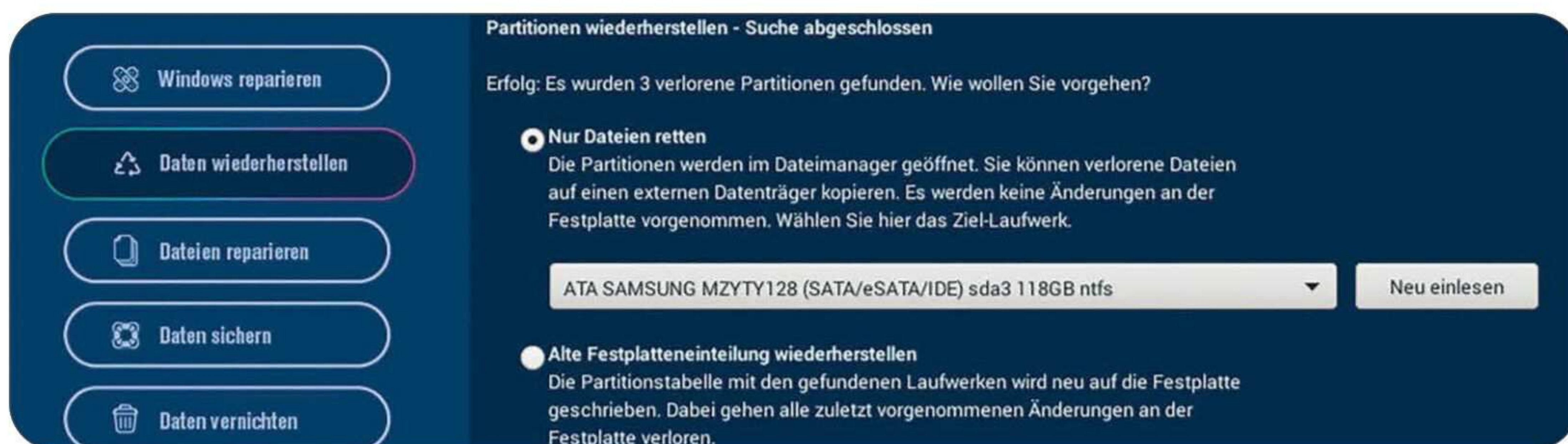
CD/DVD retten

Ist eine CD, DVD oder Blu-ray unter Windows nicht mehr lesbar, klicken Sie auf **CD/DVD retten**. Dann legen Sie die Scheibe ins Laufwerk und folgen den Anweisungen zum Klonen oder Sichern. Blockiert die Notfall-DVD das einzige Laufwerk, starten Sie sie vom Notfall-Stick oder von der Festplatte, siehe Seite 33.

Fotos: iStock; Montage: COMPUTER BILD



DATEIEN WIEDERHERSTELLEN



Im Beispiel hat die Notfall-DVD drei verlorene Laufwerke (Partitionen) auf einer Festplatte entdeckt. Die lassen sich entweder komplett wiederherstellen oder öffnen, um darin enthaltene Daten zu retten.

Haben Sie versehentlich eine wichtige Datei oder sogar ein ganzes Laufwerk gelöscht? Hilfe finden Sie im Hauptmenü unter **Daten wiederherstellen**:

Gelöschte Dateien wiederherstellen

Eine Datei wurde gelöscht und der Windows-Papierkorb geleert? Ist der Speicherort der Datei noch nicht überschrieben, lässt sie sich meist noch retten. Dazu wählen Sie nach einem Klick auf **Gelöschte Dateien wiederherstellen** den betroffenen Datenträger und klicken auf den Pfeil. Im Fenster „Nach welchen Datentypen soll gesucht werden?“ markieren Sie den Dateityp mit Häkchen, etwa „Office-Dokumente“. Danach wählen Sie ein Ziellaufwerk, etwa das **Backup-Medium** auf dem Notfall-Stick, und markieren das Kästchen „Gefundene Dateien anschließend sortieren“. Nach dem Start landen alle wiederherstellbaren Dateien in den angezeigten Rettungsordnern auf dem Ziellaufwerk. Da sich Dateinamen leider nicht wiederherstellen lassen, haben die Dateien zunächst noch merkwürdige Bezeichnungen. Um den Inhalt zu sehen, öffnen Sie die Dateien in Windows per Doppelklick. Zum Umbenennen klicken Sie darauf, drücken **F2**, tippen den Namen ein und drücken **↵**.

Kamerabilder wiederherstellen

Haben Sie Fotos direkt in der Kamera gelöscht? Falls sich das Gerät in den Massenspeichermodus („USB-Verbindung“) versetzen lässt, stöpseln Sie es per USB-Kabel am PC an. Andernfalls stecken

Sie die Speicherkarte in den Kartenleser des Computers. Retten Sie die Bilder dann wie im vorigen Abschnitt mit der Suchauswahl „Fotos und Bilder“.

Laufwerke wiederherstellen

Unter **Gelöschte Partitionen wiederherstellen** zeigt die Notfall-DVD angeschlossene Festplatten mit beschädigten Laufwerken („Partitionen“). Nach Auswahl des betroffenen Datenträgers wird er nach alten Partitionen durchforstet – das dauert. Danach können Sie Partitionen wiederherstellen oder öffnen, siehe Bild oben.

Datensicherung verwenden

Eventuell lassen sich verlorene Daten aus einer Sicherung („Backup“) wiederherstellen:

■ **Windows-Sicherung:** Wussten Sie, dass Windows im Hintergrund automatisch Backups erstellt? Um diese sogenannten „Volumenschattenkopien“ mit der Notfall-DVD zu öffnen, klicken Sie auf **Backup zurückspielen** und **Windows-Sicherungen durchsuchen**. Nach Auswahl des Ziellaufwerks durchforsten Sie den Ordner „VSS“ und ziehen die benötigten Dateien ins Fenster „Sicherung“ – fertig.

■ **Image-Datei:** Haben Sie selbst mit einer Backup-Software ein Datenträger-Abbild („Image“) Ihrer Festplatte erstellt, nutzen Sie alternativ die Funktion **Image-Datei durchsuchen**. Die öffnet unter anderem Sicherungen mit den Dateiendungen .iso, .vhd, .vhdx, .vmdk und .dmg. Gehen Sie vor wie im vorigen Punkt, um darin enthaltene Dateien zu retten.



DATEIEN REPARIEREN

Bei beschädigten Dateien helfen die Werkzeuge im Menü **Dateien reparieren**:

Outlook-Dateien retten

Startet Outlook mit einer Fehlermeldung, ist meist die „PST“-Datendatei beschädigt. Nach Klick auf **Beschädigte Outlook-Postfächer retten** öffnen Sie diese mit der Notfall-DVD. Sie können Ihre Nachrichten dann lesen, beantworten und weiterleiten. Nutzen Sie den Notfall-Stick (Seite 33), lassen sich Outlook-Mails auch zurückspielen. Folgen Sie dazu den Hinweisen des Assistenten.

JETZT NEU

Firefox-Kennwörter retten

Meldet Firefox „Ihr Profil kann nicht geladen werden“, sind neben Lesezeichen auch alle Online-Kennwörter futsch. Die erweiterte Funktion **Firefox-Profil reparieren** listet alle Zugangsdaten des Browsers wie im Bild oben rechts als csv-Datei auf. Falls Sie einen Notfall-Stick (Seite 33) nutzen, bietet dieser an, die Firefox-Datenbanken automatisch im Ordner „Firefox-Retter“ zu sichern. Nach einem Klick auf den Pfeil startet der Notfall-

Browser, mit dem Sie Ihre Profildaten wie gewohnt nutzen. Zudem erscheint dort eine Anleitung, mit der Sie die gesicherten Datenbanken nach erfolgter Firefox-Neuinstallation unter Windows zurückspielen.

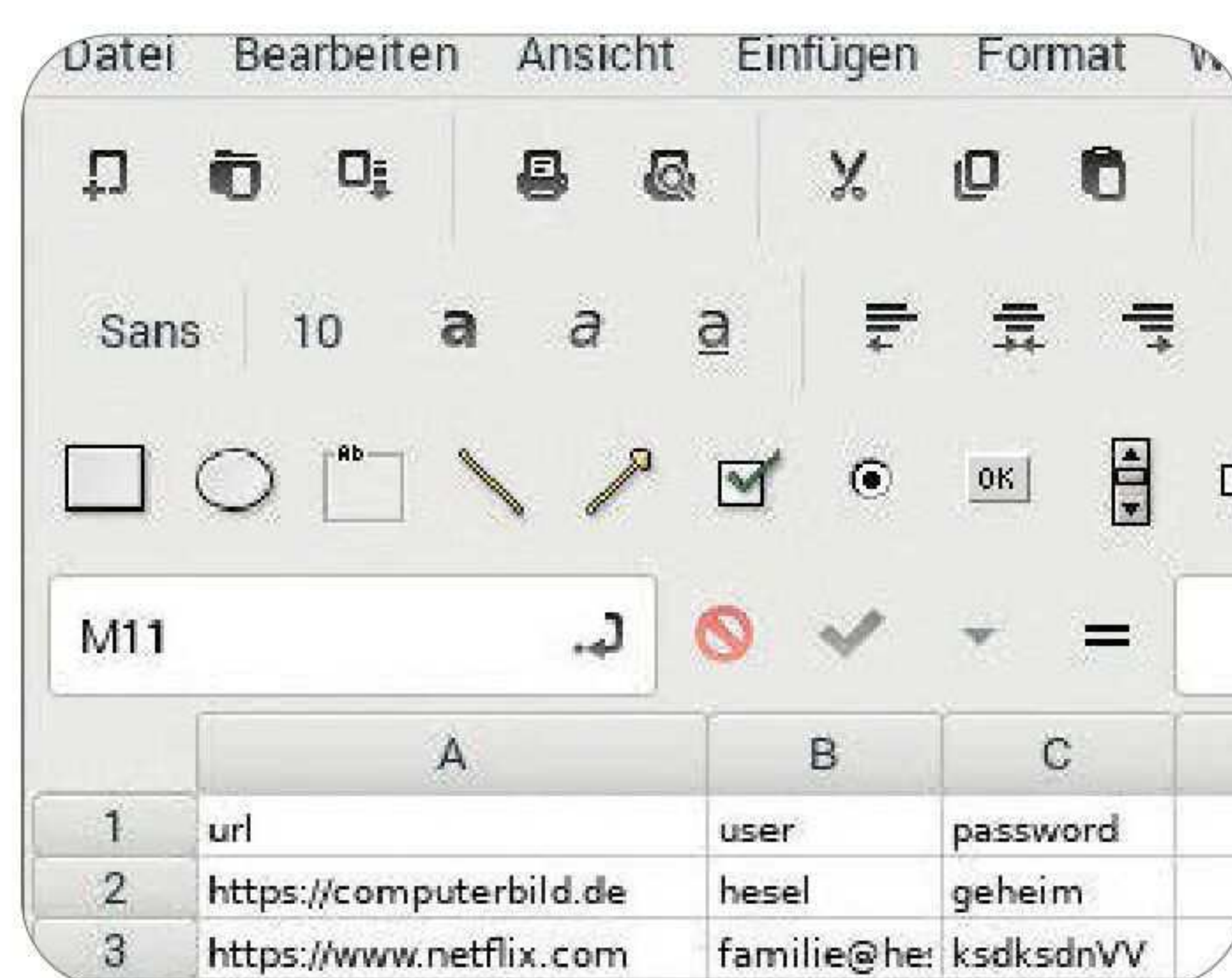
JETZT NEU

Thunderbird-Profil reparieren

Wie bei Firefox zeigt der neue „Thunderbird-Retter“ die Zugangsdaten Ihrer Thunderbird-Postfächer als csv-Datei und sichert die Datenbanken im Ordner „Thunderbird-Retter“ des Notfall-Sticks. Um die nach erfolgter Neuinstallation von Thunderbird unter Windows wiederherzustellen, kopieren Sie die drei Dateien „cert9.db“, „key4.db“ und „logins.json“ in den neuesten Thunderbird-Profilordner. Den finden Sie, wenn Sie im Adressfeld des Windows-Explorers die Adresse **%appdata%/Thunderbird/Profiles** eintippen und die Taste **↵** drücken.

Word-Dateien retten

Lässt sich ein Dokument mit der Endung .doc, .docx, .rtf oder .odt nicht mehr in Word öffnen, ist es nicht zwangsläufig verloren. Mit



der Funktion **Word-Dateien reparieren** sichern Sie die Inhalte als neue Datei mit der Endung .txt oder auch .htm auf dem gewünschten Ziellaufwerk. Die können Sie in Word öffnen, bearbeiten und neu speichern.

Unlesbare Dateien reparieren

Ist eine Datei unter Windows nicht lesbar, sind meist Dateisystemfehler die Ursache. Mit der Funktion **Unlesbare Datei retten** erstellt die Notfall-DVD ein Datenträger-Abbild des betroffenen Laufwerks und versucht, die unlesbare Datei daraus wiederherzustellen.



MICROSOFT-LIZENZSCHLÜSSEL AUSLESEN

Müssen Sie Windows oder Microsoft Office neu installieren, brauchen Sie unter Umständen den dazugehörigen Lizenzschlüssel („Key“). Doch was tun, wenn das Windows-Echtheitszertifikat auf dem Computer längst verblichen oder die Packung mit dem wichtigen Freischaltcode schon vor Jahren ins Altpapier gewandert ist? Kein Problem: Mit der Notfall-DVD lesen Sie Ihre Lizenzschlüssel direkt aus der Festplatte aus. Das geht so:

1 Klicken Sie auf **Office- und Windows-Keys auslesen** und anschließend auf den Pfeil. Daraufhin durchstöbert die Notfall-DVD die Registrierungsdatenbank von Windows und zeigt die gefundenen Freischaltcodes wie im Bild rechts an.

2 Sie können die Schlüssel einfach abtippen oder mit dem Smartphone knipsen und dann auf **X** klicken. Um sie als Textdatei zu speichern, binden Sie wie auf dem Bildschirm beschrieben das gewünschte Ziellaufwerk ein. Danach klicken Sie auf den Pfeil und im erscheinenden Texteditor auf **File**. Nach Mausklicks auf **Save as**, das Ziellaufwerk und **Save** sind die Schlüssel in der Datei „winkeys.txt“ gesichert.

Lizenzschlüssel sichern

Nachfolgend sehen Sie die gefundenen Lizenzschlüssel für Windows und Office. Sie können die Codes abtippen, abfotografieren oder als Textdatei auf einem angeschlossenen USB-Laufwerk sichern. Ist kein Laufwerk angeschlossen, holen Sie jetzt nach. Danach klicken Sie im Dock auf „Laufwerke“ und binden das gewünschte Laufwerk schreibbar ein. Anschließend klicken Sie auf „Weiter“, „File“, „Save as“, das Laufwerk und „Save“

Windows-Schlüssel: VK7JG-NPHTM-C97JM-9MPGT-3V66T
Office-Schlüssel (2016): JNRGM-WHDWX-FJJG3-K47QV-DRTFM

Klicken Sie hier, die gefundenen Schlüssel im Texteditor zu öffnen und zu speichern.

Klicken Sie hier, um abzubrechen und zum Startbildschirm zurückzukehren.

Die Notfall-DVD zeigt nur bei der Installation eingetippte Schlüssel. Bei Microsoft 365 und elektronisch aktivierten Windows-Versionen klappt das nicht – ist dort aber auch nicht nötig.



„Mit nur zwei Klicks machen Sie die Lizenzschlüssel von Microsoft sichtbar.“

André Hesel
Stellv. Ressortleiter Software

WIRKSAM IHRE DATEN SCHÜTZEN

Mit diesen Werkzeugen bringen Sie Ihre Daten in Sicherheit und sorgen mit einer Datensicherung schlimmen PC-Notfällen vor.

DATEN VERNICHTEN

Daten vernichten

 Schnellreinigung

 Tiefenreinigung

 Freien Speicherplatz bereinigen

 Datenmüll löschen

Laufwerk löschen

Wer den PC oder eine Festplatte entsorgen will, sollte die Daten zuvor unwiederbringlich löschen. Dazu klicken Sie unter **Daten vernichten** auf **Tiefenreinigung** und folgen den Anweisungen. Mit der **Schnellreinigung** löschen Sie einzelne Festplatten-Partitionen. Es ist beispielsweise sinnvoll, die Windows-Partition vor Installation des Betriebssystems zu löschen.

Freien Speicher bereinigen

In Windows gelöschte Dateien lassen sich mit Datenrettungsprogrammen leicht wiederherstellen. Möchten Sie das verhindern, klicken Sie auf **Freien Speicherplatz bereinigen**, wählen das Windows-Laufwerk, klicken auf den Pfeil und **OK**.

Datenmüll löschen

Mit dieser Funktion werfen Sie Datenmüll über Bord oder leeren den Windows-Papierkorb für alle Benutzer. Zudem können Sie hier „hängende Druckaufträge“ beseitigen. Mehr dazu auf Seite 44.

DATEN SICHERN ODER UMZIEHEN

Benutzerkonto auswählen

Die Notfall-DVD hat auf diesem Computer eines oder mehrere Windows-Benutzerkonten gefunden zu sichernden Konten. Die dazugehörigen Benutzer-Ordner mit Bildern, Dokumenten, Musik und V Kontakten, Internet-Favoriten, Downloads und dem Desktop-Ordner werden dann komplett gesichert.

☐ sda3 /Users/Administrator (206MB)

☐ sda3 /Users/defaultuser0 (261MB)

☒ sda3 /Users/hesi (16652MB)

☐ sda3 /Users/jette (222MB)

 Windows reparieren

 Daten wiederherstellen

 Dateien reparieren

 Daten sichern

Die Schnellsicherung der Notfall-DVD ermittelt alle verfügbaren Windows-Benutzerkonten. Nach Auswahl der Profile und des Ziel-Laufwerks werden alle darin gespeicherten Dateien in einem Rutsch gesichert.

Hat die PC-Prüfung auf Seite 34 Festplatten-Probleme gemeldet, bringen Sie Ihre Daten unverzüglich in Sicherheit. Im Hauptmenü unter dem Punkt **Daten sichern** gibt es diese Möglichkeiten:

Eigene Dateien schnell sichern

Mit dieser Funktion sichern Sie auf schnellstem Weg Ihr komplettes Windows-Benutzerkonto samt aller darin gespeicherten Dateien, siehe Bild oben.

Daten manuell sichern

Hier können Sie die zu sichernden Daten selbst wählen. Es gibt drei Optionen:

■ **Daten auf lokalem Laufwerk sichern:** Wählen Sie das Sicherungslaufwerk, und klicken Sie auf den Pfeil. Dann erscheinen zwei Fenster: In „Disk“ sehen Sie alle PC-Laufwerke – die haben keine Buchstaben wie bei Windows, sondern fortlaufende Bezeichnungen wie „sda1“, „sda2“ und so weiter. Das Fenster „Sicherung“ ist Ihr Ziel-Laufwerk. Ziehen Sie die gewünschten Daten dort hinein – fertig! Übrigens: Die Notfall-DVD kann auch auf Laufwerke zugreifen, die mit der BitLocker-Funktion von Windows 10/11 Pro verschlüsselt wurden. Dazu geben Sie Laufwerkspasswort oder Wiederherstellungsschlüssel ein. Haben Sie den verlegt, hilft die Funktion „Windows entsperren“ (Seite 40).

■ **Daten auf anderem PC sichern:** Haben Sie einen weiteren Windows-PC, können Sie die manuelle Datensicherung auch dort vornehmen. Dazu starten Sie diese Funktion am angeschlagenen PC, um

dessen Laufwerke im Heimnetzwerk freizugeben. Greifen Sie dann gemäß Anweisung vom Zweit-PC auf Ihre Daten zu, und kopieren Sie die Dateien.

■ **Daten in der Cloud sichern:** Wählen Sie diese Option, und folgen Sie den Anweisungen, um einzelne Dateien vom PC auf eine Online-Festplatte wie Dropbox oder OneDrive zu retten.

Komplette Festplatte sichern und wiederherstellen

Die Notfall-DVD kann auch ganze Laufwerke sichern: Folgen Sie den Anweisungen unter **Neue Sicherung erstellen**, um ein komplettes Festplatten-Abbild („Image“) Ihrer PC-Festplatte zu erstellen. Im Notfall stellen Sie es mit der Option **Laufwerks-Abbild zurückspielen** wieder her.

Festplatte klonen

Hier kopieren Sie Ihre Festplatte eins zu eins auf ein neues Laufwerk. Sie haben zwei Möglichkeiten:

■ **Festplatte auf ein lokales Laufwerk klonen:** Wählen Sie diese Option, wenn Quell- und Ziel-Laufwerk direkt am PC angeschlossen sind. Geht das nicht, nutzen Sie ein USB-Laufwerk als Zwischenspeicher oder die nächste Option.

■ **Festplatte auf einen anderen PC klonen:** Ersetzen Sie den PC durch einen neuen, können Sie sich den Aus- und Einbau der Laufwerke sparen. Dazu starten Sie beide PCs von der Notfall-DVD und verbinden sie mit demselben Netzwerk direkt per LAN-Kabel. Starten Sie dann am alten PC diese Funktion, und folgen Sie den Anweisungen.

WINDOWS 7, 8 ODER 10 RETTEN ...

Obwohl Windows 11 seit einem halben Jahr verfügbar ist, laufen die meisten PCs noch mit Windows 10, viele sogar mit dem veralteten Windows 7. Wer mit dem Upgrade zögert, zum Beispiel wegen in Windows 11 entfernter Windows-Funktionen und inkompatibler Programme, kann mit der Notfall-DVD die komplette Windows-Festplatte als virtuellen PC sichern. Der lässt sich unter Windows 11 beziehungsweise 10 in einem Fenster starten und so weiternutzen.

1 Quelle wählen: Löschen Sie zuerst überflüssige Programme und Daten im alten Windows. Nach dem Start der Notfall-DVD wählen Sie **Daten sichern**, **Windows-Retter** und die PC-Festplatte. Wichtig: Lassen Sie den Haken **1** stehen, wird das Abbild weiter verkleinert. Das kann Windows bei Laufwerksfehlern jedoch be-

schädigen. Prüfen Sie daher zuerst die Festplatte (Seite 34). Im Zweifel entfernen Sie den Haken.

2 Ziel wählen: Nach einem Klick auf den Pfeil schließen Sie eine freie USB-Festplatte an. Damit die angezeigt wird, muss sie mindestens so groß wie die Quelle und mit dem Dateisystem NTFS formatiert sein. Dies holen Sie gegebenenfalls im Expertenmodus nach, siehe Seite 47.

3 Sicherung starten: Nach Klick auf den Pfeil wird die Festplatte aus technischen Gründen im Ordner „**Windows-7-Retter**“ gesichert, es klappt aber auch mit Windows 10 oder 8. Der Vorgang dauert eine Weile. Sobald der Hinweis **2** erscheint, klicken Sie auf **OK**.

Windows auswählen

Wählen Sie die Windows-Installation, die als virtueller PC gesichert werden soll. Achtung: Um das erstellte Laufwerksabbild möglichst klein zu halten, kann die Notfall-DVD freie Speicherbereiche der Quell-Festplatte vorher überschreiben. Ist die Festplatte oder das Dateisystem vorgeschädigt, sollten Sie diese Option deaktivieren, um Schäden an Windows zu vermeiden. Dadurch wird das Abbild jedoch deutlich größer.

ATA SAMSUNG MZYT128 - 119GB - sda (SATA/eSATA/IDE/N

Neu einlesen

☒ Freie Speicherbereiche überschreiben

1

Mit wenigen Klicks sichern Sie Windows 7 als virtuellen Computer.

Sicherung läuft

Das gewählte Windows wird jetzt als virtueller PC gesichert. Dieser Fortschrittsbalken

Auskunft

2

Aktion erfolgreich abgeschlossen

Windows wurde als virtueller PC auf dem gewünschten Laufwerk gesichert. Um es zum Beispiel unter Windows 11 zu starten, installieren Sie dort das Gratis-Programm VirtualBox von der Webseite cobi.de/12062 und starten es. Klicken Sie dann nacheinander auf „Datei“ und „Appliance importieren“. Danach wählen Sie den Ordner „Windows-Retter“, die Konfigurationsdatei „win7.vbox“ und klicken auf „Öffnen“. Das kopierte Windows startet dann mit Internetzugriff in einem geschützten Fenster und lässt sich wie gewohnt weiternutzen. Verlagern Sie den Ordner „Windows-Retter“ zuvor auf die PC-Festplatte, arbeitet es flotter.

OK

... UND ALS VIRTUELLEN PC STARTEN

Wie Sie das gerade gesicherte Windows als virtuellen PC zum Beispiel unter Windows 11 starten, lesen Sie hier:

1 Virtuellen PC vorbereiten: Installieren Sie das Gratis-Programm VirtualBox von der Webseite cobi.de/12062. Danach schließen Sie das USB-Laufwerk mit dem virtuellen PC an. Ist auf der PC-Festplatte genug Platz, verschieben Sie den Ordner „Windows-7-Retter“ am besten dorthin – der virtuelle PC läuft dann in der Regel wesentlich schneller. Klicken Sie danach im Ordner „Windows-7-Retter“ auf die blaue **win7**-Datei.

2 Virtuellen PC einrichten: Klicken Sie auf **Ändern**, und passen Sie die folgenden Einstellungen an:

■ **Name:** Ändern Sie **Win7** gegebenenfalls in **Win10** oder **Win8**.

■ **Netzwerk:** Ist der Haken „Netzwerkadapter aktivieren“ gesetzt, kommt der PC ins Internet. Falls Sie Windows 7 kopiert haben, ist das aus Sicherheitsgründen nicht mehr ratsam.

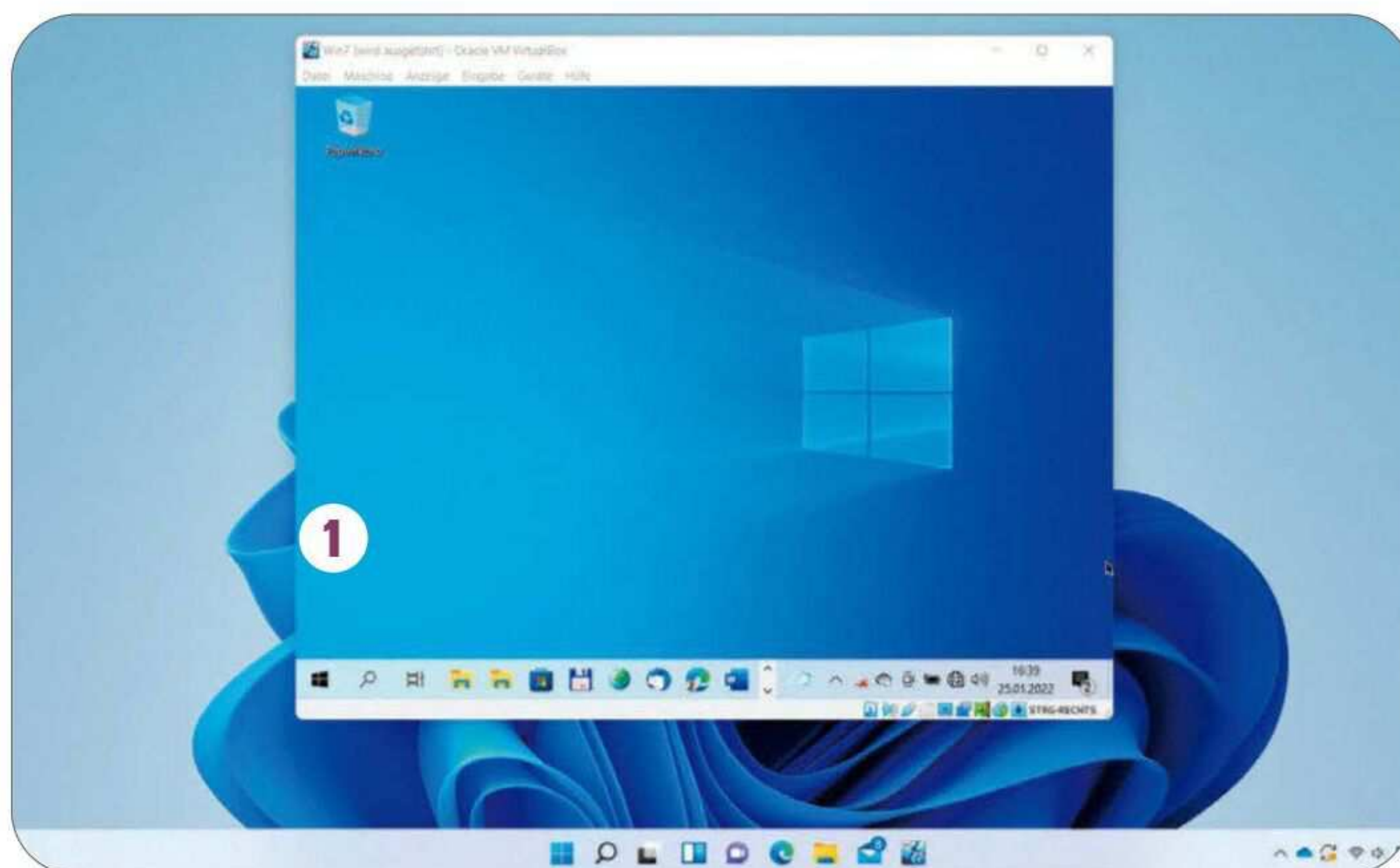
■ **CD/DVD:** Damit der virtuelle PC auf das Laufwerk zugreifen kann, klicken Sie unter **Massenspeicher** auf die Scheibe mit dem Pluszeichen, den dazugehörigen Laufwerksbuchstaben und **Auswählen**.

■ **Drag 'n' Drop:** Um Dateien per Maus zwischen dem virtuellen und dem „echten“ PC kopieren zu können, wählen Sie unter **Allgemein**, **Erweitert** und „Drag 'n' Drop“ die Option **bidirektional**.

■ **System:** Hat der Original-PC ein UEFI-BIOS, muss hier der Haken **Efi aktivieren** gesetzt sein, damit der virtuelle PC startet. Das ist

meist der Fall, wenn der PC mit Windows 8/10 ausgeliefert wurde.

3 Virtuellen PC starten: Nach Klicks auf **OK** und **Starten** erscheint das alte Windows im Fenster **1**. Lassen Sie ihm Zeit, und folgen Sie den Hinweisen von VirtualBox und Windows, etwa zur Konfiguration des (virtuellen) Netzwerks und zur Windows-Aktivierung. Danach lässt sich das alte Windows wie gewohnt nutzen. Scheitert der Start mit einer Fehlermeldung, müssen Sie im PC-BIOS die Virtualisierungsfunktion des Prozessors einschalten. Auf der Seite cobi.de/go/vtx gibt's eine Anleitung.



ALLES FÜR DIE PC-SICHERHEIT

Hier prüfen Sie den Computer auf Viren und Schwachstellen, hebeln Laufwerkssperren aus und finden Sicherheitslücken in Ihrer Technik.



VIREN AUFSPÜREN UND LÖSCHEN

Veraltete Programme und ignorierte Sicherheitsempfehlungen führen trotz Virenschutz immer wieder zu Infektionen. Ist Ihr PC merkwürdig langsam oder fehleranfällig, prüfen Sie ihn mit der Notfall-DVD auf Viren. Da PC-Schädlinge meist sehr klein sind, ist der neue Viren-scanner ClamAV so eingestellt, dass er Dateien nur bis zu einer Größe von 50 Megabyte scannt. Für eine Intensiv-Prüfung nutzen Sie den „Tiefenscan“ im Expertenmodus, siehe Seite 47.

1 Internetverbindung herstellen: Klicken Sie auf **PC-Sicherheit** und **Computer auf Viren prüfen**. Ist Ihr PC bereits mit dem Internet verbunden, geht's gleich mit Schritt 2 weiter. Andernfalls wählen Sie im Fenster „Netzwerkeinrichtung“ Ihr WLAN, damit ClamAV seine Virendefinitionen aktualisieren kann. Ist kein Internet verfügbar, wählen Sie **Ohne Netzwerkverbindung fortfahren**.

2 Virensuche: Nun legen Sie die Einstellungen wie im Bild oben rechts fest, klicken auf den Pfeil und markieren die zu prüfenden Laufwerke mit Häkchen. Nach dem Start aktualisiert sich ClamAV und prüft den PC. Ergebnisse sehen Sie nach einem Klick auf **Protokoll anzeigen**. Möchten Sie das Protokoll sichern, binden Sie das Ziellauf-

Einstellungen für die Virensuche

Sollen Archive nach Schadsoftware durchsucht werden? Dies verlangsamt die Suche, birgt das Risiko von Suchabbrüchen, steigert jedoch die Erkennungsrate.

- ☐ Ja, Archive durchsuchen
- ☒ Nein, Archive ignorieren

Wie soll nach einem Fund von Schadsoftware weiter vorgegangen werden?

- ☐ Reparieren (löschen wenn nicht möglich)
- ☒ Reparieren (unschädlich machen)
- ☐ Funde nur anzeigen

JETZT
NEU

werk schreibbar ein (Seite 46), klicken auf **File, Save as**, das Laufwerk und **Save**. Sie erhalten dann die Datei „virusscan.log“, und können sie später etwa unter Windows anschauen.

3 Windows laden: Starten Sie den PC neu (siehe Seite 32). Waren Systemdateien infiziert, könnte es sein, dass Windows nicht mehr startet. In diesem Fall sichern Sie Ihre Daten (siehe Seite 38) und installieren es mit der Setup-DVD (siehe Seite 34) neu.



WINDOWS ENTSPPERREN

Haben Sie das Windows-Kennwort vergessen? Ist ein Laufwerk verschlüsselt? Keine Sorge: Unter PC-Sicherheit finden Sie einen Schlüsseldienst für Ihren PC:

Windows-Kennwort zurücksetzen

Um Windows zu entsperren, wählen Sie diese Funktion, bestätigen das Laufwerk und Ihr Benutzerkonto. Nach Klicks auf den Pfeil und **OK** starten Sie Windows neu und kommen nun ohne Passwort rein. Legen Sie am besten gleich ein

neues Passwort fest. Dazu klicken Sie in den Windows-Einstellungen auf **Konten, Anmeldeoptionen, Kennwort** und folgen den Anweisungen. Falls Sie sich per Microsoft-Konto bei Windows anmelden, ändern Sie das Kennwort direkt bei Microsoft. Dazu klicken Sie in dieser Notfall-DVD-Funktion auf **Passwort-Rücksetzfunktion online öffnen**.

BitLocker-Schlüssel anzeigen

Ist Ihre Festplatte mit der BitLocker-Funktion von Windows 10/11 Pro verschlüsselt, brauchen Sie Ihr Laufwerkskennwort, um mit der Notfall-DVD an die Daten zu kommen. Haben Sie es vergessen, tut es auch der 48-stellige „Wiederherstellungsschlüssel“ (Recovery Key), der im Microsoft-Konto versteckt ist. Mit dieser Option zeigt die Notfall-DVD ihn im Browser an – dazu einfach ins Microsoft-Konto einloggen.



„Die Notfall-DVD erkennt auch Viren, die sich unter Windows tarnen können.“

Andy Voss
Redakteur Software





SCHWACHSTELLEN FINDEN

Schwachstellen gefunden

Offene Ports: Bei Geräten mit offenen Ports sollten Sie den jeweiligen Netzwerk-Webserver: Checken Sie auch Geräte, auf denen ein Webserver (HTTP- oder

Nmap scan report for fritz.box (192.168.178.1)

```
Nmap scan report for fritz.box (192.168.178.1)
Host is up (0.0031s latency).
Not shown: 8283 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
5060/tcp  open  sip
8089/tcp  open  unknown
8181/tcp  open  intermapper
8182/tcp  open  vmware-fdm
8183/tcp  open  proramote
8184/tcp  open  itach
49000/tcp open  matahari
MAC Address: 24:65:11:59:21:68 (AVM GmbH)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.20
Network Distance: 1 hop
```

Bitte prüfen Sie die folgenden Dienste:

Windows-Datei- oder Druckdienste, Internet-Telefonie

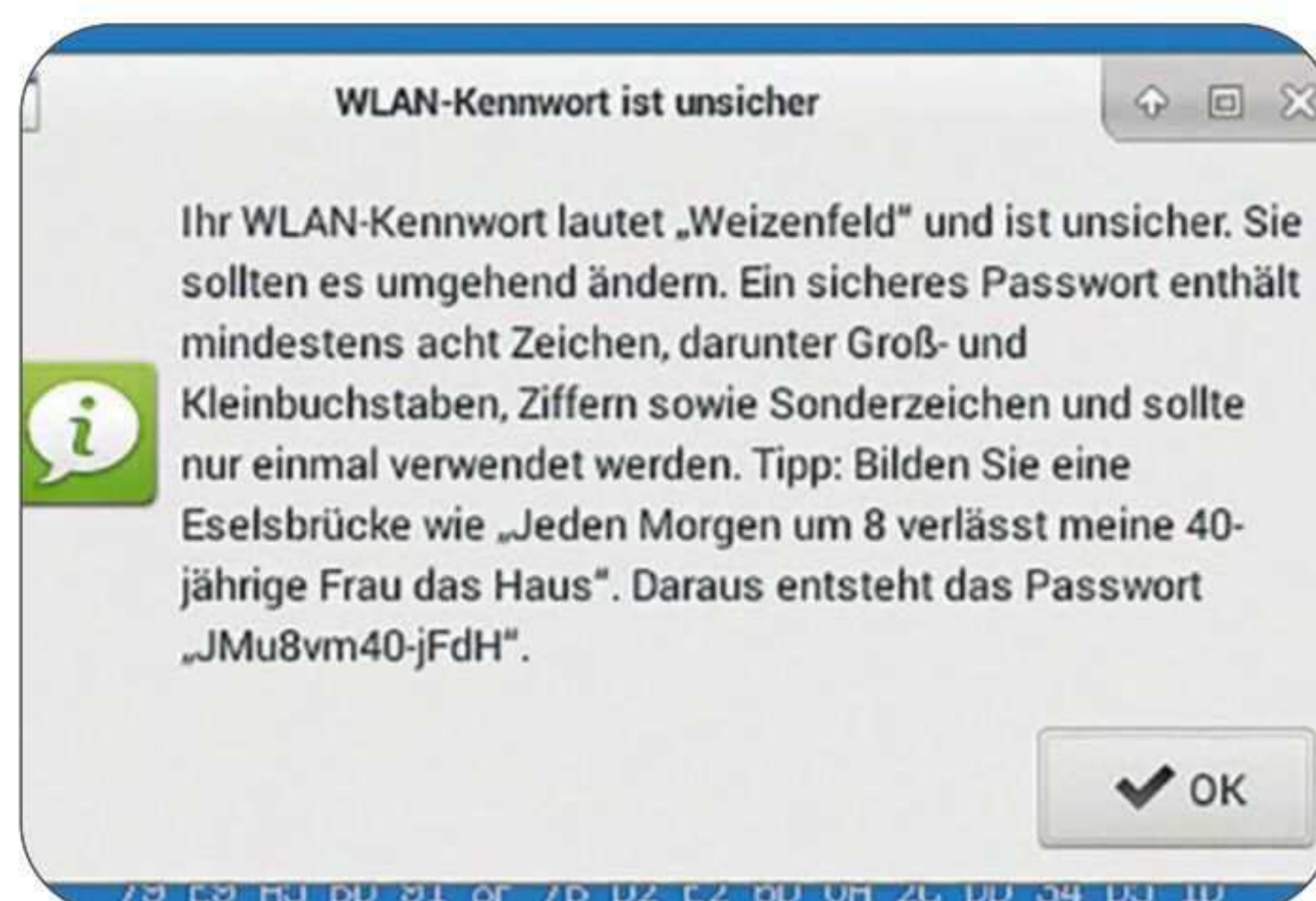
[Startseite des Servers öffnen.](#)

Der Schwachstellen-Scanner nennt unsichere Geräte im Heimnetz, hier Einfallstore einer Fritz Box.

Die Notfall-DVD hilft, Ihre Computer sowie Ihr gesamtes Heimnetzwerk gegen Angriffe aus dem Internet und vor Ort abzusichern. Im Menü **PC-Sicherheit** unter **Sicherheits-Check** finden Sie dazu folgende Werkzeuge:

WLAN-Sicherheit ermitteln

Mit dieser Funktion ermitteln Sie die Verschlüsselungsstärke Ihres WLANs und unterziehen Ihr Kennwort einem waschechten Hackerangriff. Für die sogenannte Brute-Force-Attacke probiert die Notfall-DVD bis zu 67 Millionen Passwörter durch – das kann dauern. Nach dem Start wählen Sie Ihr WLAN, die Passwortquelle und starten die Prüfung. Die Notfall-DVD zeigt dann, ob Ihr WLAN mit einer schwachen (WEP, WPA1) oder starken Verschlüsselung (WPA2, WPA3) geschützt ist. Bei WPA2 und WPA3 prüft sie nach einem Klick auf **OK** das Kennwort. Lässt es sich wie im Bild unten links knacken, sollten Sie es umgehend ändern. Beachten Sie dazu die Hinweise auf dem Bildschirm.



Unsichere WLAN-Passwörter haben bei der Notfall-DVD keine Chance.

Browser und Mailprogramm prüfen - Fertig

In der folgenden Liste sehen Sie alle auf diesem Computer gefundenen Nutzerprofile. Um welche Programme und Nutzer es sich handelt, erkennen Sie am jeweiligen Verzeichnisnamen. Bei Profilen mit dem Hinweis „unsicheres Profil“ sollten Sie tätig werden und möglichst ein Hauptkennwort festlegen. Bei Firefox und Thunderbird klicken Sie dazu in den Einstellungen auf „Datenschutz und Sicherheit“, setzen den Haken bei „Hauptpasswort verwenden“ beziehungsweise „Master-Kennwort verwenden“ und legen den Zugangscode fest. Ist Chrome oder Outlook betroffen, stellen Sie sicher, dass die Programme auf dem neuesten Stand sind und Windows per Kennwort geschützt ist.

```
/media/disk/sda3/Users/hesi/AppData/Roaming/Mozilla/Firefox, yizcu9fi.default-release-1608649134037 <- unsicheres Profil
/media/disk/sda3/Users/hesi/AppData/Roaming/Thunderbird, wd98dd4b.default <- unsicheres Profil
DETAILS:
/media/disk/sda3/Users/hesi/AppData/Roaming/Mozilla/Firefox, yizcu9fi.default-release-1608649134037, DETAILS:
Website: https://computerbild.de
Username: 'hesel'
```

Klicken Sie hier, um abzubrechen und zum Startbildschirm zurückzukehren.

Im Beispiel hat die Notfall-DVD ungeschützte Passwörter in Firefox und Thunderbird gefunden.

Geräte auf Schwachstellen abklopfen

An Bord der Notfall-DVD befindet sich auch ein „Portscanner“. Der prüft alle im Heimnetzwerk angemeldeten Geräte wie Computer, Handys, smarte Fernseher und den Router auf potenzielle Risiken. Das können ungeschützte Netzwerkanschlüsse („Ports“) oder auch im Netzwerk unbemerkt laufende Server sein. Falls nicht schon geschehen, verbinden Sie sich nach dem Start mit Ihrem WLAN und beginnen die Netzwerkanalyse per Klick auf den Pfeil. Sie benötigt mindestens 15 Minuten – sind viele Geräte im Netzwerk, dauert es auch länger. Warten Sie, bis der Fortschrittsbalken verschwunden ist. Geschieht dies auch nach Stunden nicht, wurde der Angriff von Ihrem Router erkannt und blockiert. In diesem Fall ist Ihr Netzwerk sicher, und Sie können den Vorgang stoppen. Andernfalls erscheint das Sicherheitsprotokoll wie im Bild oben links – beachten Sie die Hinweise darin. Sie können das Protokoll nach einem Rechtsklick darauf und Klick auf **Seite speichern unter** auf einem Laufwerk sichern. Beachten Sie dazu die Hinweise auf Seite 46.

Browser & Mail-Programm prüfen

Die automatische Kennwortsicherung im Browser oder Mail-Programm ist praktisch. Sorgt sie doch dafür, dass Sie Ihre Passwörter für Webseiten oder Postfächer nicht jedes Mal neu eingeben müssen. Ohne ausreichende Absicherung sind die Daten aber leichte Beute für Schnüffler vor Ort. Mit diesem Werkzeug machen Sie die Probe aufs Exempel: Nach dem Start zeigt die Notfall-DVD wie im Bild oben gefundene Nutzerprofile von Firefox, Chrome, Thunderbird und

Outlook. Die betroffenen Programme und Nutzer stehen in den Programmpfaden. Steht der Hinweis „unsicheres Profil“ dahinter, sind darin gespeicherte Daten offen sichtbar – wenn Sie mit der Seitenleiste nach unten blättern, sehen Sie Ihre Passwörter! Folgen Sie in diesem Fall den Hinweisen, um Ihre Profile abzusichern.

Analyse "/media/disk/nvme0n1p1/Users/Hub/AppData/Roaming/Mozilla/Firefox, yizcu9fi.default-release"

Für die folgenden Logins können Passwörter leicht aus...

- https://login.microsoftonline.com, Nutzernamen: auto

[So geht's: Passwörter sicher verwalten.](#)

Analyse "/media/disk/nvme0n1p1/Users/Hub/AppData/Roaming/Thunderbird, wd98dd4b.default"

Für die folgenden Logins können Passwörter leicht ausgelesen werden:

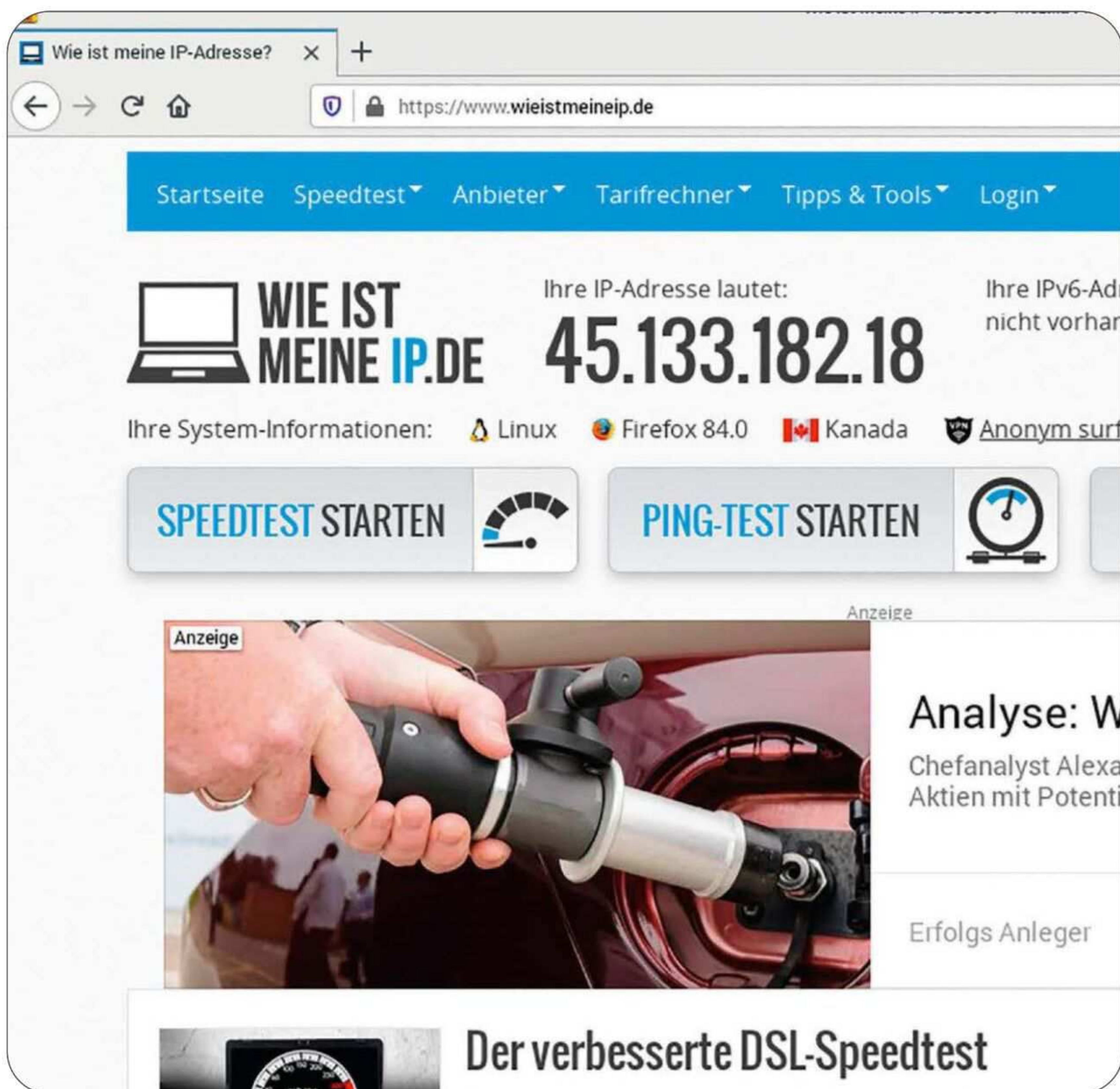
- http://www.musiker-sucht-musiker.de, Nutzernamen: j...
- https://freemail.web.de, Nutzernamen: j...
- http://line6.com, Nutzernamen: j...
- http://www.gmx.net, Nutzernamen: j...
- http://www.facebook.com, Nutzernamen: bobporst@web.de
- http://login.live.com, Nutzernamen: bobporst
- http://wendysforum.net, Nutzernamen: bobporst
- https://www.telltalegames.com, Nutzernamen: j...

Basis-Sicherheitscheck

Diese neue Funktion ist eine Weiterentwicklung der Browser- und Mail-Programmprüfung. Sie zeigt zwar keine Passwörter an, nennt dafür aber auch Programme, deren Kennwortspeicher sich nicht auslesen lässt – etwa die Passwortdatenbanken der Browser Edge und Chrome. Bei beanstandeten Schwachstellen blendet der Check zudem Links zu passenden Ratgebern im Internet ein. Klicken Sie nach dem Start auf **Ich bin mir bewusst, dass die Anwendung auf fremden Computern strafbar ist** und dann auf **Jetzt Sicherheitscheck durchführen**. Im Anschluss erscheinen die Ergebnisse im Browser, wie im Bild oben.

JETZT NEU

VPN ANONYM SURFEN MIT DEM VPN-FOX



Mit dem VPN-Fox surfen Sie im Tarnmodus durchs Netz. Im Beispiel gaukelt der Gratisdienst „Hide.me“ der Prüfseite vor, Sie wären in Kanada.

Wenn Windows nicht startet, kommen Sie immer noch mit der Notfall-DVD ins Internet, siehe Seite 46. Dabei müssen Sie nicht auf den Schutz Ihrer Privatsphäre verzichten, denn die Software enthält Erweiterungen für VPN-Dienste (Virtuelles Privates Netzwerk). Damit surfen Sie anonym und umgehen Ländersperren im Internet:

1 Internet verbinden: Stellen Sie zunächst eine Internetverbindung her (siehe Seite 33). Nach Klicks auf **PC-Sicherheit**, **Sicher surfen** und **VPN-Fox** erscheinen VPN-Funktionen oben rechts im Firefox-Browser.

2 Erweiterung wählen: Diese VPN-Dienste stehen Ihnen bereit (von links nach rechts):

■ **Hide.me:** Das Gratis-VPN funktioniert ohne Anmeldung und bietet Server in Kanada, den Niederlanden und Deutschland – ohne Beschränkungen bei Datenvolumen und Tempo. Erscheint „Proxy-Server verweigert die Verbindung“, wählen Sie statt „Automatic“ ein Land.

■ **HMA:** Hier müssen Sie sich registrieren („Sign up“) oder anmelden („Log in“). Gratis gibt es fünf Länder ohne Volumenbeschränkung: USA, Großbritannien, Frankreich, Deutschland und die Niederlande.

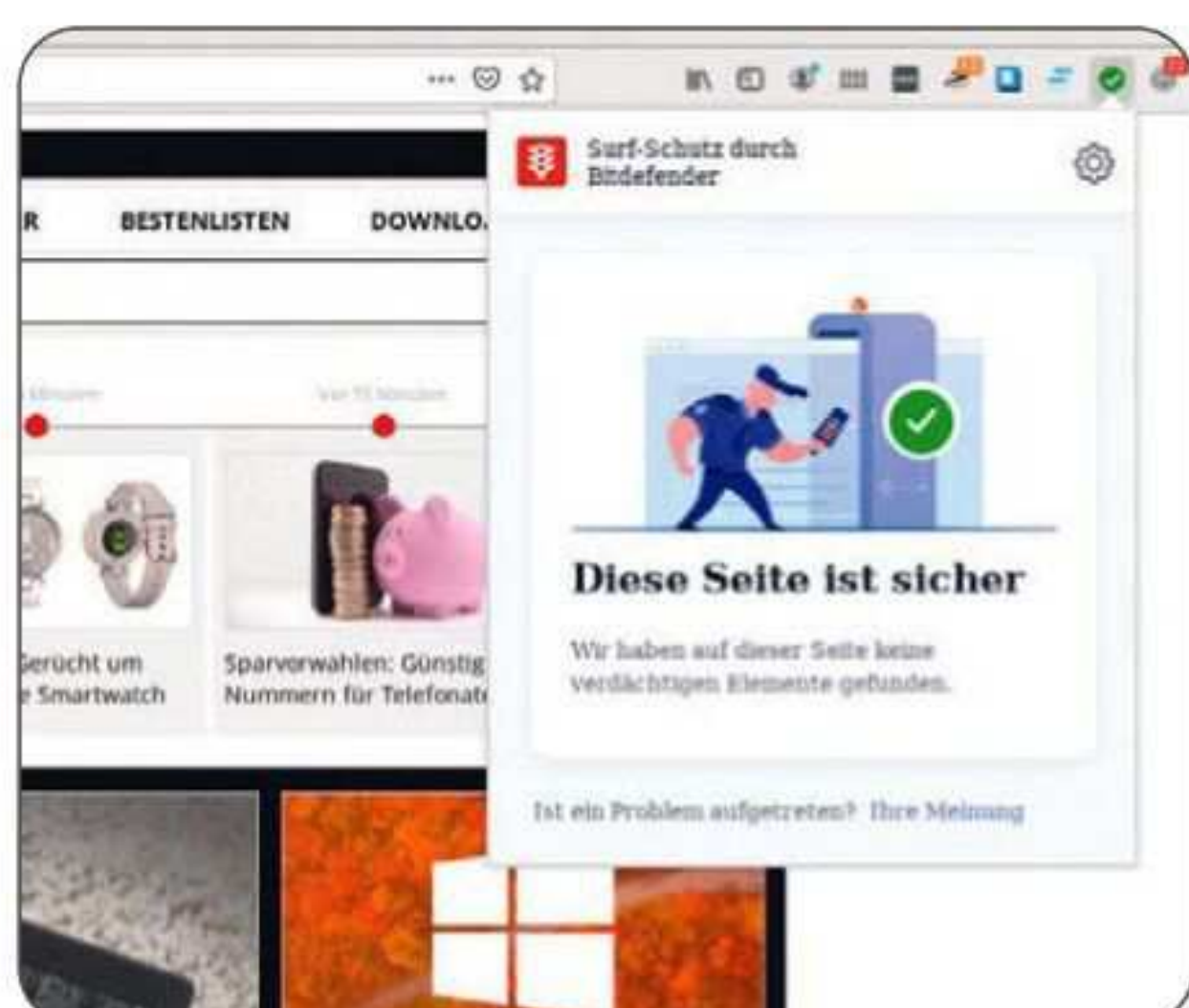
■ **TunnelBear:** Auch dieser Dienst setzt eine Anmeldung voraus. Danach haben Sie kostenlosen Zugriff auf 26 Länder – bis 250 Megabyte im Monat. Bei der Registrierung gibt's noch 500 Megabyte dazu.

■ **ZenMate:** Ein Nutzerkonto ist hier nicht nötig. Um den Dienst gratis zu nutzen, klicken Sie auf **Schließen** und den Schild. Sie haben dann unbegrenzt Zugriff auf Server in Deutschland, Rumänien, Singapur und den USA, gedrosselt auf 2 Megabyte pro Sekunde.

■ **NordVPN und SurfShark:** Dabei handelt es sich um reine Kaufdienste. Auf der Seite cobi.de/12676 finden Sie Daten und Preise zu den Anbietern.

3 Anonym surfen: Klicken Sie auf eine Erweiterung, und melden Sie sich bei Bedarf an. Sobald Sie den Schalter aktiviert haben, sind Sie getarnt – zum Testen laden Sie die Seite weistmeineip.de (siehe Bild). Wichtig: Aktive VPNs stören sich gegenseitig. Nach Drücken von **Strg** + **U** + **A** sollten Sie nicht benötigte Erweiterungen deaktivieren.

SICHER SURFEN MIT DEM SAFE-FOX



TrafficLight zeigt, ob die besuchte Website sicher ist.

■ **LastPass:** Damit nutzen Sie gesicherte Passwörter bei LastPass beim Surfen mit der Notfall-DVD. Nach einem Klick auf **Annehmen** können Sie sich dort anmelden oder ein **Konto erstellen**.

Unter **PC-Sicherheit** und **Sicher surfen** finden Sie auch den **Safe-Fox**. Diese Firefox-Variante bietet Sicherheit beim Surfen auch ohne VPN. Und das sind die enthaltenen Funktionen:

■ **Facebook Container:** Die Erweiterung verhindert, dass Facebook Ihre Webaktivitäten nachverfolgen kann. Nach einem Klick auf das Zaunsymbol sehen Sie, ob die besuchte Webseite Facebook-Tracker einsetzt.

■ **Privacy Badger:** Dieses Add-on zeigt und blockiert Überwachungsfunktionen („Tracker“) auf beliebigen Webseiten. Blenden Sie dazu die Einführung mit **X** aus.

■ **HTTPS Everywhere:** Das Tool lädt die verschlüsselte Version von Internetseiten. Dazu den Schalter „Alle geeigneten Seiten verschlüsseln“ aktivieren.

■ **Popup Blocker:** Dieses Add-on öffnet Pop-up-Fenster nur mit Ihrer Erlaubnis. Per Klick schalten Sie den Schutzschalter aus (rot) und wieder ein (blau).

■ **Bitdefender TrafficLight:** Die Erweiterung schützt vor Schädlingen und betrügerischen Websites („Phishing“), siehe Bild links.

■ **Cookie AutoDelete:** Damit löschen Sie Webseiten-Protokolle automatisch. Klicken Sie dazu auf **Automatisches Aufräumen deaktiviert**.

■ **Startpage:** Tippen Sie einen Suchbegriff bei Firefox ein, leitet dieses Werkzeug ihn anonymisiert an Google weiter.

REPARIEREN SIE IHRE HARDWARE

Die Notfall-DVD hilft sogar bei Hardware-Problemen und erkennt gefährliche Verschleißerscheinungen.



PC-KOMPONENTEN ÜBERPRÜFEN

Hinter Abstürzen und Fehlermeldungen stecken oft Hardware-Schäden. Sind Laufwerke betroffen, droht sogar Datenverlust! Nach Klicks auf **Hardware reparieren** und **Hardware testen** kommen Sie Problemen auf die Schliche. Diese Werkzeuge helfen dabei:

PC-Inspektion

Hier unterziehen Sie Ihren PC einem Fitness-Test. Die PC-Inspektion checkt wichtige Komponenten wie Arbeitsspeicher, Festplatte, Prozessor und die PC-Lüfter. Zum Abschluss gibt es eine Systembewertung mit Ampelfarben und konkreten Hinweisen, was zu tun ist. Achtung: Der Vorgang kann mehrere Stunden dauern.

Ergebnis des SSD-Schnelltests

Hier sehen Sie die in Ihrem Computer erkannten SSD-Laufwerke. Je voller ein Fortschrittsbalken ist, desto höher die Speicherzellen auf dem Laufwerk bereits beschrieben. Schon ab 2.500 Schreibvorgängen pro Speicherzelle Beispiel viele ältere SSDs nicht mehr als zuverlässig. Falls der Fortschrittsbalken voll ist oder sich bei Test-W immer schneller füllt, kommt der Speicher seiner Verschleißgrenze näher und Sie sollten eine Sicherheitskopie erstellen. Dies ist aber nur eine grobe Faustformel. Manche SSD-Laufwerke gelten bei bis zu 10.000 Schreibvorgängen als zuverlässig.

ATA CT480BX500SSD1 - 447GB - sda (SATA/eSATA/IDE/NVME)

Der SSD-Schnelltest zeigt den Speicherzellen-Verschleiß eines eingebauten SSD-Speichers.

SSD-Schnelltest

Während die PC-Inspektion Diagnosedaten („SMART-Werte“) aus den Selbsttest-Protokollen mechanischer Festplatten liest, liefert der **SSD-Schnelltest** eine Zustandsprognose der Speicherzellen schneller „Solid State Drives“. Nach dem Start erscheinen gefundene SSDs mit einem Fortschrittsbalken (siehe Bild oben). Je voller er ist, desto näher ist das Laufwerk an seiner Verschleißgrenze. Keine Panik: Bei ungünstiger Prognose müssen Sie das Laufwerk nicht gleich ersetzen, fertigen aber vorsorglich eine Komplettsicherung (siehe Seite 38) an. Hinweis: Viele neuere SSDs liefern nicht mehr die von der Notfall-DVD benötigten Daten. In diesem Fall erscheint der oben gezeigte Speicherzellen-Verschleiß-Balken leider nicht.

Es wurden Fehler entdeckt

Einige beim Start der Notfall-DVD in den RAM geschriebenen Testdaten konnten nicht gelesen werden. Die DVD hat die defekten Bereiche des Arbeitsspeichers gesperrt, sodass Sie vorläufig weiteren Betrieb aber zusätzliche Speicherdefekte zutage treten, sodass keine Systemdaten verloren gehen. Sie sollten den Arbeitsspeicher daher auswechseln. Wie es geht, zeigt die Schritt-für-Schritt-Anleitung.

Bitte QR-Code anklicken oder scannen:



Entdeckt der RAM-Test Probleme, liefert er eine Anleitung zum Austausch des Arbeitsspeichers.

RAM-Prüfung

Die Notfall-DVD prüft den Arbeitsspeicher (RAM) des PCs schon beim Start und meldet Defekte automatisch. Mit der **RAM-Prüfung** erhalten Sie weitere Details und gegebenenfalls eine Anleitung zum Tausch des Speichers. Die öffnen Sie mit einem Klick auf den QR-Code (Bild oben) direkt am PC-Bildschirm oder scannen ihn mit dem Smartphone. Detaillierte Messergebnisse liefert das Programm Memtest86+, das Sie im Startmenü der Notfall-DVD per Klick auf **Arbeitsspeicher testen** starten. Zeigt es auch nach Stunden keine rot markierten Fehler, ist alles in Ordnung. Hinweis: Da Memtest86+ Probleme beim Start auf neueren UEFI-PCs hat, erscheint dort möglicherweise nur ein blauer Bildschirm. In diesem Fall schalten Sie den PC durch längeres Drücken des Ein/Aus-Schalters aus und starten ihn neu.

Monitor-Pixeltest

Dieses Werkzeug macht Pixelfehler sichtbar. Das sind „tote“ oder dauerhaft leuchtende Bildpunkte in LED-Monitoren. Klicken Sie im Erklärfenster auf **OK** und danach auf eine beliebige Stelle. Daraufhin wird der Bildschirm komplett schwarz. Mit weiteren Klicks wechseln Sie die Farben, per Rechtsklick geht es rückwärts. Achten Sie auf andersfarbige Punkte, denn die verraten Pixelfehler.

Finden Sie störende oder besonders viele, sollten Sie von Ihrem Widerrufsrecht Gebrauch machen.

USB-Verschleißtest

Auch USB-Sticks verschleßen mit der Zeit. Um die Datensicherheit zu gewährleisten, starten Sie den USB-Verschleißtest unter **USB-Laufwerk prüfen**. Wählen Sie danach das Laufwerk aus, und klicken Sie auf den Pfeil. Daraufhin wird der Speicher mit bestimmten Datenmustern beschrieben und wieder ausgelesen. Bleiben Daten auf der Strecke, arbeitet das Laufwerk nicht mehr zuverlässig, und Sie erhalten eine entsprechende Meldung – andernfalls Entwarnung. Tipp: Der Stick sollte für den Test möglichst leer sein, vorhandene Daten werden aber nicht überschrieben.

Laufwerk auswählen

Klicken Sie in der Auswahl-Liste auf das Laufwerk, das Sie testen möchten. Anschließend mit einer großen Maus oder einem Joystick auf den Pfeil klicken. Bereits stark verschlissene Laufwerke sollten Sie daher bei Bedarf zuvor sichern.

SanDisk Ultra Fit - 57GB - sdb
General UDisk - 250GB - sdc

Kapazitätsprüfung

Leider tauchen vor allem im Versandhandel aus Fernost immer wieder gefälschte USB-Sticks und Speicherkarten auf, die eine viel zu hohe Kapazität vorgaukeln. Darauf gespeicherte Daten sind dann oft verloren. Mit dieser Funktion finden Sie heraus, ob die Größenangabe des Speichers stimmt. Wählen Sie den Stick aus der Liste – im Beispiel einer mit angeblich 250 Gigabyte. Nach einem Klick auf den Pfeil wird er untersucht. Je länger der Stick „durchhält“, desto wahrscheinlicher ist er echt. Am Ende gibt es das Ergebnis – in diesem Beispiel ist der Stick gefälscht:

Gefälschtes Laufwerk erkannt!

Das USB-Laufwerk hat den Test leider nicht bestanden. Ein Vergleich der Datenmuster weist darauf hin, dass die Kapazitätsangabe nicht mit den tatsächlich kopierten Daten, die in den vorgedruckten Speicherbereich kopiert wurden, übereinstimmt.

Viel Stick für wenig Geld? Die Notfall-DVD entlarvt gefälschte USB-Laufwerke.



PC-KOMPONENTEN REPARIEREN

Selbst bei bestimmten Hardware-Defekten lässt die Notfall-DVD Sie nicht im Stich. Im Menü **Hardware reparieren** macht die Software zum Beispiel beschädigte USB-Laufwerke wieder flott und behebt PC-Probleme, die das Netzwerk und das Drucken behindern. So funktioniert's:

USB-Stick reparieren

Bietet ein USB-Stick plötzlich viel weniger Speicherplatz als draufsteht? Oder hagelt es unter Windows Fehlermeldungen beim Zugriff auf das Gerät? Dahinter stecken meist Dateisystemfehler oder unsichtbare Partitionen, die sich nur mit Spezial-Software entfernen lassen – Formatieren bringt dann leider nichts. Mit der Funktion **USB-Stick reparieren** setzen Sie zickige Sticks sowie störrische USB-Festplatten in den Werkszustand zurück und machen den Speicherplatz wieder vollständig verfügbar. Dabei werden auch Datenträger-Probleme behoben, die zum Beispiel eine Neuformatierung des Laufwerks verhindern. Nach dem Start der Funktion wählen Sie das betroffene Laufwerk, klicken auf den Pfeil und schließlich auf **OK**. Tipp: Die Funktion formatiert das Laufwerk mit dem Microsoft-Dateisystem NTFS. Im Expertenmodus können Sie zum Beispiel auf das herkömmliche FAT32-Format umsteigen, siehe Seite 47.

Auch bei softwarebedingten Druckerstaus hilft die Notfall-DVD.



Hängende Druckaufträge löschen

Ist ein Drucker beim Start des Druckvorgangs ausgeschaltet oder unerreichbar, bleibt der Auftrag manchmal dauerhaft in der Warteschlange hängen und blockiert alle nachfolgenden Druckvorhaben. Diesen ärgerlichen Stau lösen Sie leicht mit der Notfall-DVD: Klicken Sie dazu im Hauptmenü auf **Daten vernichten** und **Datenmüll löschen**. Im nächsten Fenster stellen Sie sicher, dass bei „Hängende Druckaufträge“ ein Häkchen steht, und klicken auf den Pfeil. Ganz „ne-

benbei“ können Sie mit dieser Funktion auch Datenmüll in Windows löschen:

■ **Temporäre Dateien:** Setzen Sie hier ein Häkchen, löscht die Notfall-DVD den Datenmüll aller PC-Nutzer in Windows. Verwenden Sie die Funktion also mit Bedacht, wenn andere Personen den Computer mit einem eigenen Windows-Konto nutzen.

■ **Inhalt des Mülleimers:** Wählen Sie diese Option, leert die Notfall-DVD den Windows-Papierkorb. Auch hier wird der Datenmüll aller Windows-Benutzerkonten gelöscht.

Internet-Probleme beheben

Zeigt der Internet-Browser unter Windows plötzlich Fehlermeldungen wie „Verbindung zum Proxy-Server kann nicht hergestellt werden“ oder „Verbindung unterbrochen“, kann neben Konfigurationsfehlern auch eine manipulierte Netzwerk-Einstellung dahinterstecken. Das ist insbesondere dann wahrscheinlich, wenn beim Surfen unerwünschte Webseiten erscheinen, denn die sind schlimmstenfalls auch noch virenverseucht oder sollen Ihre Daten ausspionieren. Mit der Funktion **Netzwerk reparieren** setzen Sie alle zuständigen Einstellungen zurück, reparieren die Standard-Netzwerkumleitung von Windows („Proxy“), die leicht manipulierbare Konfigurationsdatei „hosts“ und alle Internet-Optionen des Betriebssystems. Dazu installiert die Notfall-DVD ein kleines Programm,

das beim nächsten Windows-Start erscheint. Folgen Sie den Anweisungen auf dem Bildschirm.



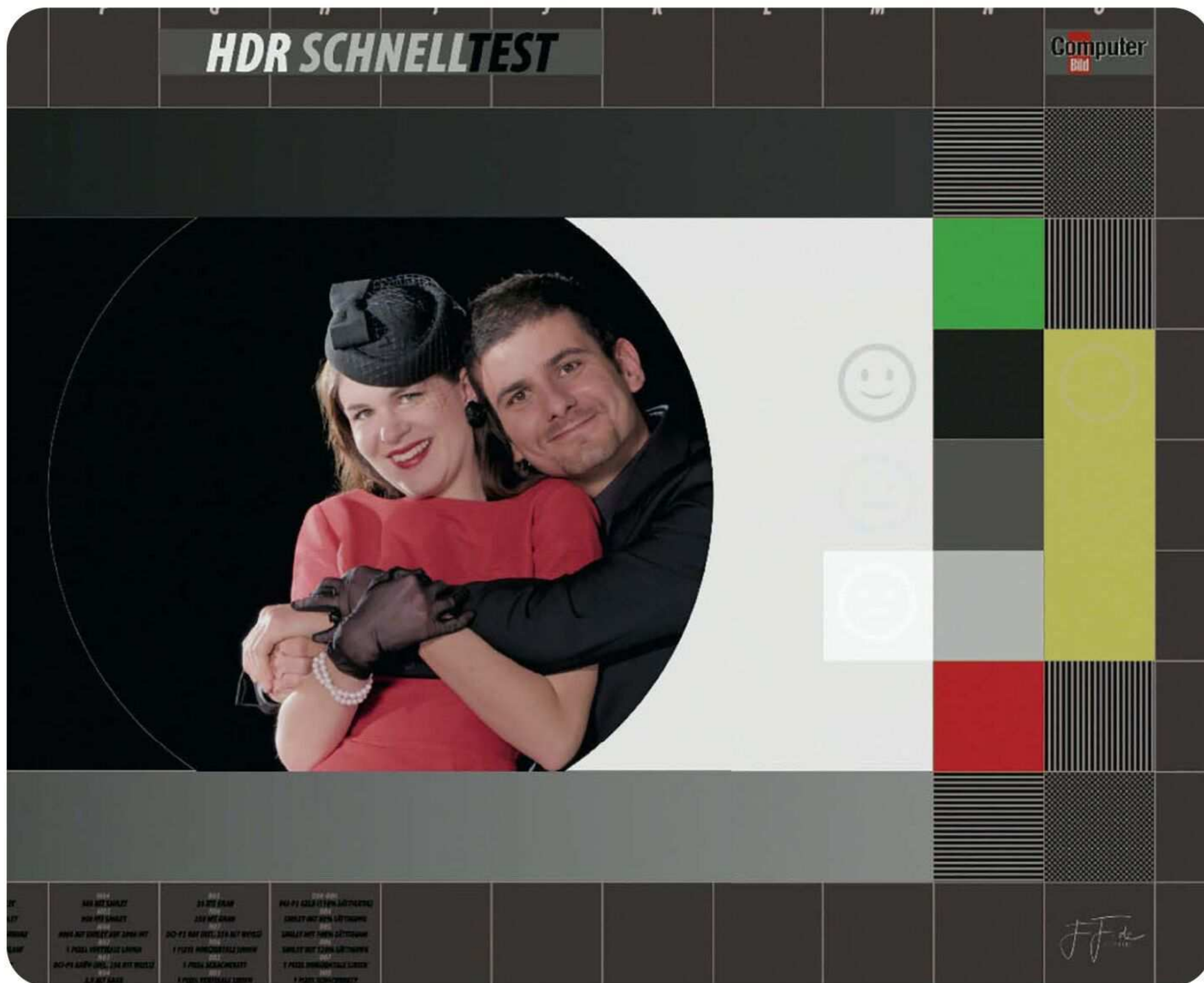
„Die Notfall-DVD hat mir vermeintlich ‚tote‘ USB-Laufwerke gerettet.“

Andreas Sauerland
Ressortleiter Software





TV-BILD OPTIMIEREN



Das Testvideo zur Einstellung von UHD-Fernsehern lädt die Notfall-DVD aus dem Internet.

Zeigt Ihr UHD-Fernseher Filme viel zu düster an, liegt es meist an ungünstigen Voreinstellungen. Kein Problem: Unter **Hardware reparieren** finden Sie die Funktion **TV-Bild optimieren**. Damit verbessern Sie das Bild ohne Fachkenntnisse. Das geht so:

1 Testvideo herunterladen: Falls nicht schon geschehen, stellen Sie eine Internetverbindung her. Danach stöpseln Sie einen USB-Stick mit wenigstens 600 Megabyte freiem Speicherplatz ein und klicken auf **Neu einlesen**. Wird er nicht angezeigt, muss er noch mit dem Dateisystem FAT32 formatiert werden, siehe Seite 47. Nach

Auswahl des Laufwerks und einem Klick auf den Pfeil wird ein Testvideo heruntergeladen. Das dauert etwas.

2 Optimierung durchführen: Erscheint „Anleitung anzeigen“, klicken Sie auf den QR-Code oder scannen ihn per Handy. Nun sehen Sie die Anleitung wie im Bild unten. Stecken Sie den USB-Stick mit dem Testvideo ins TV-Gerät, und starten Sie dort die Datei **HDR-Schnelltest.mp4**. Optimieren Sie die TV-Einstellungen mithilfe der Anleitung. Stellen Sie sicher, dass die Einstellungen für alle Signalquellen gelten: Bei Samsung etwa wählen Sie dazu in den **Experteneinstellungen** unter **Bildeinstellungen anwenden** die Option **Alle Quellen**. Ist das nicht möglich, wechseln Sie nach und nach die Signalquellen und stellen das Bild dort separat ein.



HARDWARE-DETAILS AUFLISTEN

Konnte die Notfall-DVD Ihr Hardware-Problem nicht beheben? Wer Hilfe in einem Online-Forum oder bei einer Telefon-Hotline sucht, muss dort oft erst viele Fragen zum Computer und zu dessen Innereien beantworten. Können Sie das nicht, hilft ebenfalls die Notfall-DVD. Das geht so:

1 Funktion starten: Klicken Sie auf **Hardware reparieren** und **PC-Profil erstellen**.

2 Laufwerk anschließen: Falls Sie keinen Notfall-Stick verwenden, schließen Sie am besten einen USB-Stick an. Klicken Sie dann auf **Neu einlesen**.

3 Laufwerk wählen: Wählen Sie das Ziel-Laufwerk aus der Liste. Möchten Sie das Profil direkt auf dem Notfall-Stick sichern, klicken Sie auf das Laufwerk mit dem Zusatz **Backup-Medium**. Sie können auch das Windows-Laufwerk auswählen. Wie das geht, steht auf Seite 46.

4 Profil öffnen: Klicken Sie auf den Pfeil, wird die Liste auf dem Laufwerk im Ordner **PC-Profil** als Datei **PC-Profil.htm** gesichert – also im Format einer Webseite. Die öffnen Sie per Doppelklick im Browser. Dazu nutzen Sie entweder den Expertenmodus (siehe

Seite 46) oder wechseln zu Windows. Teilen Sie die Datei dann einfach mit Ihrem PC-Support oder Helfer, etwa per E-Mail.

PC-Profil

Allgemeine Informationen

- Prozessor: Intel(R) Pentium(R) CPU 4405U @ 2.10GHz
- Zahl der Kerne: 3
- Arbeitsspeicher: 7817 MB

PCI-Geräte

- 8086:1904 Intel Corporation Skylake Host Bridge/DRAM Registers (Host Bridge)
- 8086:1906 Intel Corporation HD Graphics 510 (VGA compatible controller)
- 8086:9d2f Intel Corporation Sunrise Point-LP USB 3.0 xHCI Controller (USB 3.0)
- 8086:9d31 Intel Corporation Sunrise Point-LP Thermal subsystem (Signal processing)
- 8086:9d60 Intel Corporation Sunrise Point-LP Serial IO I2C Controller #0 (I2C controller)
- 8086:9d61 Intel Corporation Sunrise Point-LP Serial IO I2C Controller #1 (I2C controller)
- 8086:9d3a Intel Corporation Sunrise Point-LP CSME HECI #1 (Communication)
- 8086:9d03 Intel Corporation Sunrise Point-LP SATA Controller [AHCI mode]
- 8086:9d14 Intel Corporation Sunrise Point-LP PCI Express Root Port #5 (PCI Express)

Das PC-Profil liefert umfassende Informationen zur Hardware Ihres Computers.

EXPERTENMODUS PROFI-TRICKS

WEITERE FUNKTIONEN

Klicken Sie im Dock auf **Anwendungsmenü** 5 oder drücken Sie die Taste , erscheinen noch mehr Funktionen. Hier eine Auswahl:

VLC Player

Möchten Sie bei der Arbeit Musik hören oder Videos schauen, binden Sie das Windows-Laufwerk nur lesbar ein (siehe rechts unten), klicken im Anwendungsmenü auf **Multimedia** und **VLC Media Player**. Nach Klicks auf **Fortfahren**, **Medien**, **Datei öffnen** und **Computer** klicken Sie je doppelt auf **/**, **media**, **disk** und das Laufwerk. Ihren Musik- und Videoordner finden Sie unter **Users** im Ordner mit Ihrem Namen.

VeraCrypt

Brauchen Sie Zugriff auf einen VeraCrypt-Safe, klicken Sie bei **Zubehör** auf **VeraCrypt**, **Select File**, das eingebundene Laufwerk, die Container-Datei, **Öffnen**, **Slot 1** und **Mount**. Geben Sie das Container-Passwort und danach ein beliebiges Administrator-Kennwort ein. Der VeraCrypt-Safe erscheint nach einem Klick auf **Home directory** 6.

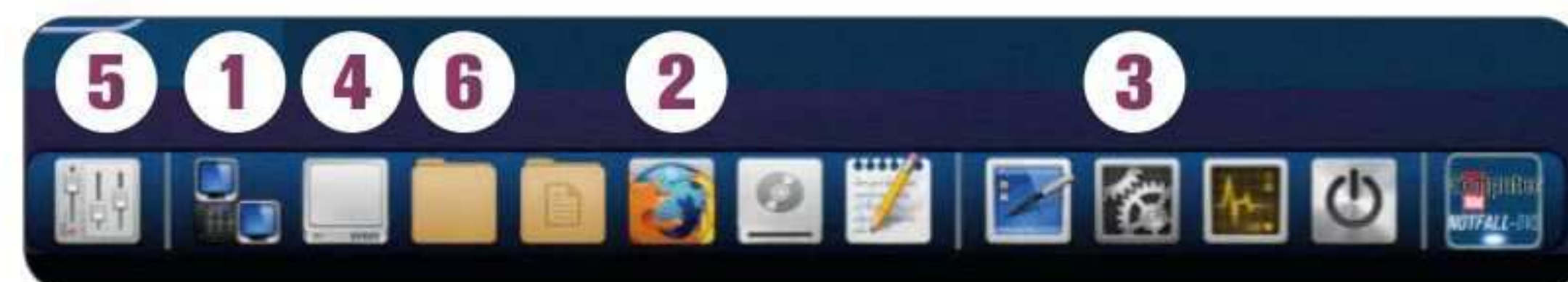
Registry Editor

Startet Windows wegen einer Fehlkonfiguration der Registrierungsdatenbank nicht, hilft der **FRED Registry Editor** im Menü **Weitere Wartungswerkzeuge**. Unter **cobi.de/go/fred** erfahren Sie, wie Sie die Windows-Registry öffnen, um den Fehler rückgängig zu machen.

Im Expertenmodus steht Ihnen ein Notfall-Arbeitsplatz mit mehr als 70 Spezialprogrammen zur Verfügung.

IM INTERNET SURFEN

Der Expertenmodus der Notfall-DVD bietet Zugriff auf einen Browser, Libre Office und zahlreiche Rettungsprogramme, die auch von IT-Profis verwendet werden. Sie erkennen den Expertenmodus an der Bedienleiste am unteren Bildrand – dem „Dock“.



Lesen Sie hier, wie Sie im Expertenmodus mit der Notfall-DVD ins Internet kommen und Dateien überspielen:

1 Internet verbinden: Falls nicht schon geschehen, verbinden Sie die Notfall-DVD wie auf Seite 33 beschrieben mit dem Internet. Sie finden die nötige Netzwerk-Einrichtung auch im Dock 1.

2 Surfen: Klicken Sie auf das Firefox-Symbol 2, und surfen Sie los. Der Mozilla-Browser wurde für die Notfall-DVD 17 auf die jüngste Version 97

gebracht und ist updatefähig. Möchten Sie eine Datei so aus dem Internet überspielen, dass sie unter Windows verfügbar ist, binden Sie das Ziellaufwerk „schreibbar“ ein, wie im folgenden beschrieben. Dann gibt es zwei Möglichkeiten:

■ **Speichern unter:** Klicken Sie auf der Webseite mit der rechten Maustaste auf den Download, im erscheinenden Menü auf **Ziel speichern unter**, das eingebundene Laufwerk und **Speichern**.

■ **Kopieren:** Klicken Sie mit der linken Maustaste auf den Download, dann auf **Datei speichern** und **OK**. Danach klicken Sie im Dock auf das Ordnersymbol **Home directory** und ziehen den Ordner **Downloads** mit der Maus auf das eingebundene Laufwerk.

3 Updates laden: Per Klick auf das Symbol **Nach Aktualisierungen suchen** 3 überspielen Sie gegebenenfalls Verbesserungen für die Notfall-DVD aus dem Internet. Klicken Sie auf **Yes** und **OK**. Starten Sie vom Notfall-Stick mit „Backup-Medium“, bleiben die Updates dort erhalten.

LAUFWERKE EINBINDEN

In der Notfall-DVD sind aus Sicherheitsgründen alle PC-Laufwerke vor Zugriffen geschützt. So machen Sie Laufwerke lesbar oder beschreibbar:

1 Einbinden: Klicken Sie auf **Laufwerke** 4. Im neuen Fenster erscheint dann unten der Notfall-Stick (im Beispiel: „SanDisk Ultra Fit“). Um dort Daten speichern zu können, setzen Sie den Haken **schreibbar?** und klicken auf ... **einbinden**. Der In-



halt des Laufwerks erscheint dann im neuen Fenster. Wichtig: Laufwerke tragen hier nicht die von Windows bekannten Buchstaben wie „C:“. Im Beispiel heißt der USB-Stick „sdb1“.

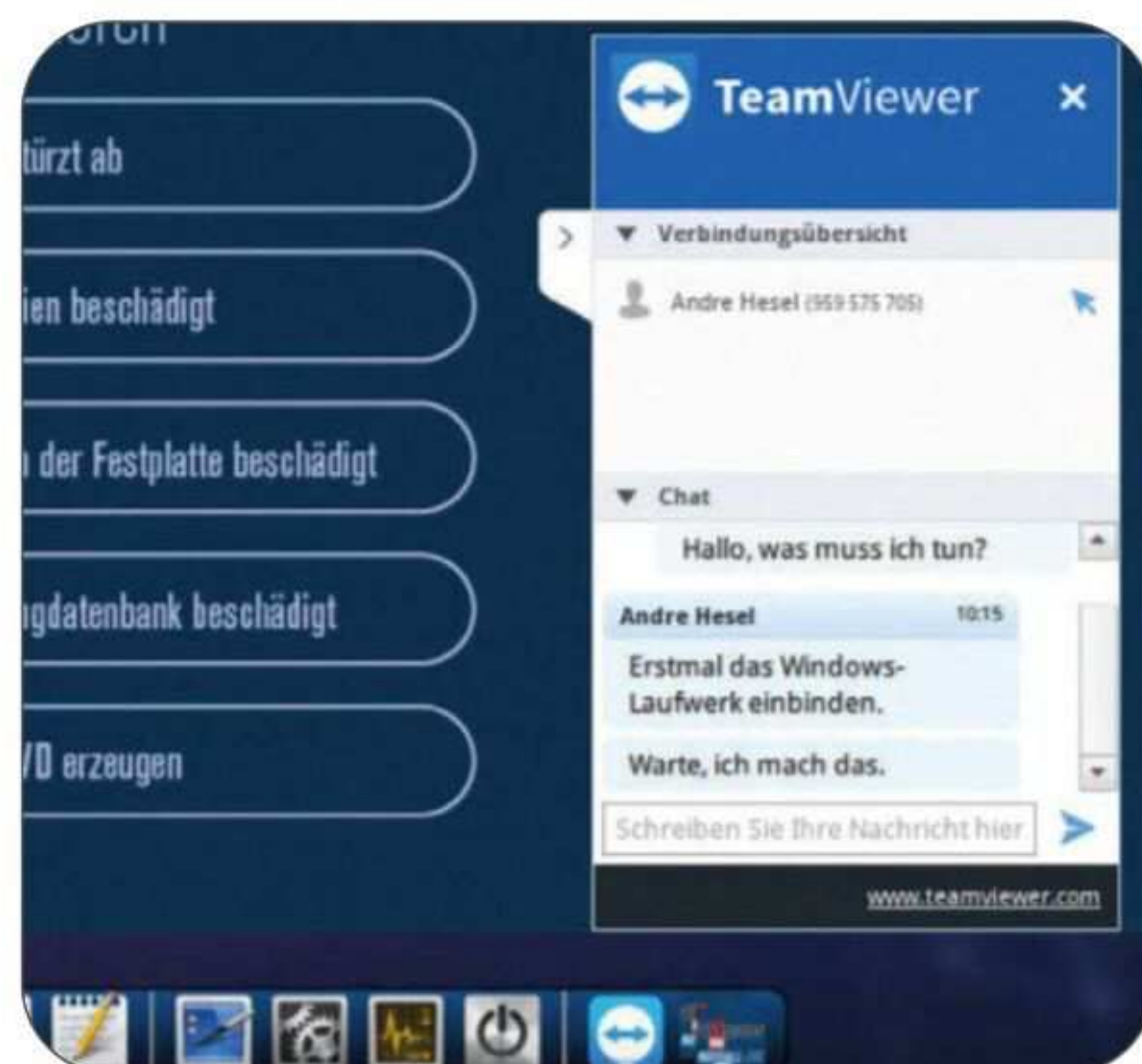
2 Kopieren: Um Dateien zum Stick zu kopieren, ziehen Sie sie im Beispiel per Maus ins Fenster „sdb1“. Auf die gleiche Weise klappt es beim Windows-Laufwerk. Die Partition finden Sie in der Regel auf der Festplatte mit dem Zusatz „ATA“ und dort auf der ersten Partition mit angehängtem „ntfs“ – im Beispiel „sda3“. Sie erkennen das Laufwerk auch daran, dass sich dort der Ordner „Windows“ befindet. Vorsicht: Löschen Sie dort nichts! Möchten Sie Dateien nur anzeigen, binden Sie die Partition besser ohne das „schreibbar?“-Häkchen ein. Ein Klick auf ... **lösen** stoppt die Einbindung.

FERNWARTUNG MIT TEAMVIEWER

Konnten Sie ein Problem nicht im Alleingang lösen, schafft es vielleicht ein Freund. Dank TeamViewer schaut er übers Internet auf Ihren Bildschirm und greift notfalls ein. Dazu startet er ebenfalls die Notfall-DVD oder TeamViewer für Windows von der Webseite www.cobi.de/11374. So funktioniert's:

1 TeamViewer starten: Klicken Sie bei bestehender Internetverbindung aufs Kopfhörer-Symbol oben rechts oder im Dock auf **Anwendungsmenü 5**, **Weitere Wartungswerkzeuge** und **TeamViewer**. Nach dem Klick auf **Lizenzabkommen akzeptieren** nennen Sie dem Helfer die Codes bei „Ihre ID“ und „Passwort“. Bleiben die Felder leer, müssen Sie die Notfall-DVD-Oberfläche neu starten. Dazu klicken Sie einfach im erscheinenden Fenster auf **Yes**. Erscheint der TeamViewer danach verdeckt, klicken Sie im Dock aufs TeamViewer-Symbol, um ihn wieder einzublenden.

2 Verbinden: Bitten Sie den Freund, unter „Computer fernsteuern“ Ihre Daten einzugeben. Nach einem Klick auf **Verbinden** sieht er Ihren Bildschirm, kann bei der Problemlösung assistieren und sogar Ihren PC bedienen. Nach einem Klick auf **Chat** lassen sich Textnachrichten austauschen. Mit **X** trennen Sie oder der Freund die Verbindung mit dem TeamViewer wieder.



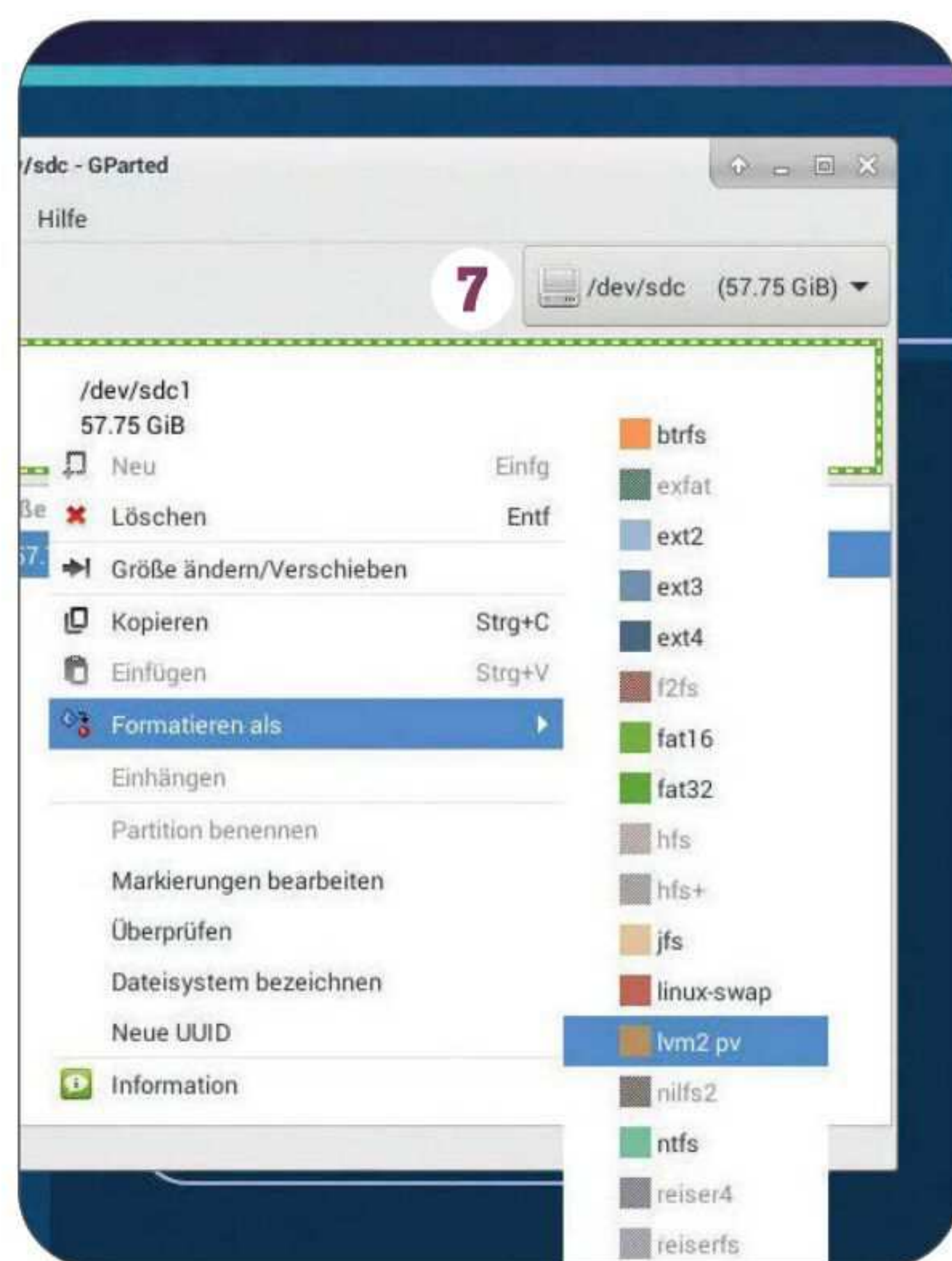
LAUFWERKE FORMATIEREN

Die Notfall-DVD kann Datenträger aufteilen (partitionieren) und formatieren. Um etwa eine USB-Festplatte mit „NTFS“ statt „FAT32“ zu formatieren, schließen Sie sie an und gehen wie folgt vor. Achtung: Dabei gehen alle Daten auf dem Laufwerk verloren!

1 Programm starten: Klicken Sie auf **Anwendungsmenü 5**, **Weitere Wartungswerkzeuge** und **GParted Partitionsierungswerkzeug**.

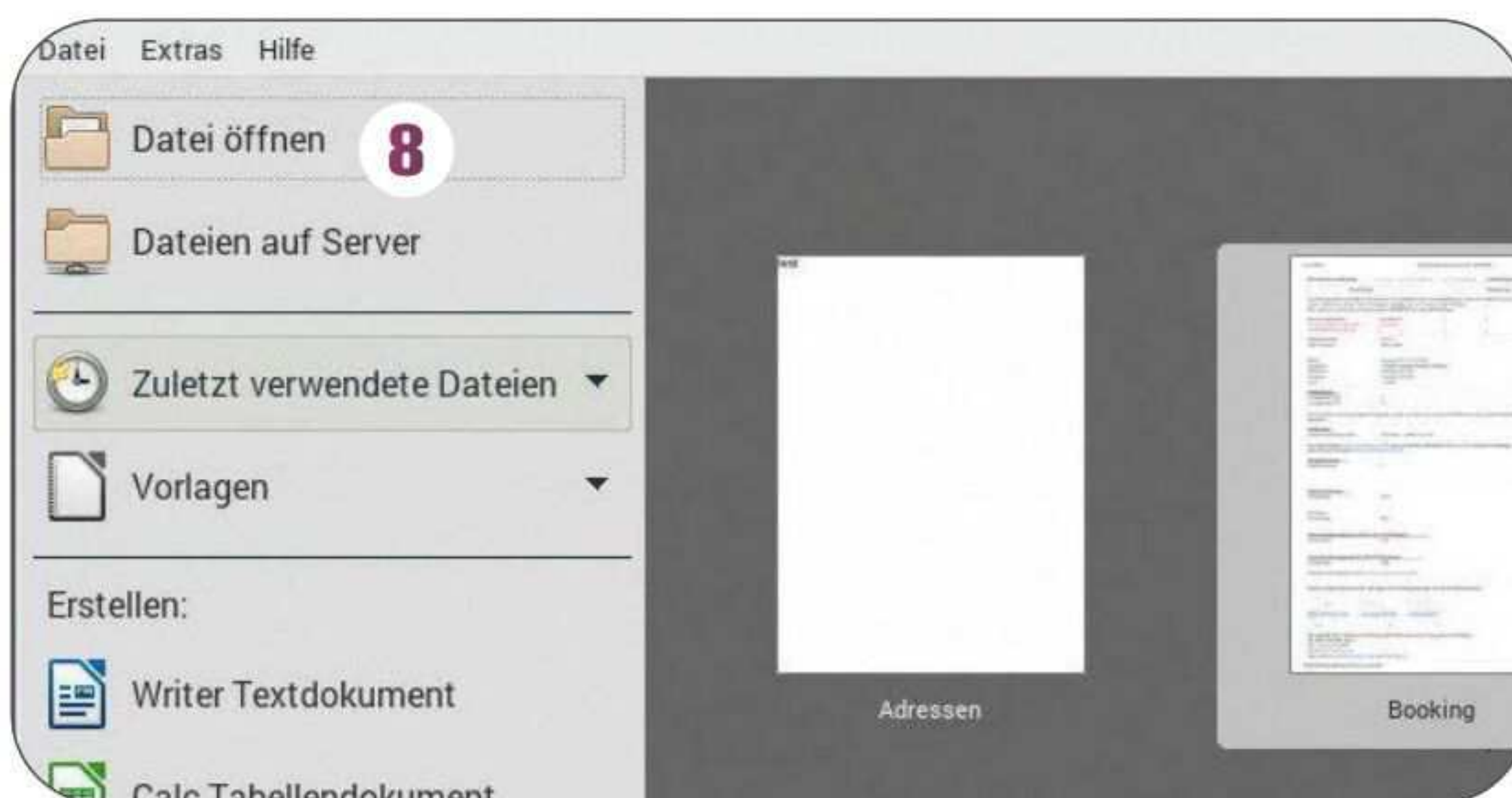
2 Laufwerk formatieren: Ganz wichtig: Im erscheinenden Fenster stellen Sie rechts oben sicher, dass das richtige Laufwerk ausgewählt ist **7** – im Zweifel mit der Funktion **Laufwerke 4** nachprüfen. Dann klicken Sie mit der rechten Maustaste in den umrandeten Speicherbereich, auf **Formatieren als** und **ntfs**. Nach Klicks

auf **Bearbeiten, Alle Operationen ausführen, Anwenden** und **Schließen** ist der Stick neu formatiert.



NOTFALL-ARBEITSPLATZ

Startet Windows nicht, bleiben Sie dank der Notfall-DVD produktiv. Im **Anwendungsmenü 5** unter **Büro** finden Sie unter anderem das Softwarepaket **Libre-Office**. Möchten Sie damit zum Beispiel eine unter Windows begonnene Word-Datei bearbeiten, binden Sie das Laufwerk wie auf Seite 46 beschrieben „schreibbar“ ein. Liegt die Datei etwa im Dokumentenordner, klicken Sie auf **Datei öffnen 8**, im Beispiel **sda3** für das Windows-Laufwerk, je doppelt auf **Users**, Ihren Benutzerordner, **Documents** und die Datei. Nehmen Sie nun die Änderungen vor. Zum Speichern klicken Sie auf **Datei, Speichern** und gegebenenfalls **Microsoft Word...** Im Anschluss schließen Sie Libre-Office mit **X** und lösen das Laufwerk wieder.



TIEFEN-SCAN

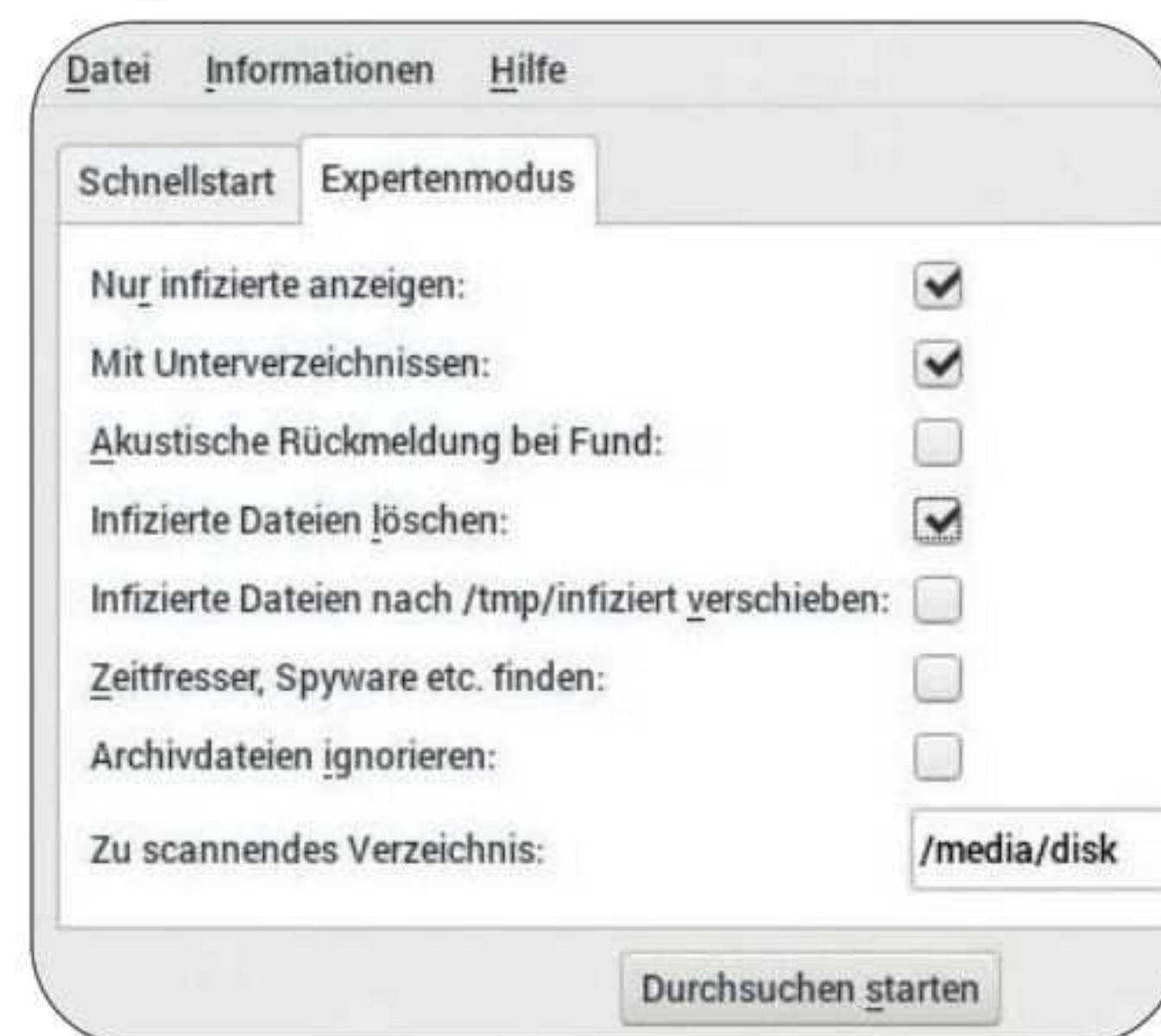
So nutzen Sie den Virens Scanner der Notfall-DVD (Seite 40) für eine Intensiv-Prüfung:

1 Scanner starten: Klicken Sie im **Anwendungsmenü 5** auf **Rettungswerkzeuge** und **ClamAV**. Möchten Sie

Virenfunde nur anzeigen, lassen Sie die folgende Einstellung unverändert und klicken auf **Weiter**. Andernfalls klicken Sie zuvor auf **Alle NTFS- und FAT-Laufwerke automatisch schreibbar einbinden**.

2 Updates holen: Klicken Sie auf **Yes**, um die Virensignaturen zu aktualisieren. Warten Sie, bis das folgende Fenster verschwindet. Nach einem Klick auf **Expertenmodus** passen Sie die Scan-Einstellungen zum Beispiel wie im Bild unten an.

3 Scan starten: Klicken Sie auf **Durchsuchen starten**. Die Prüfung dauert je nach Einstellung etwa drei- bis zehnmal so lange wie im Assistenten. Am besten lassen Sie sie über Nacht laufen. Erscheint beim Abschluss die Meldung „Beendet mit Code 0“, sind die Laufwerke virenfrei, bei „Code 1“ wurden Viren gefunden. Beachten Sie die Hinweise.



INSTALLATION & REGISTRIERUNG

Rufen Sie bis zum 15. Oktober 2022 die Seite **vorteilcenter.de** auf, geben Sie den Vorteilcenter-Code von der Heft-DVD-Hülle ein, und klicken Sie auf **eingeben**. Als Nächstes laden Sie die Internetseite **http://my.steganos.com** und registrieren ein kostenloses Benutzerkonto oder melden sich in einem bestehenden Konto an. Dann installieren Sie die Software von der Heft-DVD. Anschließend loggen Sie sich ins erstellte Konto ein. Jetzt melden Sie sich auf der Webseite **http://my.steganos.com** erneut an, klicken auf **Steganos Privacy Suite**, **Seriennummer eingeben**, fügen den kopierten Code ein und klicken auf **Einlösen**. Starten Sie schließlich noch die Privacy Suite neu, und wählen Sie **Aktualisieren**.

INTERNET:
www.steganos.com

STEGANOS PRIVACY SUITE 22

DATEN SICHER VERWAHREN

Mit der Privacy Suite von Steganos schützen Sie Ihre
Passwörter und Daten vor fremden Blicken.

Die Privacy Suite ist das Schutzpaket gegen neugierige Blicke von Fremden und Freunden. Dank Datensafe und Passwort-Tresor sind Ihre persönlichen Daten vor dem Zugriff durch Dritte abgeschirmt.

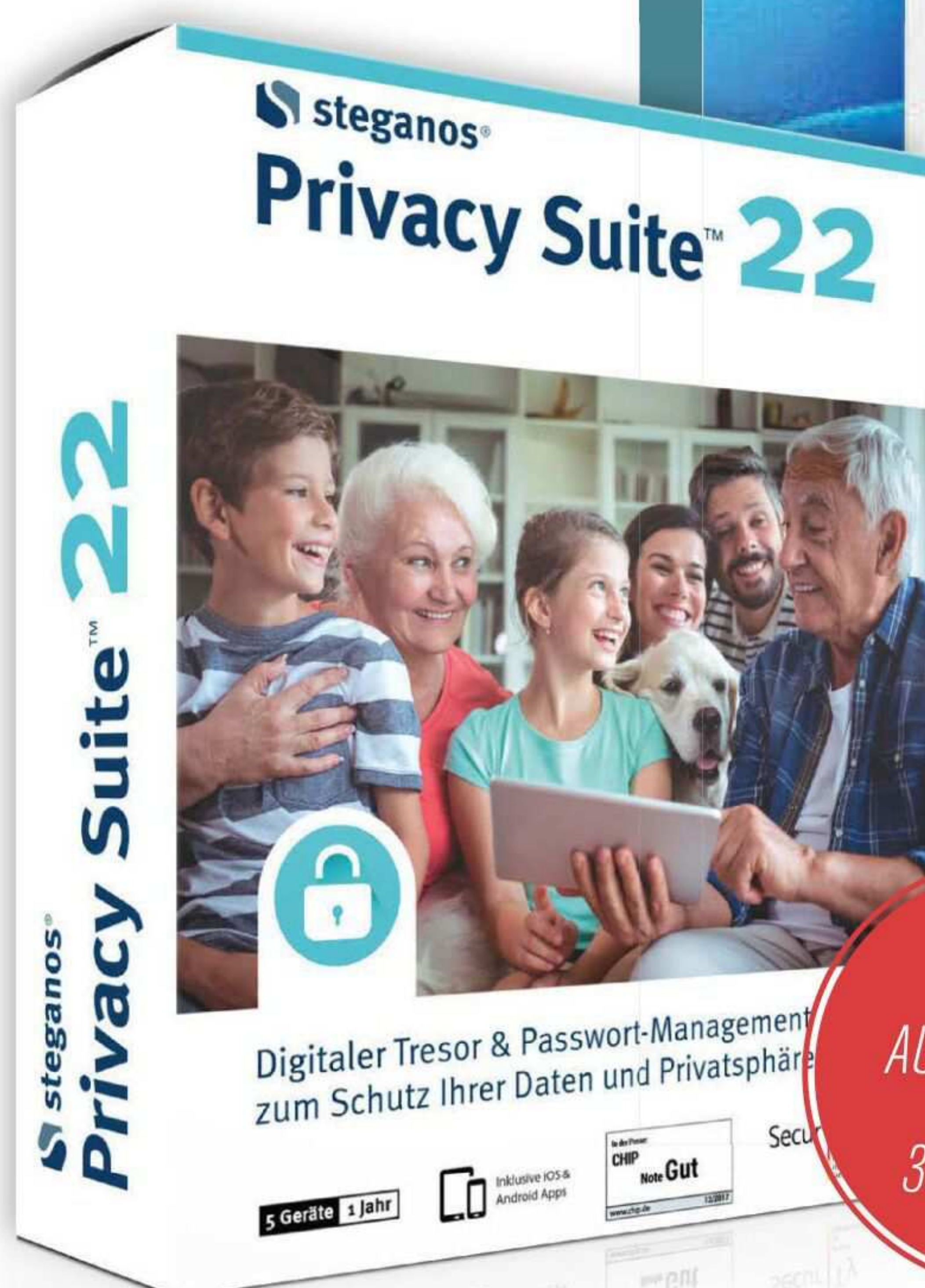
Sie haben die Wahl, ob Sie den Datensafe auf der Festplatte, einem USB-Stick oder in einem Cloud-Speicher einrichten. Auch innerhalb von Dateien versteckte Safes sind möglich. Einmal eingerichtet, bleibt Ihre Privatsphäre geschützt – selbst wenn Ihr Notebook in fremde Hände fällt oder wenn Freunde und Bekannte damit arbeiten. Die Vollversion von

Steganos erhalten Sie für ein Jahr kostenlos. Auch danach können Sie angelegte Safes und Passwort-Listen weiter öffnen.

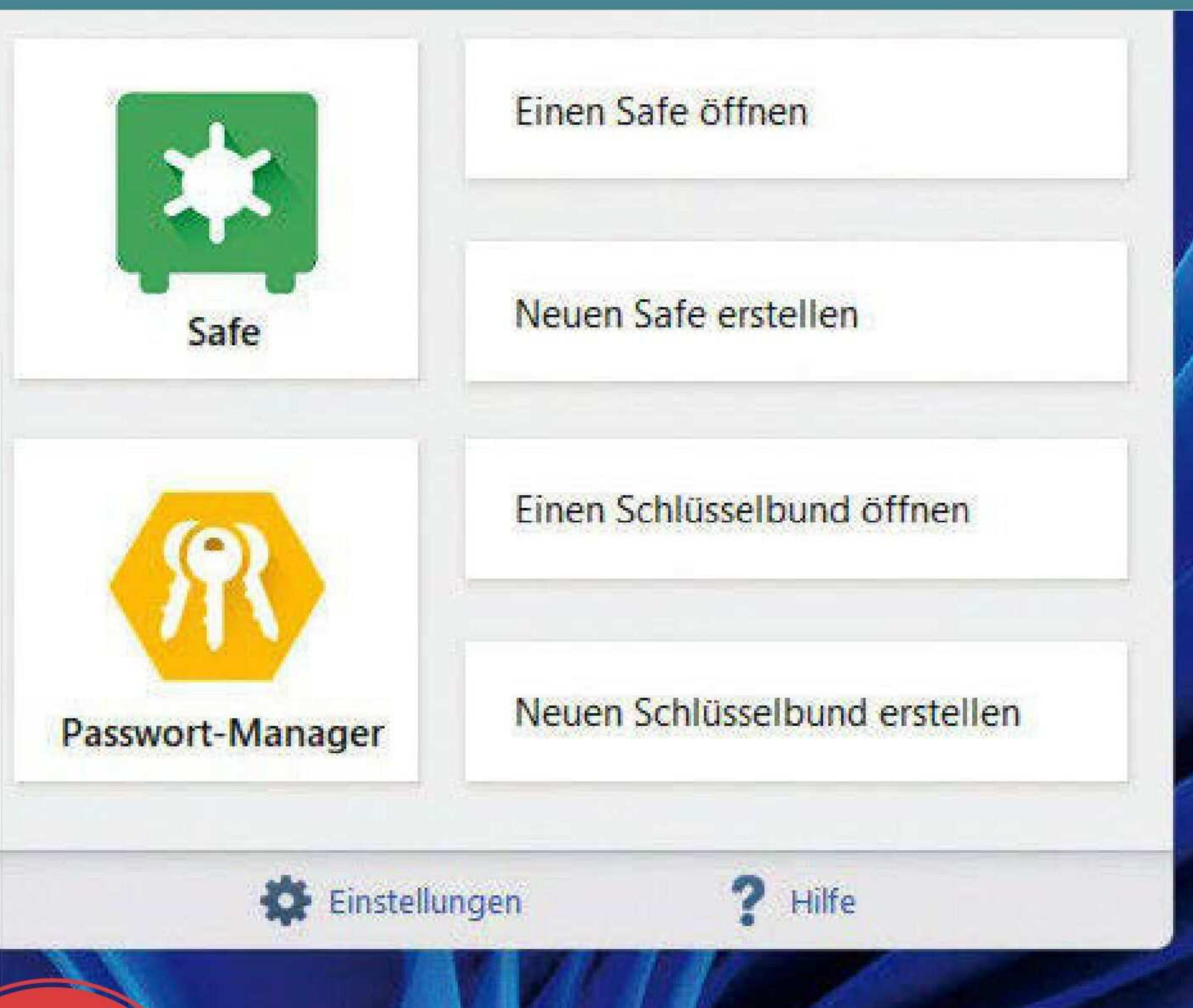
Viele Neuerungen

Die brandneue Version 22 bringt einige Neuerungen mit. So ist der in der Vorversion weggefallene Datenschredder jetzt wieder an Bord. Haben Sie etwa eine Datei sicher im Safe gespeichert, schreddern Sie damit die ungeschützte Kopie. Um sicherzugehen, dass sich gelöschte vertrauliche Dateien nicht wiederherstellen lassen, können Sie damit außerdem freien Speicherplatz

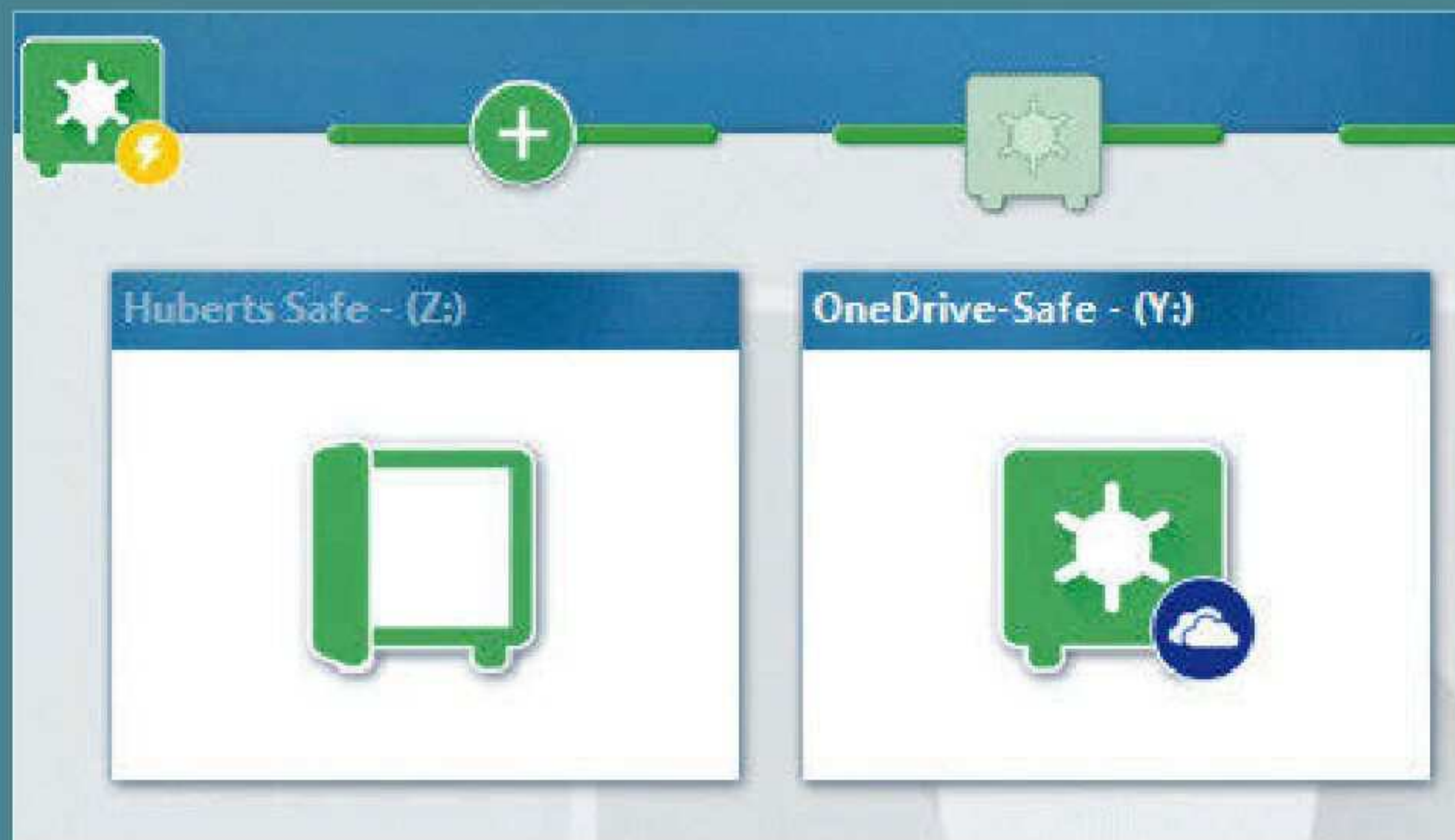
auf der Festplatte überschreiben. Neu ist die Möglichkeit, bei der Safe-Erstellung ein Notfallpasswort zu wählen, das Sie dann etwa beim Notar hinterlegen. Im Fall der Fälle kann eine Person Ihres Vertrauens damit den Inhalt Ihres Safes einsehen. Aus Sicherheitsgründen lässt sich das Notfallpasswort nicht nachträglich einrichten oder ändern, und es ermöglicht keine Änderungen am Inhalt des Safes. Zudem gibt's verbesserte Browser-Add-ons, mehr Übersicht im Passwort-Manager, einen Indikator für die Passwort-Stärke, eine Hilfsfunktion zur Datensicherung und mehr. [bp]



GRATIS
AUF HEFT-DVD
STATT
39,99 EURO*



Vom Hauptfenster des Programms aus starten Sie alle Programmteile der Steganos Privacy Suite. Obwohl es sehr übersichtlich ist, stecken eine Menge Funktionen dahinter.



Einrichtung eines Safes

Welchen Safe möchten Sie erstellen?

- ➔ Ich möchte nur Daten auf diesem Computer oder einem Netzlaufwerk verschlüsseln.
- ➔ Ich möchte verschlüsselte Daten in meiner Dropbox, meinem Google Drive, meinem Microsoft OneDrive oder meiner MagentaCLOUD ablegen.
- ➔ Ich möchte einen Portable Safe auf einem USB-Stick oder einer externen Festplatte ablegen.
(Mehr erfahren)
- ➔ Ich möchte eine Festplatten-Partition zu einem Safe machen.
(Erfahrung mit Partitionen empfohlen)

SAFE FÜR IHRE DATEN EINRICHTEN

1 Um einen Datensafe anzulegen, klicken Sie auf **Safe** und das Plus. Wählen Sie, ob Sie den Tresor auf der Festplatte, einem USB-Stick oder in der Cloud erstellen wollen. Alternativ lässt sich eine bestehende Partition verschlüsseln.

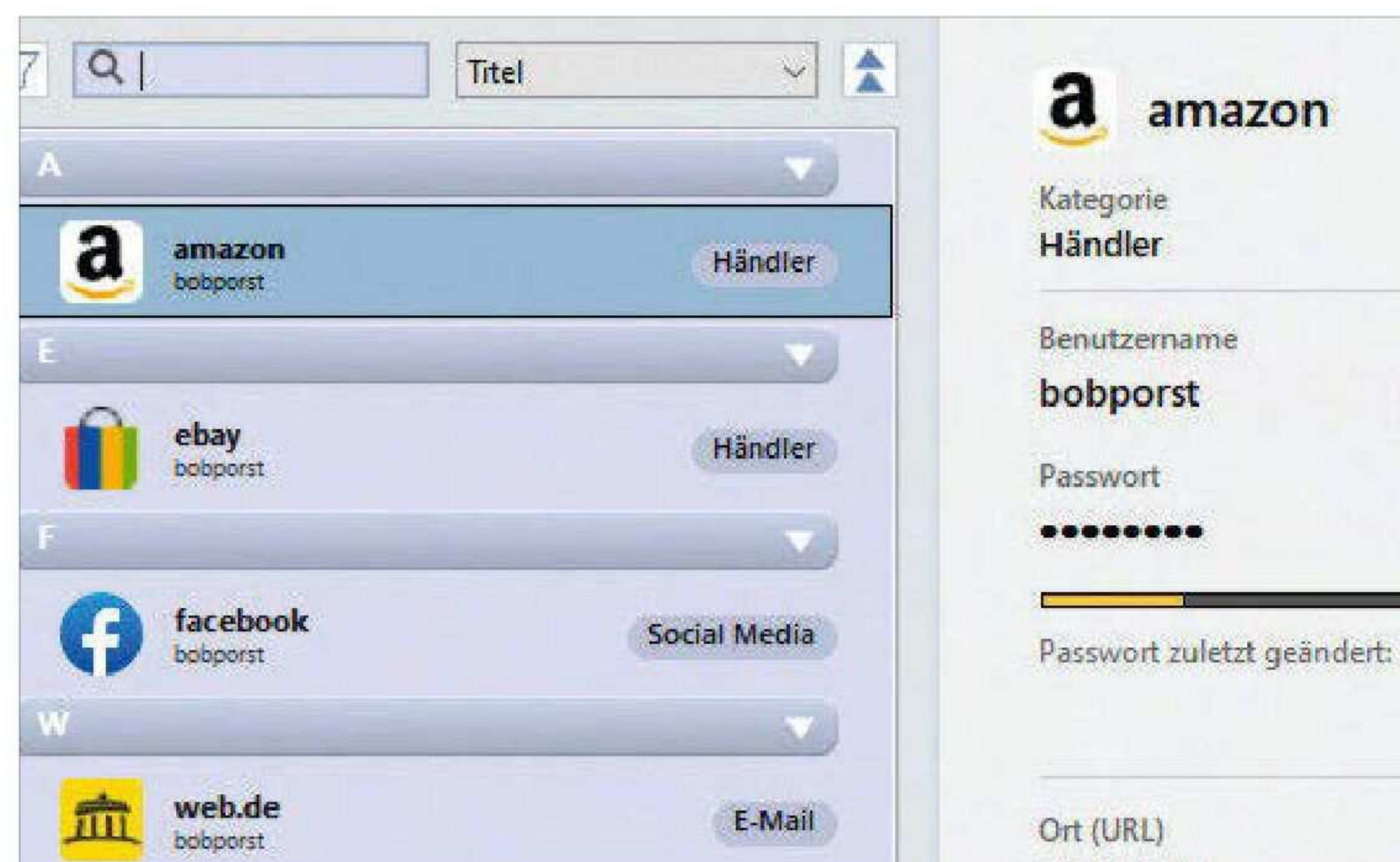
2 Für einen lokalen Datentresor klicken Sie auf den obersten Pfeil und geben einen Namen ein, klicken zweimal auf **Weiter** und setzen einen Haken bei „Laufwerk wächst dynamisch“. So passt sich die Größe des Tresors automatisch an.

3 Jetzt klicken Sie auf **Weiter**, wählen ein Passwort, klicken auf **Weiter**, **OK**, **Ja** und **Fertigstellen**. Der Safe erscheint in der Übersicht. Um ihn im Windows-Explorer zu öffnen, klicken Sie darauf, geben das Passwort ein und klicken auf **OK**. Ziehen Sie nun alle wichtigen Dateien und Ordner hinein, und schließen Sie den Safe per Klick darauf.

PASSWÖRTER VERSCHLÜSSELN

Im Passwort-Manager sind Ihre Zugangsdaten sicher aufgehoben. Merken müssen Sie sich künftig nur noch ein einziges Master-Passwort. Wenn Sie eine Ihrer Lieblingsseiten besuchen, melden Sie sich dank Steganos ganz einfach an. So einfach geht's: Klicken Sie im Hauptfenster auf **Neuen Schlüsselbund erstellen**. Geben Sie einen Namen ein, klicken Sie auf **OK**, und vergeben Sie das Master-Kennwort, das künftig als Generalschlüssel dient. Nach zwei Klicks auf **OK** und **Passwort-**

Manager tippen Sie das Master-Passwort ein und bestätigen mit zwei Klicks auf **OK**. Um nun Zugangsdaten zu speichern, klicken Sie aufs **Plus**-Symbol, füllen die Felder aus und klicken auf **OK**. Die Anmeldung auf Webseiten mit Zugangsdaten aus Ihrem Safe klappt am besten mit den Browser-Erweiterungen von Steganos. Um die einzurichten, klicken Sie auf **Hilfe, Browser-Erweiterungen installieren...** und folgen den weiteren Anweisungen auf dem Bildschirm.



FREIEN SPEICHER SCHREDDERN

Den Windows-Papierkorb zu leeren, klappt in der Regel blitzschnell. Der Grund: Das Betriebssystem löscht die enthaltenen Dateien nicht vollständig von der Festplatte, sondern markiert nur den von ihnen belegten Speicherplatz als frei für neue Daten. Nicht selten ist daher eine komplette Wiederherstellung möglich, was im Fall von vertraulichen Dateien katastrophal sein kann. Damit sensible Daten nicht auf diesem Weg in die falschen Hände

NEU:
DATEN-
SCHREDDER



fallen, sorgen Sie mit Steganos Shredder vor: Das Programm überschreibt auf Wunsch den freien Speicherplatz und macht so eine Wiederherstellung praktisch unmöglich. So einfach geht's:

Klicken Sie im Hauptmenü des Programms auf **Safe** und oben auf das rote Schredder-Symbol. Im neuen Fenster klicken Sie auf **OK**, anschließend auf **Free-Space-Shredder**, gegebenenfalls zweimal auf **Ja** und dann auf **Start**.

Fotos: iStock; Montage: COMPUTER BILD

SCHUTZ FÜR ALLE IHRE D

Ihre privaten Dateien gehen niemand etwas an. Mit diesem Programm schützen Sie Ihre Dokumente vor fremdem Zugriff!

Jeder hat Dateien auf dem PC, die niemand anders etwas angehen. Das können zum Beispiel Rechnungen oder Kontoauszüge sein, private Fotos oder auch Firmengeheimnisse. Mit den Programmen auf dieser Doppelseite

schützen Sie sensible Daten vor fremdem Zugriff – und zwar gleich mehrfach: So sind die Dokumente nicht nur auf Ihrem PC selbst geschützt, Sie können sie bei Bedarf auch sicher an andere verschicken. Und selbst für den

Fall, dass Sie Ihren PC oder die Festplatte einmal verkaufen wollen, können Sie das ohne Sorge um Ihre vertraulichen Daten tun: Das passende Programm zum Beseitigen jeglicher Spuren gibt's ebenfalls auf DVD! [av]

GUARDIAN OF DATA

Kostenlose Registrierung für die Vollversion von **Guardian Of Data**

Schritt 1:

Klicken Sie den folgenden Link und registrieren Sie sich:

[Jetzt registrieren](#)

Schritt 2:

Geben Sie die Kundennummer ein, die Sie nach der Registrierung per E-Mail erhalten haben:

Kundennummer:

Schritt 3:

Laden Sie die Vollversion herunter und installieren Sie diese auf Ihrem Computer:

Private Dateien auf dem heimischen PC sind unsicherer, als Sie vielleicht denken: Cyberkriminelle versuchen mit ausgefeilten Tricks Fernzugriff auf fremde PCs zu erhalten. Aber auch neugierige Kollegen, Kinder oder der Partner spionieren manchmal. Wenn Sie wirklich sicher sein wollen, dass bestimmte Dateien privat bleiben, müssen Sie die entsprechenden Dokumente oder Fotos verschlüsseln. Mit dem genialen Programm „Guardian Of Data“ funktioniert das kinderleicht:

1 Starten Sie die Installation von der Heft-DVD. Klicken Sie dann auf **Jetzt registrieren**, und folgen Sie den Anweisungen, um sich beim Hersteller zu registrieren. Sie erhalten dann eine Kundennummer per E-Mail.

2 Fügen Sie die Kundennummer in das Installationsprogramm ein, und klicken Sie auf **Vollversion herunterladen**.

3 Folgen Sie den Anweisungen, und schließen Sie die Installation ab. Das Programm startet automatisch.

4 Klicken Sie auf **Encrypt, Hinzufügen** und entweder auf **Verzeichnis einlesen** oder **Einzelne Dateien laden**.

5 Wählen Sie die Datei oder das Verzeichnis aus, das Sie nun verschlüsseln wollen. Wiederholen Sie das gegebenenfalls, um weitere Dateien oder Verzeichnisse hinzuzufügen.

6 Nach einem Klick auf **Weiter** bestimmen Sie, ob Sie die Originale oder Kopien der Dateien verschlüsseln wollen und ob die verschlüsselte Datei selbstausführend sein soll. Es folgt ein Klick auf **Weiter**.

7 Legen Sie nun ein Passwort für die verschlüsselten Daten fest, und Starten Sie die Verschlüsselung per Klick auf **Fertig**.



OKUMENTE

FILEWHOPPER

Sie möchten wichtige Dateien verschicken, der Weg per E-Mail ist Ihnen aber zu unsicher? Dann ist FileWhopper genau das Richtige für Sie. Der Dienst verschlüsselt Ihre Daten mit sicherer 256-Bit-AES-Verschlüsselung und lädt sie auf einen Cloud-Speicher hoch. Sie schicken dem Empfänger dann nur noch den Download-Link und teilen ihm das Passwort zum Entschlüsseln des Downloads mit.

Dateien sicher übertragen

1 Um FileWhopper zu nutzen, öffnen Sie die Seite filewhopper.com. Klicken Sie dann auf **Login** und **Register**, und folgen Sie den Anweisungen, um ein kostenloses Konto zu erstellen.

2 Öffnen Sie die Seite erneut und klicken Sie auf **Choose file** or **Choose folder**, um eine Datei oder einen Ordner hochzuladen. Folgen Sie den Anweisungen.

Transfer ID: h9neq075kXbJfpe6 File size: 2,56 MB Paid: \$0,99

To secure the transfer, your file will be encrypted with a password

***** >> PROCEED WITH UPLOAD

☐ Save the password to my desktop as a .txt file

☐ Shut down PC when upload completes
☒ Automatically launch app and resume transfer upon PC reboot

© 2019-2021 FileWhopper. My Account Terms How It Works [START NEW UPLOAD](#)

3 Der erste Transfer ist kostenlos, ab dem zweiten Transfer fallen Gebühren an. Als Leser dieses Sonderhefts bekommen Sie aber ein Volumen von 100 GB gratis. Dazu



müssen Sie nach Auswahl der Datei auf **Confirm & Pay** klicken, Ihre Postleitzahl eintragen und auf **Fortfahren** sowie **Gutschein hinzufügen** klicken. Tragen Sie **CMPTBLD100** (gültig bis zum 31. 10.

2022) ein, und folgen Sie den weiteren Anweisungen. Hinweis: Sie benötigen diesen Code für jede Übertragung, speichern Sie ihn daher in einer Textdatei.

SAFE ERASE

Wenn Sie Dateien mit Windows löschen, sind die Daten nicht wirklich gelöscht – der Speicherplatz wird lediglich für die künftige Verwendung freigegeben. Datenrettungsprogramme können die gelöschten Daten wiederherstellen, solange sie nicht überschrieben wurden. Möchten Sie Ihre Festplatte oder Ihren PC verkaufen, sollten Sie private Daten darauf lieber mit Safe Erase löschen. Die Software überschreibt den Speicherplatz mehrfach mit Zufallsdaten, so dass ein Wiederherstellen unmöglich wird. Um Safe Erase freizuschalten, öffnen Sie die Seite www.oo-software.com/de/special/ste871,

tragen Ihre E-Mail-Adresse ein und klicken auf **Kostenlose Lizenz anfordern**. Sie erhalten daraufhin eine E-Mail. Klicken Sie auf den enthaltenen Bestätigungslink. Die Registrierung ist dann abgeschlossen, und Sie erhalten in den nächsten Stunden Ihre Seriennummer. Kopieren Sie diese Nummer, installieren und starten Sie das Programm. Wählen Sie „Ich möchte meine Lizenz eingeben“, tragen Sie bei Name und Firma die verwendete E-Mail-Adresse ein sowie die erhaltene Seriennummer in das entsprechende Feld, klicken Sie erneut auf **Weiter**, und folgen Sie den Anweisungen.



* Preis laut Hersteller



Tellows
Caller ID & Blocker

AN iPh

Preis der Standard-App:
gratis

Ihr App-Paket-Vorteil:
■ Kaufversion 1 Jahr
kostenlos

Wert AN 4,99 Euro
iPh 9,99 Euro

SO KOMMEN SIE RAN

Die Kaufversion gibt's gratis¹ im COMPUTER BILD-App-Center – das öffnen Sie per Handy-Scan des QR-Codes auf der DVD-Hülle:

■ **Android:** Die meisten Handys haben einen QR-Code-Leser. Sonst tippen Sie in der Idealo-App aufs Scan-Symbol, scannen den Code und wählen **Öffnen**.

■ **iOS:** Scannen Sie den Code per Kamera-App, und tippen Sie auf den Link.

App vorbereiten: Tippen Sie im COMPUTER BILD-App-Center auf **tellows**. Überprüfen, installieren und öffnen Sie die App.

■ **Android:** Tippen Sie auf die drei Balken und auf **Log-in**. Falls Sie keins haben, erstellen Sie ein Open-ID-Profil für die Tellows-Anmeldung. Tippen Sie gegebenenfalls oben mittig unter dem Tellows-Schriftzug auf **Berechtigungen fehlen** und folgen den Anweisungen. Tippen Sie dann auf die drei Balken und auf **Aktiviere Premium**. Nun geben Sie im Gutschein-Textfeld den Premiumcode **cb22tel** ein, tippen auf **Gutschein einlösen** und **OK**. Wählen Sie **Kaufe Premium**, **Zustimmen** und **Kaufen**. Bestätigen Sie das (Gratis-)Abo, gefolgt von **OK**.

■ **iOS:** Öffnen Sie die Seite **cobi.de/go/tel22** und tippen Sie bei „Apple Code erhalten“ den Code **cb22tel** ein, um einen individuellen Code zu erhalten. Tippen Sie rechts unten auf **Pro** und auf **Gutscheincode** und geben Sie Ihren individuellen Code ein. Schließen Sie dann das Gratis-Abo ab. Achtung: Bezahlungen sind zwar nötig, aber es entstehen keine Kosten.



Das Handy klingelt mit unbekannter Festnetznummer und am anderen Ende: ein dubioser „Energieberater“, der Ihnen zum x-ten Mal einen Stromvertrag andrehen möchte. Aber woher haben solch unseriöse Telefonagenturen Ihre Kontaktdaten überhaupt? Dahinter stecken oft vorschnell gesetzte Haken bei

Datenschutzbestimmungen zweifelhafter Webseiten, gedankenlos im Netz geteilte Kontaktdaten oder schlichtweg: Datenhandel. Keine Sorge: Mit Tellows weisen Sie lästige Werbeanrufe einfach ab.

Einer für alle, alle für einen

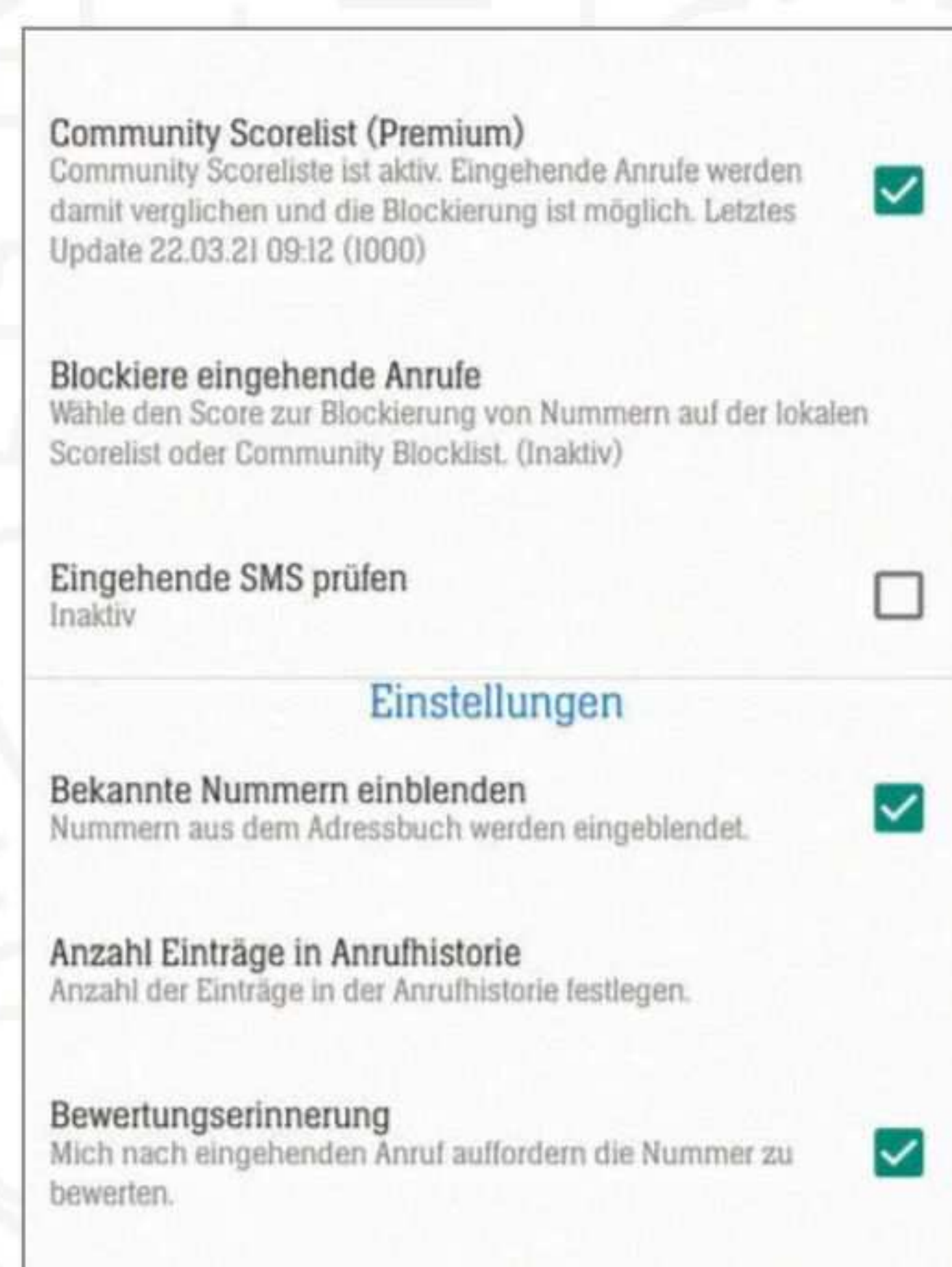
Hinter dem Tellows-Spamschutz steckt eine große Community

gebeutelter Telefonwerbe-Opfer. Die App zeigt daher auch bei Ihnen völlig unbekannten Nummern, wer dahintersteckt. Neben Infos zum Namen und Standort erscheint beim Klingeln auch der sogenannte Tellows-Score, der sich aus den Bewertungen von mehr als 200 000 Nutzern zusammensetzt. In der Datenbank ge-

SO LÄUFT DER TELEFON-SPAMSCHUTZ MIT TELLOWS:



VORBEREITEN (iPH): Öffnen Sie die **Einstellungen** von iOS. Tippen Sie auf **Telefon, Anrufe blockieren und identifizieren** und den Schalter bei Tellows.



VORBEREITEN (AN): Tippen Sie auf den Pfeil, die drei Balken und auf **Einstellungen**. Tippen Sie auf **Bekannte Nummern einblenden**.



BLOCKADE EINSTELLEN (iPH): Tippen Sie in Tellows auf **Einstellungen** und unter „Blockierung“ auf **Score**. Wählen Sie Grenzwert 7 und **Fertig**.

¹ Aus technischen Gründen kann sich die Verfügbarkeit der Apps verzögern. Alle Premiumvorteile lassen sich bis zum 15. 10. 2022 freischalten. Die Apps benötigen aktuelle Betriebssystem-Versionen, also mindestens Android 7.0 beziehungsweise iOS 11.

WERBEANRUF-BLOCKER

Werbeanrufe können schnell zum Telefonterror ausarten – erst recht wenn sich unseriöse Anrufer mit unbekannten Festnetznummern tarnen. Die App Tellows verrät schon beim Klingeln, wer dahintersteckt, und sperrt unerwünschte Anrufer.

meldete oder abgefragte Rufnummern haben einen Score zwischen 1 und 9 – je höher der Wert, desto dubioser der Anrufer.

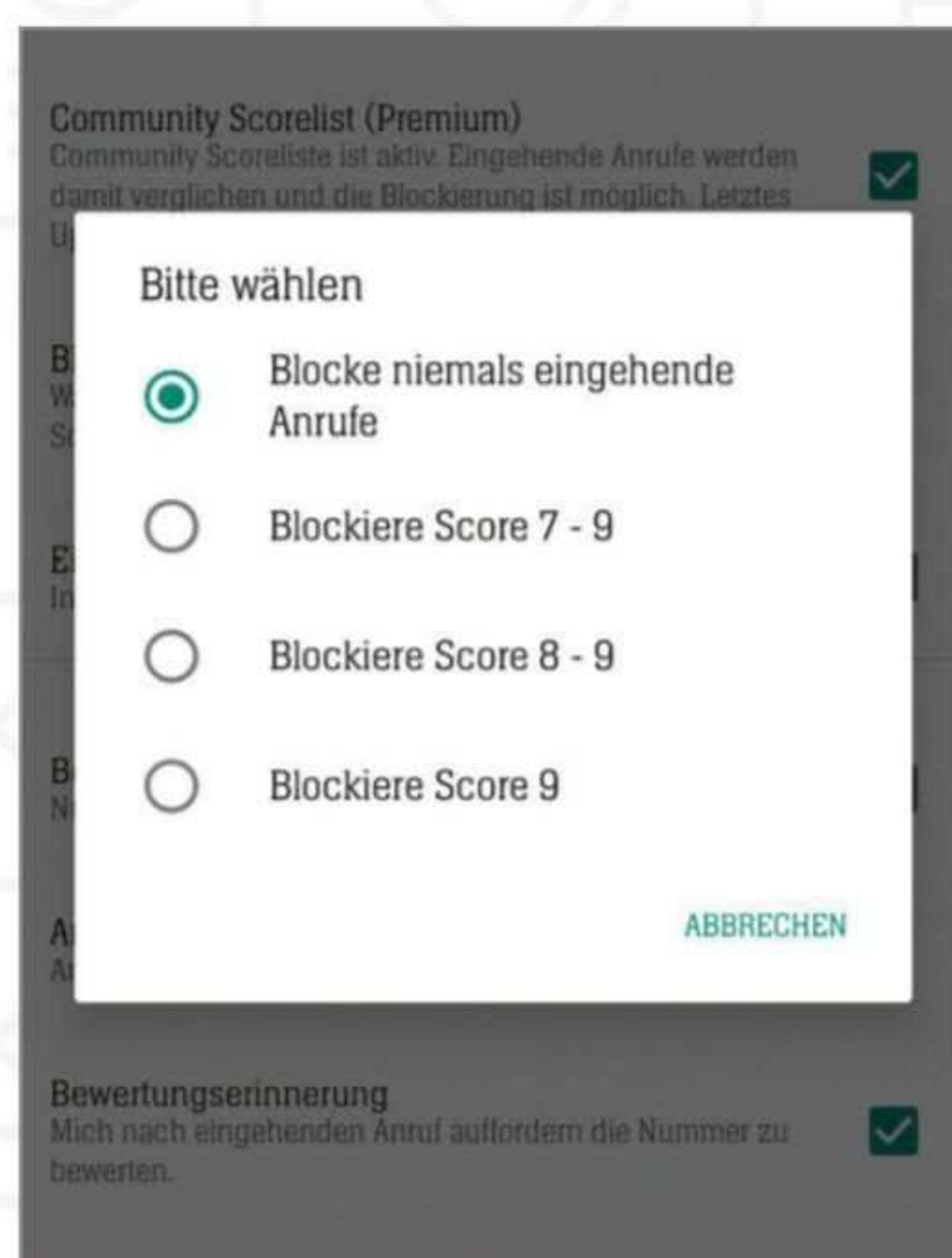
Automatischer Spamfilter

Neben den Bewertungen betroffener Nutzer berücksichtigt Tellows auch die Anzahl der Bewertungen und wie oft eine Nummer

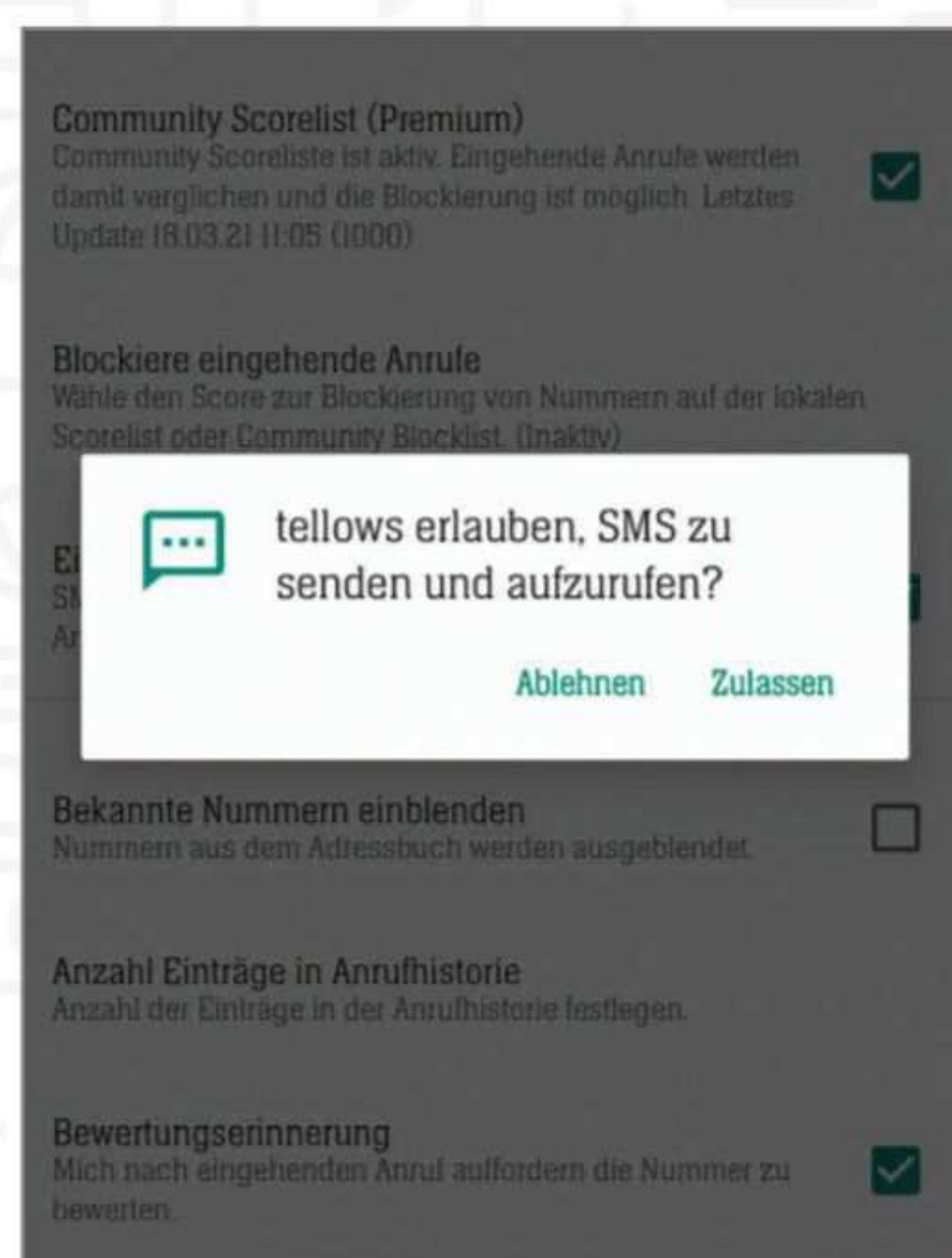
gesucht wurde. Dies soll verhindern, dass vereinzelte Meldungen seriöse Anbieter in Misskredit bringen. Als Leser dieses Sonderhefts bekommen Sie die Kaufversion von Tellows für ein Jahr kostenlos – iPhone-Besitzer sparen 9,99 Euro, Android-Nutzer 4,99 Euro. Die werbefreie Variante informiert auch ohne Internetver-

bindung detailliert über die Anrufer. Die App kümmert sich auf Wunsch auch gleich selbstständig um die Abfertigung dubioser Anrufer: Sie legen einfach einen Maximalwert für den Tellows-Score fest. Die App blockt dann alle Anrufe mit einem höheren Wert und informiert im Anschluss über den Anrufversuch.

Als Android-Besitzer prüfen Sie zudem eingehende SMS auf die Seriosität des Absenders. Praktisch, denn inzwischen schicken Betrüger täuschend echte SMS mit Phishing-Links als vermeintliche Versandinfos zu bestellten Paketen. Unten in den Tipps lesen Sie, wie Sie die Profi-Funktionen in der App einstellen. [tv]



BLOCKADE EINSTELLEN (AN): Tippen Sie in den *Einstellungen* auf **Blockiere eingehende Anrufe** und den Wert 7–9 in der Liste.



SMS SCHÜTZEN (NUR AN): Tippen Sie in den *Einstellungen* auch auf **Eingehende SMS prüfen**. Bestätigen Sie mit **Zulassen**.



MITMACHEN: Tippen Sie auf einen Anruf in der Liste, **Bewerten/Blockieren** und **Nummer bewerten** (An) oder **Bewerte Nummer** (iPh).

KÜNDIGUNG NICHT VERGESSEN

Nach Ablauf des Gratisjahres verlängert sich das Abo kostenpflichtig. Möchten Sie das nicht, kündigen Sie es wie folgt:

■ **Android:** Tippen Sie im *Play Store* auf Ihr Foto rechts oben, **Google-Konto verwalten, Zahlungen & Abos**. Es folgen Tipper auf **Abos, tellows – Anruferkennung & Blockierung, Abo kündigen, Keine Angabe, Weiter** und **Abo kündigen**.

■ **iPhone:** Tippen Sie im *App Store* rechts oben aufs Porträt. Wählen Sie **Abonnements, tellows Caller ID & Blocker, Kostenloses Probeabo kündigen** und **Bestätigen**.



Cryptomator **AN**

Preis der Standard-App:

9,99 Euro

Ihr App-Paket-Vorteil:

App gratis

Wert: 9,99 Euro

SO KOMMEN SIE RAN

Den Premium-Code für die Android-Version von Cryptomator gibt es gratis* im COMPUTER BILD-Vorteilcenter. Öffnen Sie **vorteilcenter.de** am PC. Geben Sie den Vorteilcenter-Code von der Hülle der Heft-DVD ein, und klicken Sie auf **eingeben**. Notieren Sie den angezeigten Code.

Lizenzkey erhalten: Öffnen Sie am Handy die Internetseite **cryptomator.org/de/android**, und geben Sie Ihre E-Mail-Adresse ein. Akzeptieren Sie die AGB, und wählen Sie **Zur Zahlung**. Ergänzen Sie die Ortsinfo, und tippen Sie auf **Fortfahren**. Im nächsten Fenster tippen Sie links oben auf **Gutschein hinzufügen** und tippen den zuvor notierten Gutschein ein. Tippen Sie dann auf **Gutschein hinzufügen** sowie **Checkout abschließen**. Im nächsten Fenster tippen Sie unter „APK herunterladen“ auf **Download** und überspielen die App.

App freischalten: Sie erhalten den Lizenzschlüssel per Mail. Achtung: Die Mail des Absenders „Cryptomator for Android“ kann auch im Spam-Ordner landen. Öffnen Sie die Mail am Handy, und kopieren Sie den Lizenzschlüssel in den Zwischenspeicher. Öffnen Sie nun die installierte App, und fügen Sie den kopierten Lizenzschlüssel ein. Tippen Sie abschließend zweimal auf **OK**.

DATEN- SCHÜTZER FÜR DIE CLOUD

Verträge und Dokumente immer dabei und sicher verpackt? Mit Cryptomator speichern Sie Ihre wichtigen Unterlagen direkt verschlüsselt in Ihrer Cloud und haben Sie so sicher griffbereit.

Arbeitszeugnisse, Bescheinigungen fürs Amt oder Kopien von Verträgen sind im Alltag nur selten gefragt. Wenn doch, dann ist es aber häufig dringend und wichtig. Damit die Dokumente auf Abruf parat sind, lagern sie viele Menschen mittlerweile auf dem Smartphone oder in Cloud-Speichern wie OneDrive & Co.

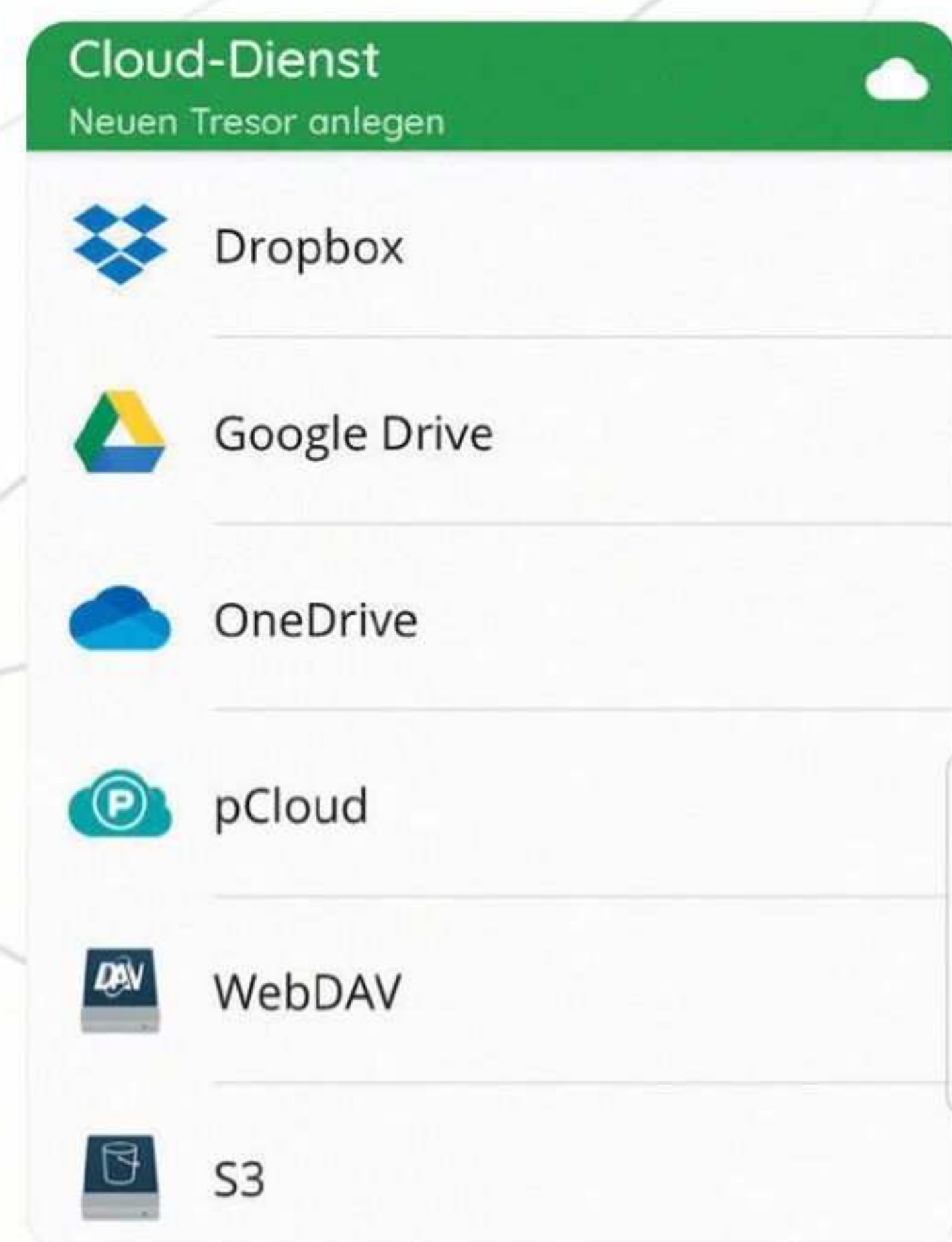
Das einzige Problem: In vielen Fällen sind die sensiblen Daten dort ungeschützt.

Digitale Sicherheitsverpackung

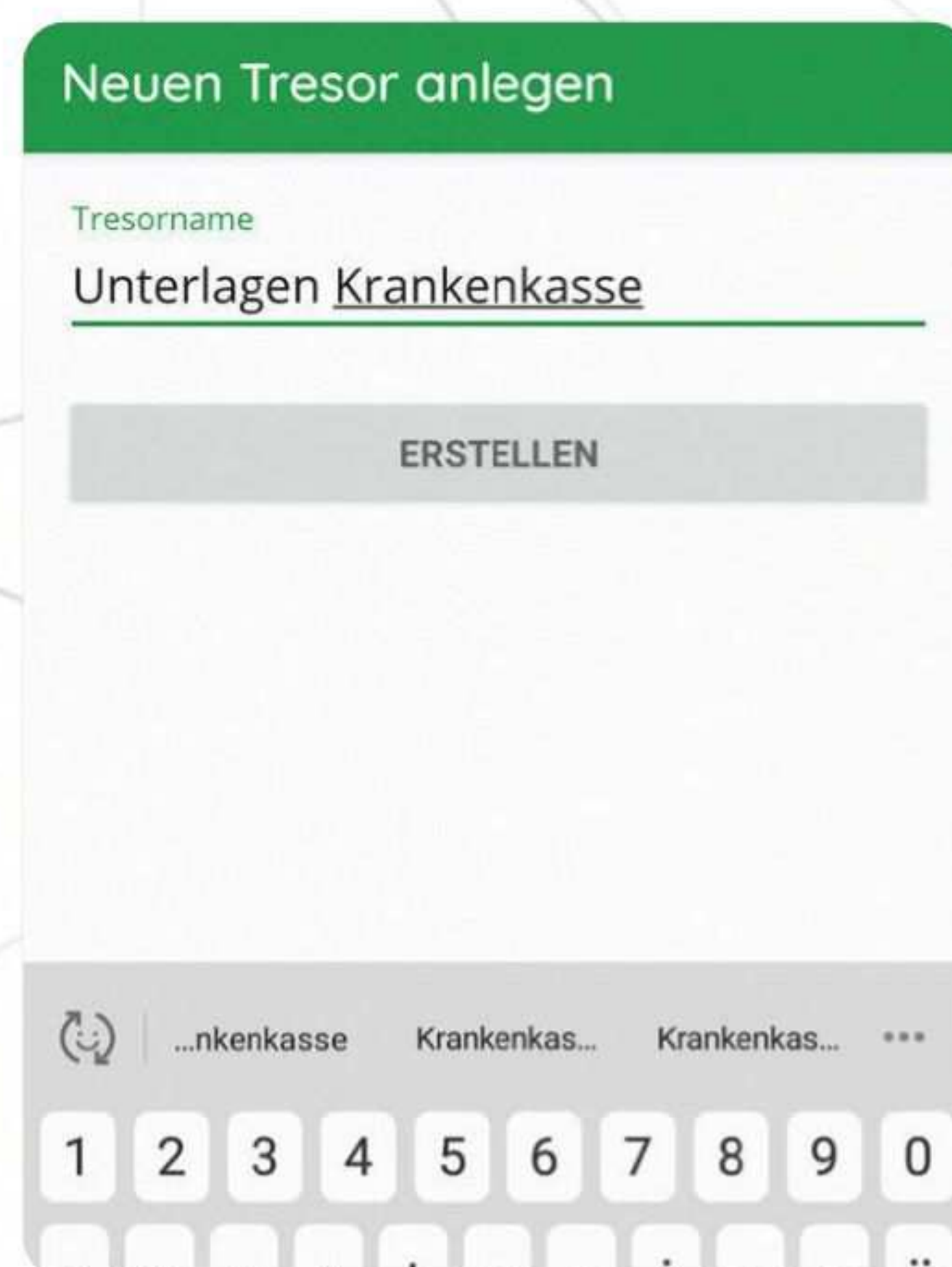
Mit dem Cryptomator sorgen Sie dafür, dass Ihre Dokumente für Dritte unlesbar sind – auch wenn die Zugriff auf Ihre Cloud erlangen sollten. Ihren Datentresor in

der Cloud befüllen Sie bei allen beliebten Diensten: etwa Google Drive, Dropbox, OneDrive und auch sogenannten WebDAV-basierten Cloud-Anbietern. Der Online-Datentresor ist per AES-Algorithmus mit einer Schlüssellänge von 256 Bit so gut wie unknackbar und nur mit Ihrem persönlichen Passwort zu öffnen.

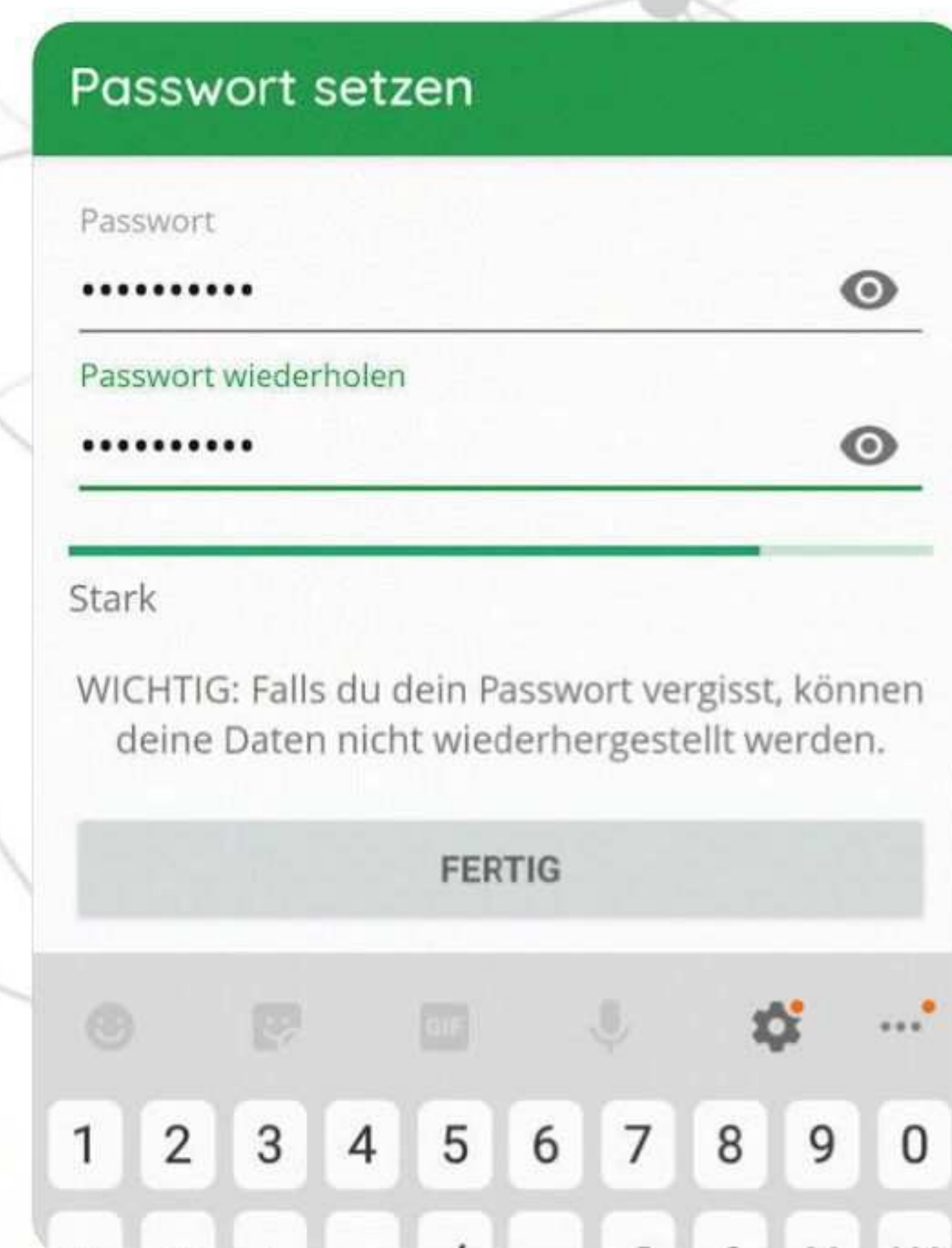
TRESOR EINRICHTEN AUF ANDROID



EINRICHTEN: Tippen Sie unten aufs **+**-Symbol sowie **Neuen Tresor anlegen** und Ihre Cloud, etwa **OneDrive**. Melden Sie sich nach Tipper aufs **+** an.



SPEICHERWAHL: Tippen Sie auf das angemeldete Cloud-Konto. Dann tippen Sie den Namen für den Tresor ein, auf **Erstellen** und auf den Zielordner.



ABSPERREN: Wählen Sie nach **Hier ablegen** ein Passwort und **Fertig**. Zur Anzeige geben Sie später das Passwort ein und tippen auf **Entsperren**.

*Die Ausgabe von Premium-Codes erfolgt, solange der Vorrat reicht. Aus technischen Gründen kann sich die Verfügbarkeit der Apps verzögern. Alle Premiumvorteile lassen sich bis zum 15. 10. 2022 freischalten. Die Apps benötigen aktuelle Betriebssystem-Versionen.



Cryptomator 2 **iPh**
Preis der Standard-App:
gratis
Ihr App-Paket-Vorteil:
Kaufversion 1 Jahr gratis
Wert: 5,99 Euro

SO KOMMEN SIE RAN

Den Premium-Code für die iPhone-Version von Cryptomator 2 gibt es gratis* auf **vorteilcenter.de**. Geben Sie den Vorteilcenter-Code von der Hülle der Heft-DVD ein und klicken Sie auf **ein-geben**. Notieren Sie den angezeigten Code. Scannen Sie dann mit der Kamera-App des iPhones den QR-Code auf der DVD-Hülle, und tippen Sie auf den Link.

App installieren: Tippen Sie im COMPUTER BILD-App-Center auf **Cryptomator 2**. Installieren Sie die App, und öffnen Sie sie.

App freischalten: Öffnen Sie am Handy **cobi.de/go/cr2**, und wählen Sie **Öffnen**. Geben Sie den Code ein, und tippen Sie auf **Enter** sowie auf **Angebot einlösen**. Bestätigen Sie das Abo. Tippen Sie auf **Cryptomator 2 öffnen** und in der App auf **Weiter**. Das Abo kündigen Sie am iPhone mit Tippen auf **Einstellungen**, Ihren Namen, **Abonnements**, **Cryptomator 2**, **Abo kündigen** und **Bestätigen**.

Falls vorhanden, nutzen Sie dazu auch die biometrischen Entsperrfunktionen Ihres Handys – also Fingerabdruck- oder Gesichtsscan.

Unterschiede auf Android & iOS

Als Leser von COMPUTER BILD bekommen Sie den Cryptomator gratis – der Wert und der Umfang der Funktionen richten sich nach

Ihrem Smartphone: So gibt es für Android-Nutzer die lebenslange Version im Wert von 9,99 Euro kostenlos. iPhone-Nutzer erhalten eine Jahresversion im Wert von 5,99 Euro, dafür aber von der moderneren App-Version Cryptomator 2. Auch die verstaut Ihre Dokumente sicher vor fremden Zugriffen im Datentresor.

Darüber hinaus ist sie direkt in die Apple-eigene Dateien-App eingebaut. So müssen Sie Cryptomator 2 auf iOS nicht jedes Mal öffnen. Stattdessen verschlüsseln Sie Daten zentral aus der Dateien-App. Wichtig: Wenn Sie kein Folgeabo für 5,99 Euro bei der iOS-Version wünschen, müssen Sie vor Ende des Gratisjahres kündigen. [tv]

TRESOR ERSTELLEN AM iPHONE



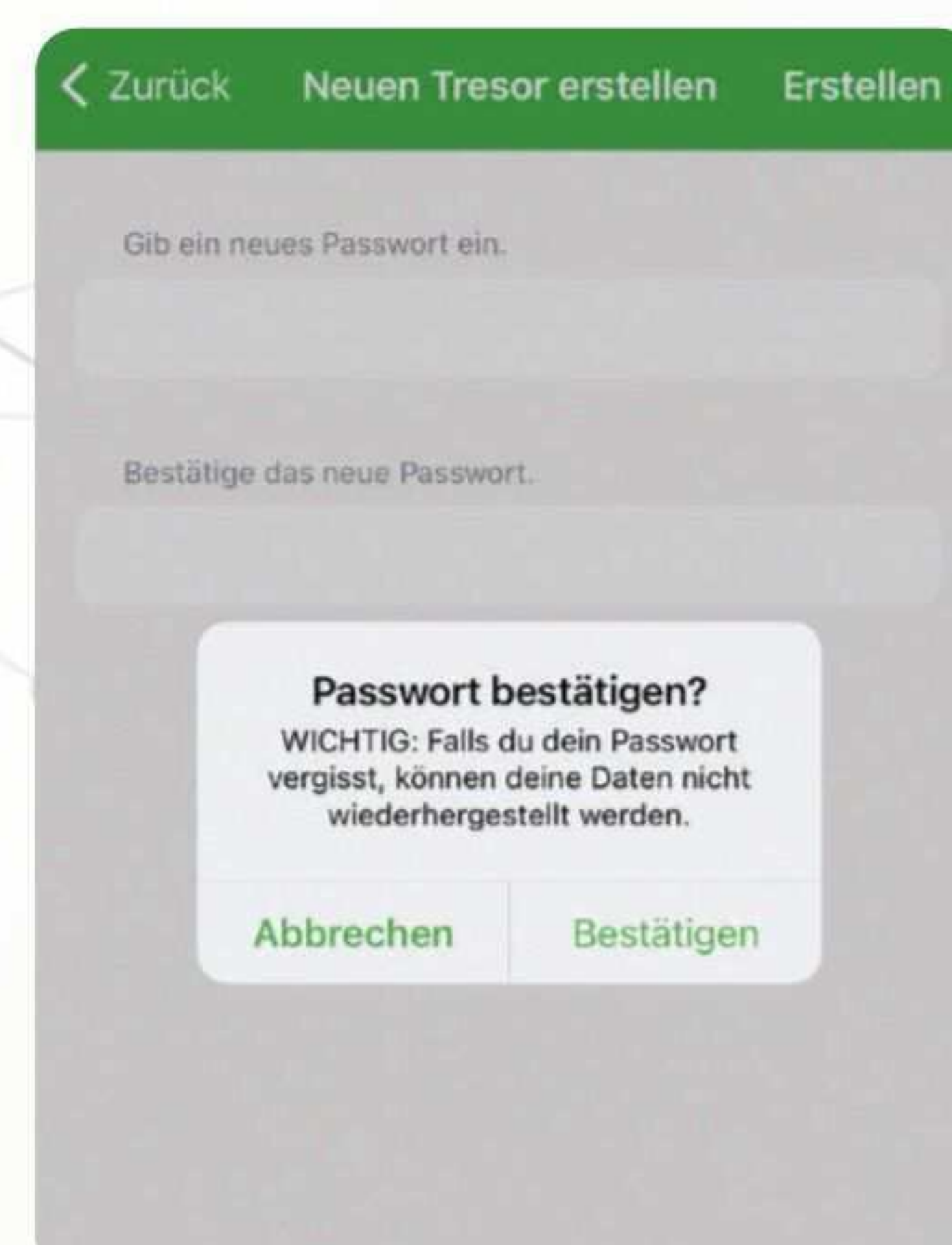
iOS EINSTELLEN: Öffnen Sie die Dateien-App am iPhone, wählen Sie **Durchsuchen**, **Weitere Orte**, **Cryptomator**, **Fertig**. Öffnen Sie die App.



EINRICHTEN: Tippen Sie aufs **+**-Symbol, auf **Neuen Tresor erstellen**, und benennen Sie ihn. Wählen Sie **Weiter** und Ihre Cloud, etwa **OneDrive**.



SPEICHERWAHL: Tippen Sie erneut auf das **+**-Symbol und auf **Fortfahren**. Melden Sie sich in Ihrer Cloud an, tippen auf **Ja** und auf den Speicherort.



PASSWORT: Wählen Sie **Ordner erstellen**. Benennen Sie ihn, tippen auf **Erstellen**, **Auswählen**, wählen ein Passwort und **Erstellen**, **Bestätigen**.



Deine Daten: geschützt

Avast One

Hurra, Ihr Smart-Scan ist abgeschlossen!

Wir empfehlen, regelmäßig einen Smart-Scan auszuführen, um sicher und privat zu bleiben.

Fertig

Avast One

WILLKOMMEN BEI AVAST ONE

Lassen Sie uns Ihren ersten Smart-Scan ausführen

Finden und entfernen Sie Sicherheitsbedrohungen und verbessern Sie Ihre Privatsphäre mit diesem optimierten Scan.

Smart-Scan ausführen

Das dauert nur einen Moment

Start Entdecken Profil

Computer Bild

„BESTER IM PRAXISTEST“

Avast One

NOTE **2,0**

Ausgabe 6/2022
8 PRODUKTE IM VERGLEICH



Deine Privatsphäre: geheim

A line-art illustration of a hand holding a key, positioned as if about to unlock a yellow padlock. The padlock is attached to a circular line that loops around the word 'geheim' in the headline above.

Sicherheit, Privatsphäre & Performance in One.



Wir schützen die digitale Freiheit für alle.

* Das Angebot ist gültig bis zum **30.09.2022** über den angegebenen Link und beinhaltet Avast One Individual für das erste Jahr als Download für bis zu 5 Endgeräte (PC, Mac, Android und iPhone/iPad). Es können zusätzliche Kosten für den Download durch den jeweiligen Internetanbieter entstehen. 2022 Copyright Avast Deutschland GmbH

DER GROSSE SECURITY- SUITEN-TEST

8
Schutzpakete
IM TEST

Virenschutz ist wichtiger denn je, **doch welches Programm schützt wirklich gut?** Das hat COMPUTER BILD für Sie getestet!

Spätestens mit Putins Angriffskrieg auf die Ukraine ist vielen klar geworden: Politische Krisen haben auch immer große Auswirkungen auf die Bedrohungslage im Internet. Russland attackierte den Nachbarn nicht nur mit Panzern und Raketen, sondern schon vor dem Einmarsch auch mit gezielten Hackerangriffen. Und die machen nicht an Grenzen halt – auch bei uns und in anderen Teilen Europas wird Infrastruktur übers Netz angegriffen. Gut möglich, dass auch Privatleute verstärkt zum Ziel werden – schließlich kann man auch so Menschen demoralisieren. Aber auch abseits des Krieges steigt die Gefahr im Internet: Immer mehr Schadprogramme, Spamkampagnen und andere Betrügereien machen den Alltag gefährlich. Als Schutz hilft vor allem eines: ein

wirksames Antiviren-Programm. Wie gut die wichtigsten Schutzprogramme auf Gefahren aller Art vorbereitet sind, hat COMPUTER BILD im großen Sicherheitstest geprüft. Dabei gab's viele Überraschungen.

Schutzpakete mit Extras

Wie bereits im vergangenen Jahr hat COMPUTER BILD auch dieses Mal die Komplettpakete der Hersteller mit allen Extras getestet. Die Gefahren im Internet sind extrem vielfältig, und für nahezu alle Nutzer lohnt so ein Paket mehr, als sich einen Schutz mit verschiedenen Programmen selbst zusammenzustellen. Auch der Verkaufstrend geht eindeutig in diese Richtung: Die Komplettpakete sind bei vielen Herstellern trotz des höheren Preises die Topseller. Was genau in der jeweiligen

Suite enthalten ist, ist je nach Anbieter unterschiedlich. Kern ist immer der Virenschutz. Häufig sind auch VPNs, Passwortmanager, Update-Assistenten und Schwachstellenscanner dabei. Einige Hersteller wie Avast bieten zudem auch Extras an, die nicht für die Sicherheit des PCs relevant sind, etwa Tuning-Funktionen. COMPUTER BILD hat solche Programmteile außen vor gelassen, weil es in diesem Test um Sicherheit geht. Diese Extras schaden aber natürlich auch nicht.

Große Schutz-Unterschiede

In den vergangenen Jahren gab es in der Schutzleistung der Testkandidaten nur geringe Unterschiede – im Großen und Ganzen lieferten so gut wie alle eine ➤

AV-HERSTELLER IM AUSNAHMEZUSTAND

Der Ukraine-Krieg erschüttert auch die Antiviren-Unternehmen – viele haben osteuropäische Wurzeln. Im Fokus: das ursprünglich aus Russland stammende Kaspersky. Auf Anfrage von COMPUTER BILD teilte das Unternehmen mit, man gewähre „keiner Strafverfolgungs- oder Regierungsorganisation Zugang zu den Nutzerdaten oder der Infrastruktur des Unternehmens“. Gründer Eugene Kaspersky äußerte sich auf Twitter vorsichtig, sprach sich für eine diplomatische Lösung der „derzeitigen Situation“ in der Ukraine aus. Zum Redaktionsschluss erfuhr

COMPUTER BILD, dass seine Ex-Frau Natalya ihren Posten im Aufsichtsrat der deutschen AV-Firma G Data niederlegen wird. Sie hält eine Minderheitsbeteiligung am Unternehmen und war in der Vergangenheit im Umfeld russischer regierungsnaher Institutionen aktiv. Das rumänische Bitdefender preschte nach vorn: Es bot Regierungseinrichtungen und Unternehmen der Ukraine Unterstützung an und erweiterte sein Angebot von freiem Virenschutz für ein Jahr auf alle EU- und NATO-Staaten. Eset und Avast hielten sich mit politischen Statements zurück.





AVIRA PRIME

MADE IN GERMANY

★★★★★

5 Devices | 2 User Accounts
1-Year License

eset

SMART SECURITY PREMIUM

Für alle Systeme macOS iOS

Total Security

BEST BRANDS 2022

Bitdefender TOTAL SECURITY

MULTI DEVICE

updates

kaspersky

Kaspersky® Total Security

Premium Security Suite for You & Your Family – on PC

Avast

One

Proactive and powerful protection for your life today

Illustration of a person surrounded by icons representing various security features like a virus, a shield, a key, and a rocket.

norton

ABONNEMENT FÜR 2 JAHRE
Elektronischer Software-Download
Windows macOS iOS 10 GERÄTE

Norton 360 Premium

Leistungsstarker, mehrschichtiger Schutz für Ihre vernetzte Welt

VIRENSCHUTZ-VERSPRECHEN

Es gelten bestimmte Einschränkungen. Einzelne oder Kombinationen von Viren, Malware, Spyware und Ransomware können nicht durch Virenscanner erkannt werden.

- Schutz vor Viren, Malware, Spyware und Ransomware
- 75 GB Cloud-Speicher für PC
- Secure VPN für Ihre Online-Privatsphäre
- Kindersicherung für PCs oder Smartphones

ordentliche Leistung ab. Das ist dieses Jahr anders: Die Unterschiede im Virenschutz sind wieder größer. Nur fünf von acht Programmen erhielten die Note „gut“ oder besser. Vorneweg das Spitzenduo Norton und Bitdefender, die beide einen „sehr guten“ Virenschutz boten. Auf dem letzten Platz landet in diesem Jahr Eset. Der Schutz dieser Suite ist zwar noch ausreichend, aber schlechter als der des kostenlos mit dem Betriebssystem mitgelieferten Windows Defender. Wer das Programm installiert, reduziert die Sicherheit des PCs.

Norton und Bitdefender top

Norton und Bitdefender lieferten sich im Testparcour ein wahres Kopf-an-Kopf-Rennen. Beide erhielten zum Schluss die Gesamtnote „gut (1,7)“. Beim wichtigsten Testpunkt, dem Virenschutz, lieferten beide ein Top-Ergebnis (Testnote 1,4). Die Zusatzausstattung von Bitdefender ist um einiges besser, dafür lässt sich Norton viel einfacher bedienen und verstehen. Am Ende entschied der günstigere Preis über den Testsieg zugunsten von Bitdefender.



Extrem hoher Testaufwand

Für wirklich aussagekräftige Ergebnisse ist ein hoher Testaufwand erforderlich. COMPUTER BILD arbeitet dazu mit dem renommierten Testinstitut AV-Comparatives zusammen und prüft die Schutzprogramme zusätzlich im eigenen Labor. Was genau die Programme leisten müssen, lesen Sie auf der nächsten Seite.

Wie gut ist der Windows Defender?

Der Windows Defender ist in jedem aktuellen Windows enthalten und soll einen Grundschutz vor Schädlingen aller Art bieten. Microsoft ist stetig dabei, die Software zu verbessern. Und über die Jahre hat sich das Programm zu einer durchaus brauchbaren Alternative gemausert. Im aktuellen Test belegt der Defender den siebten Platz mit der Note „befriedigend (3,1)“. Damit liegt er zwar hinter fast allen Kaufprogrammen zurück, ist aber trotzdem ein ausreichender Schutz – gerade einmal 0,09 Prozent der Malware im Labortest ging ihm durch die Lappen. Allerdings ist die Bedienung des Programms über die Windows-Einstellungen eher etwas für Profis. Wer damit zurechtkommt, findet im Defender aber eine brauchbare Gratis-Alternative.

Stark unterschiedliche Preismodelle

Die Lizenzangebote der Hersteller unterscheiden sich sehr stark. Zwar bieten fast alle auch ein Paket für Einzelgeräte, doch wer mehr möchte, muss genau hinschauen und vergleichen. Denn teilweise unterscheiden sich die Kosten um den Faktor 3. Ein Beispiel: Für fünf Lizenzen bei Testsieger Bitdefender zahlen Nutzer nur 32 Euro, bei Kaspersky sind es hingegen knapp 100 Euro. Sind wiederum zehn Lizenzen nötig, sieht die Sache komplett

anders aus, dann ist Norton mit 39,99 Euro am günstigsten. COMPUTER BILD hat die Preise verglichen und eine Übersicht für übliche Anzahlen von Lizenzen erstellt (siehe Tabelle unten). Die hier aufgelisteten Preise sind Herstellerangaben. Bei Plattformen wie Ebay sind die Lizenzen zwar oft günstiger zu finden, diese stammen aber häufig aus dubiosen Quellen und laufen Gefahr, vom Hersteller deaktiviert zu werden. Schlecht, wenn von einem Moment auf den anderen der Schutz weg ist.

Taugt das mitgelieferte VPN etwas?

Bis auf G Data, Eset und Windows Defender liefern alle Hersteller ein VPN mit. Das ist in den meisten Fällen aber nur dafür geeignet, sich in einem unsicheren WLAN abzusichern. Wer beispielsweise Filme im Ausland sehen möchte oder besonders viel Wert auf Anonymität legt, ist mit einem eigenständigen VPN besser beraten. Eine Übersicht der besten VPNs gibt es auf www.cobi.de/12676. [av]

FAZIT

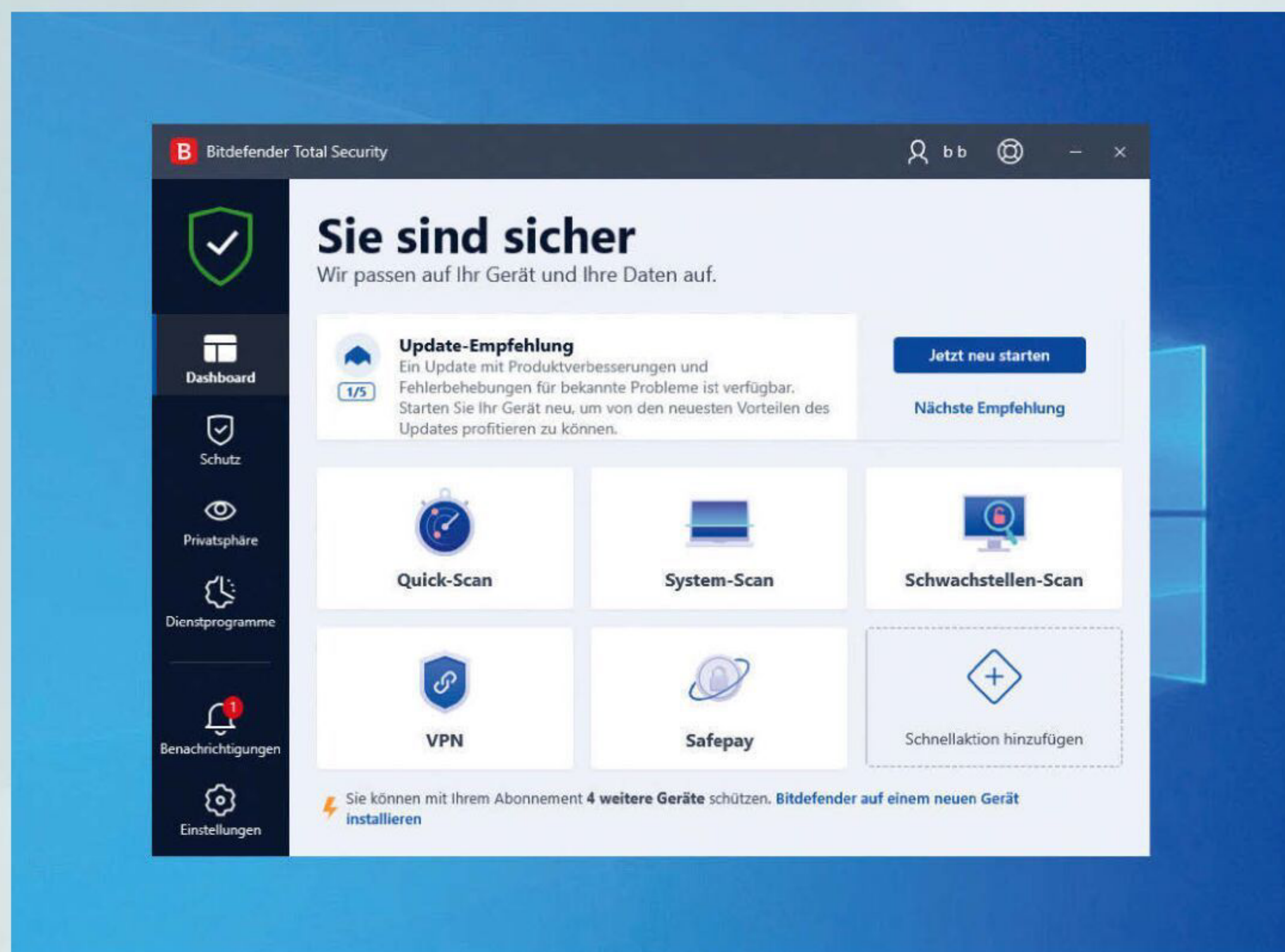
Die Unterschiede bei Schutzprogrammen werden wieder größer – und zwar vor allem beim wichtigsten Punkt: der Schutzleistung. Statt auf Extras oder Bedienung wie in den vergangenen Jahren sollten Nutzer also mehr auf die Sicherheit schauen. Hier ganz vorn: Norton und Bitdefender, die beide ein „sehr gut“ in der Schutznote erreichten. Testsieger Bitdefender setzte sich am Ende aufgrund des Preises auf den ersten Platz. Schlusslicht Eset muss beim Virenschutz hingegen dringend nachbessern. Im Testzeitraum war der schlechter als der des Windows Defender! Großes Manko bei fast allen Kandidaten: Bedienung und Verständlichkeit. Einzig der Zweitplatzierte Norton 360 Premium punktet hier mit einer guten Note.

DAS KOSTET DER VIRENSCHUTZ

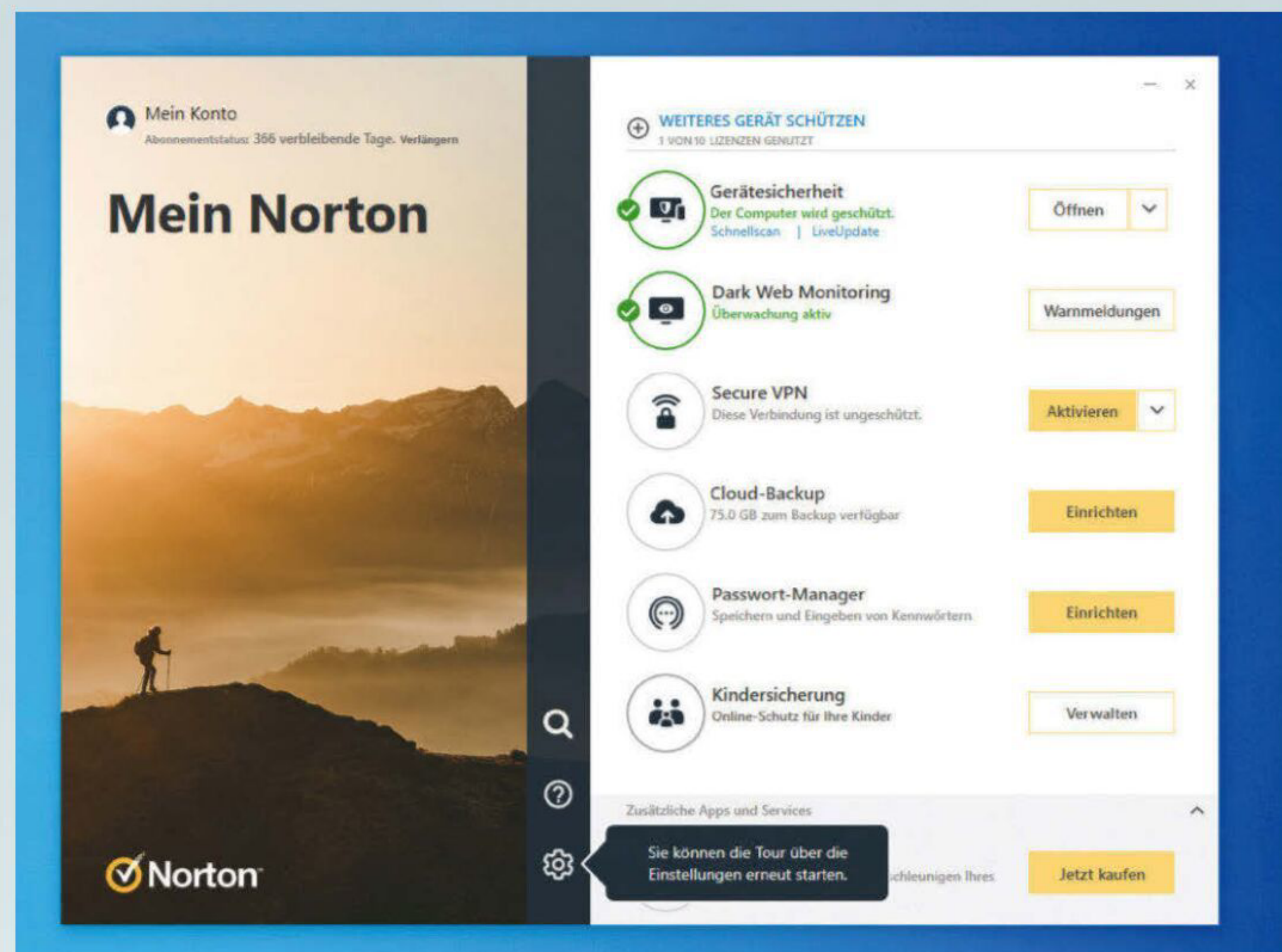
Die Lizenzmodelle der Hersteller sind sehr verschieden: So bietet beispielsweise G Data Pakete mit einer, drei, fünf oder zehn Lizenzen an, Norton hingegen gibt es pauschal nur mit zehn Lizenzen. Auch bei der Preisgestaltung weichen die Anbieter stark voneinander ab.

Damit Sie das beste Paket für die von Ihnen benötigte Anzahl an Lizenzen finden, hat COMPUTER BILD eine Übersicht für Sie zusammengestellt. Die zeigt, wie viel Sie zahlen müssen, wenn Sie eine, fünf, zehn oder zwanzig Lizenzen brauchen.

Produktname	Preis für 1 Lizenz	Preis für 5 Lizenzen	Preis für 10 Lizenzen	Preis für 20 Lizenzen
BITDEFENDER TOTAL SECURITY	32 Euro	32 Euro	64 Euro	128 Euro
NORTON 360 PREMIUM	39,99 Euro	39,99 Euro	39,99 Euro	79,98 Euro
AVAST ONE	45 Euro	45 Euro	59,88 Euro	59,88 Euro
G DATA TOTAL SECURITY	27,96 Euro	50,36 Euro	100,72 Euro	201,44 Euro
AVIRA PRIME	59,99 Euro	59,99 Euro	77,95 Euro	77,95 Euro
KASPERSKY TOTAL SECURITY	49,95 Euro	99,95 Euro	199,90 Euro	399,80 Euro
ESET SMART SECURITY PREMIUM	49,94 Euro	89,95 Euro	139,96 Euro	279,92 Euro



Die Bitdefender Total Security bietet das beste Paket aus Virenschutz, Zusatz-ausstattung und bremst den PC kaum aus – es ist damit verdienter Testsieger!



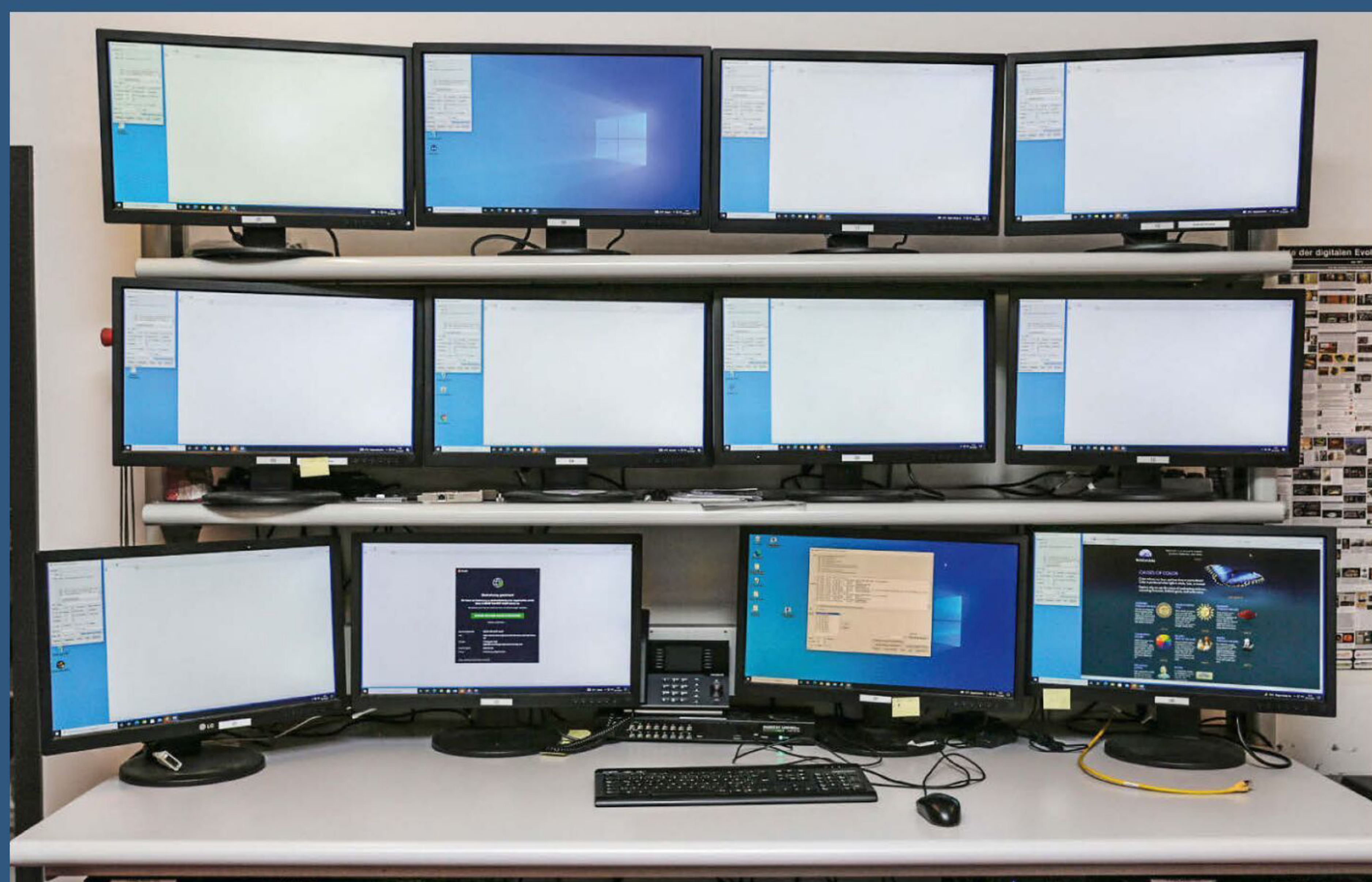
Norton liegt nur wegen des höheren Preises auf Platz 2. Die Suite bietet sehr gute Schutzleistung, Übersichtlichkeit und Verständlichkeit – auch für Laien!

SO TESTET COMPUTER BILD

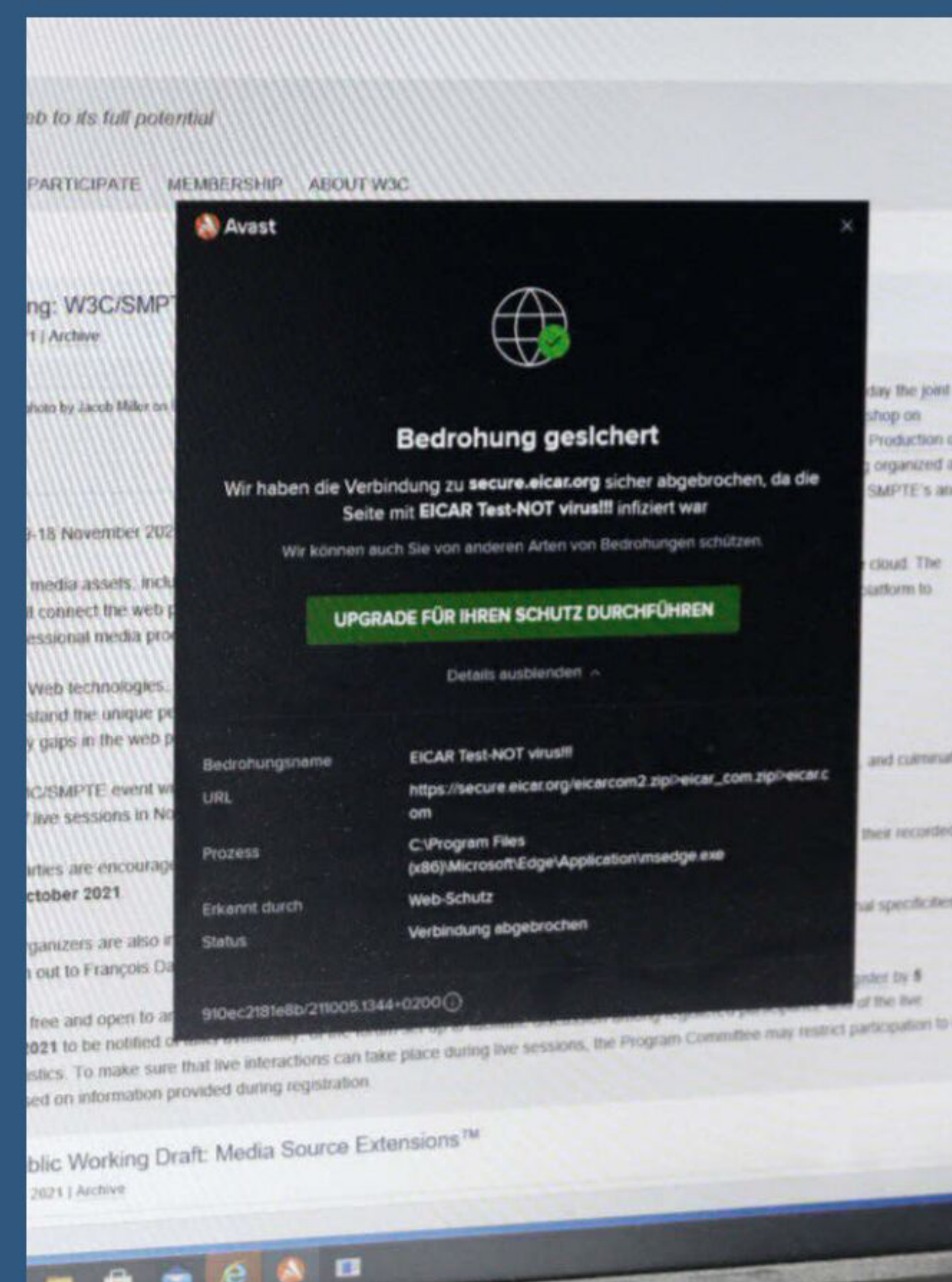
Der Schutz des PCs ist extrem wichtig, und deshalb testet COMPUTER BILD Security-Suiten mit besonders großem Aufwand – insbesondere die Schutzfunktion vor Bedrohungen aus dem Internet: Die prüft COMPUTER BILD in Zusammenarbeit mit dem renommierten Testlabor AV-Comparatives. Für diesen Test mussten alle Programme im Langzeittest über Monate hinweg insgesamt 20 042 Schädlinge erkennen und beseitigen. Zudem mussten die Testkandidaten im Praxistest auf 1479 echten, verseuchten Inter-

netseiten ihr Können unter Beweis stellen. Und dabei sollten die Suites natürlich am besten weder Fehlalarme auslösen noch den PC spürbar bremsen. Einige Schutzprogramme verlangsamen aber beispielsweise das Aufrufen von Internetseiten oder die Arbeit mit Office. Andere melden und blockieren harmlose Programme aufgrund von vermeintlichem Gefahrenpotenzial. Darüber hinaus prüfte COMPUTER BILD im eigenen Testlabor die Ausstattung der Schutzpakete – beim Testpunkt „VPN“ mit einem aufwendigen Zuverlässigkeitstest,

da es bei den anonymen Internetzugängen deutliche Qualitätsunterschiede gibt. Auch der beste Schutz bringt wenig, wenn der Nutzer im Ernstfall nicht versteht, was eigentlich gerade am oder im Computer passiert und was er tun muss, um die Bedrohung abzuwenden. Daher schauten sich die Experten von COMPUTER BILD auch den Programmaufbau, die Hilfsfunktionen und die Warnmeldungen genauestens an. Denn auch normale Nutzer ohne professionelles IT-Wissen müssen sich in dem Programm zurechtfinden.



Jedes Schutzprogramm installiert COMPUTER BILD auf jeweils baugleichen PCs. So lassen sich gleichzeitig Tests durchführen und die Programme unter identischen Bedingungen vergleichen.



Nicht immer sind die Meldungen so verständlich wie diese von Avast.

Fotos: iStock, Montage: COMPUTER BILD

DAS SIND DIE BESTEN

BITDEFENDER TOTAL SECURITY

Preis: 32 Euro* für 5 Geräte

Die Bitdefender Total Security setzte sich durch und überzeigte vor allem mit sehr gutem Virenschutz und Top-Ausstattung. Zwar war Bitdefender im Labortest minimal schlechter als Zweitplatzierte Norton und ließ 0,01 Prozent der Angriffe durch, dafür gab es weniger Fehlalarme, und der Schutz bleibt auch ohne Internetverbindung noch „gut“. Die Zusatzausstattung bei Bitdefender ist die zweitbeste im Test, nur Kaspersky liefert noch ein bisschen mehr. Beispielsweise ist das enthaltene VPN zusammen mit dem in der Kaspersky Total Security das beste unter allen Testkandidaten. Mit der Testnote „befriedigend“ ist es mehr als nur eine Notlösung in öffentlichen WLANs. Aber auch sonst ist fast alles enthalten, was man

sich von einer Sicherheits-Suite wünscht: Firewall, Kinderschutz, Schwachstellen-scanner, Diebstahlschutz und vieles mehr. Einziger Kritikpunkt ist der Bedienkomfort: Bitdefender ist teils etwas umständlich, und nicht alle Warnmeldungen sind ohne Fachwissen verständlich. Die Online-Hilfe ist nur auf Englisch verfügbar. Das ist aber Meckern auf hohem Niveau, die Bitdefender Total Security ist ein erstklassiges Schutzprogramm und wehrt zuverlässig alle Gefahren aus dem Internet ab. Über den Testsieg entschied letztlich der Preis: Norton und Bitdefender erhielten beide das Testergebnis „gut (1,7)“. COMPUTER BILD testete Pakete mit mindestens fünf Lizenzen. Fünf sollten für eine drei- bis vierköpfige Familie



Beste
GESAMT-
LEISTUNG

reichen, eine für jeden und ein bis zwei Geräte extra. Für dieses Paket ist Bitdefender rund 8 Euro günstiger.

- + Sehr guter Virenschutz, tolle Extras.
- Umständliche Menüs, teils unverständliche Meldungen.

TESTERGEBNIS **gut 1,7**

2

NORTON 360 PREMIUM

Preis: 39,99 Euro*

Norton 360 Premium liegt gleichauf mit Testsieger Bitdefender. Das gelang dem Programm durch einen tadellosen Labor-Test und einen sehr guten Virenschutz! Nicht eins der mehr als 20 000 getesteten Viren schaffte es, sich vorbeizuschleichen. Das ist einsame Spitze und besser als alle Konkurrenzprodukte. Auch im Praxistest (siehe Seite 61) machte das Programm eine gute Figur und wehrte 99,86 Prozent aller Angriffe ab. Ohne Internetverbindung lässt der Schutz allerdings stark nach und ist dann nicht mehr ausreichend. Zudem meldet Norton auch dieses Jahr wieder zu viele Fehlalarme. Vorbildlich sind die



Einfachste
BEDienung

Bedienung des Programms und die Verständlichkeit von Warnmeldungen.

- + Bester Virenschutz, verständlichste Menüs und Meldungen.
- Schlechter Schutz ohne Internet, wichtige Extras fehlen.

TESTERGEBNIS **gut 1,7**

3

AVAST ONE

Preis: 45 Euro*

Avast One ist das neue Schutzprogramm des bekannten Herstellers und löst den Testsieger aus dem vergangenen Jahr ab. Und der Neuling knüpft auch gleich an die guten Ergebnisse an: Bei der Schutzleistung liegt er knapp hinter den beiden Top-Platzierten, im Praxistest lieferte One sogar das beste Ergebnis und leistete sich keine großen Patzer. Avast One wirbt damit, ein Paket aus Schutz, Tuning und VPN zu sein. Leider fehlen einige Module wie ein Kinder- und Diebstahlschutz sowie ein Schwachstellen-scanner. Und das im Paket enthaltene VPN ist nur „ausreichend (3,5)“. Auch bei Avast gibt es Ver-



Top im
PRAXISTEST

besserungspotenzial in der Bedienung: Größtes Manko ist das Fehlen von Warnmeldungen der Firewall.

- + Guter Virenschutz, bester im Praxistest.
- Wichtige Extras fehlen, unlogische Menüs.

TESTERGEBNIS **gut 2,0**

* Bei gleicher Note führt der niedrigere Preis zur besseren Platzierung. Die Preise wurden direkt nach Abschluss des Tests am 22. 2. 2022 ermittelt. Sie gelten jeweils für ein Jahrespaket mit mindestens fünf Lizenzen.

4

**AVIRA
PRIME**

Preis: 59,99 Euro*

Avira Prime schützt den PC zuverlässig, wehrte 99,98 Prozent der getesteten Schadprogramme im Labortest ab. Mit der Spitzengruppe kann es trotzdem nicht ganz mithalten, da die Erkennungsrate im Praxistest auf etwa 99 Prozent und ohne Internetverbindung sogar auf nur 90 Prozent sank. Insgesamt bietet es aber einen zuverlässigen Schutz vor allen Gefahren im Internet. Größter Kritikpunkt an Prime bleibt die Zusatzausstattung: Alle anderen Testkandidaten bieten mehr Extras und Funktionen. Bei Avira fehlen etwa Firewall, Kinderschutz und Diebstahlschutz. Für ein derart teures Komplettpaket ist das derzeit etwas wenig, weshalb

Zuverlässig
IM LABOR-
TEST

es das Programm nur auf einen guten vierten Platz schafft.

- +** Guter Virenschutz.
- Wichtige Extras fehlen, schlecht im Praxistest.

TESTERGEBNIS gut 2,2

5

**G DATA
TOTAL SECURITY**

Preis: 50,36 Euro*

Die G Data Total Security lieferte zwar gute Ergebnisse im Labortest, leistete sich aber manche Ausrutscher im Praxistest: Knapp 1 Prozent aller Schädlinge auf echten verseuchten Seiten entdeckte das Programm nicht. Das ist bei der Masse der Malware im Internet nur „ausreichend“. Das Programm bietet andererseits den besten Schutz ohne Internetverbindung (95,5 Prozent Erkennungsrate) und zeigt nur wenig Fehlalarme. Fürs Podium reichte es trotzdem nicht ganz, unter anderem weil neben Diebstahlschutz und Schwachstellenscanner auch kein VPN im Paket enthalten ist. Die G Data Total Security

Guter
ALL-
ROUNDER

landete aber im soliden Mittelfeld und bekommt insgesamt noch die Testnote „gut“.

- +** Kaum Fehlalarme, guter Schutz ohne Internetverbindung.
- Wichtige Extras fehlen, kein VPN.

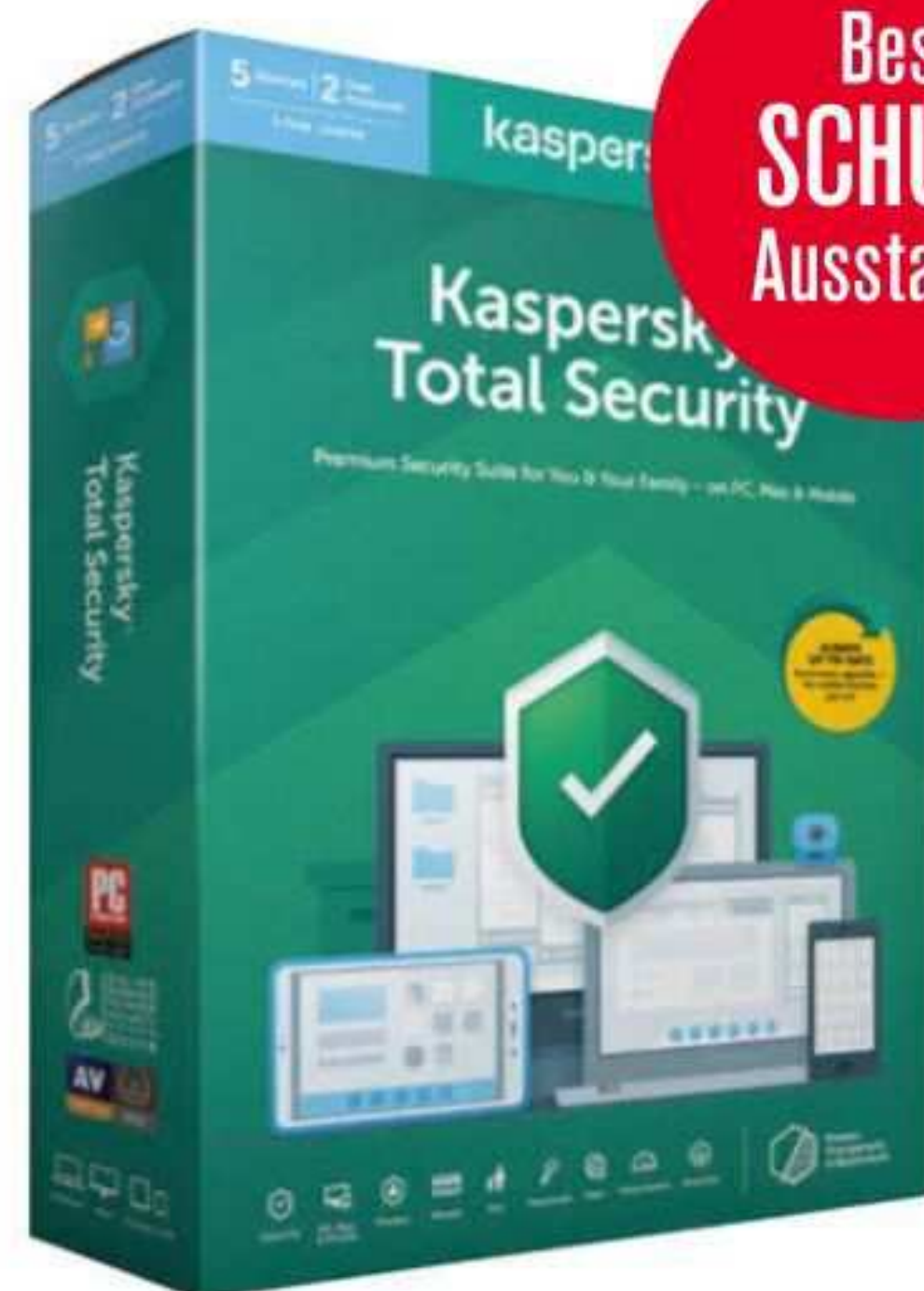
TESTERGEBNIS gut 2,3

6

**KASPERSKY
TOTAL SECURITY**

Preis: 99,95 Euro*

Die Kaspersky Total Security belastet den PC kaum und bietet die beste Zusatzausstattung. Leider schwächelt sie etwas beim Virenschutz: Im Test blieben 0,07 Prozent der aktuellen Viren uner-

Beste
SCHUTZ-
Ausstattung

kannt, ohne Internetverbindung erkennt die Suite nur 84,3 Prozent. Zu wenig für einen Top-Platz. Achtung: Aufgrund möglicher Risiken im Zusammenhang mit dem russischen Ursprung der Software warnt das Bundesamt für Sicherheit in der Informationstechnologie (BSI) vor dem Einsatz von Kaspersky!

- +** Beste Schutzausstattung, geringer Ressourcenverbrauch.
- Kein Diebstahlschutz, umständlicher Aufbau. BSI-Warnung!

TESTERGEBNIS befriedigend 2,5

7

**MICROSOFT
WINDOWS DEFENDER**

Preis: kostenlos

Der Windows Defender belastet den PC am stärksten, ist nicht besonders zugänglich und verständlich, bietet kaum Extras und kann mit den Erkennungs-raten der Konkurrenz nicht mithalten. Aber er ist kostenlos und auf Windows-Rechnern vorinstalliert – und bietet mit Internetverbindung akzeptable Erkennungsraten. Nur wer sich gut auskennt und auf den Komfort der Kaufprogramme verzichten kann, findet in dem Grundschutz von Windows eine akzeptable Alternative.

KOSTENLOS
für jeden

- +** Kostenlos.
- Schlechter Schutz ohne Internet, wichtige Extras fehlen.

TESTERGEBNIS befriedigend 3,1

8

**ESET
SMART SECURITY**

Preis: 89,95 Euro*

Die Hauptaufgabe eines Schutzprogramms ist es, den PC zu schützen. Das gelang Eset dieses mal nicht gut genug: Nach der Installation des Programms kamen im Labortest mehr Schädlinge durch (0,15 Prozent) als vorher mit dem Windows Defender (0,09 Prozent). Ähnlich sieht es beim Praxistest aus. Das darf einem Schutzprogramm einfach nicht passieren, auch wenn die Schutzleistung insgesamt noch „ausreichend“ ist. Die Smart Security landet daher auf dem letzten Platz.

Besonders
ressourcen-
SCHONEND

- +** Geringer Ressourcenverbrauch.
- Schlechterer Virenschutz als vorinstallierter Windows Defender.

TESTERGEBNIS ausreichend 3,8



1 **BITDEFENDER**
TOTAL
SECURITY
Preis: 32 Euro*



2 **NORTON**
LIFELock
NORTON 360
PREMIUM
Preis: 39,99 Euro*

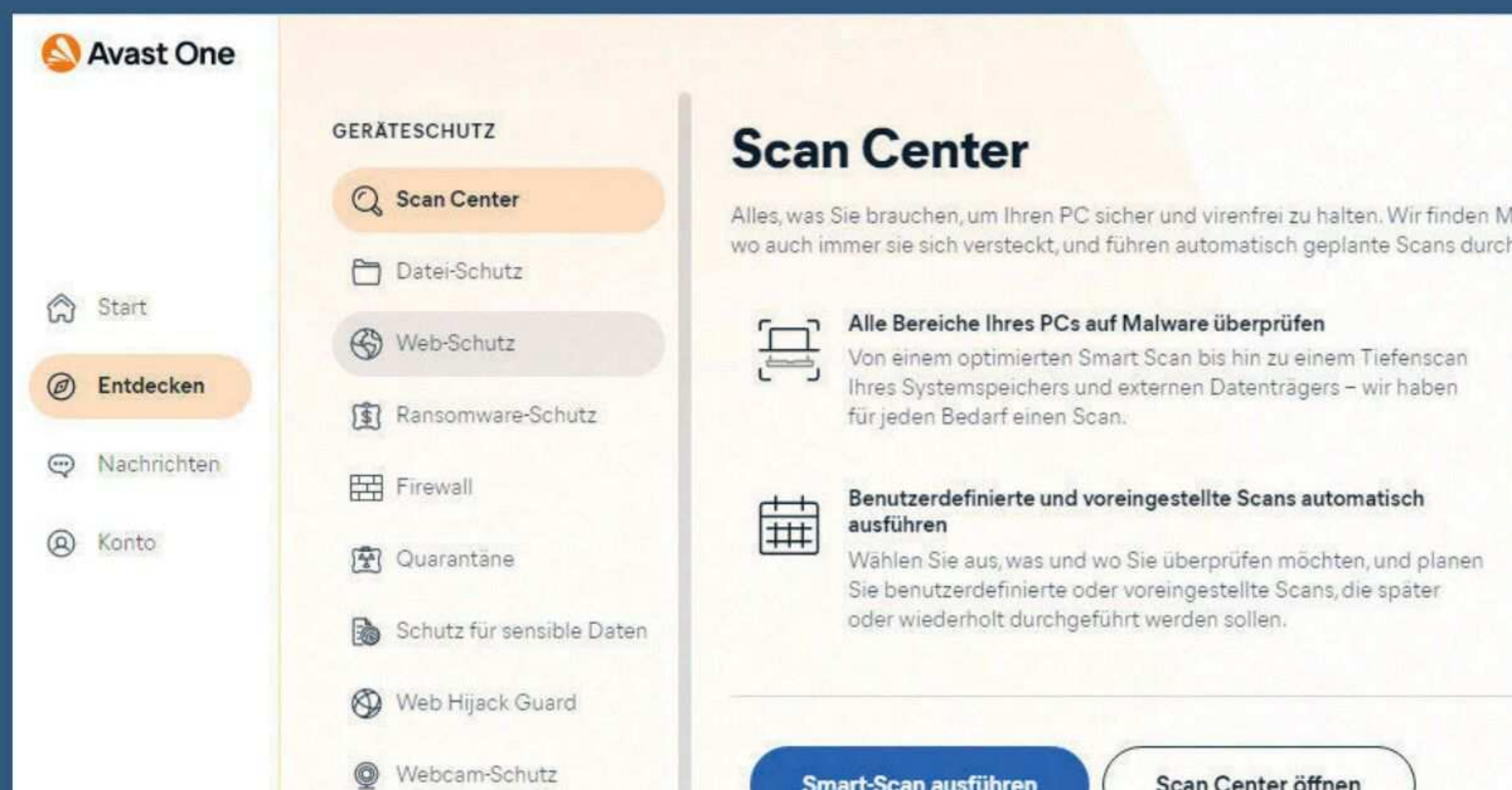


3 **AVAST**
ONE
Preis: 45 Euro*

TESTERGEBNISSE

		Geeignet für: Windows 8, 10, 11 für 5 Geräte		Geeignet für: Windows 8, 10, 11 für 10 Geräte		Geeignet für: Windows 8, 10, 11 für 5 Geräte	
Wie gut schützt das Programm vor Bedrohungen allgemein?	67,5 %	Bester Virenschutz im Test	1,4	Sehr guter Online-Schutz	1,4	Guter Virenschutz	1,5
Langzeittest: Infektionsrisiko bei vorherrschenden Schädlingen (20 042 Testfälle)		sehr gering (0,01 %)	1,3	sehr gering (0,00 %)	1,0	gering (0,02 %)	1,5
Langzeittest: Schutz vor verseuchten Internetseiten (1479 Testfälle)		gut (99,80 % verhindert)	1,7	sehr gut (99,86 % verhindert)	1,5	sehr gut (99,93 % verhindert)*	1,2
Langzeittest: Fehlalarme (beim Aufruf von nicht infizierten Internetseiten / beim Scannen von nicht infizierten Dateien)		wenige (5 / 13)	1,6	viele (60 / 36)	4,1	wenige (26 / 3)	2,0
Erkennungsrate bei Scan ohne Internetverbindung (20 042 Testfälle)		gut (95,3 %)	2,2	sehr schlecht (83,6 %)	5,1	etwas schlecht (92,2 %)	3,0
Welche weitere Schutzausstattung bietet das Softwarepaket?	7 %	Gute Zusatzausstattung	2,0	Einige Extras fehlen	3,1	Wenige Extras	3,8
Eigene Firewall		ja	1,0	ja	1,0	ja	1,0
Anonymes Surfen im Internet per VPN		wenige Server, kaum Extras	3,0	Schwächen beim Datenschutz	3,6	wenige Server, kein WireGuard	3,5
Kinderschutzfunktion enthalten		ja	1,0	ja	1,0	nein	6,0
Lücken- bzw. Schwachstellenscanner im Programm vorhanden		ja	1,0	nein	6,0	nein	6,0
Anti-Diebstahl-Funktion für mobile Computer enthalten		ja	1,0	nein	6,0	nein	6,0
Weitere Schutzausstattung: Update-Assistent / Backup-Funktion / Spurenbeseitiger / Passwort-Manager (und 8 weitere)		ja / nein / nein / ja	2,7	nein / ja (inkl. 75 GB Cloud-Speicher) / nein / ja	3,3	ja / nein / ja / nein	4,3
Macht das Programm den PC langsamer?	10 %	Office minimal langsamer	1,3	Office minimal langsamer	1,3	Office etwas langsamer	1,3
Verlangsamung beim Anzeigen von Internetseiten / Dateiverwaltung / Office- und Multimedia-Anwendungen		sehr gering / sehr gering / gering	1,3	sehr gering / sehr gering / gering	1,3	sehr gering / sehr gering / etwas hoch	1,3
Wie einfach ist die Bedienung?	15,5 %	Umständliche Bedienung	3,5	Einfachstes Programm	2,4	Umständliche Bedienung	3,7
Grundlegende Bedienelemente wie Menüs sowie Hilfefunktionen und Installation		unlogische Menüstruktur, keine Funktionssuche, Hilfe englisch	3,6	unlogische Menüstruktur, Hilfe fast nur online, Handbuch englisch	2,8	unlogische Menüs, keine Funktionssuche, keine Suche in der Hilfe	3,6
Handhabung im Alltag (etwa einfaches Aktivieren und Deaktivieren des Programms sowie einzelner Module, problemlose Scans)		Deaktivierung umständlich, standardmäßig keine Auswahlmöglichkeit bei Virenfund	3,7	einige Funktionen nur über zweite Programmoberfläche	2,2	etwas wenig Infos bei Virenfund, Texte teils missverständlich	3,3
Qualität und Häufigkeit der Warnmeldungen		Meldungen selten, wenig hilfreich	3,4	verständliche Meldungen	2,3	sehr seltene Firewallmeldungen	4,3
AGB und Lizenzbedingungen / Datenschutzerklärung Programm		ausreichend / zufriedenstellend	3,3	zufriedenstellend / gut	2,3	ausreichend / zufriedenstellend	3,3
TESTERGEBNIS		gut 1,7		gut 1,7		gut 2,0	

BESONDERHEITEN AUS DEM TEST



Avast One ist der Neuling im Testfeld, hat aber den Vorteil, auf dem Testsieger aus dem vergangenen Jahr aufzubauen. Das hat geklappt: dritter Platz zum Einstieg!

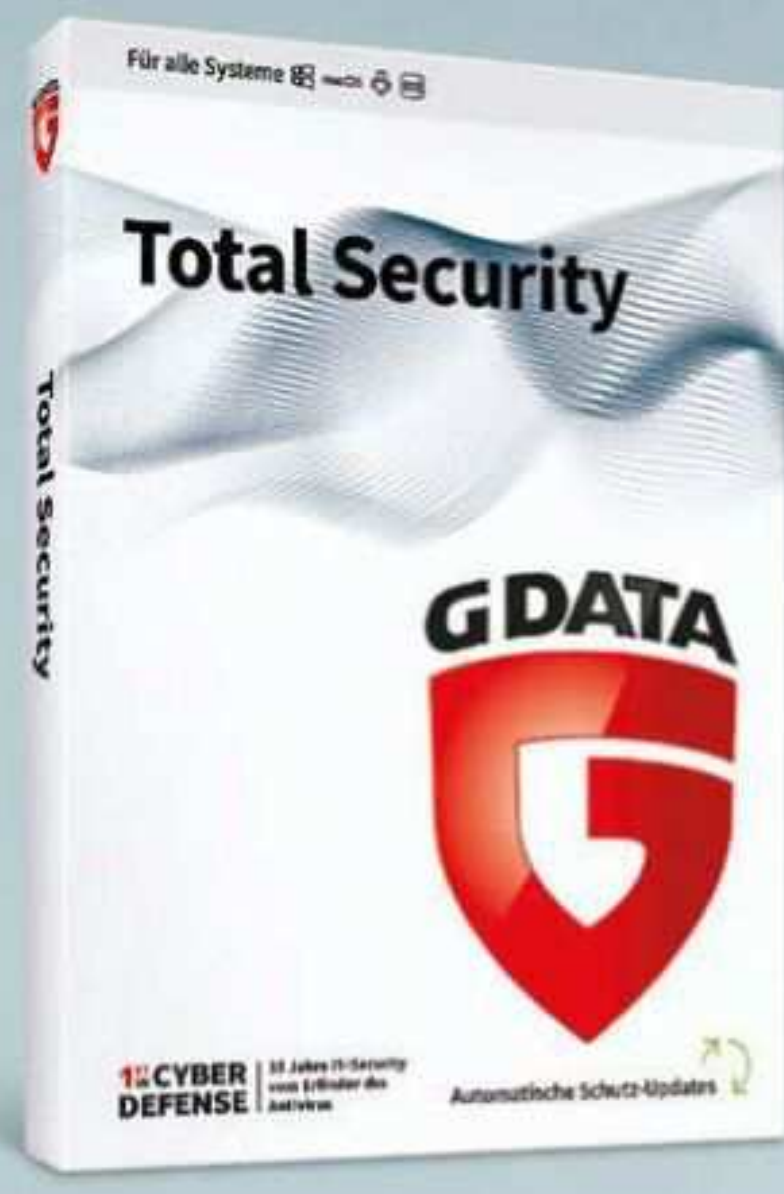


Der Fünftplatzierte G Data zeigt viele Infos auf einen Blick. Per Klick lassen sich Funktionen ein- und ausschalten.

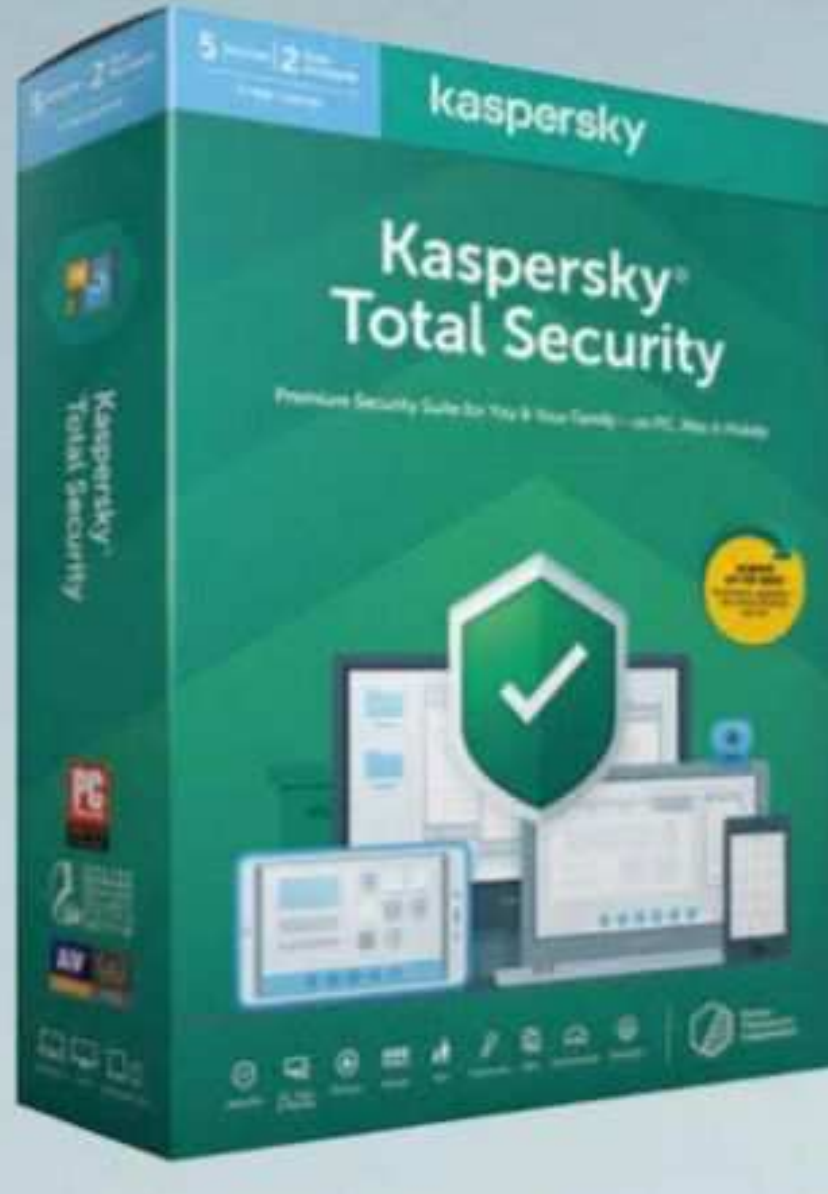
* Bei gleicher Note führt der niedrigere Preis zur besseren Platzierung. Die Preise wurden direkt nach Abschluss des Tests am 22. 2. 2022 ermittelt. Sie gelten jeweils für ein Jahrespaket mit mindestens fünf Lizenzen.



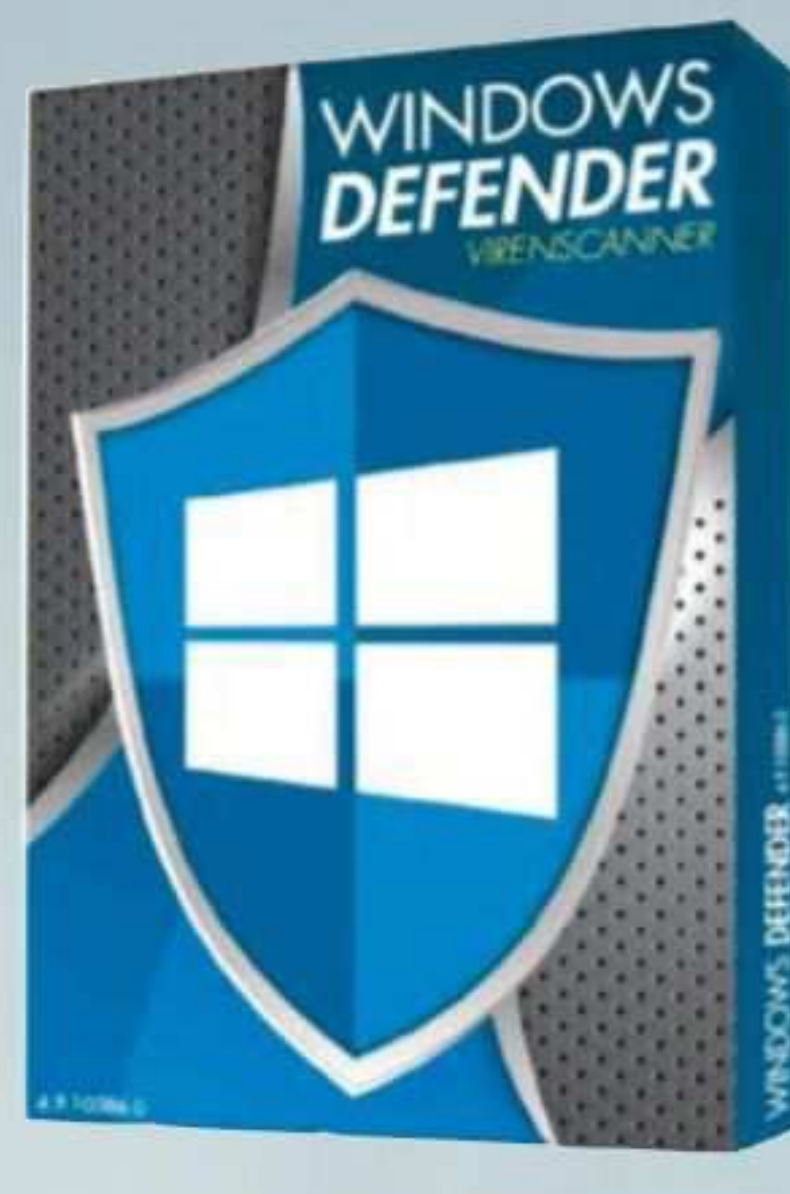
4 AVIRA PRIME
Preis: 60 Euro*



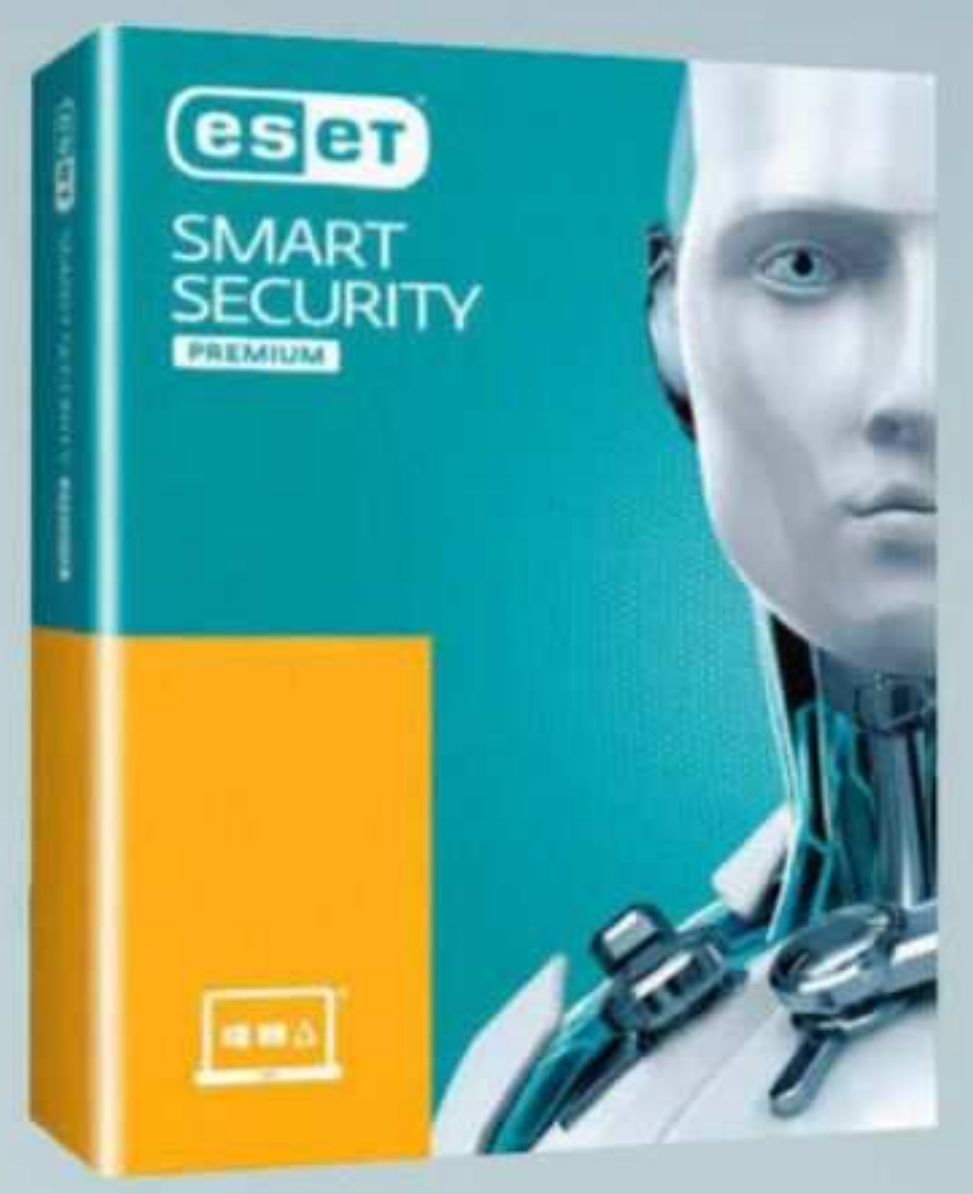
5 G DATA TOTAL SECURITY
Preis: 50,36 Euro*



6 KASPERSKY TOTAL SECURITY
Preis: 100 Euro*

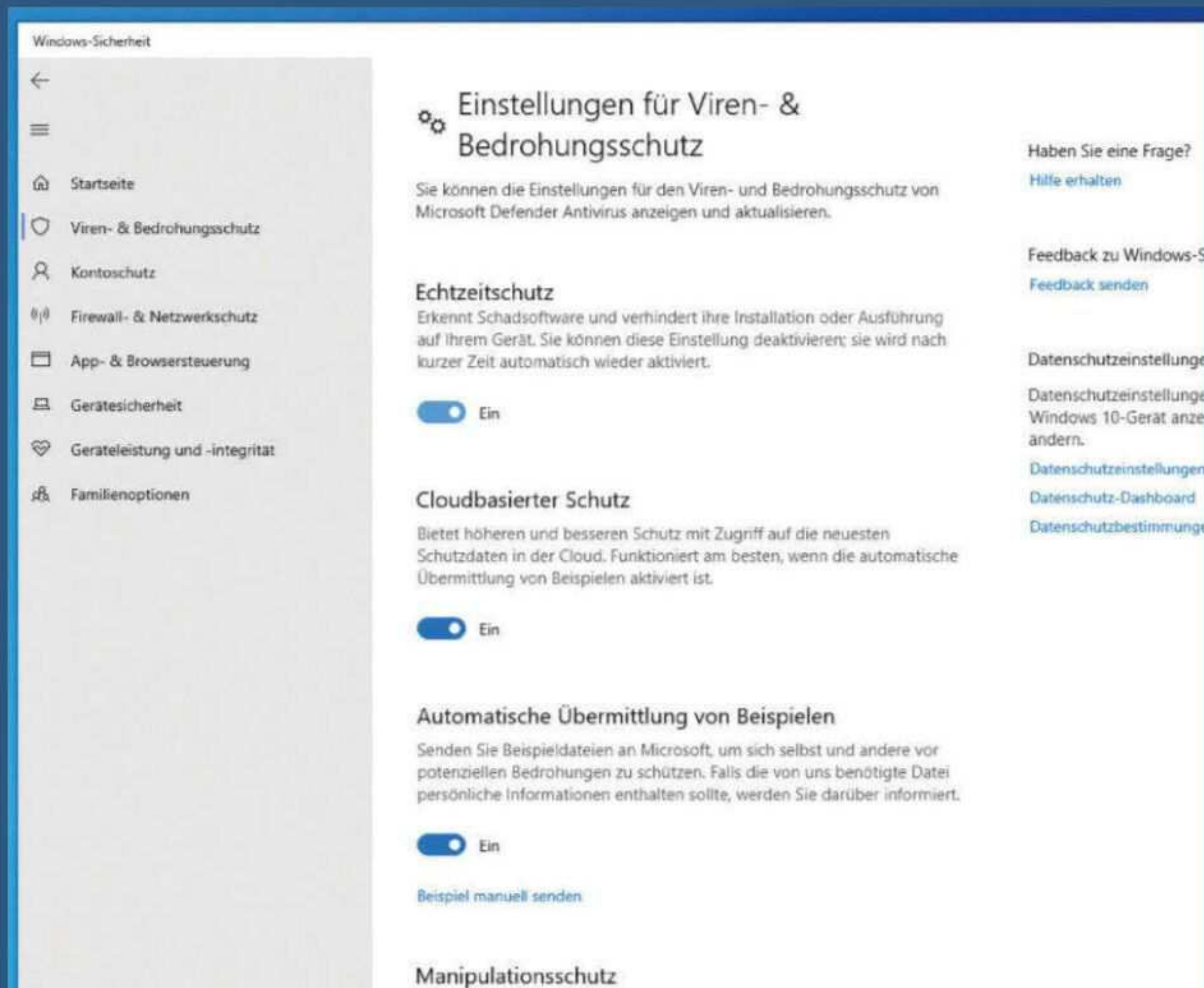


7 MICROSOFT WINDOWS DEFENDER
Preis: kostenlos*

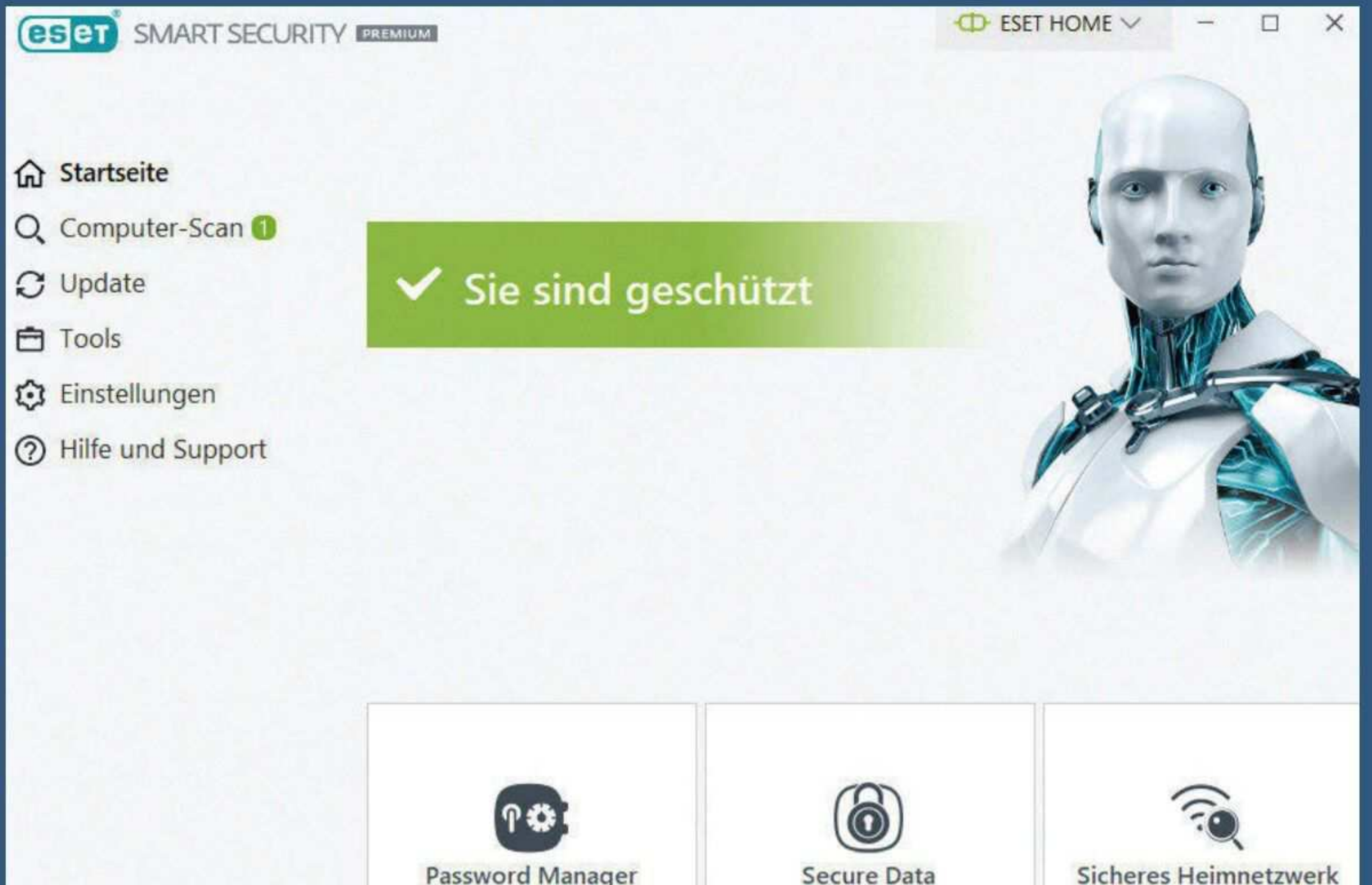


8 ESET SMART SECURITY
Preis: 90 Euro*

Geeignet für: Windows 8, 10, 11 für 5 Geräte		Geeignet für: Windows 8, 10, 11 für 5 Geräte		Geeignet für: Windows 8, 10, 11 für 5 Geräte		Geeignet für: Windows 11		Geeignet für: Windows 8, 10, 11 für 5 Geräte	
Guter Virenschutz	2,2	Guter Virenschutz	2,0	Ordentlicher Online-Schutz	2,5	Noch zuverlässiger Schutz	3,3	Schlechter Schutz	4,4
gering (0,02 %)	1,5	gering (0,02 %)	1,5	etwas hoch (0,07 %)	2,8	etwas hoch (0,09 %)	3,3	hoch (0,14 %)	4,5
schlecht (99,05 % verhindert)	4,2	schlecht (99,19 % verhindert)	3,7	gut (99,73 % verhindert)	1,9	etwas schlecht (99,26 % verhindert)	3,5	sehr schlecht (98,78 % verhindert)	5,1
fast keine (4 / 6)	1,3	wenige (10 / 10)	1,7	fast keine (0 / 3)	1,1	fast keine (3 / 5)	1,3	fast keine (0 / 1)	1,0
etwas schlecht (90,95 %)	3,3	gut (95,5 %)	2,1	sehr schlecht (84,3 %)	4,9	zu schlecht (61,81 %)	6,0	schlecht (88,85 %)	3,8
Wichtige Extras fehlen	3,0	Einige Extras fehlen	3,2	Beste Zusatzausstattung	1,8	Einige Extras fehlen	3,0	Einige Extras fehlen	3,6
Windows-Firewall	1,0	ja	1,0	ja	1,0	Windows Firewall	1,0	ja	1,0
etwas langsam, wenige Server	3,5	nein	6,0	nur 300 MB pro Tag, wenige Server	3,0	nein	6,0	nein	6,0
nein	6,0	ja	1,0	ja	1,0	ja	1,0	ja	1,0
ja	1,0	nein	6,0	ja	1,0	nein	6,0	nein	6,0
nein	6,0	nein	6,0	nein	6,0	ja	1,0	ja	1,0
ja / nein / nein / ja	3,0	nur für Microsoft Produkte / ja / ja / ja	2,1	ja / ja / ja / ja	1,0	nur für Microsoft Produkte / ja / ja / ja	2,3	nein / nein / nein / ja	4,3
Office etwas langsamer	1,5	Kopiervorgänge langsamer	1,8	Office minimal langsamer	1,1	Kopiervorgänge langsamer	2,1	Office minimal langsamer	1,2
sehr gering / gering / etwas hoch	1,5	sehr gering / etwas hoch / gering	1,8	sehr gering / sehr gering / gering	1,1	sehr gering / hoch / gering	2,1	sehr gering / sehr gering / gering	1,2
Etwas umständlich	2,7	Etwas umständlich	3,3	Umständliche Bedienung	3,6	Etwas umständlich	3,0	Etwas umständlich	3,0
keine Funktionssuche, Hilfe nur online	3,2	keine Funktionssuche, nur Direkthilfe auch offline verfügbar	3,2	keine Funktionssuche, nur Direkthilfe auch offline verfügbar	2,8	unlogische Menüstruktur, nur Direkthilfe auch offline verfügbar	3,2	keine Funktionssuche, nur Direkthilfe auch offline verfügbar	2,8
Programmoberfläche nicht immer verständlich, Grundfunktionen per Taskleiste erreichbar	3,4	Systemscan umständlich zu starten, zu wenig Infos bei Virenfund verunsichern	3,2	standardmäßig keine Auswahlmöglichkeit bei Virenfund, Bedienschritte etwas kompliziert	3,3	Programmbestandteile nicht eindeutig benannt, keine klare Nutzerführung	3,8	Systemscan etwas umständlich, wenig Einstellmöglichkeiten bei Virenfund, sonst meist einfach	2,8
erfreulich selten Meldungen	2,4	Meldungen unverständlich	3,9	Meldungen selten, wenig hilfreich	3,4	verständlichste Meldungen im Test	1,7	Meldungen verständlich	2,6
zufriedenstellend / gut	2,3	gut / zufriedenstellend	2,7	mangelhaft / ausreichend	4,3	zufriedenstellend / ausreichend	3,7	mangelhaft / zufriedenstellend	3,7
gut 2,2		gut 2,3		befriedigend 2,5		befriedigend 3,1		ausreichend 3,8	



Der Windows Defender setzt auf Windows-Menüs. Das ist nicht immer leicht verständlich oder gar übersichtlich.



Der Schutz von Eset ist lückenhaft – sogar der in Windows mitgelieferte Defender arbeitete im Test besser.

AVAST ONE

TOP- VIRENSCHU GRAT

Avast One überzeugte im Test mit erstklassigem Virenschutz. Exklusiv bei COMPUTER BILD bekommen Sie es **bis zum 21. April 2023 gratis!**

Noch nie war das Internet so gefährlich wie jetzt! Nicht nur, dass klassische Malware wie Ransomware, Banking-Trojaner und Phishing-Angriffe in Mails und SMS weiter rasant zunehmen. Mit dem Krieg in der Ukraine ist eine neue Dimension dazugekommen, die viele Menschen bisher wohl nur aus Science-Fiction-Filmen kannten: der Cyberwar. Russische Hacker haben bereits Firmen in der Ukraine mit Angriffen lahmgelegt und machen auch auf Putin-Kritiker in Russland Jagd. Unklar ist, ob Deutschland und Europa schon ins Fadenkreuz geraten sind. Umso wichtiger ist es, dass Sie sich

und Ihre Daten schützen! Dafür brauchen Sie ein zuverlässiges Schutzprogramm wie Avast One. Das Programm wappnet Ihren PC hervorragend gegen alle denkbaren Angriffe. Das Beste: Käufer dieses Sonderhefts bekommen es bis zum 21. April 2023 gratis.

Neue Gefahr: Cyberwar

Zuvor zielten Cyberkriminelle fast ausschließlich auf Geld ab. Seit dem Krieg geht es auch darum, möglichst viel und großen Schaden zu verursachen. Zudem scheinen russische Hacker auch den Auftrag zu haben, Identitäten aufzudecken, etwa von Menschenrechtlern und Journalisten.

Wie die Angreifer vorgehen, erklärt Michal Salat, Threat Intelligence Director bei Avast, im Interview oben rechts. Ein gutes Schutzprogramm ist für die Abwehr dieser Gefahren heute und in Zukunft unerlässlich.

Zuverlässiger Virenschutz

Avast One bietet genau das: Mit einer Erkennungsrate von 99,99 Prozent bewies das Programm im COMPUTER BILD-Test ab Seite 58, dass es bestens auf jede Art von Schadsoftware und Cyber-Angriff vorbereitet ist. Selbst staatlich engagierte Hacker werden sich an der Schutzsoftware die Zähne ausbeißen!

Viele Extras

Avast One bietet aber noch viel mehr als effektiven Virenschutz. Zusätzlich gibt es viele sinnvolle Security-Extras, unter anderem den Tresor für sensible Daten, einen Extra-Schutzwall gegen Ransomware-Attacken, einen Webcam-Schutz und einen Privacy-Advisor. All das hilft Ihnen, die Sicherheit Ihres Computers und Ihrer Daten zu stärken.

Und das ist immer noch nicht alles. Denn mit Avast One bekommen Sie ein vollständiges VPN zum anonymen Surfen im Internet – auch das ist in Zeiten wachsender Bedrohungen wichtig. Last but not least dürfen Sie sich



„Seit dem Krieg gibt es viele schwere Cyber-Angriffe.“

Michal Salat
Threat Intelligence Director, Avast



COMPUTER BILD: Stellen Sie im Zusammenhang mit dem Ukraine-Krieg vermehrt Cyber-Attacken fest?

Michal Salat: Unmittelbar vor der Invasion haben wir deutlich mehr Phishing-Angriffe gesehen. Ziele waren zum Beispiel ein Produzent von Netzwerk-Technik und ein Domainverwalter. Aber auch Logistiker, Web-Hoster und Job-Plattformen waren unter Beschuss.

Kann man die Angriffe direkt mit Russland in Verbindung bringen?

Man kann nie sicher sein, wer wirklich hinter einem Angriff steckt. Profis verschleiern ihre Spur über mehrere Stationen im Internet. Manchmal findet man Hinweise im Schadcode, wenn etwa der Schädling so programmiert ist, dass er auf Computern mit russischen Tastaturen nicht aktiv wird. Aber oft werden Angriffsmodule auch auf internationalen Hacker-Märkten gehandelt und geteilt. Die Suche nach Urhebern ist sehr zeitintensiv.

Wie arbeiten staatliche Hacker?

Je nach Gruppe ganz unterschiedlich. Aber im Prinzip ist ihr Ziel kein anderes als das von traditionellen Spionen: Sie sammeln Informationen, am besten an strategisch wichtigen Positionen. Dazu nutzen sie oft auch exklusive Informationen über Sicherheitslücken. Die kaufen sie zum Beispiel von privatwirtschaftlichen Unternehmen wie Zerodium.

über die Tuningfunktionen der Suite freuen, mit denen Sie die Leistung des PCs verbessern beziehungsweise wiederherstellen.

Bis April 2023 gratis für Sie

Als Käufer dieses COMPUTER BILD Sonderhefts erhalten Sie Avast One bis zum 21. April 2023 gratis. Dafür müssen Sie das Programm spätestens bis zum 15. Oktober 2022 wie ab Seite 70 beschrieben installieren und aktivieren. Die Version auf der Heft-DVD ist identisch mit Avast One Individual (siehe Kasten rechts). Der einzige Unterschied: Die Lizenz ist nur für ein Gerät pro Avast-Account gültig.

DAS STECKT IN IHREM AVAST ONE

Als Käufer dieses Sonderhefts erhalten Sie Avast One mit allen Funktionen der Individual-Version (siehe rechts im Vergleich mit der kostenlosen Essential-Variante). Die Lizenz läuft bis zum 21. April 2023 und ist auf ein Gerät begrenzt. Wer mehr benötigt, bekommt auf cobi.de/42134 die 5-Geräte-Version für 26,28 Euro und die 30-Geräte-Variante für 35,88 Euro – eine Ersparnis von bis zu 70 Prozent gegenüber dem regulären Verkaufspreis.

IHRE SICHERHEIT GANZ NACH IHREN WÜNSCHEN

	AVAST ONE ESSENTIAL	AVAST ONE INDIVIDUAL
Blockieren Sie Viren und andere Malware	✓	✓
Überwachen Sie Apps auf verdächtige Aktivitäten	✓	✓
Erweiterte Firewall, um Eindringlinge zu blockieren	✓	✓
Blockieren Sie Spionageangriffe per Webcam	X	✓
Schützen Sie sich vor gefälschten und gefährlichen Webseiten	X	✓
Geben Sie Ihren sicheren Dateien zusätzlichen Schutz	X	✓
Genießen Sie ein unbegrenztes VPN mit 55 Standorten	X	✓
Überwachen Sie Ihre Online-Konten auf Datenlecks	X	✓
Aktualisieren Sie Ihre Treiber automatisch	X	✓
Schützen Sie sich davor, von Werbe-Unternehmen verfolgt zu werden	X	✓
Bereinigen und optimieren Sie Ihre Geräte	X	✓

SCHNELLER

Auch für Mac

Ob Sie lieber einen Windows-PC oder einen Mac mit Avast One schützen möchten, entscheiden Sie selbst: Die COMPUTER BILD-Lizenz gilt für beide Systeme – Sie finden beide Programmversionen auf der Heft-DVD.

Schritt für Schritt erklärt

Wie bei allen Schutzprogrammen gilt auch bei Avast One: Mehrere Antiviren-Programme auf demselben Gerät behindern sich gegenseitig, und Installationsreste vorheriger Schutzpakete können Probleme verursachen. Sie müssen das alte Programm daher vor der Installation von Avast One restlos entfernen. Wie Sie das am besten machen, den Aktivierungscode einlösen und das neue Avast One installieren, erklärt COMPUTER BILD Schritt für Schritt ab Seite 70. Planen Sie dafür circa eine Stunde ein.

Und natürlich erfahren Sie auch, wie Sie bei einem Virenfund richtig reagieren und alles aus den vielen nützlichen Zusatzfunktionen der Suite rausholen.

Kostenlose Hilfe

Wenn Sie die Anleitungen befolgen, sollte bei Einrichtung und Nutzung des Programms nichts schiefgehen. Falls dennoch etwas nicht klappt oder Sie Fragen zum Programm haben, erreichen Sie die COMPUTER BILD-Redaktion unter der E-Mail-Adresse redaktion@computerbild.de und die Experten vom Avast-Kundensupport auf der Internetseite support.avast.com. [av]

LINKS IM PROGRAMMFENSTER FINDEN SIE VIER MENÜPUNKTE:

START: Gibt einen Überblick über den Schutzstatus. Hier können Sie auch einen Smart-Scan starten.

ENTDECKEN: Nach einem Klick darauf sehen Sie alle Funktionen des Programms übersichtlich aufgelistet.

NACHRICHTEN: Hier finden Sie beispielsweise Informationen zu neuen Updates.

KONTO: Nach Klick darauf erscheinen die Funktionen für Ihr Avast-Konto.

Im Beispiel sehen Sie das Fenster „Entdecken“. Darin listet Avast alle Schutz- und Tuningfunktionen auf. Wählen Sie eine aus, und Sie sehen weitere Infos.

Unter der Funktionsbeschreibung stehen eine oder mehrere Schaltflächen, um die jeweilige Funktion auszuwählen und zu starten.

Avast One



Start



Entdecken



Nachrichten



Konto

GERÄTESCHUTZ



Scan



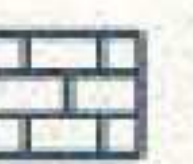
Dateien



Web-Schutz



Ransomware



Firewall



Quarantäne



Schutz



Web-Hygiene

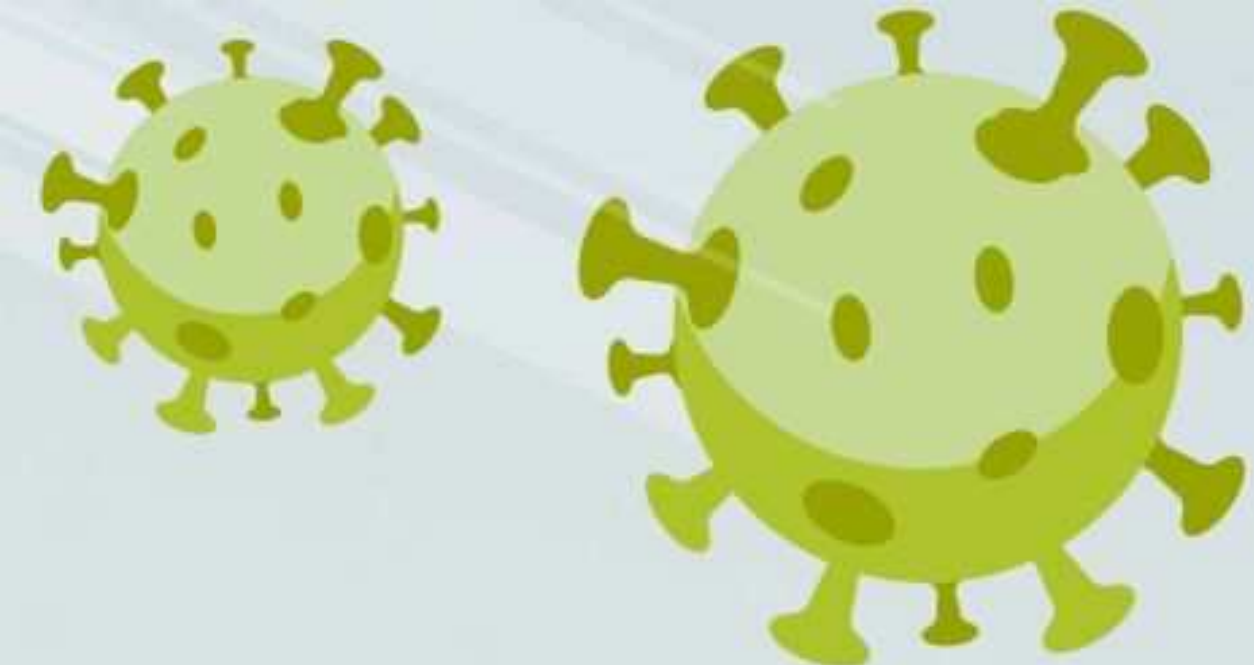


Web-Reinigung

PRIVATSPHÄRE



VPN



ÜBERBLICK



UTZ

Center

Schutz

Schutz

mware-Schutz

all

antäne

z für sensible Daten

Hijack Guard

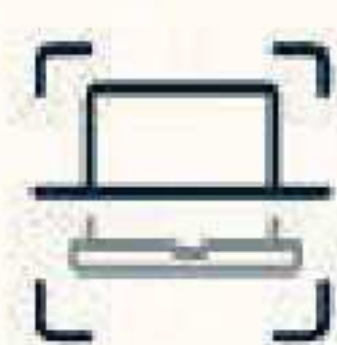
am-Schutz

RE IM INTERNET

Sichere Verbindung

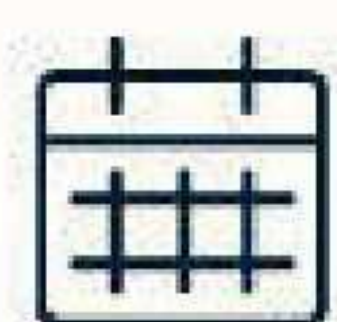
Scan Center

Alles, was Sie brauchen, um Ihren PC sicher und virenfrei zu halten. Wir finden Malware, wo auch immer sie sich versteckt, und führen automatisch geplante Scans durch.



Alle Bereiche Ihres PCs auf Malware überprüfen

Von einem optimierten Smart Scan bis hin zu einem Tiefenscan Ihres Systemspeichers und externen Datenträgers – wir haben für jeden Bedarf einen Scan.



Benutzerdefinierte und voreingestellte Scans automatisch ausführen

Wählen Sie aus, was und wo Sie überprüfen möchten, und planen Sie benutzerdefinierte oder voreingestellte Scans, die später oder wiederholt durchgeführt werden sollen.

Smart-Scan ausführen

Scan Center öffnen

Letzter Smart-Scan: niemals

INSTALLATION UND FREISCHALTUNG

So installieren Sie die Jahresversion von **Avast One** und schalten die Vorteile der COMPUTER BILD-Version frei.

Der Umstieg auf ein neues Schutzprogramm ist leider etwas aufwendiger. Vor der Installation müssen Sie Ihre alte Antiviren-Software deinstallieren und letzte Spuren beseitigen. Dann

erst ist Ihr Rechner bereit für die neue Security Suite.

Aber keine Sorge, COMPUTER BILD erklärt Ihnen Schritt für Schritt, wie Sie das machen. Sie können Ihre Avast-One-Lizenz für

Windows oder MacOS verwenden. Beide Versionen finden Sie auf der Heft-DVD. COMPUTER BILD erklärt auf dieser Doppelseite, wie der Umstieg mit Windows 10 funktioniert. Die Schritte mit

Windows 11 und MacOS sind fast alle identisch. Sollten Sie trotzdem Probleme haben, finden Sie auf www.cobi.de/go/avastmac eine Anleitung zur Installation auf MacOS.

1 ALTE SCHUTZSOFTWARE DEINSTALLIEREN

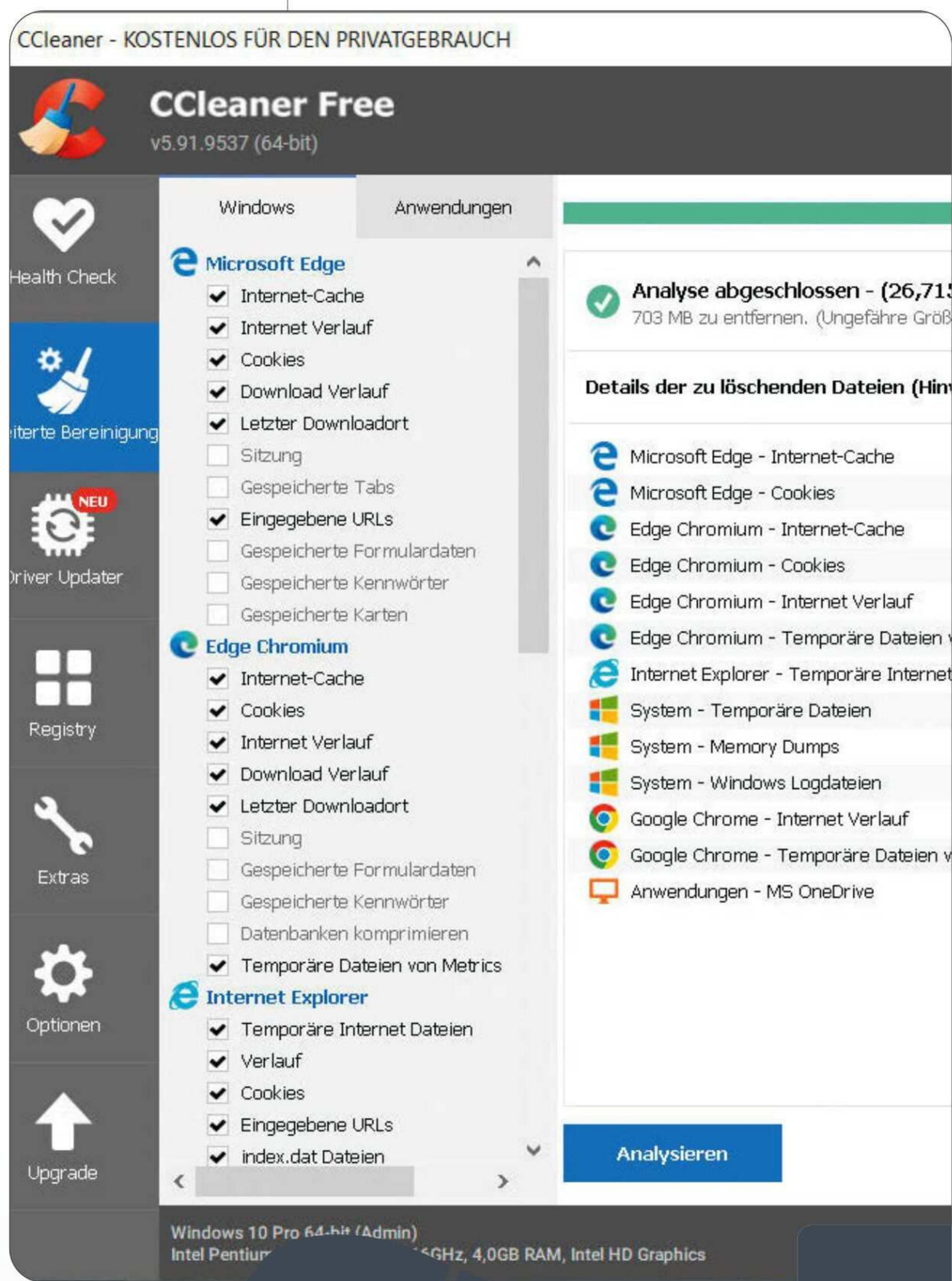
Bevor Sie mit der neuen Avast-One-Suite loslegen können, müssen Sie Ihr altes Schutzprogramm deinstallieren. Anschließend entfernen Sie letzte Spuren, die bei der Installation Probleme machen könnten.

1 Öffnen Sie zur Deinstallation die Windows-Einstellungen mit + , und klicken Sie auf **Apps**. Im neuen Fenster suchen Sie den Eintrag des alten Schutzprogramms, klicken darauf und auf **Deinstallieren**. Nach einer Windows-Sicherheitsabfrage und einem Klick auf **Ja** startet das Deinstallationsprogramm des Herstellers. Folgen Sie den Anweisungen, und deinstallieren Sie das Programm. Falls Sie gefragt werden, ob Sie Daten für eine Neuinstallation behalten wollen, verneinen Sie das.

2 Nach der Deinstallation ist ein Neustart notwendig. Falls das Deinstallationsprogramm das nicht schon automatisch getan hat, starten Sie den PC manuell neu. Falls Sie TuneUp installiert haben, müssen Sie das auf dieselbe Weise deinstallieren.

3 Nun entfernen Sie übrig gebliebene Installationsreste und Registry-Schlüssel. Dazu benötigen Sie den CCleaner. Sie finden ihn unter cobi.de/12545. Starten Sie das Programm, und klicken Sie auf **Erweiterte Bereinigung** und **Analysieren**. Nach Abschluss der Analyse folgen Klicks auf **Cleaner starten** und **Fortfahren**.

4 Zum Entfernen der Registry-Schlüssel klicken Sie anschließend auf **Registry** und **Nach Fehlern scannen**. Nach der Suche folgen Klicks auf **Ausgewählte Probleme untersuchen**, **Ja**, **Speichern**, **Ausgewählte Fehler beheben** und **Schließen**. Holen Sie sich dann Ihren Aktivierungscode, wie auf der nächsten Seite beschrieben.



2 AKTIVIERUNGSCODE HOLEN UND AVAST-ACCOUNT ERSTELLEN

Bevor Sie mit der eigentlichen Installation starten, holen Sie sich Ihren persönlichen Aktivierungscode. Den aktivieren Sie dann in Ihrem Avast-Konto. So geht's:

1 Klicken Sie auf der Heft-DVD beim Eintrag von Avast One auf **Code**. Leser ohne Laufwerk öffnen die Seite **vorteilcenter.de**. Dort finden Sie auch den Download für den nächsten Schritt. Auf der folgenden Internetseite geben Sie den Vorteilcenter-Code von der Rückseite der DVD-Hülle ein. Anschließend sehen Sie Ihren Aktivierungscode für Avast One. Kopieren Sie ihn per Klick auf **Ko-**

pieren, und klicken Sie auf **Zur Aktionsseite**, um zur Avast-Aktivierungsseite zu gelangen.

2 Auf der sich öffnenden Internetseite fügen Sie den Aktivierungscode in das dafür vorgesehene Feld und klicken auf **Continue**. Anschließend melden Sie sich mit Ihrem Avast-Konto an. Falls Sie noch kein Avast-Konto haben, klicken Sie auf **Create an account** und folgen den Anweisungen, um einen zu erstellen. Die Lizenz wird dann in beiden Fällen in Ihrem Benutzerkonto aktiviert, und es geht mit der Installation des Programms weiter.

Activate your subscription

Enter your activation code

Try looking for your code in the same place where you found the link to this screen.

Activation code

Enter a valid activation code

By clicking "Continue", you confirm that you've read and agree to our [Privacy Policy](#) and [End User License Agreement](#).

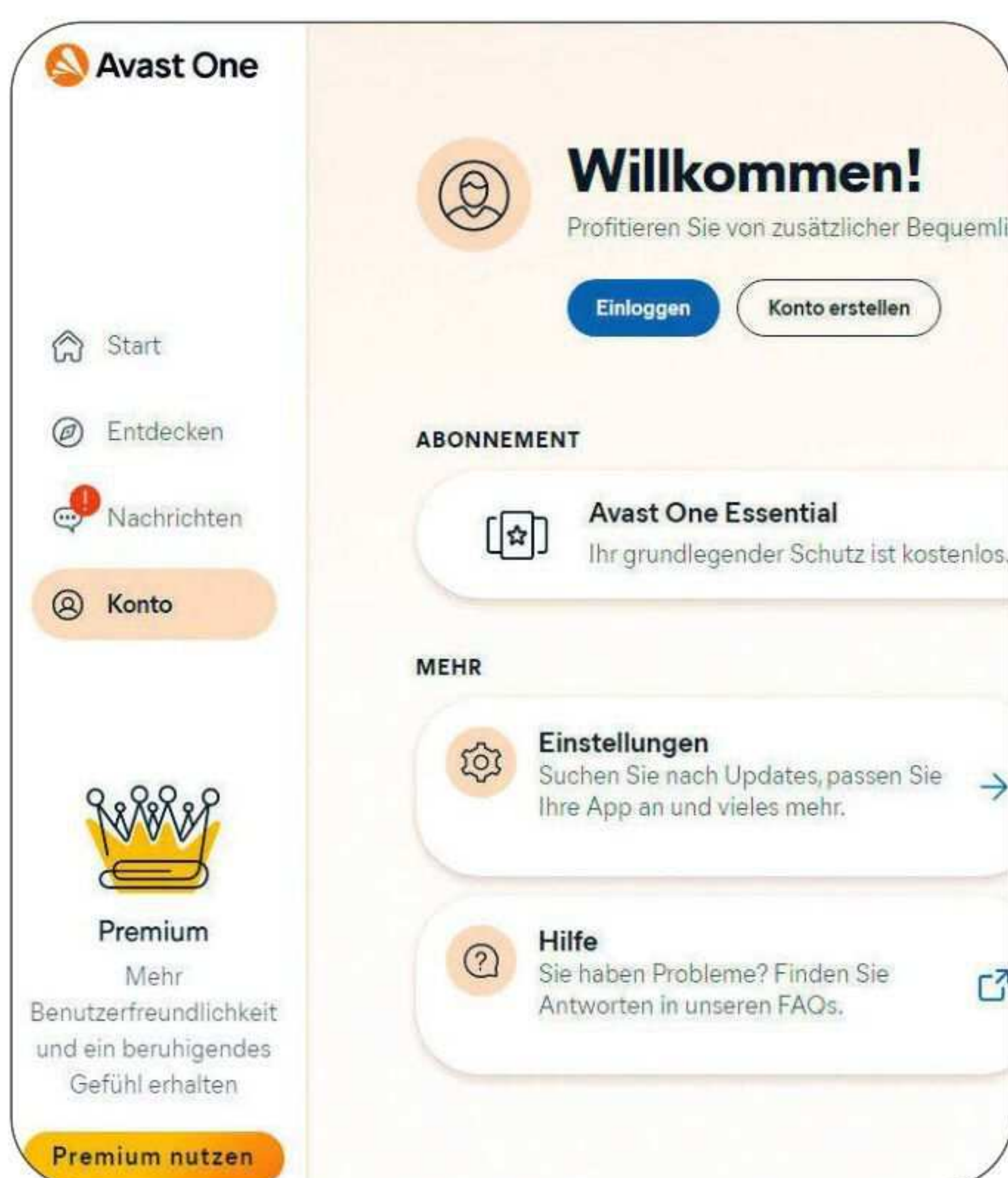
CONTINUE

3 DIE AVAST-ONE-SUITE INSTALLIEREN UND FREISCHALTEN

1 Starten Sie die Installation von der Heft-DVD mit einem Klick auf **Windows** oder **Mac** beim Eintrag von Avast. Leser ohne Laufwerk öffnen stattdessen **vorteilcenter.de** und laden dort die passende Programmversion herunter.

2 Folgen Sie bei der Installation den Anweisungen auf dem Bildschirm. Die Installation selbst ist in wenigen Minuten erledigt.

3 Nach der Installation ist ein Neustart notwendig. Danach öffnet sich Avast One automatisch. Auf dem Mac müssen Sie noch einige Zugriffsberechtigungen erteilen, Avast One erklärt Ihnen aber direkt, wie das geht.



4 Nun müssen Sie sich in der Software anmelden. Auf dem Mac werden Sie direkt dazu aufgefordert. Folgen Sie einfach den Anweisungen auf dem Bildschirm. Auf Windows-PCs müssen Sie zuvor einen Smart-Scan starten. Klicken Sie nach dem Scan direkt auf **Konto** und oben auf **Einloggen**.

5 Daraufhin öffnet sich Ihr Browser. Melden Sie sich auf der Avast-Seite mit Ihrem Avast-Konto an, und klicken Sie im erscheinenden Browser-Popup auf **Avast One öffnen**. Die Lizenz wird dann in das Programm übernommen und Avast One von der kostenlosen auf die volle Version umgestellt.

Fotos: iStock, Hersteller; Montage: COMPUTER BILD

DAS KANN IHR AVAST ONE

Neben dem Virenschutz enthält Avast One noch eine Menge zusätzlicher Funktionen für mehr Sicherheit, Leistung und Privatsphäre.

1 ERSTE VIRENSUCHE MIT SMART-SCAN

Wer sich nicht mit jeder einzelnen Funktion des Programms beschäftigen oder nur einen kurzen Check machen möchte, startet einfach den Smart-Scan. Der prüft alle Einstellungen und behebt Probleme automatisch.

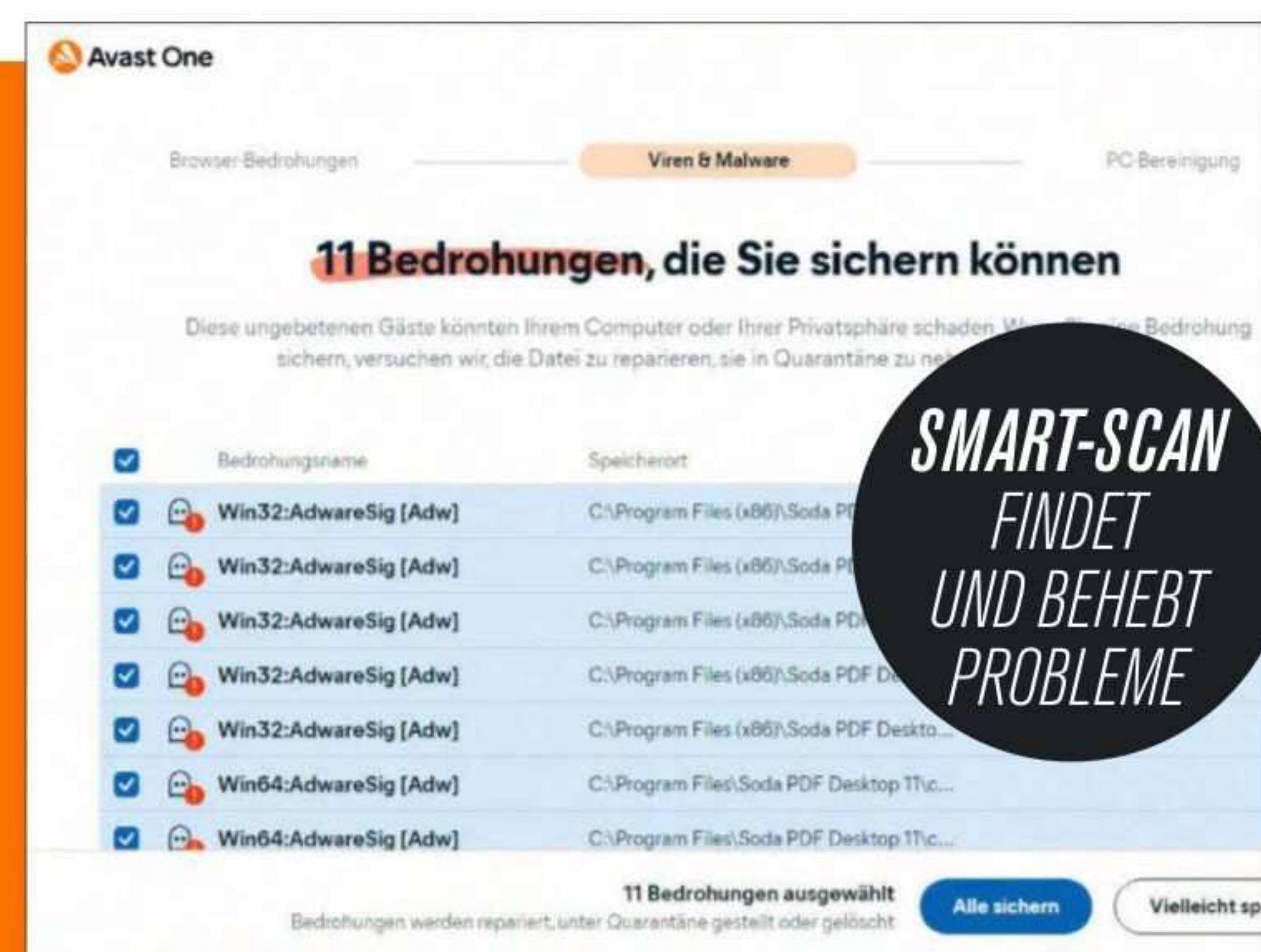
1 Klicken Sie nach dem Programmstart auf **Smart-Scan ausführen**, und lassen Sie Avast One Ihren PC checken.

2 Das Programm führt Sie in drei Schritten durch den Scan: Browser-Bedrohungen, Viren & Malware und PC-Bereinigung. Nach jedem Scan zeigt es gefundene Probleme an und behebt sie.

3 Nach dem ersten Smart-Scan bietet das Programm an, diesen regelmäßig

automatisch durchzuführen. Lassen Sie sich dazu einfach die Vorauswahl aktiviert und klicken auf **Fertig**.

4 Der Smart-Scan scannt alle kritischen Bereiche des PCs und entdeckt alle akuten Gefahren. Möglicherweise verstecken sich aber inaktive Viren in unüblichen Verzeichnissen. Um solche Schadprogramme gleich aufzustoßern, starten Sie einen Tiefenscan mit Klicks auf **Entdecken, Scan Center, Scan Center öffnen** und **Tiefenscan**. So finden Sie wirklich alle Schädlinge. Der Tiefenscan benötigt aber deutlich mehr Zeit und kann gerade beim ersten Mal ein paar Stunden dauern.



Scan Center

Alles, was Sie brauchen, um Ihren PC sicher und virenfrei zu halten. Wir finden Malware, wo auch immer sie sich versteckt, und führen automatisch geplante Scans durch.

Jetzt scannen Benutzerdefinierte Scans Scan-Verlauf



Smart-Scan

Finden und entfernen Sie Viren und lösen Sie die häufigsten Probleme in den Bereichen Privatsphäre und Leistung.

Smart-Scan ausführen



Tiefenscan

Letzter Scan: nie



Gezielter Scan

Letzter Scan: nie



Startzeit-Prüfung

Nicht geplant

2 BESONDERER SCHUTZ FÜR SENSIBLE DATEN

Einige Dateien auf der Festplatte sollten besser nicht in die Hände Dritter fallen – etwa eingescannte Ausweise, Rechnungen und Dokumente mit Infos über Sie. Mit dem Schutz für sensible Daten bestimmen Sie, welche Programme und Personen solche Dateien öffnen dürfen.

1 Öffnen Sie Avast One, und klicken Sie auf **Entdecken, Schutz für sensible Daten** und **Schutz für sensible Da-**

ten öffnen. Klicken Sie auf **Auf sensible Dokumente überprüfen**. Avast One sucht nun automatisch nach Dokumenten mit Hinweisen auf Ihre Identität. Mit dem Button unten können Sie später aber auch selbst Dateien hinzufügen.

2 Mit Klicks auf **Nutzerberechtigungen** und **App-Berechtigungen** bestimmen Sie dann, welche Personen und Programme diese Dateien öffnen dürfen.

Schutz für sensible Daten

Wir finden und schützen Dokumente, die Ihre persönlichen Daten enthalten, sodass Sie sicher sein können, dass Ihre Identität nicht durch Eindringlinge oder Malware gefährdet wird.

[Auf sensible Dokumente überprüfen](#)

Geschützte Dokumente

Nutzerberechtigungen

App-Berechtigungen

☐ Dokument

Speichern

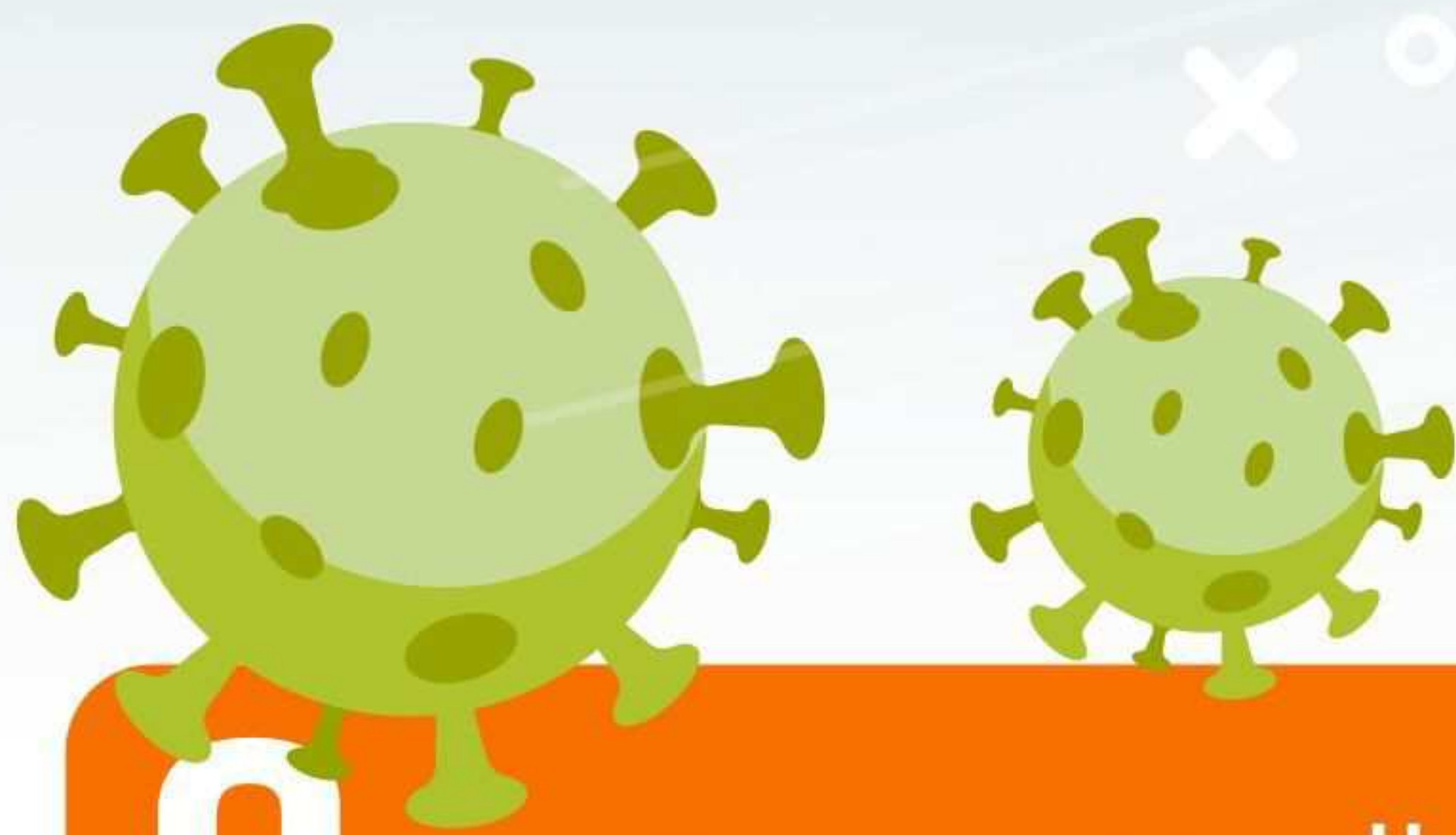
☐ Ausweise.docx

C:\Users\

☐ Lebenslauf.docx

C:\Users\





3 IM FALL DER FÄLLE: VIRENFUND GENAU ANALYSIEREN

Avast schützt Ihren PC automatisch vor Viren und anderen Schädlingen. Findet das Programm etwas, reagiert es auch automatisch und verschiebt Dateien in die Quarantäne oder blockiert Zugriffe.

Sie sehen dann die unten gezeigte Meldung. Das ist zu tun:

1 Prüfen Sie in solchen Fällen, was genau passiert ist. In diesem Beispiel hat Avast One eine infizierte Datei entdeckt und in die Quarantäne geschoben.

2 Schauen Sie, ob Sie das Programm kennen und benötigen. Kryptische Namen wie hier sind ein Anzeichen dafür, dass es tatsächlich ein Schadprogramm ist. Weitere Informationen finden Sie nach einem Klick auf **Details anzeigen**. Dort

sehen Sie etwa den Dateipfad und auch warum es verschoben wurde. In diesem Fall war es eine Adware, die Teil eines nützlichen Programms ist, aber ständig mit Werbung nervt.



4 ANONYM UND SICHER IM INTERNET SURFEN

VPNs (Virtuelle private Netzwerke) sind äußerst beliebt – etwa, um auf Streaming-Angebote im Ausland zuzugreifen. Und die Dienste erhöhen auch die Sicherheit beim Surfen. Ein VPN baut nämlich eine verschlüsselte Verbindung auf und verhindert damit, dass jemand im Netzwerk mitlesen kann. Das ist vor allem für öffentliche WLANs wichtig. Zudem verschleiern VPNs Ihre IP-Adresse, sodass auch die besuchte Seite Sie nicht erkennt. Das Avast VPN finden Sie mit Klicks auf **Entdecken** und **VPN Sichere Verbindung**. Wollen Sie nur schnell eine sichere Verbindung herstellen, klicken Sie einfach auf den Schalter, und schon surfen Sie verschlüsselt über einen Avast-Server. Wollen Sie sich stattdessen mit einem Server in einem bestimmten Land verbinden, klicken Sie auf **VPN öffnen**. Hier können Sie das Verbindungsland frei wählen. Anschließend

können Sie auch einstellen, dass sich das VPN automatisch aktivieren soll, wenn Sie im öffentlichen WLAN sind oder anfällige Seiten besuchen. Zudem finden Sie hier den Kill-Switch, der sofort die komplette Internetverbindung kappt, wenn die VPN-Verbindung einmal ausfallen sollte.



KURZTIPPS

5 Ransomware-Schutz

Avast One kontrolliert den Zugriff auf wichtige Dateien und verhindert, dass Schadprogramme Ihre Daten verschlüsseln. Gängige Speicherorte schützt es automatisch. Weitere fügen Sie nach Klicks auf **Entdecken, Ransomware-Schutz, geschützte Ordner anzeigen** und **einen neuen Ordner schützen** hinzu. Zudem bestimmen Sie dort, welche Dateitypen grundsätzlich geschützt werden und können Apps den unbeschränkten Zugriff erlauben.



6 Privates Surfen

Der private Modus Ihres Browsers verhindert nur, dass Spuren auf Ihrem PC zurückbleiben. Für die besuchten Seiten sind Sie alles andere als anonym. Avast One bietet einen echten privaten Modus. Dabei verhindern Tracking-Schutz und VPN, dass Sie auf den besuchten Seiten oder im öffentlichen WLAN erkannt werden. Sie finden die Funktion unter **Entdecken** und **Privater Modus**.



7 Mehr Privatsphäre

Google, Facebook & Co. speichern eine Menge Daten über Sie. Der Privacy Advisor führt Sie durch deren Einstellungen, um die Sammelwut zu begrenzen. Sie öffnen ihn mit Klicks auf **Entdecken, Privacy Advisor** und **Privacy Advisor starten**.

Fotos: Hersteller, iStock; Montage: COMPUTER BILD

8 DATENMÜLL ENTSORGEN

Auf dem PC sammelt sich mit der Zeit immer mehr Datenmüll an: Installationsreste, Überbleibsel alter Windows-Versionen und Downloads sind Speicherfresser, die auf fast jedem PC zu finden sind. Avast One hilft Ihnen dabei, die Festplatte zu entrümpeln. Klicken Sie dazu auf **Entdecken, Speicher-Bereinigung** und **Überprüfen Sie... XX GB an Datenmüll**. Im neuen Fenster zeigt Avast die gefundenen Dateien in vier Kategorien mit der entsprechenden Größe an. „Download und Papierkorb“ ist nicht ausgewählt, weil Sie die Downloads ja eventuell noch benötigen. Per Klick auf die Pfeile hinter den einzelnen Kategorien sehen Sie, was genau Avast löschen möchte. Die Reinigung starten Sie per Klick auf **Jetzt bereinigen**.

9 SOFTWARE AKTUELL HALTEN

Alte Programmversionen enthalten oft Sicherheitslücken und stellen damit ein Risiko dar. Sie sollten daher alle installierten

Programme aktuell halten. Leider bietet nicht jede Software eine eingebaute Update-Funktion an. Hier springt der Software-Updater ein: Nach Klicks auf **Entdecken, Software-Updater** und **Software-Updater öffnen** prüft Avast alle Programme und zeigt Ihnen an, wenn es neuere Versionen gibt. Mit Klicks auf **Aktualisieren** hinter dem Eintrag starten Sie das Update. Teilweise startet der Klick nur den Download des Updates. Zur Installation ist dann ein weiterer Klick auf **Aktualisieren** nötig.

5 Apps, die Sie aktualisieren können

Wir halten Ihre installierten Anwendungen auf dem neuesten Stand und sorgen so für weniger Fehler, mehr Sicherheit und eine optimale Leistung. [Auf Updates überprüfen](#)

App-Name	Aktualisieren auf
<input type="checkbox"/> Mozilla Thunderbird Ihre Version 68.2.2	68.12.1
<input type="checkbox"/> 7-Zip Filemanager (64 Bit) Ihre Version 19.0.0.0	21.7
<input type="checkbox"/> AnyDesk Ihre Version 6.2.6.0	7.0.7
<input type="checkbox"/> CCleaner Ihre Version 5.88.0.9346	
<input type="checkbox"/> Mozilla Firefox (64 Bit) Herunterladen...	98.0

1 App wurde in den letzten 14 Tagen aktualisiert
Steam

10 COMPUTER-LEISTUNG FÜR WICHTIGE PROGRAMME OPTIMIEREN

Viele Programme bleiben auch dann aktiv, wenn sie geschlossen sind. Sie starten automatisch mit dem Hochfahren von Windows. Das macht Ihren PC langsam und verzögert Arbeiten mit den Programmen, die Sie wirklich nutzen. Mit Avasts PC-Beschleunigung optimieren Sie Hintergrundprozesse und automatisch startende Programme. So wird Ihr PC wieder schnell wie am ersten Tag.

1 Klicken Sie auf **Entdecken, PC-Beschleunigung** und **XX nicht optimierte Apps überprüfen**.

Nach der Suche schließen Sie das Hinweisenster per Klick auf **OK**.

2 Avast zeigt nun alle Apps an, die im Hintergrund laufen, und ordnet sie nach Einfluss auf die Leistung Ihres PCs. Mit einem Klick auf **Optimieren** hinter den Einträgen lassen Sie Avast die Programme so optimieren, dass sie Ihre Arbeit nicht wesentlich stören. Das bedeutet, unnötige Hintergrundprozesse werden abgeschaltet oder starten künftig gar nicht mehr automatisch. Sie können die Programme trotzdem

weiterhin normal nutzen. Lediglich der Programmstart kann ein wenig länger dauern. Optimieren Sie nun nach Wunsch alle Apps.

3 Oben sehen Sie die Gesamtbeeinträchtigung der Systemleistung. Achten Sie darauf, dass diese am Ende „niedrig“ ist. Unter den aufgelisteten Programmen finden Sie zudem ein FAQ mit den häufigsten Fragen und Antworten zu diesem Thema.

28 Apps verlangsamen Ihr Gerät

Einige Apps sind auch dann aktiv, wenn sie geschlossen sind. Optimieren Sie sie, um unnötige Hintergrundaktivität zu verhindern und Ihren PC zu beschleunigen.

Die gesamte Beeinträchtigung Ihrer Leistung ist **hoch** ⓘ

0 % 100 %

Programm	Leistungsbeeinträchtigung
Microsoft 365 Apps for Enterpris... Ein Office-Paket. Optimieren ... Details »	<div><div></div></div> Mittel
Advanced SystemCare Uns liegen derzeit keine Infor... Details »	<div><div></div></div> Niedrig
PDF Architect 7 Uns liegen derzeit keine Infor... Details »	<div><div></div></div> Niedrig
Rohos Logon Key 4.0 Uns liegen derzeit keine Infor... Details »	<div><div></div></div> Niedrig

11 ALLE TREIBER AUF STAND BRINGEN

Ohne Treiber funktionieren Ihre angeschlossenen Geräte nicht. Diese Programme „übersetzen“ systemweit Befehle an die Geräte. Dafür benötigen sie aber recht weitreichende Rechte. Und genau das macht sie besonders angreifbar. Sicherheitslücken in Treibern oder Malware, die sich als Treiber tarnt, können verheerende Auswirkungen haben. Mit dem Treiber-Updater von Avast gehen Sie sicher, dass Sie immer die neu-

este Version haben und sich keine gefälschten Treiber einmischen.

1 Klicken Sie auf **Entdecken, Driver Updater** und **Überprüfen Sie XX Updates**, um die Updatesuche zu starten.

2 Avast zeigt Ihnen dann eine Liste mit Treibern an, für die es neue Versionen gibt (siehe Bild rechts). Treiber, die aktuell sind, finden Sie ausgeblendet

darunter. Mit Klicks auf **Jetzt aktualisieren** und **Treiber aktualisieren** bringen Sie alle Treiber auf den neuesten Stand. Davor sollten Sie alle offenen Programme schließen und Dokumente speichern. Die Aktualisierung kann einige Minuten dauern, gegebenenfalls ist ein Neustart nötig. Anschließend ist Ihr System wieder sicher. Zudem verbessern die Treiber-Updates häufig auch die Funktionsweise der Geräte und beheben Fehler.

TREIBER-UPDATES
SCHLIESSEN SICHERHEITSLÜCKEN

3 Treiber, die Sie aktualisieren können

Weniger Abstürze, mehr Sicherheit und einen schnelleren PC genießen, indem wir Ihre Gerätetreiber aktualisieren. Wir werden Sie benachrichtigen, wenn Treiber-Updates verfügbar sind. [Nach neuen Treibern suchen](#)

☒ Treiber

<input checked="" type="checkbox"/>	 Audio Realtek High Definition Audio	Neue Veröffentlichung: 17. Aug. 2021	>
<input checked="" type="checkbox"/>	 System Intel(R) Trusted Execution Engine Interface	Neue Veröffentlichung: 3. Jan. 2017	>
<input checked="" type="checkbox"/>	 USB OEM Geneic Radio Switch Device	Neue Veröffentlichung: 16. Mai 2018	>

☒ **48 Treiber sind auf dem neuesten Stand**
Akku, Audio, Bluetooth und 9 weitere...

3 Treiber ausgewählt

Die Aktualisierung der Treiber kann eine Weile dauern

Jetzt aktualisieren

...

DIE VERBOTEN GUTE HEFT-DVD

GUTE TOOLS

BÖSE TOOLS

GRATIS
AUF HEFT-
DVD

**HACKER
TOOLS**
2021

H
HACKER
TOOLS
2021

- 🔍 Verschollene Daten finden
- 🕒 Datenspuren auswerten
- 🔑 Passwörter knacken

**ERK ABSICHERN
KENNWÖRTER STEHLEN**



**KINDER SCHÜTZEN
SURFVERHALTEN AUFDECKEN**



**GEHEIMNISSE WAHREN
CHATS ENTHÜLLEN**



**ANGRIFFE AUFDECKEN
KOLLEGEN ÜBERWACHEN**



**PRIVATSPHÄRE SCHÜTZEN
DATEN AUSSPIONIEREN**



**FESTPLATTE TESTEN
ARBEITSZEIT KONTROLLIEREN**



**WINDOWS ENTPERREN
DEN PC SABOTIEREN**



**IST DIE HACKER-DVD
LEGAL?**



„Wer die DVD nur zum
Schutz eigener Geräte
und Daten nutzt, ist
rechtlich auf der
sicheren Seite!“

Dirk General-Kuchel
Chefredakteur

Nur wer die Tricks der Hacker kennt, ist dagegen gefeit – mit dieser DVD **schützen Sie Ihren PC und Ihre Daten.**

Angriff ist bekanntlich die beste Verteidigung – das gilt auch für die IT-Sicherheit. Denn wer vorab mit Profi-Werkzeugen einen Angriff auf eigene Geräte durchspielt, kennt die Fallstore der Gauner anschließend ganz genau. Kommt noch etwas Fachwissen hinzu, so sind die Schwachstellen schnell behoben und die Cyberkriminellen künftig chancenlos. Mit der Heft-DVD und diesem COMPUTER BILD-Sonderheft halten Sie alles Wichtige schon in der Hand: Software, mit der Sie Sicherheitslücken auf dem PC und im Heimnetzwerk aufspüren, und die passenden Anleitungen, um erkannte Risiken zu beheben!

Böse Tools, guter Zweck

Die Hacker-DVD enthält Forensik-Tools, wie sie auch Experten von Polizei und Geheimdiensten nutzen. Damit werten Sie im Handumdrehen Protokoll-Dateien und andere Nutzungsspuren auf dem PC aus. So fördern Sie etwa flott zutage, welche Internetseiten Sie besucht haben, ohne sich in Windows anmelden zu müssen. Sogar längst gelöschte E-Mails, Chats und Internetverläufe lassen sich oft noch rekonstruieren!

Mit weiteren Tools prüfen Sie, ob Ihr WLAN-Passwort sicher ist – indem Sie es teilweise knacken. Und haben Sie das Kennwort eines lokalen Windows-Kontos vergessen, entfernen Sie die Kennwortabfrage einfach mit wenigen Mausklicks.

Brandneu bei den Hacker-Tools sind zwei Funktionen zur Suche nach Schwachstellen: Mit der einen entlarven Sie Sicherheitsrisiken auf Netzwerkgeräten wie Druckern oder NAS-Festplatten – mit der anderen prüfen Sie, ob sich gespeicherte Kennwörter leicht auslesen lassen.

Hacker-Stick erstellen

Um gleich loszulegen, starten Sie einfach Ihren Computer von der beiliegenden Sonderheft-DVD, wie es auf der folgenden Seite beschrieben ist. Sollten Sie kein DVD-Laufwerk besitzen, so erhalten Sie den Download eines DVD-Abbilds der Tools. Damit lassen sich die Hacker-Tools auch problemlos auf einen USB-Stick übertragen und von dort aus starten. Das bietet sogar einige weitere Vorteile, etwa einen deutlich schnelleren Start der Tools.

[hes/hp]



HACKER-STICK MACHEN

Die Hacker-Tools lassen sich auch von einem USB-Stick starten. Das geht flotter als von DVD. Achtung: Der Stick muss wenigstens 16 Gigabyte groß sein und wird vor der Einrichtung komplett gelöscht. So erstellen Sie den Stick: Stöpseln Sie ihn in den PC ein und andere externe Laufwerke aus. Je nachdem, ob Sie ein DVD-Laufwerk haben, geht's folgendermaßen weiter:

■ **Mit DVD-Laufwerk:** Klicken Sie im Windows-Explorer aufs DVD-Laufwerk, doppelt auf **USB-Stick erstellen** und **Ja**. Achten Sie darauf, dass im neuen Fenster rechts der richtige USB-Stick ausgewählt ist. Wählen Sie dann **Schreiben** und **Yes**, nach dem Überspielen **OK** und **Beenden**. Wichtig: Erscheint bei Ihnen „Fehler 5“, beachten Sie die Hinweise auf der Seite **cobi.de/12433**. Oder Sie starten wie rechts beschrieben von der DVD, klicken im Hauptmenü aufs USB-Symbol, wählen den Stick als Ziel-Laufwerk, klicken auf **Installation starten** und **Ja**.

■ **Ohne DVD-Laufwerk:** Holen Sie sich bis zum 15. Oktober 2022 die Hacker-Tools von der Website **vorteilcenter.de** mit dem Vorteilcenter-Code von der Heft-DVD-Hülle. Nach dem Download entpacken Sie die überspielte ZIP-Datei und starten die USB-Installation ganz ähnlich wie oben beschrieben.

TOOLS STARTEN

Um die Hacker-Tools zu nutzen, starten Sie den PC von der Heft-DVD oder dem USB-Stick:

PC VORBEREITEN

Legen Sie die Heft-DVD ein, oder stellen Sie wie links beschrieben einen „Hacker-Stick“ her, und starten Sie den PC neu.

LAUFWERK WÄHLEN

Lädt Windows, wiederholen Sie den Start und öffnen das Bootmenü:

■ **BIOS-PC (bis Windows 7):** Drücken Sie nach dem Start mehrmals die Bootmenü-Taste – meist **F8**, bei einigen PCs auch **F2**, **F9**, **F10**, **F11**, **F12**, **Alt** oder **F12**. Im Bootmenü wählen Sie per Pfeiltaste das DVD- oder USB-Laufwerk und drücken **↵**.

■ **UEFI-PC (ab Windows 8):** Bei modernen PCs klappt es auch so: Drücken Sie in Windows die Taste **Win+R**, klicken Sie auf **Ein/Aus**, bei gedrückter **Win**-Taste auf **Neu starten** und gegebenenfalls auf **Trotzdem neu starten**. Wählen Sie **Ein Gerät verwenden** und die DVD oder den Stick. Taucht der nicht auf, stecken Sie ihn in eine andere USB-Buchse, wählen **Zurück**, **Ein Gerät verwenden** und versuchen es erneut.

STARTMODUS AUSWÄHLEN

Im Menü mit dem Eintrag **COMPUTER BILD Hacker-Tools 2021 starten** drücken Sie **↵**. Bei Startproblemen wählen Sie **Hacker-Tools abgesichert starten** beziehungsweise die Optionen unter **Abgesicherter Start**.

DAS PROGRAMM IM ÜBERBLICK



Aufklären

Hat sich jemand an Ihrem Computer zu schaffen gemacht? Möchten Sie wissen, was andere auf Ihrem PC mit Hacker-Werkzeugen aufspüren könnten? Finden Sie's heraus auf **Seite 83**



HACKER-TOOLS



Gelöschte Inhalte auslesen



Internetspuren aufspüren



WLAN- & Netzwerkanalyse



Festplatten-Analyse



Überwachen

Viele Eltern machen sich Sorgen um den Internetkonsum ihrer Kinder. Denn dort gibt es viele Seiten, die für junge Menschen schädlich und gefährlich sind. Ein Blick in den Browserverlauf verrät, ob Ihr Kind solche Seiten besucht hat. Selbst bei gelöschtem Verlauf verrät der Browser-Cache noch Informationen. Wie das geht, steht auf **Seite 82**



M

Geheimnisse enthüllen, Spionage enttarnen, Sicherheitsrisiken aufspüren: Wie Sie die Hacker-Tools startklar machen und was sie bieten, zeigt COMPUTER BILD.



Auslesen

Wurden vertrauliche Dateien wirklich gelöscht, oder lassen sich noch (pikante) Datenreste auf der Festplatte finden? Wie Sie das herausbekommen, erfahren Sie auf **Seite 81**



2021

Gelöschte Inhalte auslesen



Gelöschte Dateien suchen & wiederherstellen



Caches von Browser, Skype & Co suchen



Gefundene Daten aufbereiten

Enthüllen

Sind vertrauliche Dateien oder freizügige Fotos via Skype oder E-Mail in falsche Hände geraten? Die Hacker-DVD findet es heraus. Wie das funktioniert, steht auf **Seite 84**



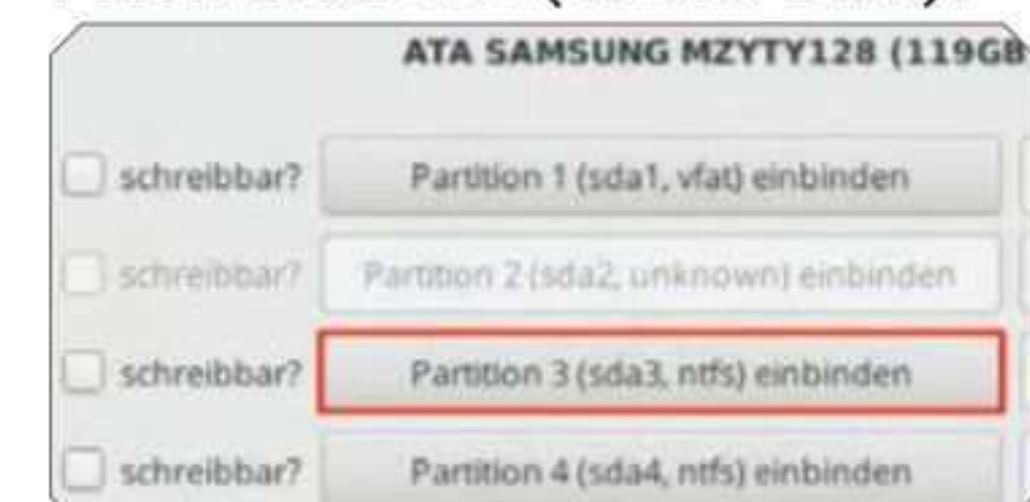
ERSTE SCHRITTE

Die Hacker-Tools nutzen statt Windows ein eigenes Betriebssystem, das mit der Übersicht der wichtigsten Werkzeuge startet. Über die Menüleiste („Dock“) am unteren Bildschirmrand rufen Sie alle Funktionen der Software auf. Zuvor machen Sie sich mit den Besonderheiten der Software vertraut:



Ein Laufwerk einbinden

Um Daten von einem Laufwerk lesen zu können, muss es „eingebunden“ sein. Klicken Sie dazu auf die Laufwerke-Schaltfläche im Dock (siehe kleines rundes Bild links an dieser Textspalte). Im neuen Fenster sehen Sie alle verfügbaren Datenträger mit den jeweiligen Laufwerken („Partitionen“). Die auf den nächsten Seiten beschriebenen Funktionen verlangen die Einbindung der Windows-Partition. Um sie zu finden, klicken Sie auf den ersten Knopf mit dem Hinweis **ntfs** (siehe Bild).



Erscheinen im nächsten Fenster die Ordner „Windows“ und „Users“, sind Sie richtig. Andernfalls klicken Sie wieder auf den Knopf, um das Laufwerk zu lösen, und suchen weiter.

Einige Werkzeuge erfordern zudem die Berechtigung, Daten auf der Partition zu speichern. Dafür müssen Sie vor dem Einbinden das Häkchen vor „schreibbar?“ setzen. Andernfalls kann die Hacker-DVD die Daten auf dem Laufwerk nur anzeigen, aber nicht verändern.



WLAN verbinden

Manche Funktionen brauchen eine WLAN-Verbindung. Um die herzustellen, klicken Sie im Dock aufs Netzwerk-Symbol (siehe Bild links oben) und im neuen Fenster auf **Wireless**. Nach einem Doppelklick aufs gewünschte Funknetz tippen Sie das WLAN-Passwort ein und klicken auf **OK**.

Absichern

Bieten Schwachstellen in Ihren Netzwerkgeräten Einfallstore für Kriminelle? Lassen sich gespeicherte Passwörter leicht auslesen? Wie Sie beides ausschließen, steht auf **Seite 80**



Bewerten

Ist der gebraucht gekaufte Computer nun wirklich ein Schnäppchen oder eine alte Möhre? Wie Sie die Nutzungszeit der Festplatte ermitteln, lesen Sie auf **Seite 83**



Entsperren

Haben Sie ein Passwort vergessen? Das kann passieren. Wie Sie das Windows-Kennwort umgehen oder sogar Ihr WLAN-Kennwort knacken, verraten Anleitungen auf **Seite 85**





EINFALLSTORE SCHLIESSEN

Neu: Mit der Hacker-DVD prüfen Sie Netzwerkgeräte und Kennwortspeicher auf Sicherheitslücken.

EINSATZ ALS WERKZEUG

GERÄTE ABSICHERN

Sind die Daten auf Ihrer Netzwerkfestplatte sicher vor Hacker-Angriffen? Lauern im Heimnetz Einfallstore durch offene Ports oder Serversoftware, die ungeahnt läuft? So finden und stopfen Sie Sicherheitslücken im Netzwerk:

Nach Schwachstellen scannen

Stellen Sie sicher, dass Ihr PC per Kabel oder WLAN (siehe Seite 79) mit dem Heimnetzwerk verbunden ist. Klicken Sie dann im Hauptmenü auf **WLAN- & Netzwerkanalyse** und auf **Netzwerkschwachstellen-Scan**. Im neuen Fenster klicken Sie auf **Ich bin mir bewusst, dass die Anwendung in fremden Netzwerken strafbar ist** und anschließend auf **Jetzt verwundbare Geräte finden**.

Gerät mit IP-Adresse 192.168.178.43

Geöffnete Ports: 1

Keine Auffälligkeiten.

Gerät mit IP-Adresse 192.168.178.47

Geöffnete Ports: 5

- Bei diesem Gerät scheint es sich um einen Netzwerkdrucker zu handeln. Da solche Geräte häufig Sicherheitslücken haben, prüfen Sie, ob ein Firmware-Update bereitsteht.

Schwachstellen erkennen und schließen

Sobald der Scan abgeschlossen ist, erscheint eine Ergebnisseite, siehe Bild oben. Darauf sind Geräte mit ihrer Netzwerkadresse („IP-Adresse“) aufgelistet. Geräte mit dem Ergebnis „Keine Auffälligkeiten“ – etwa der obere Eintrag im Bild – sind sicher. Stehen dort andere Hinweise, ermitteln Sie zunächst jeweils, welches Gerät hinter der IP

steckt. Verrät das nicht schon der Hinweis-text wie beim Drucker im Bild oben, kann der Router helfen: Nutzen Sie etwa eine Fritz Box, öffnen Sie im Browser die Seite **fritz.box**, melden sich an und sehen nach Klicks auf **Heimnetz** und **Netzwerk** eine Liste Ihrer Geräte – jeweils mit Namen und IP-Adresse. Ist das Gerät identifiziert, befolgen Sie die Tipps von der Ergebnisseite.

EINSATZ ALS WERKZEUG

PASSWÖRTER SCHÜTZEN

Ist Ihr Windows-Laufwerk unverschlüsselt und speichern Sie Passwörter in installierten Programmen, etwa im Browser? Aufgepasst, falls Sie beide Fragen mit „Ja“ beantworten: Dann lassen sich diese Kennwörter leicht auslesen, wenn jemand Zugriff auf Ihren Computer erlangt. Mit dem Basis-Sicherheitscheck prüfen Sie Ihren PC auf solche Sicherheitslücken. Sind sie vorhanden, verweist die Funktion auf COMPUTER BILD-Ratgeber im Internet, mit denen Sie die Lücken schließen.

Sicherheits-Scan durchführen

Um nach unsicher gespeicherten Kennwörtern zu suchen, klicken Sie im Hauptmenü der Hacker-Tools auf **Festplatten-Analyse** und auf **Basis-Sicherheitscheck**. Im neuen Fenster klicken Sie auf **Ich bin mir bewusst, dass die Anwendung in fremden**

Netzwerken strafbar ist und anschließend auf **Jetzt Sicherheitscheck durchführen**.

Risiken erkennen und beheben

Sobald der Scan abgeschlossen ist, erscheint eine Ergebnisseite. Sie beginnt mit einer Auflistung der unverschlüsselten NTFS-Laufwerke – typischerweise sind alle unverschlüsselt. Gefährlich wird's erst bei den Einträgen unter „Unverschlüsselte NTFS-Laufwerke mit Profilen“, denn dort sind Kennwörter gespeichert. Weiter unten listet die Seite leicht auslesbare Passwortdatenbanken auf diesen Laufwerken auf, siehe Bild rechts. Gibt es keine solchen Einträge, sind Ihre Kennwörter sicher. Andernfalls haben Sie folgende Möglichkeiten, für

EINSATZ ALS WAFFE

PASSWORT- UND DATENDIEBSTAHL

mehr Sicherheit zu sorgen: Entweder verschlüsseln Sie gefährdete Partitionen – eine Anleitung gibt's nach einem Klick auf **So geht's: Bitlocker und Veracrypt aktivieren**. Das ist sehr sicher, die Einrichtung allerdings aufwendig, und das Windows-Tempo kann darunter leiden. Alternativ setzen Sie einen Passwort-Manager ein. Wie das geht, lesen Sie nach einem Klick auf **So geht's: Passwörter sicher verwalten**.

Analyse "media/disk/nvme0n1p1/Users/Hub/AppData/Roaming/Mozilla/Firefox/Profiles/qoxn83va.default"

Für die folgenden Logins können Passwörter leicht ausgelesen werden:

- http://www.musiker-sucht-musiker.de, Nutzernamen: j...
- https://freemail.web.de, Nutzernamen: j...
- http://line6.com, Nutzernamen: j...
- http://www.gmx.net, Nutzernamen: j...
- http://www.facebook.com, Nutzernamen: bobporst@web.de
- http://login.live.com, Nutzernamen: bobporst
- http://wendysforum.net, Nutzernamen: bobporst
- https://www.telltalegames.com, Nutzernamen: j...
- http://www.scorehero.com, Nutzernamen: j...
- http://www.ubuntu-forum.de, Nutzernamen: j...

DATENSPEICHER

AUSLESEN

Sind **vertrauliche Daten** nach dem Löschen **wiederherstellbar**? Mit der Hacker-DVD finden Sie es heraus.

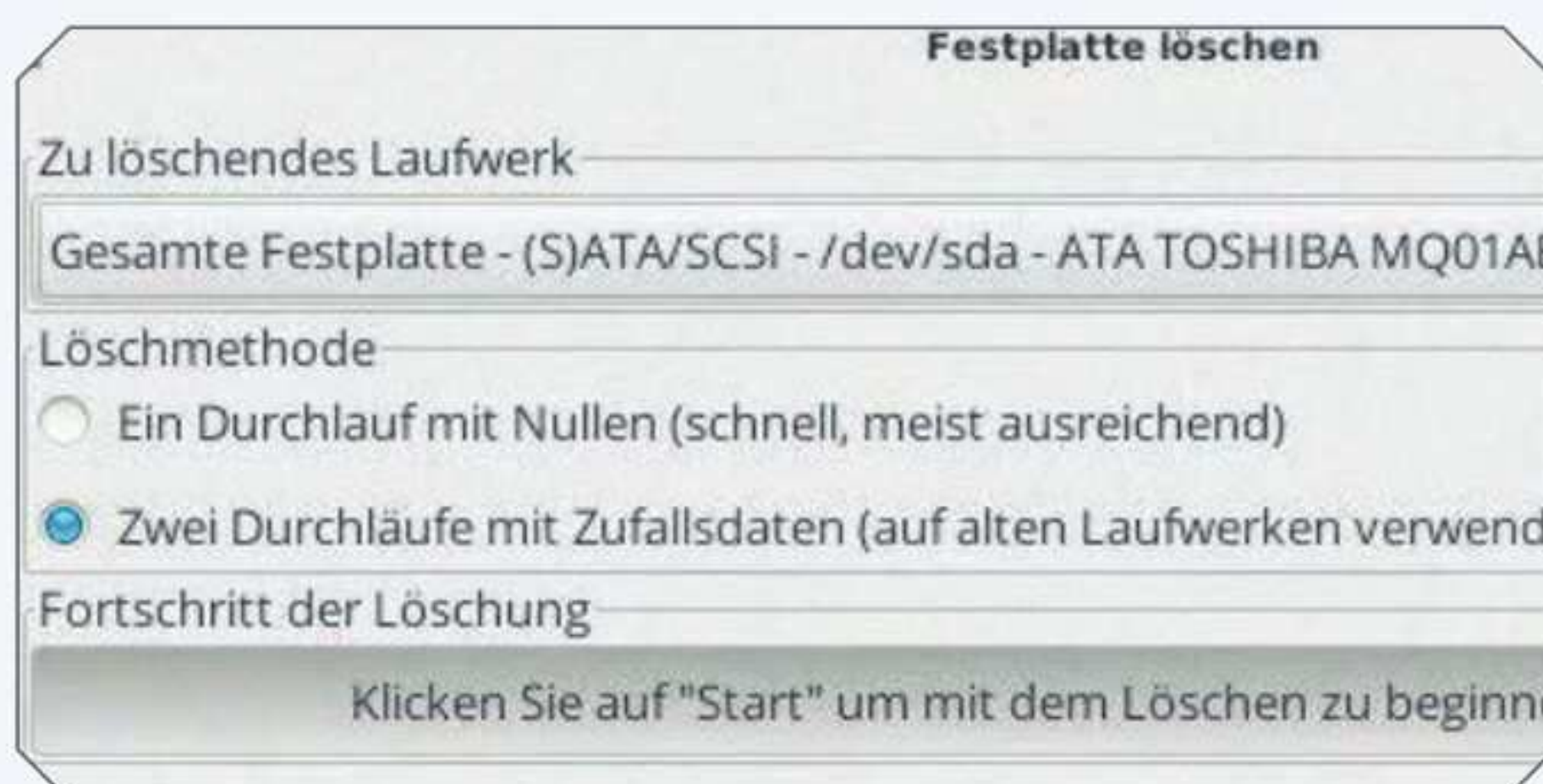
EINSATZ ALS WERKZEUG

DATEN SICHER LÖSCHEN

Mit der Hacker-DVD und anderen Programmen können Neugierige vermeintlich gelöschte Daten auf Datenträgern wieder sichtbar machen und so ihre Besitzer ausspionieren. Um sich davor zu schützen, löschen Sie mit der Software persönliche Daten unwiederbringlich. Dann lässt sich zum Beispiel ein altes Laufwerk ruhigen Gewissens entsorgen oder in fremde Hände geben – die Hacker-DVD sorgt dafür, dass keine persönlichen Daten zurückbleiben.

Daten endgültig löschen

Möchten Sie sichergehen, dass sich keine Daten wiederherstellen lassen, löschen Sie die Festplatte nicht nur, sondern überschreiben sie auch mit Zufallsdaten. Dazu starten Sie die Hacker-DVD auf dem PC mit dem alten Laufwerk oder schließen es per USB an. Nun klicken Sie im Dock auf **Anwendungsmenü**, **Rettungswerkzeuge** und **Sicher löschen**. Wählen Sie unter „Zu löschendes Laufwerk“ die Festplatte oder Partition aus, deren Daten auf Nimmerwiedersehen verschwinden sollen (siehe Bild rechts oben). Die Liste zeigt angeschlossene Datenträger mit dem Hinweis „Gesamte Festplatte“ und darunter jeweils die vorhandenen Partitionen. Waren auf dem Datenträger vertrauliche Daten wie Kontoauszüge gespeichert, wählen Sie **Zwei Durchläufe mit Zufallsdaten**. Überprüfen Sie, ob Sie die richtige Festplatte gewählt haben, bevor Sie auf **Starten** und **Ja** klicken. Hat das Programm zu arbeiten begonnen, sind die Daten nämlich verloren. Nach dem Start ist Geduld gefragt, denn die Software überschreibt die gesamte Festplatte oder Partition mit Zufallsdaten. Ist der Prozess abgeschlossen, kann selbst die Hacker-DVD nichts wiederherstellen.



Hacker-Angriff simulieren

Haben Sie eine gelöschte Festplatte, die Sie weitergeben oder vernichten wollen? Dann prüfen Sie vorher, ob sie auch wirklich sauber ist: Schließen Sie einen USB-Stick oder eine externe Festplatte als Sicherungslaufwerk an. Da Sie zunächst nicht wissen, wie viele Daten die Hacker-DVD findet, sollte es möglichst genauso groß sein wie das überschriebene Laufwerk. Binden Sie das Sicherungslaufwerk mit Schreibrechten ein (siehe Seite 79). Danach klicken Sie im Hauptmenü der Hacker-DVD auf **Gelöschte Inhalte auslesen** und **Gelöschte Dateien suchen & wiederherstellen**. Im neuen Fens-

ter klicken Sie auf **Vor**, wählen die zu analysierende Festplatte oder Partition aus und klicken zweimal auf **Vor**. Nach einem Klick auf **(keine)** wählen Sie das zuvor eingebundene Sicherungslaufwerk, klicken erneut auf **Vor**, überprüfen alle Angaben und starten die Wiederherstellung im Fenster „Zusammenfassung“ (siehe Bild unten) per Klick auf **Anwenden**. Die Suche öffnet ein weiteres Fenster (siehe großes Bild ganz unten), das Sie über bereits gefundene Dateien und die geschätzte Restlaufzeit informiert. Ist die Wiederherstellung fertig, öffnet sich ein Fenster mit den gefundenen Dateien. Nichts zu sehen? Dann ist die geprüfte Platte wirklich sauber.

Zusammenfassung

Wollen Sie die Wiederherstellung mit den vorgenommenen Einstellungen durchführen?

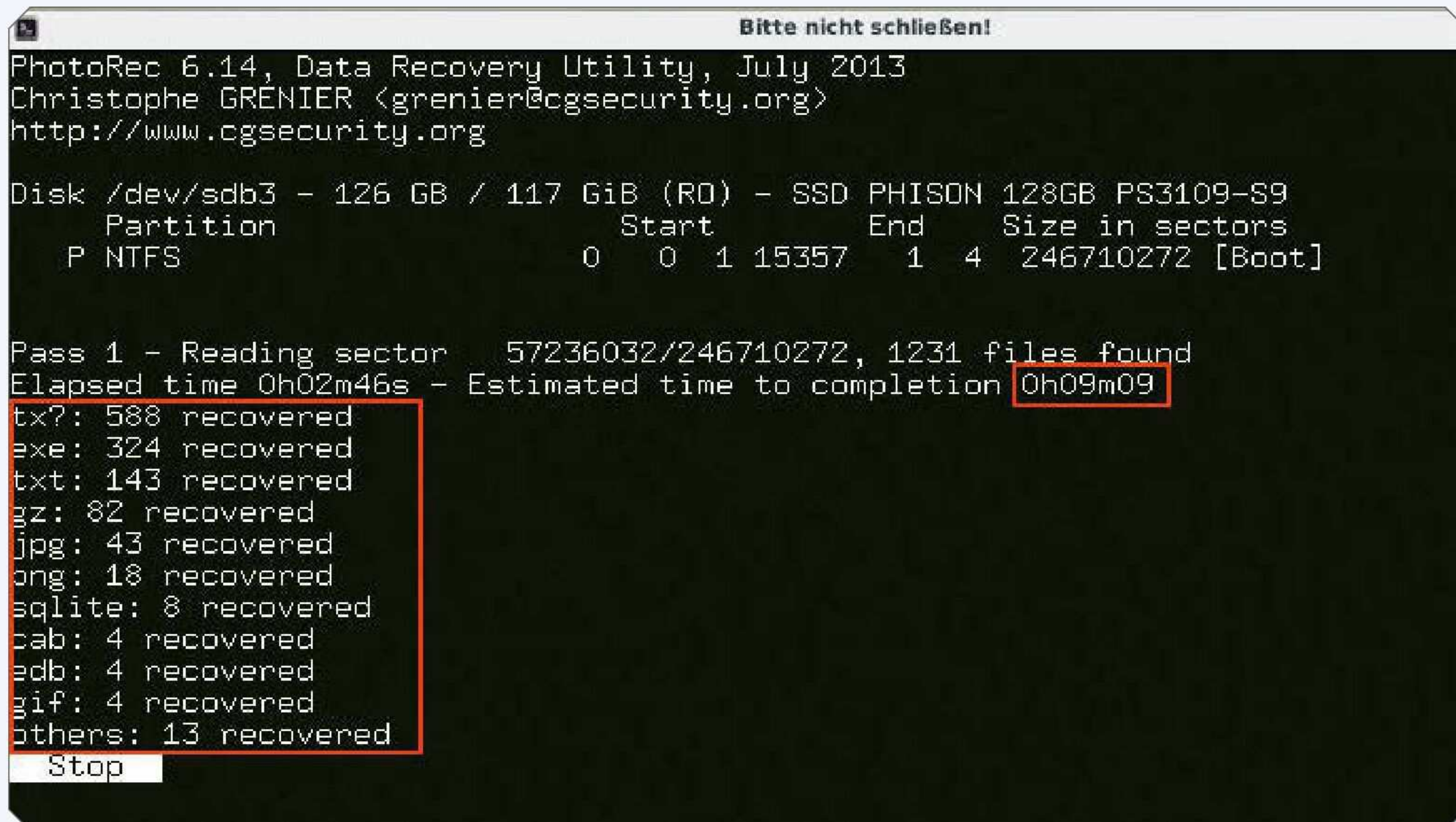
Suche auf: ATA SSD PHISON 128GB (IDE/SATA, 119GB) Partition sdb3 (ntfs, 118GB)

Suche nach: Alle bekannten Dateitypen suchen

Gefundene Dateien speichern in: /media/disk/sdd1/photorec_20161124-214420.1

Benötigte Zeit: 63 bis 315 Minuten (geschätzt)

Nach einem Klick auf "Anwenden" startet die Suche nach Dateien in einem neuen Fenster.





COMPUTER ÜBERWACHEN

Mit diesen Funktionen **schützen** Sie Ihre Kinder vor Gefahren im Internet und **entlarven** Fremdzugriffe auf Ihren PC.

KURZ-TIPPS

Fernwartung

Sie kommen bei einem PC-Problem nicht weiter, aber ein Freund kennt sich aus? Der kann sich mit der Software Team-Viewer (Download: www.cobi.de/11374) auf Ihren Desktop schalten. Dazu klicken Sie bei bestehender Internetverbindung aufs kleine Headset (Bild) und auf **Verbinden**. Nennen Sie dem Freund die angezeigte ID samt Passwort. Ist nichts zu sehen, klicken Sie auf **Yes**.



WLAN zurücksetzen

Bleibt die Netzwerkliste bei der WLAN-Einrichtung leer? Dann klicken Sie unter **Wireless** auf **ON** und **OFF**, um den Adapter neu zu initialisieren. Hilft das nicht, müssen Sie WLAN im BIOS abschalten und einen linuxkompatiblen WLAN-Stick einstecken, etwa den Edimax EW-7811Un (siehe Bild) für 6 Euro.

COMPUTER BILD Hacker-Tools starten
Hacker-Tools abgesichert starten (im
Hacker-Tools abgesichert starten (an
Windows starten
*Hacker-Tools von USB deinstallieren

Stick deinstallieren

Sie haben wie auf Seite 78 beschrieben den Hacker-Stick eingerichtet, möchten ihn aber in den Werkszustand zurücksetzen? Kein Problem: Starten Sie den PC vom Stick, und wählen Sie die Option **Hacker-Tools von USB deinstallieren**. Fertig!

EINSATZ ALS WERKZEUG

KINDER SCHÜTZEN

Firefox, Chrome und Edge protokollieren alle Klicks im Internet. Diese Listen lassen sich mit Spezialwerkzeugen von der Hacker-DVD auslesen. So lässt sich auch ohne laufendes Windows das Surfverhalten eines PC-Nutzers auskundschaften. Der sinnvolle Einsatz: Sie können prüfen, ob Ihre Kinder gefährliche Webseiten aufrufen. Aber: Allzu neugierige Kollegen oder Familienmitglieder können herausfinden, wo Sie sich im Netz herumtreiben!

Surfspuren suchen

Zunächst binden Sie die Windows-Partition mit Schreibrechten ein, siehe Seite 79 rechts. Im Anschluss klicken Sie im Hauptmenü auf **Internet Spuren aufspüren** und **Browserverläufe suchen & anzeigen**. Im neuen Fenster klicken Sie unter „Zu untersuchendes Verzeichnis“ auf **disk** und die zuvor eingebaute Partition, dann auf **Suche starten**.

Browserverlauf öffnen

Es erscheint ein Fenster mit mehreren Dateien, siehe Bild rechts oben. Klicken Sie doppelt auf **history_index.csv**. In der Tabelle sehen Sie, welche Browser und Windows-Nutzer hinter den gefundenen Protokollen stecken – verbreitern Sie die Spalte A, bis alles zu sehen ist. Ist der Nutzer identifiziert, sehen Sie in Spalte B das dazugehörige Surfprotokoll. Firefox-Protokolle tragen die Bezeichnung „FF_history_...csv“, Google Chrome und Microsofts Chromium-Edge verwenden den Namen „Chrome_history_...csv“. Öffnen Sie das Protokoll wiederum per Doppelklick. In der Übersicht (Bild unten) sehen Sie alle vom Browser angesteu-

EINSATZ ALS WAFFE

KOLLEGE LIEST MIT!

40a686c36a1dedcf fc561bd8dbec50f6 cb72e2c.csv	28b1b5366e999d7 6ef197768d8856fa 7d5044d0.csv	41ca30fa8a9f4a8d 9e3a8d93f47d77cf 655033.csv
Chrome_history_e 46622ea85f6e25f4 2999af7bc5c465d4 818d58b.csv	FF_history_946ecf 1aad42553dcf8935 cc4cd74c3d9f0f53 9.csv	history_index.csv

erten Internetseiten. Schließen Sie die Protokolle anschließend jeweils mit **x** und **Verwerfen**.

Windows-Sicherung durchsuchen

Wurden keine Protokolle gefunden, finden Sie vielleicht etwas in den automatischen Windows-Sicherungen. Um sie zu öffnen, klicken Sie im Dock auf **Anwendungsmenü, Weitere Wartungswerkzeuge, VSS-Zugriff** und **Alle Einbinden**. Sind Sicherungen vorhanden, erscheinen sie als eingebaute Laufwerke in einem neuen Fenster. Wiederholen Sie dann die vorherige Analyse dort.

Browser-Cache durchsuchen

Sind alle Verläufe geleert, gibt vielleicht der Firefox-Zwischenspeicher noch Details preis. Um den abzufragen, klicken Sie im Hauptmenü auf **Gelöschte Inhalte auslesen** sowie **Caches von Browser, Skype & Co. suchen**. Starten Sie die Suche wie oben beschrieben. Nun erscheinen zahlreiche Fenster. Suchen Sie das mit dem Ordner **entries**, und klicken Sie doppelt darauf. Er zeigt alle vom Browser gespeicherten Bilder – was Rückschlüsse zulässt.

	Titel	Zahl der Besuche
://www.elephantli	The Free Private Voyeur - Amateur and Voyeur Mai	37
://www.reddit.co	Hot Chicks With Tattoos	
://www.reddit.co	Hot Chicks With Tattoos	
://www.mybabes.	YOUNG BABES, nude teen girls, hot girls, anal sex,	
://www.beate-uhs	Beate-Uhse ist Ihr Onlineshop für Dessous, Mode u	
://www.google.d	Killerspiel herunterladen - Google-Suche	
://www.pyromark	Colour Salute Extra Laut - 1,10 EUR - Sonstige Böll	
://www.pyromark	Rauchkörper / Bengalos / Fakeln verschiedener He	
://movie4k-to.cor	Cornered - Das Killerspiel online anschauen und d	
://www.kampfspo	Mixed Martial Arts (MMA) Kampfsportzentrum Dre	
://ww10.zensurfre	ww10.zensurfrei.org	
://pics777.info/	Pics777.info	
://www.elephantli	YOUNG BABES, nude teen girls, hot girls, anal sex,	
://www.privatevo	The Free Private Voyeur - Amateur and Voyeur Mai	19



EINSATZ ALS WERKZEUG

FREMDZUGRIFF AUFDECKEN

Die „Sprunglisten“ von Windows sind eine feine Sache, zeigen Sie doch nach einem Rechtsklick auf das Taskleisten-Symbol eines Programms automatisch die letzten damit verwendeten Dateien. So können Sie zwar feststellen, ob andere sich an Ihrem PC zu schaffen gemacht haben. Allerdings könnten Nutzer auch herausfinden, was Sie zuletzt am PC gemacht haben.

Sprunglisten suchen

Zuerst binden Sie die Windows-Partition wie auf Seite 79 rechts beschrieben ohne Schreibrechte ein. Danach klicken Sie im Hauptmenü auf **Internetspuren aufspüren** und **Windows-Aktivitäten aufspüren**. Im



neuen Fenster klicken Sie unter „Zu untersuchendes Verzeichnis“ auf **disk** oder (**keine**), das Windows-Laufwerk und **Suche starten**. Das Hacker-Tool durchforstet anschließend die Festplatte nach Spuren zuletzt geöffneter Dateien und zeigt die Ergebnisse in mehreren Textdateien. Nicht wundern, die Suche dauert sehr lange, und der Fortschrittsbalken bewegt sich während dieser Zeit mitunter länger nicht.

Sprunglisten auswerten

Im Anschluss erscheint das Fenster im Bild unten links mit zahlreichen Textdateien. Die beginnen alle mit „Win_Jumplist“ und lassen sich per Doppelklick öffnen. Jede dieser Dateien enthält einen Eintrag über die zuletzt geöffneten Dateien oder Programme. Wie das Bild rechts oben zeigt, ist der Aufbau immer gleich: Die erste Zeile **1** verrät den Speicherort des angezeigten Eintrags. Hier steht auch der Benutzername des Kontos, im Beispiel „Max“, von dem die Aktion ausgeführt wurde. Die nächste Zeile **2** zeigt Datum und Uhrzeit des Ereignisses, und die dritte Zeile **3** verrät, wo was passiert ist. Im

EINSATZ ALS WAFFE

PC-NUTZUNG AUSSPÄHEN



Beispiel hat der Nutzer „Max“ am 10. November 2021 zwischen 08:29 Uhr und 08:54 Uhr drei Bilder (Lydia.jpg, Julia.jpg, Nina.jpg) geöffnet. Die sind oder waren zu dem Zeitpunkt im Ordner „Privat“ auf dem Desktop gespeichert.

Akribische Detektivarbeit

Um Erkenntnisse zur PC-Nutzung zu gewinnen, schauen Sie sich alle Dateien an. Notieren Sie sich ungewöhnliche Ereignisse, um den Überblick nicht zu verlieren. Stoßen Sie bei den Ermittlungen auf weniger eindeutige Ergebnisse, muss Google helfen – im Dock finden Sie einen **Webbrowser** sowie einen **Dateimanager**. Damit können Sie verdächtige Dateien etwa auf einem zuvor eingebundenen USB-Laufwerk sichern.

EINSATZ ALS WERKZEUG

BETRUG VERHINDERN

Die Hacker-DVD hat ein Spezialwerkzeug zur Diagnose von Festplatten an Bord. Damit finden Sie etwa heraus, wie alt eine gebraucht gekaufte Festplatte wirklich ist. Ein hinterhältiger Chef könnte aber auch feststellen, wie lange Sie wirklich am PC gearbeitet haben. So geht's:

Diagnosedaten auslesen

Um die Laufleistung einer Festplatte zu ermitteln, müssen Sie die sogenannten SMART-Werte abfragen. Diese Selbsttest-Protokolle erstellen moderne Festplatten automatisch. Die SMART-Werte dienen eigentlich zur frühzeitigen Erkennung von Ausfällen, lassen sich aber auch zu Überwa-



chungszwecken nutzen. Um das entsprechende Tool zu starten, klicken Sie im Dock der Hacker-DVD auf **Anwendungsmenü**, **Rettungswerkzeuge** und **Platte testen**. In der folgenden Laufwerksübersicht (siehe Bild unten links) wählen Sie das zu analysierende Laufwerk per Doppelklick und öffnen im neuen Fenster den Tab **Attributes**. Nun werden alle von der Festplatte gemeldeten Werte wie im großen Bild unten angezeigt.

Daten auswerten

Die Anzahl der Betriebsstunden ist in Zeile 9 („Power-On Time“) **1** vermerkt, Zeile 12 („Power Cycle Count“) **2** verrät die Zahl der Ein- und Ausschaltungen. Der jeweilige Messwert ist in der Spalte „Raw value“ **3** aufgeführt,

EINSATZ ALS WAFFE

CHEF CHECKT ARBEITSZEIT

im Beispiel 526 Stunden sowie 187 Neustarts. Bei einer täglichen Laufleistung von drei (Heim-PC) oder neun Stunden (Büro-PC) wäre die Platte bereits etwa sechs beziehungsweise zwei Monate in Betrieb – vielleicht ein Vorführmodell? Liest ein misstrauischer Chef (illegalerweise) solch ein Protokoll, könnte er aber auch darauf kommen, dass Sie im Home-Office das Arbeits-Notebook ungewöhnlich selten eingeschaltet hatten.

Identity

Attributes

Capabilities

Error Log

Self-test Logs

Perform Tests

SMART Attributes Data Structure revision number: 16

ID	Name	Failed	Norm-ed value	Worst	Threshold	Raw value
7	Seek Error Rate	never	100	0	0	0
8	Seek Time Performance	never	100	0	0	0
9	Power-On Time	never	99	526	0	526
10	Spin-Up Retry Count	never	103	0	0	0
12	Power Cycle Count	never	100	0	0	187
191	G-Sense Error Rate	never	100	100	0	0
192	Head Retract Cycle Count	never	100	100	0	187

3

1

2



GEHEIMNISSE ENTHÜLLEN

Startet Outlook nicht mehr? Haben Sie Ihr Skype-Passwort vergessen? Per Hacker-DVD lesen Sie alle versendeten Inhalte nach.

EINSATZ ALS WERKZEUG

E-MAILS RETTEN

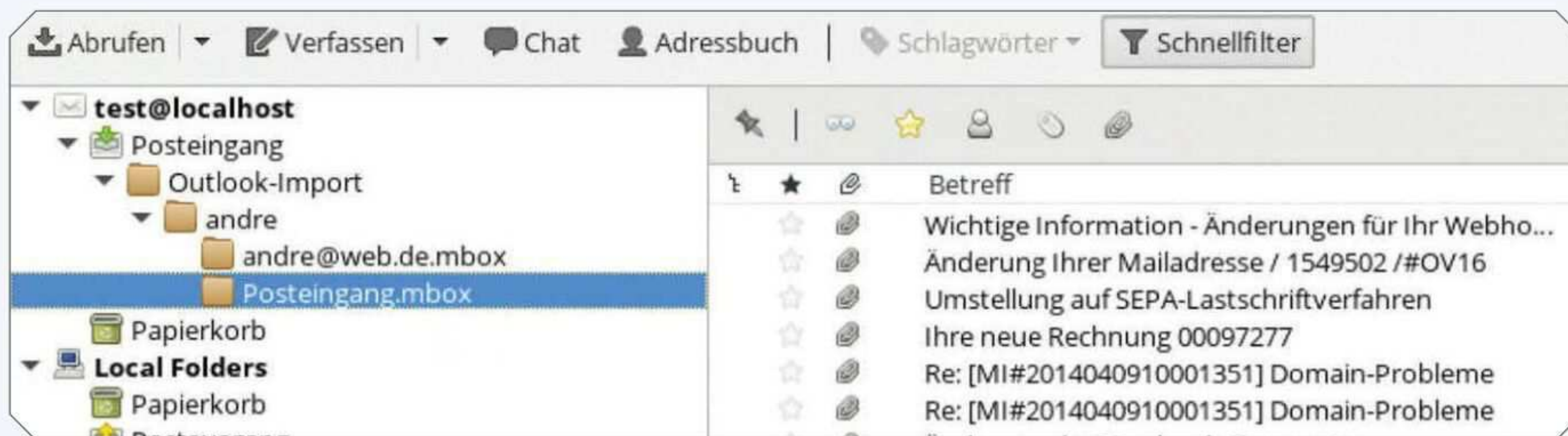
Microsoft Outlook ist das Top-Programm im Büro und im Home-Office. Stürzt es ab, sind oft alle Nachrichten verloren. Mit der Hacker-DVD können Sie die Mails retten – neugierige Kollegen oder Konkurrenten könnten Sie aber auch ausspionieren.

Mail-Datenbank suchen

So geht's: Binden Sie wie auf Seite 79 beschrieben die Windows-Partition ein. Dann klicken Sie im Hauptmenü auf **Internetquellen aufspüren** und **E-Mails auslesen**, dann auf **disk**, auf die Windows-Partition und auf **Suche starten**.

Mails anzeigen

Wurden Mails gefunden, startet das Programm Thunderbird und zeigt den Import



unter „Posteingang“ (siehe Bild oben). Klicken Sie im Beispiel je doppelt auf **Outlook-Import**, den Namen und **Posteingang**. Nun können Sie alle Mails per Klick anzeigen. Zum Sichern gibt es zwei Optionen:
■ **Weiterleiten:** Klicken Sie bei bestehender Internetverbindung (siehe Seite 79) auf **test@localhost**, **E-Mail**, und folgen Sie den Hinweisen zur Postfach-Einrichtung. Nun

wählen Sie eine Mail, **Weiterleiten**, **Heinz Mustermann**, Ihr Postfach und **Senden**.
■ **Kopieren:** Nachdem Sie ein USB-Laufwerk (schreibbar, siehe Seite 79) eingebunden haben, klicken Sie mit der rechten Taste auf eine Mail, **Speichern unter**, das Laufwerk und **Speichern**. Die gespeicherte Datei öffnen Sie unter Windows per Doppelklick in Outlook und Klick auf **Speichern**.

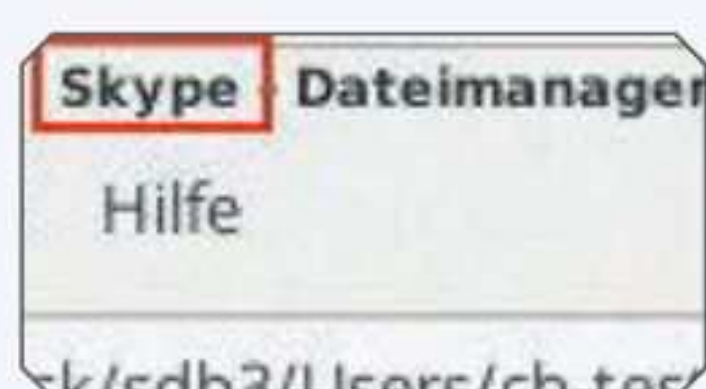
EINSATZ ALS WERKZEUG

SKYPE-INHALTE RETTEN

Skype war früher für berufliche Meetings und private Plaudereien beliebt. Inzwischen sind viele auf andere Plattformen gewechselt – und es fällt oft zu spät auf, dass in Skype noch wichtige Chats liegen. Mit der Hacker-DVD machen Sie die wieder sichtbar. Aber Vorsicht: Kollegen könnten private Daten ausspähen, etwa geteilte Bilder!

Chats suchen

Binden Sie die Windows-Partition ein, wie auf Seite 79 beschrieben. Dann klicken Sie auf **Gelöschte Inhalte auslesen**, **Caches von Browser**, **Skype & Co suchen** sowie **disk**, wählen die Windows-Partition aus und klicken auf **Suche starten**. Pro gefundenem Speicherordner („Cache“) erscheint nun ein neues Fenster. Suchen Sie nach „Skype“-Fenstern (Bild) – alle anderen können Sie schließen.



Bilder anschauen

Um mit Kontakten geteilte Bilder zu sehen, öffnen Sie im Skype-Fenster den Profilordner des Nutzers per Doppelklick. In den Ordnern **Pictures**, **media_messaging** und **media_cache_v3** finden Sie alle mit Skype erzeugten oder geteilten Dateien. Bilder öffnen Sie mit Doppelklick auf die dort befindlichen JPG- und PNG-Dateien.

Gespräche auslesen

Um an die Chats zu kommen, navigieren Sie im Skype-Fenster zur Datei **main.db**. Öffnen Sie die per Doppelklick im Hilfsprogramm „DB Browser for SQLite“. Um darin zu den Chats zu gelangen, klicken Sie auf die Registerkarte **Daten durchsuchen** ①, öffnen das Ausklapp-

EINSATZ ALS WAFFE

GESPRÄCHE BELAUSCHEN

menü neben „Tabelle:“ ② und wählen dann den Eintrag **Messages** aus. In der folgenden Übersicht (siehe Bild unten) verrät die Spalte „author“ ③, wer der Verfasser der jeweiligen Nachricht ist. Die Textnachrichten finden Sie in der Spalte „body.xml“. Scrollen Sie gegebenenfalls etwas nach rechts, um sie einzublenden. Per Doppelklick auf einen Eintrag öffnet sich der jeweilige Inhalt in einem eigenen Fenster ④.

id	msg_id	conv_id	chatname	author	msg_displayname	pr_wa	guid	msg_par	timestamp
28	1248	1	1033	19:88738...			NULL	BLOB	1478253...
29	1249	1	1033	19:88738...			NULL	BLOB	1478253...
30	1250	1	1033	19:88738...	markus.sc...		NULL	BLOB	1478254...

PASSWÖRTER KNACKEN

Windows-Kennwort vergessen? Die Hacker-DVD ist Ihr Schlüsseldienst! Zudem prüfen Sie damit, ob Ihr WLAN-Kennwort sicher ist.

EINSATZ ALS WERKZEUG

PC ENTSPERREN

Haben Sie Ihr Windows-Kennwort vergessen und kommen nicht mehr rein? Falls es sich um ein lokales Benutzerkonto handelt, lässt es sich mit der Hacker-DVD im Nu aufhebeln. Das können aber leider auch Einbrecher nutzen.

Windows wählen

Klicken Sie im Dock ganz links auf das Symbol **Anwendungsmenü**, dann auf **Rettungswerkzeuge** und **Kennwort neu**. Die Software „Windows-Passwort zurücksetzen“ sollte nach dem Start automatisch die Windows-Partition erkennen – auch ohne vorherige Einbindung. Sind auf dem Computer mehrere Windows-Versionen installiert, wählen Sie unter „1. Schritt: Auswahl der Windows-Installation“ die Partition, auf der das fragliche Benutzerkonto eingerichtet ist (siehe Bild unten).

Benutzer wählen

Anschließend wählen Sie bei „2. Schritt: Auswahl des Benutzers“ das Benutzerkonto

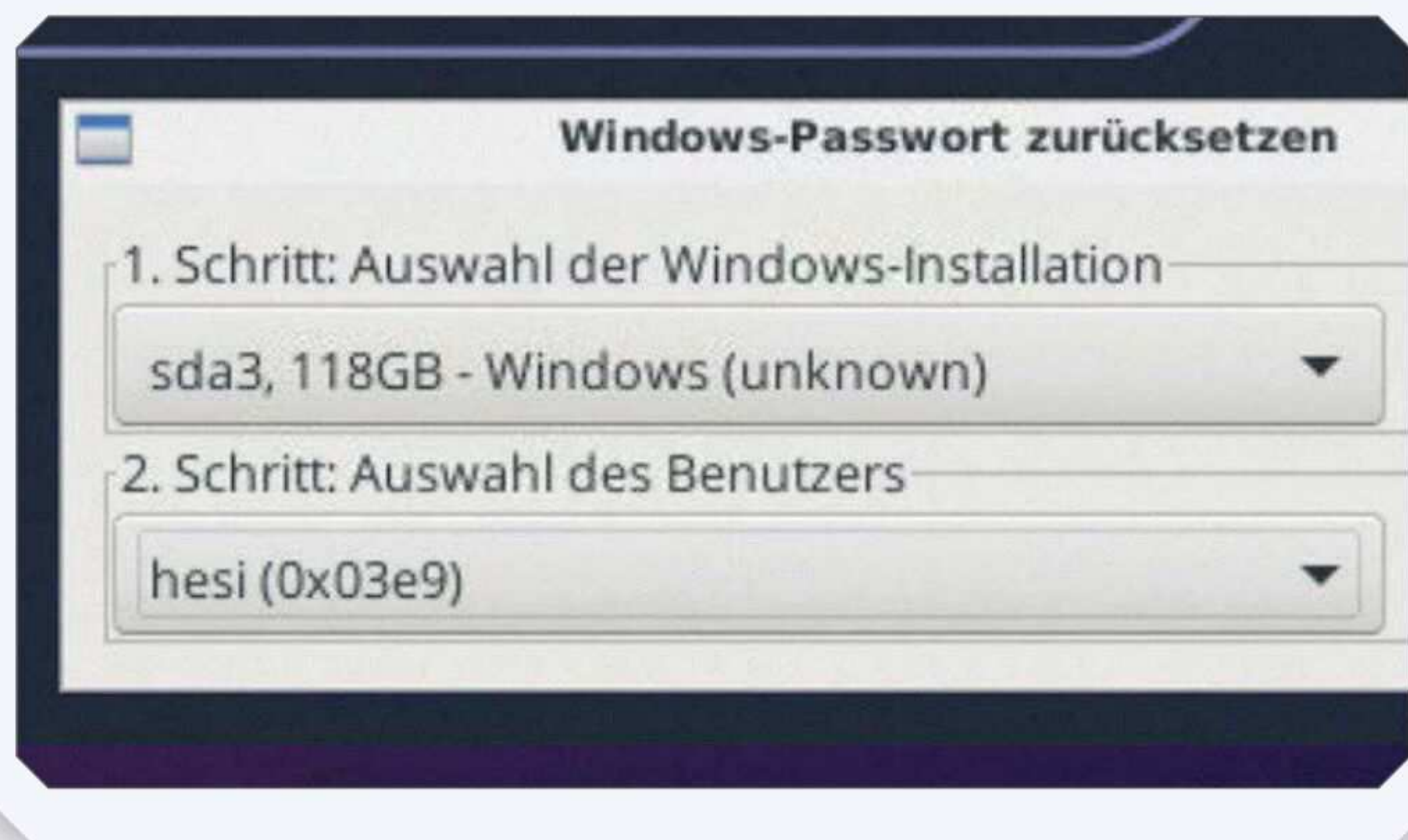
EINSATZ ALS WAFFE

PC-EINBRUCH

aus, dessen Passwort Sie zurücksetzen wollen. Ist nur ein Benutzerkonto in Windows eingerichtet, entfällt dieser Schritt. Ist alles korrekt eingestellt, klicken Sie schließlich auf **Zurücksetzen** und bestätigen die Frage nach einem Backup mit **Ja**. Nach kurzer Zeit erscheint eine Erfolgsmeldung. Klicken Sie auf **OK**.

Neues Kennwort festlegen

Sie können Windows jetzt wieder öffnen. Klicken Sie dazu im Dock auf **Computer ausschalten** und **Neu starten**. Daraufhin klappt die Anmeldung ohne Kennwort. Falls Sie sich zuletzt mit Windows Hello angemeldet haben, klicken Sie unter „Anmeldeoptionen“ auf den Schlüssel. Um den PC wieder zu schützen, vergeben Sie ein neues Kennwort. Dazu klicken Sie im Windows-Startmenü aufs Zahnrad, auf **Konten** und **Anmeldeoptionen**. Nach Klicks auf **Kennwort** und **Hinzufügen** legen Sie im neuen Fenster ein Kennwort fest, wählen **Weiter** und **Fertig**.

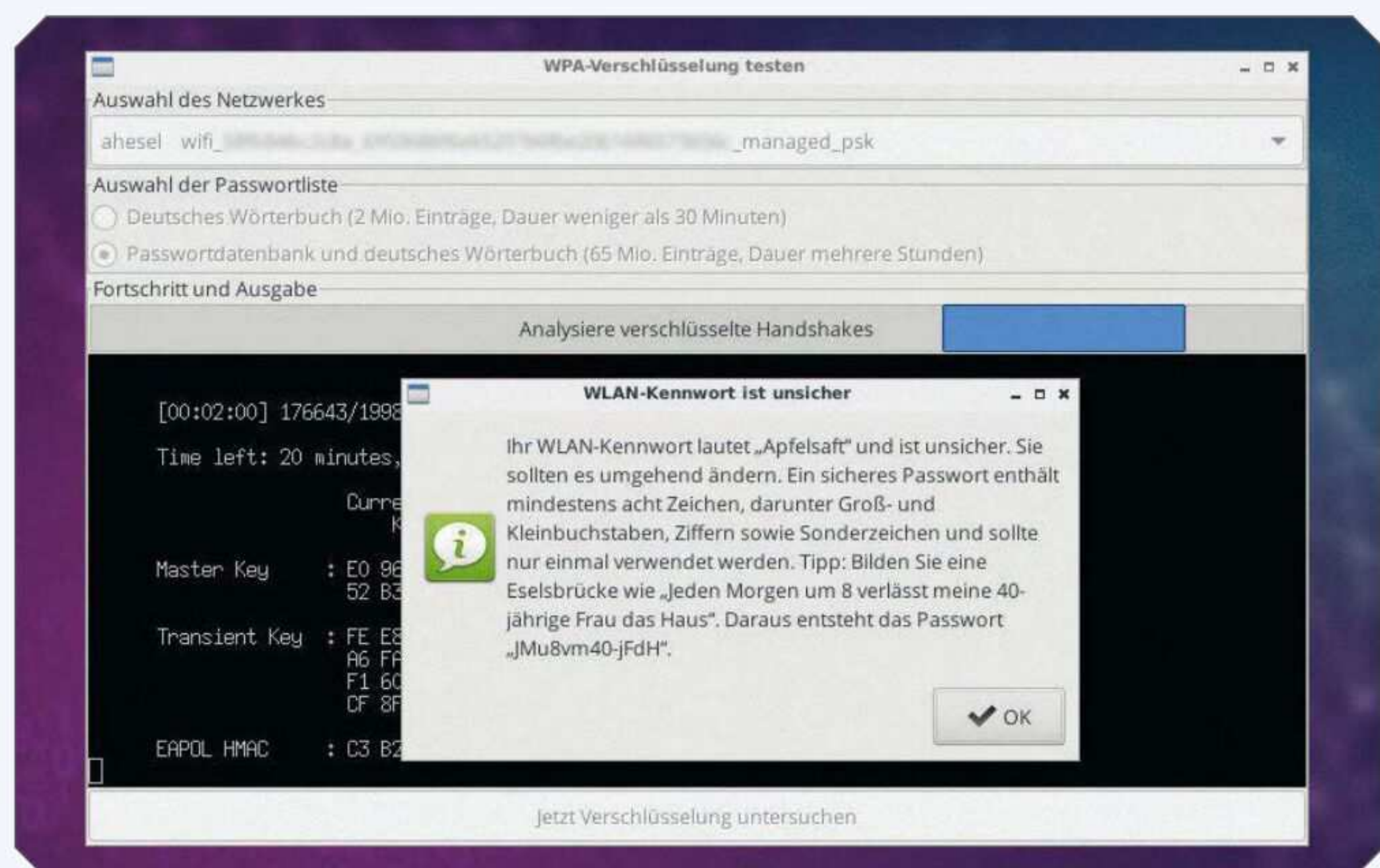


EINSATZ ALS WERKZEUG

WLAN PRÜFEN

EINSATZ ALS WAFFE

WLAN KNACKEN



Hacker lauern nicht nur im Internet, sondern auch an der Straßenecke oder im Nachbarhaus. Mit der Hacker-DVD könnten die in Ihr Heimnetzwerk eindringen und Schäden anrichten. Schlagen Sie potenzielle Eindringlinge mit den eigenen Mitteln: Denn mit der Hacker-DVD finden Sie heraus, ob Ihr WLAN sicher ist.

Datenbank wählen

Klicken Sie im Hauptmenü auf **WLAN- & Netzwerkanalyse** sowie auf **WLAN-Passwort knacken**. Im nächsten Fenster haben Sie zwei Optionen:
■ **Deutsches Wörterbuch:** Mit dieser Option sucht das Programm nach rund zwei Millionen einfachen Kennwörtern. Das dauert circa 30 Minuten.
■ **Passwortdatenbank:** Wählen Sie diese Option, um das Wörterbuch und eine Passwort-

datenbank zu verwenden, die auch Hacker nutzen. Die Suche umfasst 65 Millionen Einträge und dauert mehrere Stunden, ist dafür aber sehr zuverlässig.

Passwort knacken

In der Liste „Auswahl des Netzwerkes“ klicken Sie auf Ihr WLAN, dann auf **Jetzt Verschlüsselung untersuchen** und **OK**. Im Anschluss verbinden Sie ein anderes Gerät, etwa Ihr Smartphone, mit dem gleichen WLAN oder trennen die bestehende Verbindung und stellen sie gleich wieder her. Diesen sogenannten Handshake kann das Tool erkennen und die Anmeldedaten mitschneiden. Erscheint wie im Bild oben das Kennwort auf dem Bildschirm, sollten Sie es umgehend wie gezeigt ändern. Klicken Sie auf **OK**.

STRESSFREI DURCH DEN PC-ALLTAG

DAS UNZERS WINDOWS

Zickt Ihr Windows mal wieder rum? Mit dieser Software **setzen Sie PC oder Notebook einfach zurück** in den Zustand vor dem Problem.

Defekte Treiber, Schad-Software, Programmier- oder Bedienfehler: Viele Gefahren bedrohen Ihren Windows-PC und Ihre Daten. Wer nach einer Software-Katastrophe Windows und alle seine Programme neu einrichten muss, hat richtig Stress. Doch mit dem Windows-Retter 2022 geht das zum Glück mit ein paar Klicks. Die clevere Software sichert mit einer genialen Technik Ihr komplettes System in einem geschützten Bereich auf der Festplatte. Im Notfall stellen Sie es von da aus mit wenigen Mausklicks wieder her. Das funktioniert viel einfacher und schneller als mit jedem Backup-Programm!

Schützt Windows 8, 10 und 11

Hinter dem Windows-Retter steht das Kaufprogramm PC-Sheriff. Es kommt etwa in Schu-

len zum Einsatz, um PCs nach der Nutzung in den ursprünglichen Zustand zurückzusetzen. Hierzu erstellt die Software sogenannte Snapshots der Festplatte, und diese Momentaufnahmen enthalten neben Windows alle Programme, Einstellungen und Dateien. Geht etwas schief, machen Sie per Knopfdruck alles ungeschehen. Das dauert nur Sekunden und klappt auch, wenn Windows nicht mehr startet. Selbst „Zeitreisen“ durch verschiedene Snapshots sind möglich. Auch gelöschte Dateien stellt der Windows-Retter wieder her.

Vollversion ein Jahr gratis

Damit der Windows-Retter funktioniert, muss wenigstens ein Viertel der Festplatte frei sein. Mit dieser Ausgabe erhalten Sie die 69 Euro teure Premium-Version für ein Jahr gratis*. Da-

nach lassen sich keine neuen Snapshots mehr anlegen, vorhandene bleiben aber erhalten.

Fit für Windows 11

Der Windows-Retter funktioniert auch in Windows 11. Anders als in früheren Versionen lässt sich das Notfall-System nun bequem per Maus bedienen und mit der Taste **[R]** (statt **[Pos1]**) starten, die auf keiner Tastatur fehlt. Zudem blockt das Programm nicht mehr standardmäßig kleinere Windows-Updates. *[hp/bes]*

Jetzt auch für
**WINDOWS
11**

WEM NÜTZT DER WINDOWS-RETTER?

Der Windows-Retter 2022 ist ein kleines Wunderwerk der Technik, doch für wen ist das Programm eigentlich gedacht? COMPUTER BILD zeigt drei Nutzergruppen, deren digitaler Alltag spürbar von der pfiffigen Software profitiert.



Schüler- und Lehrer-PCs bleiben mit der Software auf einem Stand und stets einsatzbereit.



Einsteiger gewöhnen sich unbesorgt an ihren PC und machen Fehlgriffe einfach rückgängig.



Tüftler testen risikofrei Programme und wechseln bequem zwischen verschiedenen Snapshots.

*Der Preis gilt für die zeitlich unbegrenzte Kaufversion. Die Version von der Heft-DVD ist ein Jahr lang nutzbar.

Der **WINDO**
RETTER 2022
NIE WIEDER WINDOWS NEU INSTALLI



TÖRRBARE

INSTALLATION & REGISTRIERUNG

Geben Sie zuerst auf **computerbild.pcsheriff.de** Ihre Daten ein. Dann

Vorname
Nachname
Email Adresse *

klicken Sie auf **kostenlose Lizenz anfordern** und notieren sich die Produkt-ID, die per Mail kommt. Trennen Sie den PC vom Internet, damit Updates die Installation nicht stören, und beenden Sie alle Program-

Lizenz Information Bitte geben Sie Ihre Produkt ID ein (falls vorr Erzeugen einer Testversion Produkt ID
Produkt ID SCPCS-XXXXXXXXXXXXXXX

me inklusive Virenschutz. Bei Avast klicken Sie dazu mit der rechten Maustaste auf das Avast-Logo neben der Windows-Uhr, auf **avast Schutzsteuerung, Bis zum nächsten Neustart** und klicken auf **Ja**. Starten Sie die Installation des Windows-Rettens von der Heft-DVD. Im Feld „Produkt-ID“ geben Sie die ID aus der E-Mail ein. Wichtig: Sind mehrere Betriebssysteme installiert, wählen Sie das benutzerdefinierte Set-up, siehe Handbuch auf **cobi.de/go/pcsheriff20**. Im Fenster „Windows Update Einstellungen“ behalten Sie alle Voreinstellungen bei. Um das Programm zu starten, klicken



Sie neben der Windows-Uhr doppelt auf den Sheriff. Erscheint er dort nicht, blenden Sie ihn per Klick auf den Pfeil ein. ➤



„Einfach installieren,
und der PC ist gesi-
chert. So bequem kann
Sicherheit sein.“

Hubert Popiolek
Redakteur Software



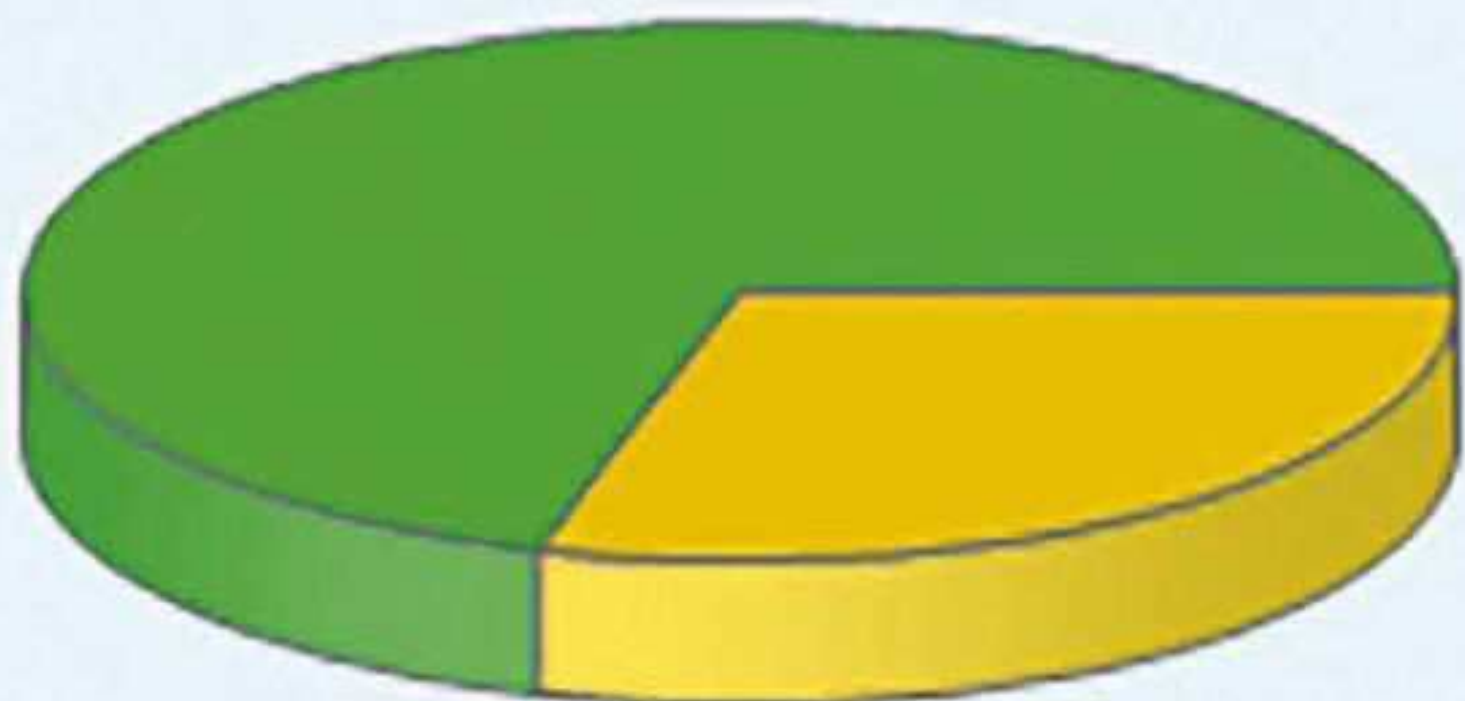
PC-SHERIFF
Premium

- Hauptmenü
- Wiederherstellung
- Snapshot - Menü
- Aufgabenplanung

PC-Sheriff Premium

Einfach, schnell und sicher - Sofortige System Rücksetzung und Wiederherstellung beim Neustart!

Version: v13.0
Build: 2707526920
Product ID: SCPCS-RM1220-817754-887315
License type: Abonnement
Ablaufdatum: 05.10.2022



Gesamt geschützt: 59,2 GB
Belegt: 21,1 GB
Noch frei: 38,1 GB

Erstellte Snapshots: 1
Letzter Snapshot am: 20.04.2022 10:16:41
Letzte Rücksetzung:
Geplante Aufgaben: 2
PC-Sheriff Premium Speichersparender Modus

Schutz auf Laufwerk:

Partition	Typ	Grösse	belegt	frei	Status
C:	NTFS	59,2 GB	21,1 GB	38,1 GB	Geschützt



WINDOWS-SICHERUNG IM DETAIL REGELN

Nach der Installation des Programms ist Ihr PC geschützt. Wie Sie die **Sicherung anpassen und eigene Snapshots erstellen**, lesen Sie hier.



WINDOWS SICHERN

Die Bedienung des Windows-Retters 2022 ist kinderleicht, denn das Programm macht alles Wichtige bereits ohne Ihr Zutun. So sichert der Windows-Retter Ihr Betriebssystem und Ihre Daten schon während seiner Installation automatisch – das dauert nur Augenblicke. Zusätzlich legt die Software in regelmäßigen Abständen weitere Sicherungen aller veränderten Daten an. In der Voreinstellung passiert das täglich beim Start Ihres Computers.

Keine Bange: Windows braucht dadurch kaum länger, bis es einsatzbereit ist.

Sie haben immer die Kontrolle

Möchten Sie nur sichergehen, dass Sie Windows im Notfall auf einen früheren Stand zurücksetzen können, müssen Sie nach der Installation des Programms nichts weiter tun. Regeln Sie hingegen lieber alle Details selbst, ändern Sie einfach die Voreinstellungen des Programms: Passen Sie den

Zeitpunkt und den Abstand der automatischen Sicherungen Ihren Bedürfnissen an. Bei Bedarf erstellen Sie außerdem zusätzlich manuelle Sicherungspunkte. Das kann beispielsweise praktisch sein, wenn Sie den Computer gerade erst einer größeren Aufräumaktion unterzogen haben oder ein langwieriges Update endlich installiert ist. Wie Sie das Erstellen von Snapshots verwalten und eigene Sicherungspunkte anlegen, lesen Sie in der Anleitung unten.

Erstellte Snapshots: 1
 Letzter Snapshot am: 20.04.2022 10:16:
 Letzte Rücksetzung:
 Geplante Aufgaben: 2
 PC-Sheriff Premium Speichersparender

1 HAUPTSICHERUNG

Nach der Einrichtung zeigt der Windows-Retter, dass er im Zuge der Installation automatisch die erste Sicherung („Snapshot“) erstellt hat, siehe auch großes Bild links. Dieser Startbildschirm erscheint jedes Mal, wenn Sie den Windows-Retter öffnen, und zeigt die Zahl aller verfügbaren Snapshots an.

Aufgabenplanung

Automatisieren Sie die Snapshot Erstellung

Hinzufügen Entfernen

Aufgabe	Aufgabenplan	Aufgaben Eigenschaften
Täglicher Snapshot	Täglich	Täglicher
System Wartung	Täglich	Täglicher

2 ZUSATZSICHERUNGEN

In der Voreinstellung erstellt das Programm täglich Sicherungen. Im Register **Aufgabenplanung** können Sie das Intervall ändern: Klicken Sie doppelt auf **Täglicher Snapshot**, wählen Sie statt „Täglich“ etwa **Wöchentlich** aus, und vergeben Sie einen Namen, etwa **Wöchentlicher Snapshot** gefolgt von **OK**.

Snapshot Name (maximal 20 Zeichen):

Saubere Basis

Beschreibung:

Frühjahrsputz erledigt

☐ Snapshot gegen Löschen schützen

3 MANUELLE SICHERUNG

Haben Sie Programme installiert, den PC ausgemistet oder eine wichtige Datei bearbeitet? Nach Klick auf den Registerreiter **Snapshot-Menü** und dann auf **Neu** erstellen Sie jederzeit einen manuellen Snapshot. Dazu geben Sie Namen und Beschreibung ein, klicken auf **Weiter** und dann auf **Ende**.

RÜCKKEHR IM NOTFALL DIE UHR ZURÜCKDREHEN



PC-SHERIFF
Premium



Hauptmenü



Wiederherstellung



Snapshot - Menü



Aufgabenplanung

Wiederherstellung

Eine Systemrücksetzung oder Wiederherstellung beschädigter Dateien dauert nur wenige Momente



System Rücksetzung

Nach einem PC-Neustart ist das System zum ausgewählten Snapshot zurückgesetzt



Dateiwiederherstellung

Suchen und Wiederherstellen von Dateien aus vorhandenen Snapshots



Durchsuche Snapshot

Einen vorhandenen Snapshot als virtuelles Laufwerk öffnen

RETTUNG
in drei simplen
SCHRITTEN

Im Notfall ist guter Rat teuer – nicht so beim bequemen Windows-Retter: Alle Infos zum **Wiederherstellen von Windows oder einzelner Dateien** finden Sie auf dieser Doppelseite.



WINDOWS ZURÜCKSETZEN

Treten Probleme auf, stellen Sie mit dem Windows-Retter im Nu einen früheren Zustand wieder her.

Die Zeitmaschine für Ihren PC

Wie einfach die Wiederherstellung klappt, lesen Sie unten. Mit dem Windows-Retter können Sie aber nicht nur einen einzelnen Snapshot wiederherstellen, sondern beliebig zwischen all Ihren Windows-Sicherungen hin- und herwechseln – Sie reisen wie mit einer Zeitmaschine durch

die Geschichte Ihres PCs. Hat etwa die Wiederherstellung wichtige Arbeitsschritte ungeschehen gemacht, wählen Sie einfach einen jüngeren Snapshot. Wer auf der Suche nach bestimmten Dateien ist, kann auch die Snapshots durchsuchen – siehe Hinweise in der Randspalte.

Windows startet gar nicht mehr? Keine Panik, in so einer Notlage können Sie den Windows-Retter dank speziellem Notfall-System trotzdem starten! Alle Infos dazu lesen Sie auf Seite 92.

Zu welchem Snapshot soll das System zurückgesetzt werden?
Bitte treffen Sie eine Auswahl. Auszunehmende Dateien wählen Sie unter "Ausnahmen".

Ausnahmen ▼

Snapshot	Grösse	Typ	Status	Erstellt
Installation	19,8 GB	Baseline	gesperrt	20.04.2022 1.
Win:Geplanter Sn...	1,34 GB	Täglich	entsperrt	21.04.2022 1.
Win:Frühjahrsputz	1,02 GB	Benutzer	entsperrt	21.04.2022 1.

1 Starten Sie den Windows-Retter, und klicken Sie auf **Wiederherstellung** und **System Rücksetzung**. Wählen Sie nun den Snapshot, zu dem Sie zurückkehren möchten. Beispiel: Nach Klick auf **Installation** stellen Sie den Zustand direkt nach der Installation des Windows-Rettens wiederher. Keine Bange, beim Zurücksetzen bleiben neuere Snapshots erhalten.

Bitte lesen Sie die nachfolgenden Informationen

Warnung!!!

Die System - Rücksetzung zu einem Snapshot setzt alles auf dem geschützten Zeitpunkt des gewählten Snapshots zurück. Zum Erhalt von Daten gibt es keine Möglichkeit.

1. Vor der System - Rücksetzung einen aktuellen Snapshot erstellen

Sie haben das System zu einem anderen Snapshot zurückgesetzt. Falls Sie zuvor wichtige Daten erstellt oder geändert haben und vor der Systemrücksetzung einen Snapshot erstellen, können Sie Daten über den Datei Wiederherstellungs Assistenten zurückholen.

☐ Diesen Dialog nicht mehr anzeigen.

OK Abbruch

2 Lassen Sie den Haken „Aktuellen Snapshot vor der System Rücksetzung erstellen“ unbedingt stehen, damit auch der aktuelle Stand gesichert wird. Nach einem Klick auf **Weiter** zeigt das Programm hierzu noch eine Warnung an. Bestätigen Sie diese jetzt mit einem Mausklick auf **Neustart**.

3 Der Computer startet jetzt neu, und der Windows-Retter zeigt eine entsprechende Meldung an. Klicken Sie darin auf **Abbruch**. Falls dann wichtige neuere Dateien oder Ordner fehlen, stellen Sie diese aus dem letzten Snapshot wieder her – wie im Abschnitt rechts beschrieben.



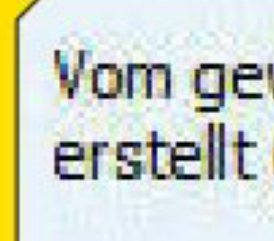
SICHERUNGEN DURCHSUCHEN

Fehlen nach der Systemrücksetzung kurz zuvor erstellte Dateien oder Ordner? Handelt es sich um eine einzelne Datei, lesen Sie auf Seite 92 oben, wie Sie die wiederherstellen. Fehlt ein wichtiger Ordner? Dann hilft eine komfortable Funktion des Windows-Rettens weiter: Das Programm kann beliebige Snapshots als virtuelle Festplatte öffnen. Der Inhalt der Sicherung erscheint dann wie ein echtes Laufwerk im Windows-Explorer. Kopieren Sie dann die vermissten Dateien oder Ordner einfach auf die „echte“ Festplatte.



Erstelle virtuelles Laufwerk, bitte warten...

1 Klicken Sie auf **Wiederherstellung** und **Durchsuche Snapshot**. Wählen Sie den zu durchsuchenden Snapshot aus. Nach einem weiteren Mausklick auf die Schaltfläche **Durchsuchen** erstellt die Software die virtuelle Festplatte. Das dauert ein paar Sekunden.



Vom gewählten Snapshot wird ein virtuelles Laufwerk erstellt (im Nur-Lesen-Modus).

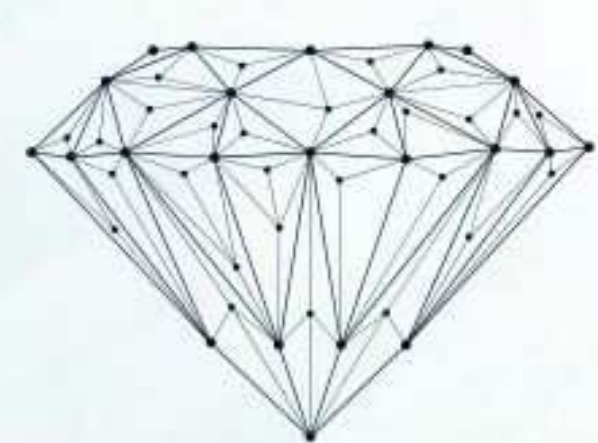
Dieses kann mit dem Windows Explorer geöffnet werden.

2 Um den Inhalt der Sicherung anzuzeigen, klicken Sie anschließend auf **Öffne virtuelles Laufwerk**. Ihre gesicherten Laufwerke erscheinen im Windows-Explorer zwar doppelt, lassen sich aber anhand der unterschiedlichen Laufwerksbuchstaben unterscheiden.



Boot (C:)	Recover (D:)
794 GB frei von 865 GB	136 MB frei von 61,2 GB
Boot (F:)	Recover (G:)
819 GB frei von 865 GB	137 MB frei von 61,2 GB

3 In diesem Beispiel hat die Sicherung des Laufwerks „C:“ den Buchstaben „F:“. „G:“ ist die Kopie von „D:“. Kopieren Sie die gesuchte Datei von der Sicherung zum Original-Laufwerk. Danach klicken Sie im Windows-Retter auf **Schließe virtuelles Laufwerk**.



EINZELNE DATEIEN WIEDERHERSTELLEN

Sind nur einzelne Dateien vermiskst, geht's per Suchfunktion noch einfacher. Aus den Snapshots lassen sich nämlich

auch gelöschte oder beschädigte Dateien wiederherstellen, etwa unersetzliche Fotos. Dazu suchen Sie die Dateien in einem

Snapshot, bei dessen Erstellung die Dateien noch vorhanden und heil waren. Erinnern Sie sich nicht mehr an den Namen

der fraglichen Datei? Dann durchsuchen Sie die Sicherungen einfach nach dem jeweiligen Dateityp oder Speicherort.

Wie möchten Sie die Dateien wiederherstellen?

☒ Ich kenne den Dateinamen der Datei (z.B. readme.doc)

☐ Ich kenne den Dateityp der Datei (z.B. *.doc)

☐ Ich kenne den Ablageort der Datei (z.B. Eigene Dateien)

Snapshot	Grösse	Typ	Status
Installation	19,8 GB	Baseline	gespeichert
Win:Geplanter Sn...	1,34 GB	Täglich	entspeichert
Win:Frühjahrsputz	1,02 GB	Benutzer	entspeichert
Geplanter Snapshot	168 MB	Neustart	entspeichert

Öffne Wiederherstellung

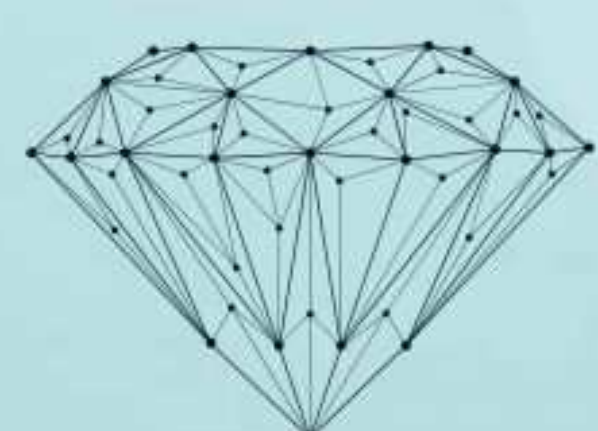
Name Speichern unter

Notizen.txt Überschreiben

1 Klicken Sie auf **Wiederherstellung** und **Dateiwiederherstellung**. Als Nächstes legen Sie die Suchmethode fest. Falls Sie den Dateinamen kennen, bleiben Sie bei der Voreinstellung und tippen den Namen ein. Andernfalls suchen Sie nach dem Dateityp oder dem Speicherort.

2 Klicken Sie anschließend auf **Weiter**, und wählen Sie dann einen Snapshot, bei dessen Erstellung die fragliche Datei noch intakt war. Nach einem Mausklick auf **Weiter** durchsucht der Windows-Retter die Sicherung. Je nach gesicherter Datenmenge kann das eine Weile dauern.

3 Nun erscheint die gesuchte Datei. Markieren Sie sie per Klick. Nach Klicks auf **Wiederherstellung** und **Überschreiben** landet sie im Originalordner. Alternativ wählen Sie nach einem Klick auf **Speichern unter** einen anderen Zielort. Zum Schluss klicken Sie auf **Ende**.



WENN WINDOWS NICHT MEHR STARTET

Der Fall der Fälle: Windows macht keinen Mucks mehr. Auch das ist dank Windows-Retter kein Grund, in Panik zu verfallen. Denn schon während der Installation legt das Programm auf Ihrer Festplatte ein Notfall-System an, das Sie bei Bedarf einfach anstelle von Windows starten. So können Sie den PC-Sheriff auch dann noch benutzen, wenn Windows beim Hochfahren versagt.

Notfall-System öffnen

Schalten Sie den Computer ein, oder starten Sie ihn gegebenenfalls neu. Da das Notfall-System noch vor Windows startet, müssen Sie rechtzeitig reagieren: Sobald der Bildschirm mit dem Bild des Sheriffs und dem Schriftzug „PC-Sheriff Premium“ erscheint, drücken Sie die Taste **⌘** auf Ihrer Tastatur. Nach kurzer Ladezeit erscheint dann das Menü im Bild rechts. Im Gegensatz zu früheren Versionen des Windows-Rettens lässt sich dieses Menü nun komfortabel mit der Maus bedienen. Welche Funktionen das Notfall-System für Sie bereithält und wie Sie diese nutzen, erfahren Sie in dieser Übersicht:

PC-Sheriff Premium

Systemrücksetzung zu Snapshot

1...	Name	Zeit
1	Installation	2022-04-20
2	Win:Geplant...	2022-04-21
3	Win:Frühjah...	2022-04-21
4	Geplanter S...	2022-04-21
5	Geplanter S...	2022-04-21
6	Win:Notizen...	2022-04-21
7	Win:Post-No...	2022-04-21

Systemrücksetzung

Mit dieser Funktion setzen Sie den PC in einen vorherigen Zustand zurück. Wählen Sie dazu wie auf Seite 91 beschrieben einfach einen Snapshot aus der Liste, und bestätigen Sie mit **Weiter**. Im Anschluss wird der PC in den gewünschten Zustand zurückversetzt.

Defrag. Snapshots Systemeinstellungen

Erweiterte Optionen

Hier finden Sie zusätzliche Werkzeuge. Mit **Defrag. Snapshots** lassen sich Ihre Sicherungen in einem Rutsch platzsparend aufräumen, was die Software aber auch regelmäßig automatisch erledigt. Mit der Funktion **Systemeinstellungen** kann der Kundendienst des PC-Sheriffs in Spezialfällen Reparaturen vornehmen.

Snapshot Name

AV-Installation

Beschreibung:

Avast installiert

Sheriff Premium

Zurueck Weiter

Snapshot erstellen

Haben Sie Windows aktualisiert oder ein neues Programm installiert, können Sie den aktuellen Systemzustand mit dieser Funktion auch aus diesem Menü heraus sichern. Dazu geben Sie einen Namen und eine Beschreibung ein und klicken auf **Weiter**. Der neue Snapshot ist sofort verfügbar.

PC SHERIFF Premium

Systemrücksetzung

Snapshot erstellen

Erweit. Optionen

Deinstallation

Ende

Deinstallation zu Snapshot..

1...	Name	Zeit
1	Installation	2022-04-20 1
2	Win:Geplant...	2022-04-21 1
3	Win:Frühjah...	2022-04-21 1
4	Geplanter S...	2022-04-21 1
5	Geplanter S...	2022-04-21 1
6	Win:Notizen...	2022-04-21 1
7	Win:Post-No...	2022-04-21 1
8	Akt. System	2022-04-21 1

Deinstallation

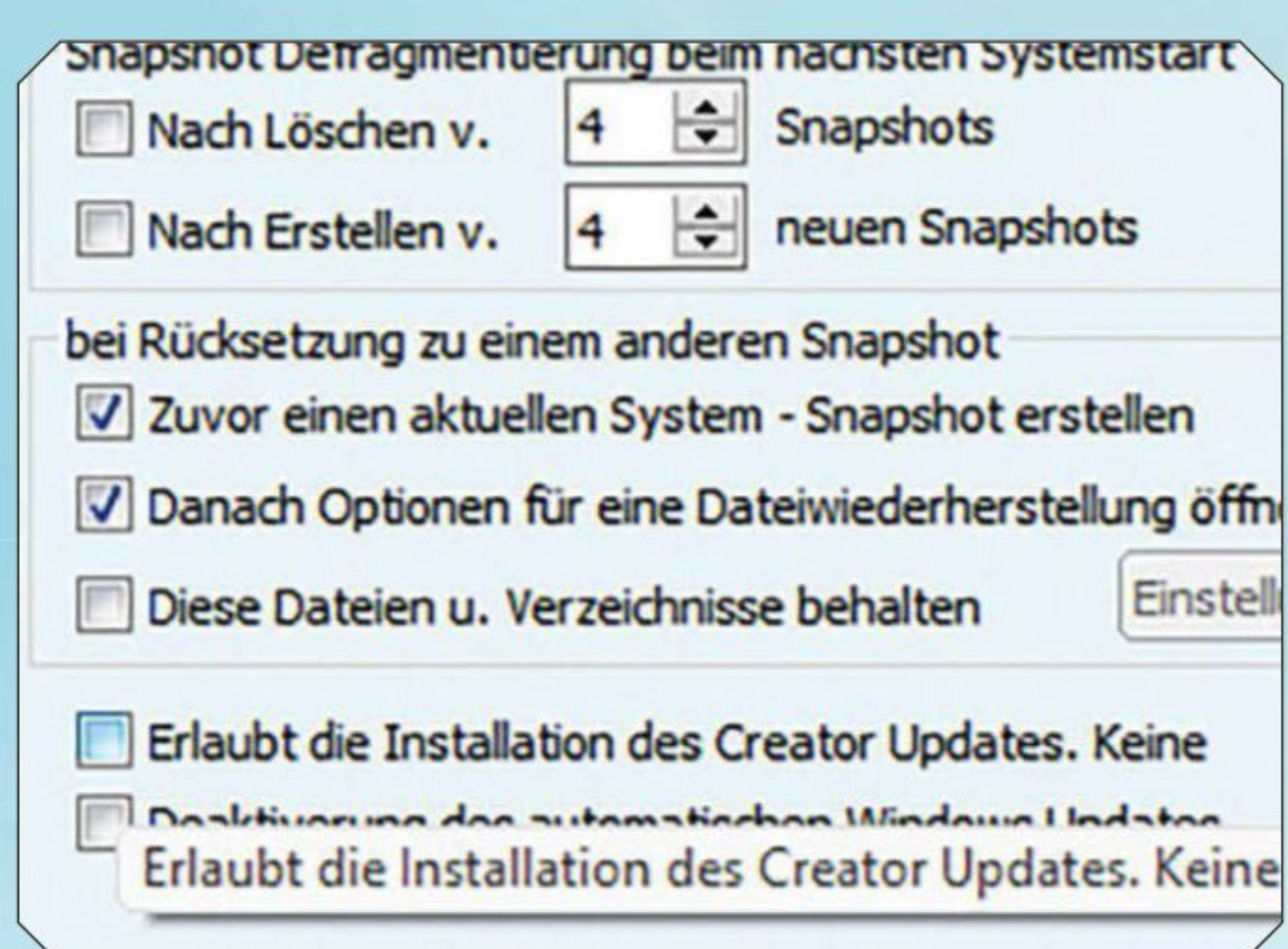
Bei Problemen oder falls Sie den PC-Sheriff nicht mehr benötigen, können Sie das Programm hier deinstallieren. Wählen Sie in der folgenden Liste den Snapshot aus, mit dem der PC-Sheriff Ihr Windows zurücklassen soll. Anschließend bestätigen Sie mit **Weiter, Ja** und **OK**.

CLEVERE TIPPS & TRICKS

Mit diesen cleveren Zusatzfunktionen **holen Sie noch mehr aus dem Windows-Retter heraus.**

FÜR WINDOWS-UPGRADES

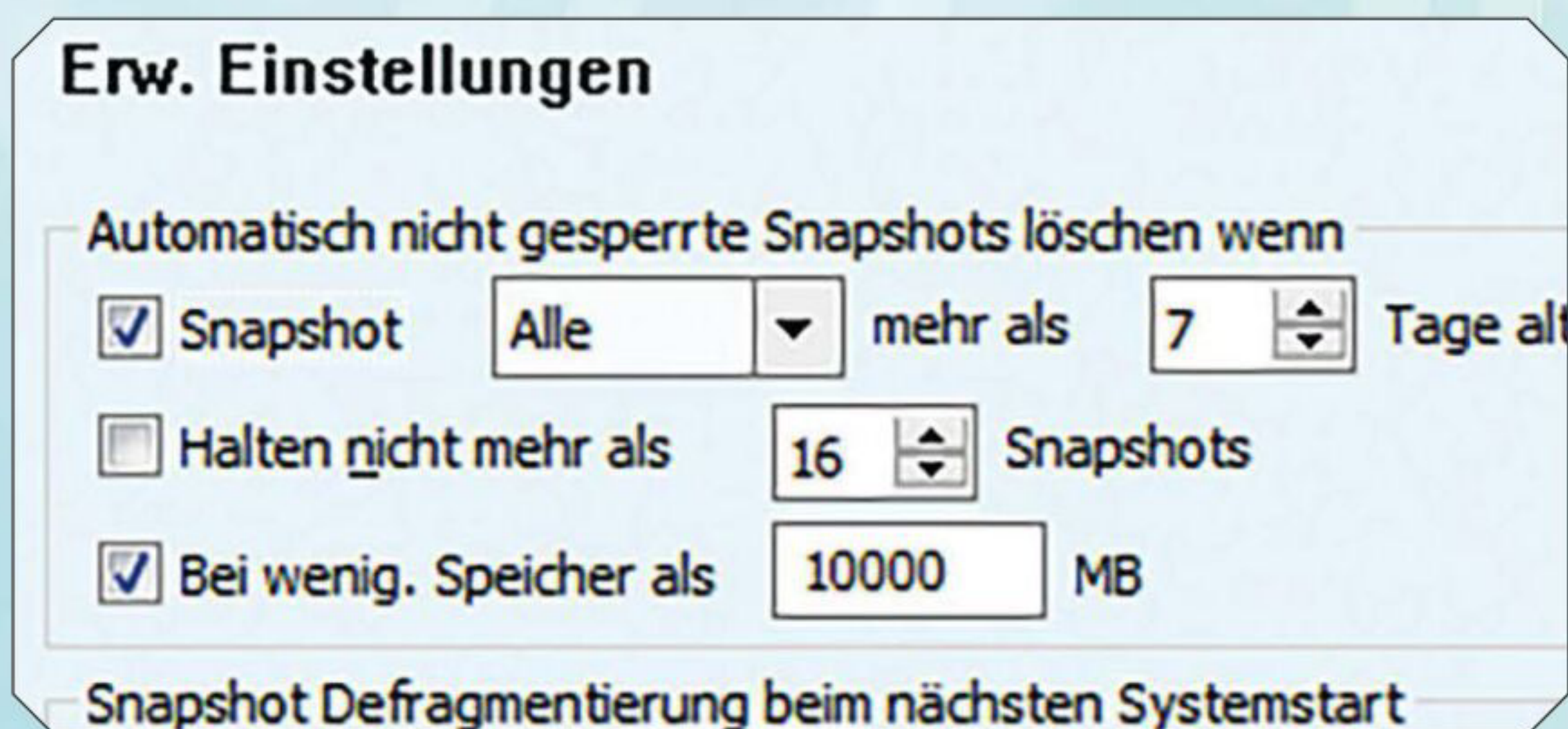
PC-SHERIFF ZURÜCKSETZEN



Microsoft veröffentlicht jährlich größere Updates für Windows 10 und 11, demnächst Windows 11 22H2. Zur Installation dieser großen Updates sowie zum Upgrade etwa von Windows 10 auf 11 müssen Sie den PC-Sheriff deaktivieren, sodass alle Snapshots verfallen. Eine Automatik macht den Vorgang ganz einfach: Ist sie eingeschaltet, deaktiviert sich der PC-Sheriff zur Installation der großen Updates automatisch, aktiviert sich danach wieder selbst und legt eine neue Erstsicherung an. Um nicht ohne Vorwarnung alle Snapshots zu verlieren, aktivieren Sie die Automatik-Funktion erst bei Bedarf: Meldet Windows, dass ein Funktions-Update verfügbar ist, wechseln Sie zu einem Datenstand, der zur neuen Erstsicherung werden soll (siehe „Windows zurücksetzen“, Seite 91). Danach klicken Sie auf das Zahnrad und auf **Erw. Einstellungen**. Setzen Sie unten im Fenster einen Haken bei **Erlaubt die Installation des Creator Updates. Keine Rücksetzung möglich**, und klicken Sie auf **OK**. Um sicherzustellen, dass nun das Update startet, drücken Sie **Windows + I**, klicken auf **Update und Sicherheit** und gegebenenfalls auf **Nach Updates suchen**. Ist das Update installiert, entfernen Sie den eben gesetzten Haken wieder und wiederholen das Vorgehen beim nächsten großen Windows-Update.

SNAPSHOTS LÖSCHEN

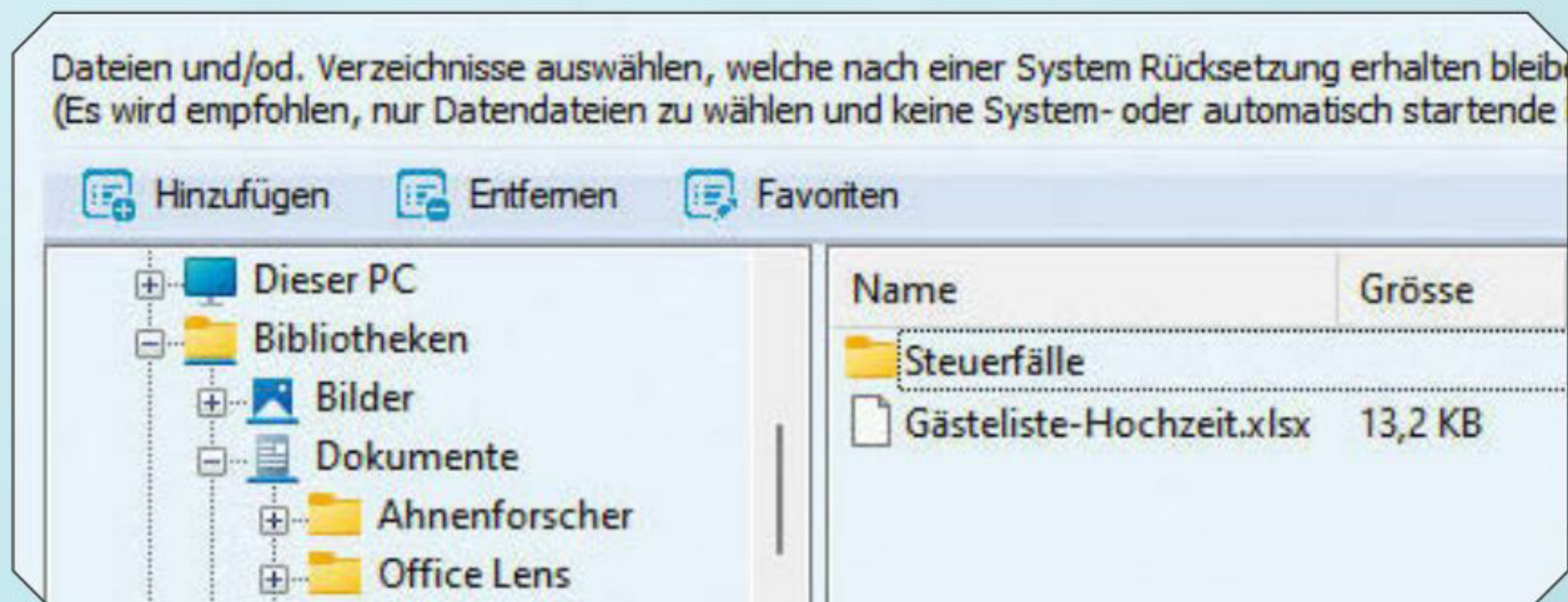
PLATZ SCHAFFEN



Um Platz zu sparen, löscht der Windows-Retter alle Snapshots, die älter sind als sieben Tage – außer der Erstsicherung. Verbleiben weniger als 10 000 Megabyte Speicherplatz auf der Festplatte, löscht die Software weitere Snapshots. Um die Einstellungen zu ändern, klicken Sie auf das Zahnrad und auf **Erw. Einstellungen**. Nun passen Sie bei Bedarf den Zeitraum und die Speichergrenze an oder schalten per Klick eine der Regeln ab. Mit der Option **Halten nicht mehr als** begrenzen Sie zusätzlich die Gesamtzahl der Snapshots.

BEIM ZURÜCKSETZEN

DATEN BEHALTEN



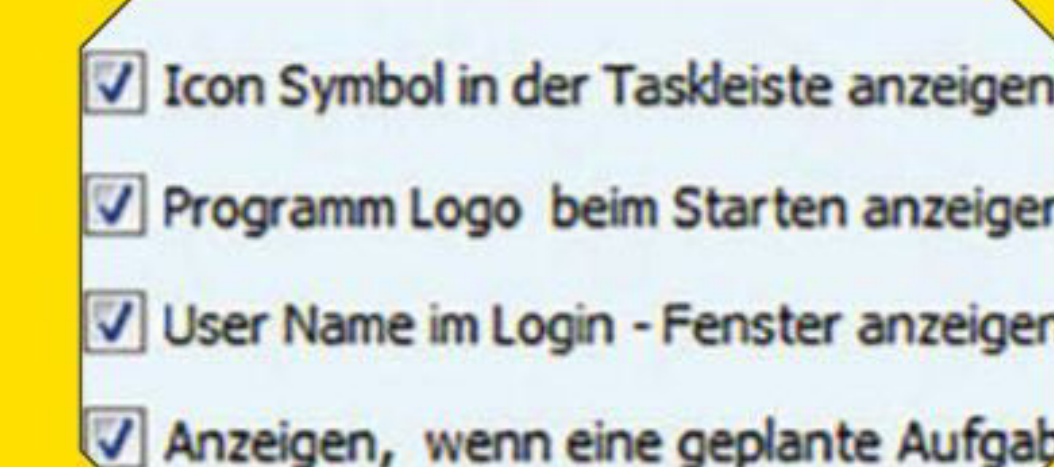
Mit dem Tipp auf der vorigen Seite stellen Sie statt eines gesamten Snapshots nur einzelne Dateien wieder her. Es geht auch umgekehrt – Sie wählen Dateien oder Ordner, die beim Zurücksetzen auf einen Snapshot unverändert bleiben: Dazu klicken Sie auf das Zahnrad, **Erw. Einstellungen**, **Diese Dateien u. Verzeichnisse behalten, Einstellungen**, wählen die Datei oder den Ordner und klicken auf **Hinzufügen**.

KURZ-TIPPS



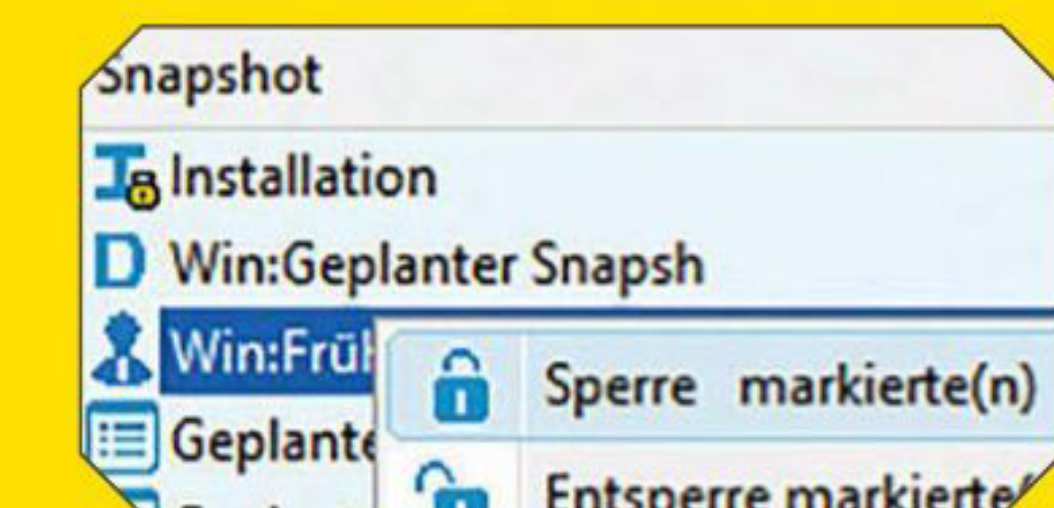
Programm schützen

Um den Zugriff auf den Windows-Retter zu schützen, klicken Sie auf das Zahnrad-Symbol, auf **Benutzerkonten** und **Aktiviere Zugriffskontrolle**, wählen ein Passwort ohne Sonderzeichen und Umlaute und klicken auf **OK**.



Sheriff ausblenden

Beim PC-Start erscheint ein riesiger Comic-Sheriff – er lässt sich ausblenden: Klicken Sie auf das Zahnrad, **Erscheinungsbild** und **Programm Logo beim Starten anzeigen**. Das Notfall-System starten Sie unverändert mit **Windows + R**.



Snapshot schützen

Möchten Sie einen Snapshot von der automatischen Löschung ausnehmen? Dann klicken Sie im Snapshot-Menü mit der rechten Maustaste auf den gewünschten Eintrag und auf **Sperre markierte(n) Snapshot(s)**.



Avast One Mobile

GRATIS

Auch für Smartphones ist ein Virenschutz unverzichtbar. Als Käufer dieses Sonderhefts bekommen Sie den **mobilen Virenschutz von Avast** gratis bis zum 21. April 2023!

Virenschutz wird immer wichtiger – auch auf dem Smartphone: Kriminelle entwickeln ständig neue Malware, die es ganz gezielt auf mobile Geräte abgesehen hat. Schließlich versprechen die auf Handys gespeicherten Passwörter sowie Daten von Kreditkarten und Online-Banking-Zugängen fette Beute. Mit SMS-Spam, Phishing-Mails und verseuchten Apps greifen die Hacker schon jetzt Millionen Geräte weltweit an. Wie Avast kürzlich herausfand, droht auf Handys zudem eine weitere Gefahr: Rund ein Drittel aller Deutschen hat auf das Handy der Partnerin oder des Part-

ners zugegriffen! In beiden Fällen hilft nur eines: eine zuverlässige Schutz-App, die unberechtigte Zugriffe blockiert und Schadsoftware entfernt. Avast One Mobile ist so eine App, und als Leser dieses COMPUTER BILD-Sonderhefts kriegen Sie die jetzt gratis!

Avast One Mobile gratis

Mit dem Code auf der Heft-DVD-Hülle können Sie Avast One Mobile bis zum 21. April 2023 kostenlos nutzen. Sie bekommen also fast ein Jahr kostenlosen Virenschutz für Ihr Smartphone – egal ob Android oder iOS. Die Lizenz gilt für ein Gerät. Wie Sie die App

installieren und freischalten, erklärt COMPUTER BILD im Kasten unten Schritt für Schritt.

Zuverlässiger Schutz

Das PC-Programm Avast One belegte im großen COMPUTER BILD-Sicherheitstest (siehe Seite 58) den dritten Platz und bewies einen guten Virenschutz mit erstklassigen Erkennungsraten. Die mobile Variante des Schutzprogramms profitiert von der gleichen Top-Schutzleistung. Das beweisen regelmäßige Tests und Auszeichnungen unabhängiger Testinstitute wie AV-Comparatives und AV-Test.

Mehr als nur Virenschutz

Avast One für Android und iOS bietet zusätzlich zum Virenschutz noch einige weitere Sicherheitsfunktionen. Welche das sind, unterscheidet sich je nach Betriebssystem in einigen Punkten. Hier die wichtigsten Extras:

■ **Web-Schutz:** Aktivieren Sie diesen Schutz, leitet die App sämtlichen Datenverkehr über ein sicheres VPN und verhindert, dass Sie auf gefährlichen oder gefälschten Internetseiten landen.

■ **Datenleck-Überwachung:** Lassen Sie Avast Ihre E-Mail-Konten überwachen. Taucht eines Ihrer Konten im Darknet auf, erhalten

AVAST ONE MOBILE: SO KOMMEN SIE RAN

COMPUTER BILD VORTEILCENTER

haben die aktuelle COMPUTER BILD, aber kein Laufwerk für die Heft-CD/DVD? Kein Problem: Hier gibt es den Inhalt des Datenträgers per Klick zum Download!

Um die Vollversionen der aktuellen Ausgabe von COMPUTER BILD herunterzuladen, benötigen Sie lediglich den Code von der Rückseite der Heft-CD/DVD-Hülle. Geben Sie diesen in das unten stehende Feld ein und Sie werden automatisch zu den Inhalten der aktuellen Ausgabe. Hinweis: Programme, die im Heft als DVD-ROM gekennzeichnet sind, stehen auch nur Lesern der DVD-Ausgabe zur Verfügung.

Bitte geben Sie Ihren Code ein

Heft-Code

Eingeben

1 Öffnen Sie die Seite **vorteilcenter.de**, und geben Sie dort den Code von der Hülle der Heft-DVD ein. Der Avast-One-Mobile-Code wird dann angezeigt.

Activate your subscription

Enter your activation code

Try looking for your code in the same place where you found the link to this screen.

Activation code

By clicking "Continue", you confirm that you've read and agree to our [Privacy Policy](#) and [End User License Agreement](#).

CONTINUE

2 Kopieren Sie den Code, und klicken Sie auf **Zur Aktionsseite**. Tragen Sie den Avast-Code ins dafür vorgesehene Feld ein und folgen den Anweisungen.



3 Scannen Sie den QR-Code oben, um die Avast-App für Ihr Smartphone herunterzuladen. Installieren und starten Sie die App.

VIREN-SCHUTZ fürs Smartphone

Sie eine Warnung und können das Passwort ändern.

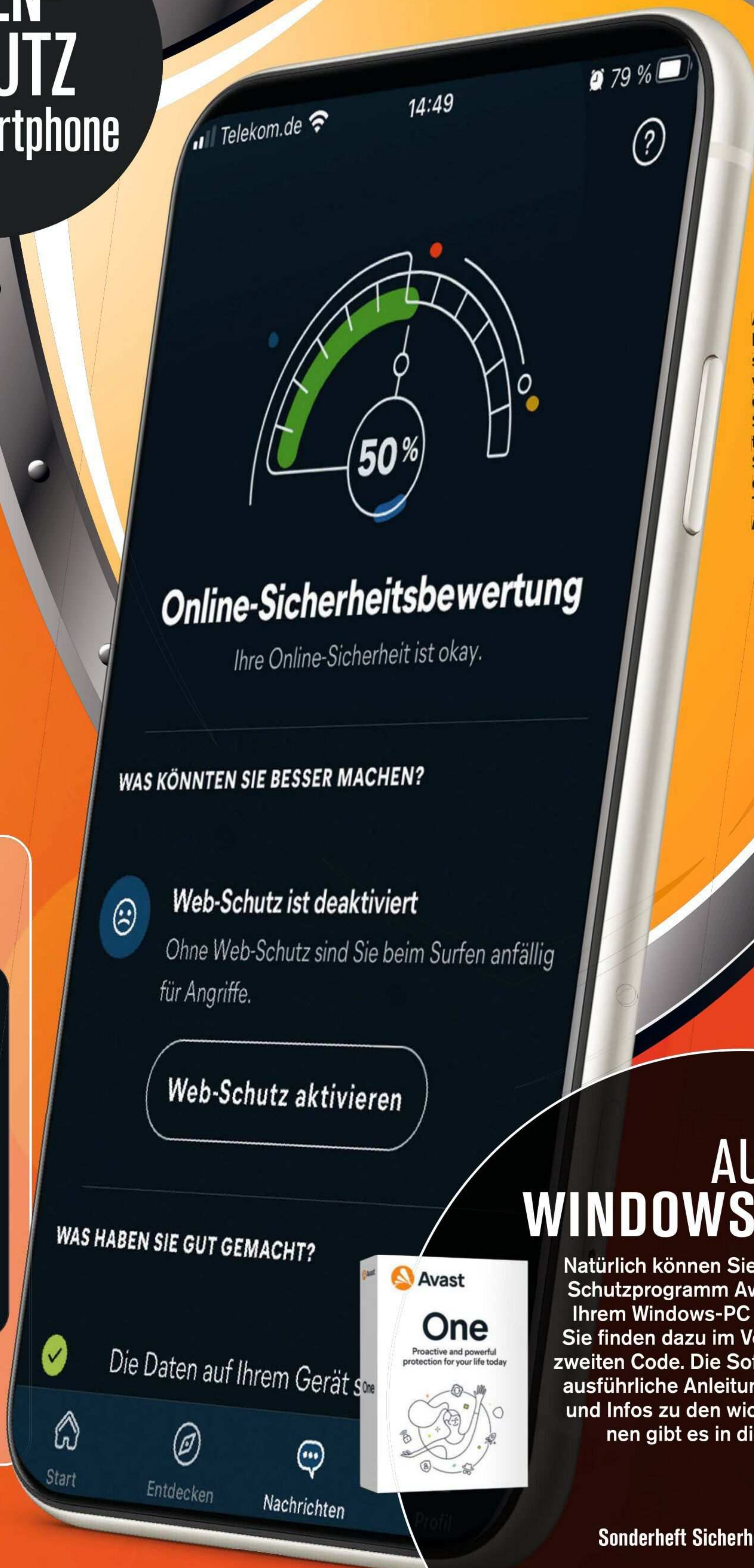
■ **VPN Sichere Verbindung:** Schalten Sie das VPN immer dann ein, wenn Sie zusätzlichen Schutz oder mehr Privatsphäre benötigen, etwa in öffentlichen WLANs.

■ **Leistungs-Scan (nur Android):** Finden und entfernen Sie Datenmüll von Ihrem Gerät.

Auch für PC und Mac

Leserinnen und Leser des COMPUTER BILD-Sonderhefts Sicherheit können das Schutzprogramm Avast One auch auf dem PC oder Mac kostenlos nutzen (siehe Artikel ab Seite 66). *[av]*

Avast One Mobile bietet neben Virenschutz noch viele weitere Funktionen, etwa eine Online-Sicherheitsbewertung für noch mehr Sicherheit. Sie finden sie nach einem Tipper auf **Nachrichten**.



← Anmelden bei Avast One

E-Mail-Adresse eingeben

Passwort eingeben

Anmelden

[Passwort vergessen?](#)

4 Folgen Sie den Anweisungen, um die Einrichtung abzuschließen. Melden Sie sich mit Ihrem Avast-Benutzerkonto an, um die Lizenz zu aktivieren.

AUCH FÜR WINDOWS & MAC

Natürlich können Sie das erstklassige Schutzprogramm Avast One auch auf Ihrem Windows-PC oder Mac nutzen. Sie finden dazu im Vorteilcenter einen zweiten Code. Die Software sowie eine ausführliche Anleitung zur Installation und Infos zu den wichtigsten Funktionen gibt es in diesem Sonderheft ab Seite 66.



INSTALLATION & REGISTRIERUNG

Vor der Installation holen Sie sich Ihren Freischaltcode. Tragen Sie auf der Seite **cobi.de/go/pwd22** Ihre Daten ein. Sie erhalten daraufhin den Freischaltcode, den Sie für die Installation bereithalten müssen. Starten Sie dann die Installation von der Heft-DVD, und folgen Sie den Anweisungen. Nach der Installation klicken Sie im Programm auf **Hilfe** und **Freischalten**. Fügen Sie den kopierten Code ein, und klicken Sie daraufhin auf OK.

INTERNET:
www.acebit.de

AUF HEFT-DVD
GRATIS
STATT
49,95 EURO*



* unverbindliche Preisempfehlung

ACEBIT PASSWORD DEPOT

PASSWÖRTER SICHERN

Gute Passwörter kann sich keiner merken. **Sichern Sie Kennwörter daher in Password Depot.** So müssen Sie nur noch eines im Kopf behalten.

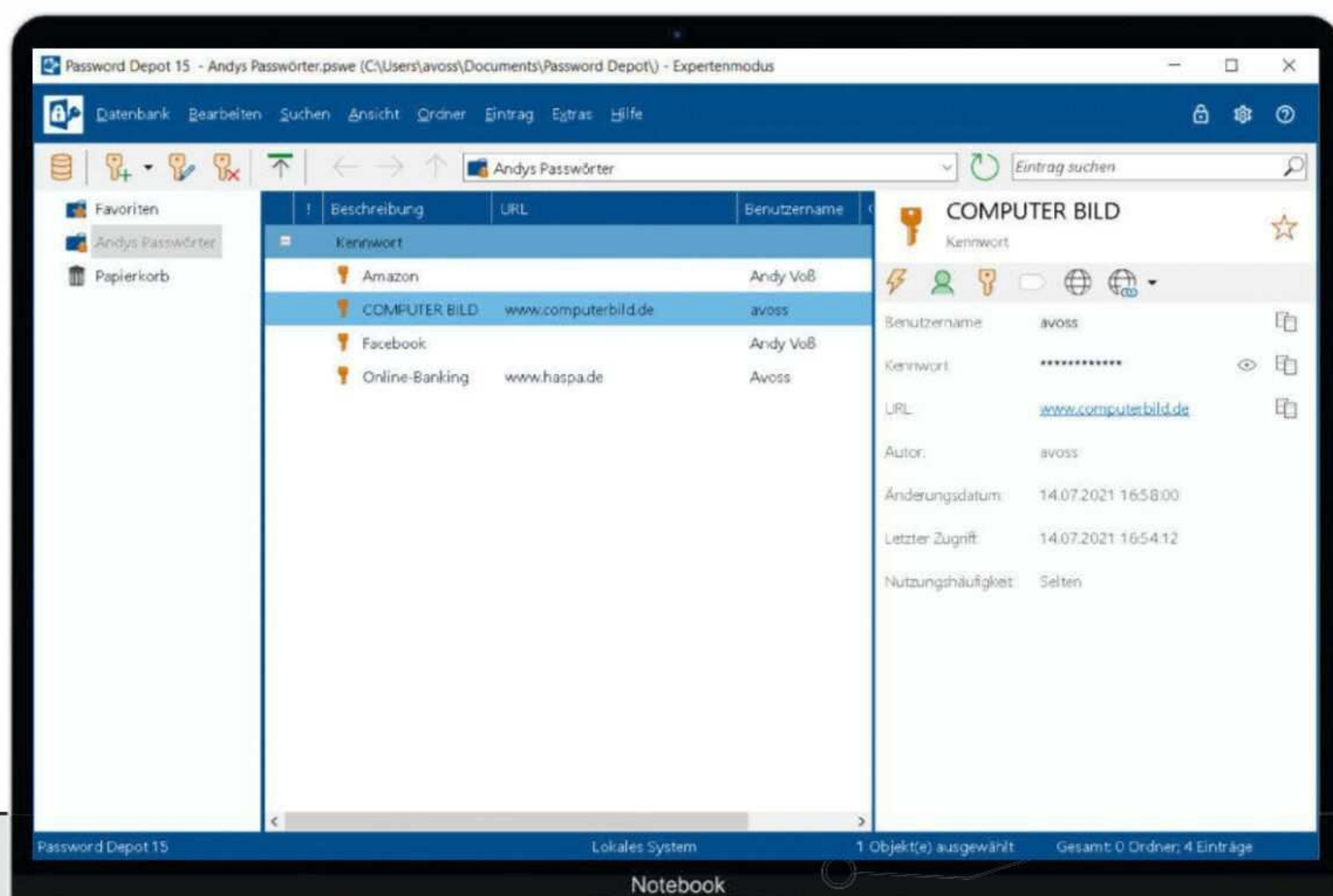
Auf Ihre Zugangsdaten haben es Internetkriminelle besonders abgesehen. Damit Gauner das richtige Passwort nicht einfach durch Wortlisten-Angriffe oder

schlichtes Ausprobieren erraten, brauchen Sie sichere Kennwörter mit Zahlen, Großbuchstaben und Sonderzeichen. Und zwar für jede Internetseite ein eigenes. Da die

keiner alle im Kopf behalten kann, speichern Sie Ihre Zugangsdaten einfach in Password Depot und merken sich künftig nur noch ein einziges Kennwort. [av]

PASSWORT-SAFE ERSTELLEN:

- 1 Nach dem ersten Programmstart klicken Sie auf Datenbank-Manager und im neuen Fenster oben rechts auf das Symbol mit dem grünen Pluszeichen.
- 2 Füllen Sie im nächsten Fenster die Angaben zu Ihrer Passwort-Datenbank aus, und legen Sie ein Master-Kennwort fest. Achtung: Dieses Kennwort müssen Sie sich unbedingt merken, denn es ist künftig der Schlüssel zu all Ihren Passwörtern. Notieren Sie es sicherheitshalber, und bewahren Sie es zu Hause auf.
- 3 Danach folgen zwei Klicks auf **OK**. Geben Sie dann das gerade festgelegte Master-Kennwort ein, und klicken Sie erneut auf **OK**. Der Passwort-Tresor ist damit erstellt.
- 4 Um den Tresor zu befüllen, klicken Sie oben links auf den Schlüssel mit dem Pluszeichen. Im neuen Fenster geben Sie die Infos für Ihr erstes Passwort ein und klicken auf **OK**. Falls das Kennwort zu unsicher ist, erscheint eine Warnung. Sie sollten es dann auf der entsprechenden Seite ändern.
- 5 Wiederholen Sie Schritt 4, um all Ihre Passwörter einzutragen. Sie können nach Klicks auf die verschiedenen Reiter eine Internet-Adresse, Anmerkungen, Zugangsnummern und Anhänge hinzufügen.
- 6 Um sich später mit den gespeicherten Daten anzumelden, öffnen Sie Ihren Passwort-Safe und klicken auf den entsprechenden Eintrag. Mit den Symbolen auf der rechten Seite können Sie dann die zugehörige Internetseite öffnen, Benutzername oder Passwort kopieren oder die Anmeldedaten automatisch ausfüllen lassen.





■ ABELSSOFT EASY BACKUP

WINDOWS-DATENSICHERUNG OHNE GROSSES GEKCLICKE

EasyBackup sichert im Hintergrund Ihre persönlichen Dateien. Vorkenntnisse oder viele Einstellungen sind dafür nicht erforderlich.



Das kann ganz schnell gehen: Ein unüberlegter Klick am PC, schon sind persönliche Dateien verloren. Mit einer Datensicherung (Backup) sind Sie auf der sicheren Seite – doch viele Backup-Programme richten sich eher an Profis. Mit EasyBackup von der norddeutschen Software-Schmiede Abelssoft müssen Sie sich keinen Kopf machen. Das Programm sichert Ihre Daten nach Einrichtung automatisch im Hintergrund und stellt sie bei Bedarf wieder her. Wie's geht, lesen Sie hier.

Installieren und freischalten

1 Vorteilcenter laden: Legen Sie die Heft-DVD ein, und klicken Sie bei „Easy Backup“ auf **Vorteilcenter**. Falls Sie kein DVD-Laufwerk haben, laden Sie die Webseite www.vorteilcenter.de.

2 Programm herunterladen: Geben Sie auf der erscheinenden Seite Ihren Vorteilcenter-Code von der Rückseite der Heft-DVD Hülle ein, klicken Sie auf **Freischalten**, und laden Sie Easy Backup.

3 Programm installieren: Starten Sie die heruntergeladene Datei **EasyBackup_setup** per Doppelklick. Nach Klicks auf **Ja**, dreimal **Weiter**, **Installieren** und **Fertigstellen** startet die Software.

4 Programm freischalten: Ist schon ein Programm des Herstellers installiert, startet EasyBackup sofort. Andernfalls tippen Sie im Fenster „Kostenlose Freischaltung“ die gewünschten Daten ein und klicken auf **Kostenlose Freischaltung per E-Mail anfordern**, dann im Fenster „Fertig“ auf **Fertig**. Erscheint es nicht gleich, klicken Sie zuvor auf den Bestätigungslink in der E-Mail von Abelssoft.

Sicherung einrichten

Das Programm ist denkbar simpel und hat nur zwei Funktionen, siehe Bild rechts. So richten sie eine Datensicherung ein:

1 Daten auswählen: Klicken Sie auf **Backup erstellen**. Um alle Dokumente, Bilder, Musik und Videos der Windows-Standardordner zu sichern, lassen Sie die Voreinstellung unverändert. Andernfalls entfernen Sie per Klick die Häkchen.

2 Ordner hinzufügen: Möchten Sie eine eigene Quelle hinzuzufügen, klicken Sie auf **Ordner hinzufügen**, das gewünschte Verzeichnis und **OK**. Wiederholen Sie das bei Bedarf mit weiteren Ordnern.

3 Laufwerk anschließen: Nach einem Klick auf **Backup starten** fordert EasyBackup zum Anschließen eines Datenträgers auf. Schließen Sie am besten ein großes USB-Laufwerk an.

4 Daten sichern: Die Sicherung startet automatisch. Lassen Sie Windows laufen, bis der Hinweis „Der Backup-Vor-

gang ist abgeschlossen“ erscheint. Nun können Sie das Fenster schließen und das Laufwerk entfernen. EasyBackup arbeitet im Hintergrund weiter. Sie müssen nur gelegentlich das Backup-Laufwerk anschließen, damit neue und geänderte Dateien gesichert werden. Gegebenenfalls erinnert das Programm Sie daran.

Daten wiederherstellen

Wurde etwas gelöscht, klicken Sie im Infobereich der Taskleiste auf das Symbol mit dem Rettungsring und im Statusfenster auf **Im Hauptfenster öffnen**. Nach einem Klick auf **Wiederherstellung starten** stöpseln Sie gegebenenfalls das Laufwerk ein, wählen das Sicherungsdatum im Kalender und klicken auf **Backup im Explorer öffnen**. Im erscheinenden Ordner finden Sie alle gesicherten Dateien, fertig! [hes]

INTERNET: www.abelssoft.de



EasyBackup gehört zu den einfachsten Datensicherungs-Programmen und hat nur zwei Funktionen – perfekt für Einsteiger und Nutzer, die es gern bequem haben.

SALFELD KINDERSICHERUNG

SICHER IM NETZ

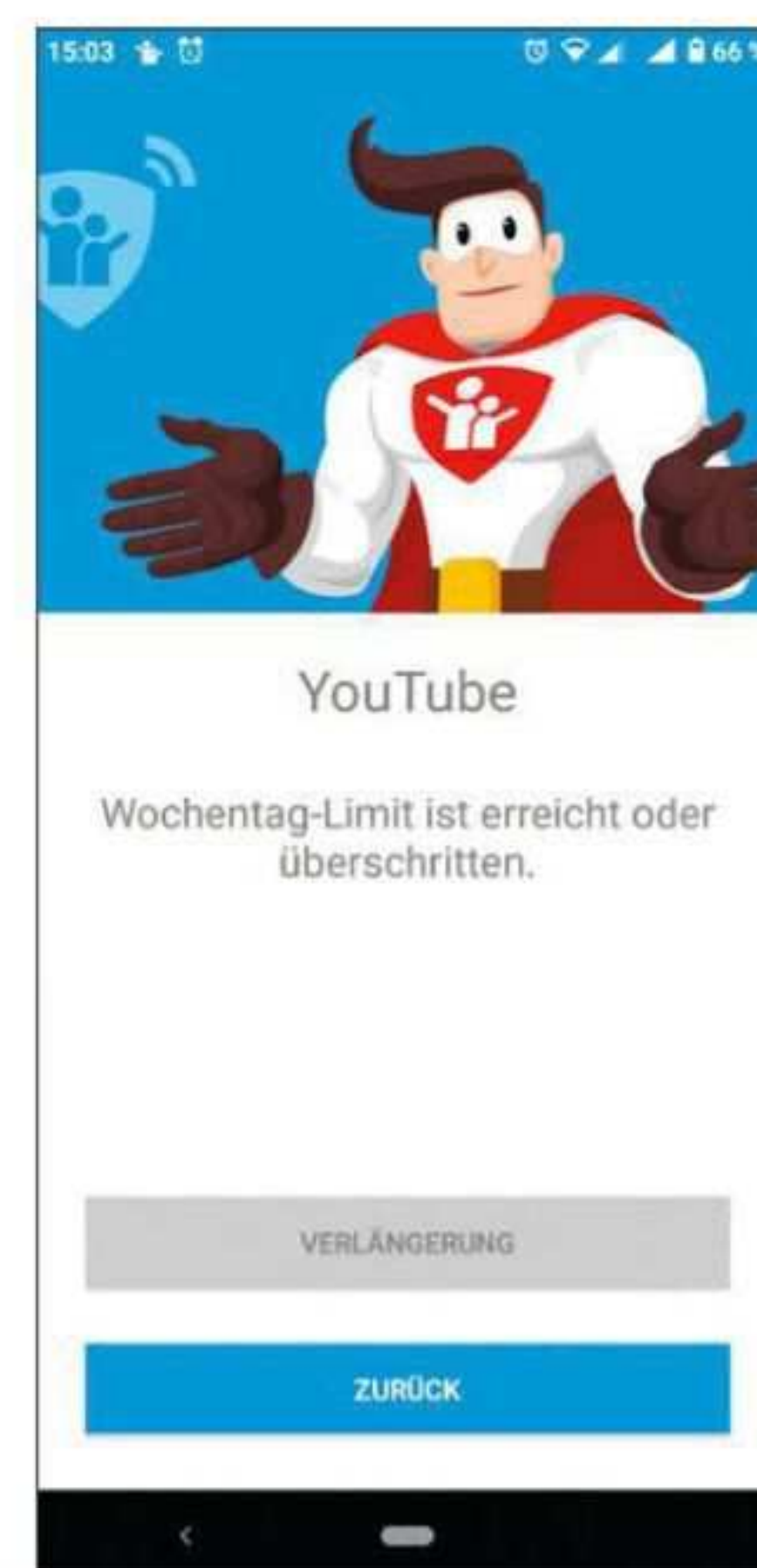
Beugen Sie Cybermobbing und Gewalt vor: Mit dieser Software machen Sie **Smartphone oder PC fit für Ihre Kinder**.

Seit Corona hat sich der Medienkonsum von Kindern stark erhöht. Da ist es wichtiger denn je, den Nachwuchs vor den Schattenseiten der digitalen Welt zu schützen. Zudem sind soziale Netzwerke auf PC und Handy oft die Quelle übler Cybermobbing-Attacken von denen Eltern oft erst etwas mitbekommen, wenn es zu spät ist. Generelle Verbote helfen hier wenig, eine gute Alternative für Eltern kann die Salfeld Kindersicherung sein. Als Leser dieses Sonderhefts erhalten Sie die Software ein Jahr zum Null-

tarif! Sie können damit sowohl einen PC als auch ein Android-Smartphone kindersicher machen. Im Salfeld-Portal haben Sie das Nutzungsverhalten des Nachwuchses nach der Einrichtung stets im Blick.

Software freischalten

Auf der Webseite **www.cobi.de/42156** lesen Sie, wie Sie Ihre Lizenz bis zum 15. Oktober 2022 freischalten und ein Android-Gerät schützen. Wie es bei einem PC funktioniert, steht in der Randspalte links. [asa/hp]



App-Filter: Mit dieser Funktion setzen Sie ganz leicht ein Zeitlimit, um etwa den Internet-Konsum Ihrer Kinder zu reglementieren.



GRATIS
AUF HEFT-DVD
STATT
29,95 EURO*

KINDER-SICHERUNG FÜR DEN PC

1. Kinder-PC vorbereiten

Falls nicht schon vorhanden, erstellen Sie ein separates Windows-Benutzerkonto fürs Kind, wie auf der Seite **cobi.de/go/kk** erklärt. Melden Sie sich am Konto an und wieder ab. Dann wechseln Sie wieder zu Ihrem eigenen Konto.

2. Programm installieren

Laden Sie die Webseite **salfeld.de/computerbild** bis zum 15. Oktober 2022. Dort geben Sie Ihre E-Mail-Adresse und den Vorteilcenter-Code von der Heft-DVD-Hülle ein und folgen den Anweisungen zum Erhalt einer Seriennummer. Installieren Sie Salfeld von der Heft-DVD auf dem Kinder-PC. Geben Sie dabei Ihre E-Mail-Adresse und ein beliebiges Kennwort ein.

3. Benutzerkonto wählen

Wählen Sie mit Klicks ein Symbol und das Windows-Konto Ihres Kindes. Klicken Sie auf **Weiter**.

4. Programm aktivieren

Klicken Sie gegebenenfalls auf **Login Portal**. Dann schalten Sie das Programm durch Eingabe der Seriennummer frei, die Sie per E-Mail vom Hersteller erhalten haben.

5. Filter einstellen

Über das Portal richten Sie die Kindersicherung ein. Das funktioniert genauso wie bei Android, siehe Anleitung rechts.

ZEITLIMIT EINRICHTEN

Wie viel Zeit Ihr Kind mit dem Handy verbringen darf, legen Sie im Salfeld-Portal fest. Dazu öffnen Sie die Seite **portal.salfeld.net** oder die Android-App „Salfeld Portal“ und loggen sich ein.

1 Klicken Sie danach auf **Zeitlimits** oder **Gesamt Limit**. Um die Nutzungszeit etwa auf 2,5 Stunden pro Tag zu begrenzen, aktivieren Sie den Schalter bei „Limit“ und stellen bei „Tag“ „02:30“ ein. Die Änderung synchronisiert Salfeld direkt mit dem Kinder-Smartphone.

2 Sollen die Kleinen am Wochenende mehr Geräte-Zeit haben, aktivieren Sie den Schalter „Wochentags-Limit“ und nehmen die Feinjustierung wie rechts vor. Unter „Gesamt-Sperrzeiten“ regeln Sie, wann das Gerät nicht benutzt werden kann. Soll das etwa zwischen 21 und 6 Uhr gelten, färben Sie die entsprechenden Kästchen mit Mausklicks rot.

Donnerstag	-	02:00	+
Freitag	-	02:00	+
Samstag	-	03:00	+
Sonntag	-	03:00	+

INHALTE KONTROLLIEREN

Vertrauen ist gut, Kontrolle manchmal besser. Mit der Salfeld Kindersicherung haben Sie im Blick, wo Ihre Kinder surfen, und sperren den Zugang zu Gewalt- oder Pornoseiten.

1 Um den Zugang zu Internetseiten zu regulieren, wählen Sie im Webportal den Eintrag **Web Filter** und aktivieren den Schalter „Web Filter“ (siehe unten). Für die ganz Kleinen wählen Sie **Unbekannte Webseiten blockiert**, dann **Hinzufügen** und tragen erlaubte Seiten (Whitelist) ein, einige geeignete Seiten sind schon voreingestellt. Alle anderen Seiten werden blockiert. Mit der Option **Unbekannte Webseiten erlaubt** ist (fast) alles erlaubt, was Sie nicht explizit verbieten (Blacklist). Zusätzlich sperrt die Software themenbezogen Unpassendes wie Pornoseiten.

2 Im Menüpunkt **Protokolle** dokumentiert die Software, was Ihr Nachwuchs so macht. Schauen Sie hier täglich nach, ob Ihre Einstellungen noch passen, und justieren Sie sie bei Bedarf nach.

ON	WEB FILTER
<input checked="" type="radio"/>	Unbekannte Webseiten erlaubt (Blacklist Modus)
<input type="radio"/>	Unbekannte Webseiten blockiert (Whitelist Modus)



■ ALL-IN-ONE KEY FINDER PRO PERSONAL EDITION

DER SCHLÜSSELDIENST FÜR IHREN COMPUTER

*Kaufbeleg verloren? Das rund 20 Euro teure Hacker-Tool **findet Lizenzschlüssel für Tausende Programme** auf der Festplatte.*

Wer Windows schon einmal neu aufsetzen musste, kennt das Schlamassel: Ohne sorgsam verwahrte Lizenzschlüssel lassen sich das Betriebssystem und die gekauften Programme nicht neu installieren. Der All-In-One Key Finder liest die nötigen „Keys“ aus der Windows-Registrierungsdatenbank aus und listet sie übersichtlich auf. Das klappt mit Windows und Office, aber auch mit Adobe-Produkten und Tausenden weiteren Kaufprogrammen.

Jahres-Version gratis

Auf der Heft-DVD finden Sie die aktuelle Personal Edition als 1-Jahres-Version.

Die kennt mehr als 2000 Programme und durchsucht den lokalen PC nach passenden Schlüsseln. Das Programm unterstützt Windows XP bis 10, läuft aber auch unter Windows 11.

So funktioniert's

Um die Software zu installieren, öffnen Sie www.vorteilcenter.de, geben den Code von der Heft-DVD-Hülle ein und folgen den Anweisungen unter dem Eintrag für das Programm. Nach dem Start des Programms klicken Sie auf **Recover Keys** und **Nein**, fertig! [hes]

INTERNET: www.xenarmor.com



GRATIS
AUF HEFT-DVD



Nach nur einem Klick listet das Programm alle auf der Festplatte gefundenen Lizenzschlüssel auf.

■ SECUPERTS ANTI-SPY CBE (1-JAHRES-VERSION)

DER SPIONAGE-STOPPER FÜR IHR WINDOWS

*So einfach bringen Sie Ihrem Windows mehr Privatsphäre bei: Mit Anti-Spy CBE können Sie 80 **Schnüffelfunktionen ganz einfach abschalten**.*

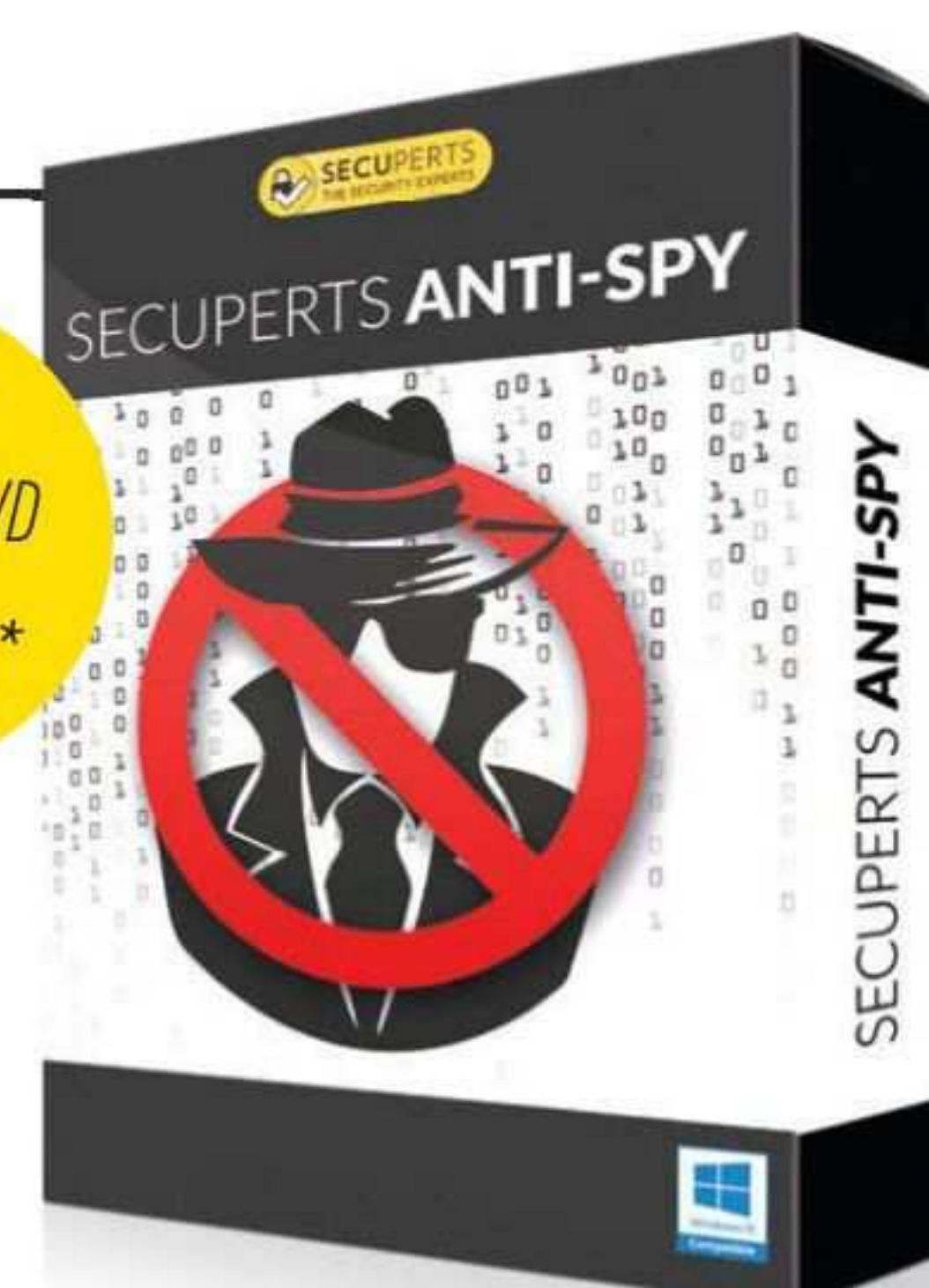
Wer ein neues Windows einfach mit den von Microsoft empfohlenen Voreinstellungen installiert, erlaubt dem Hersteller damit das uneingeschränkte Sammeln und Auswerten vieler persönlicher Daten. Mit Anti-Spy CBE unterbinden Sie das und gewöhnen Ihrem Windows an über 80 Stellen in Menüs und Untermenüs die Schnüffelei ab – einfach per Klick.

Schnüffelstopp per Klick

Fordern Sie vor der Installation Ihren Freischaltsschlüssel an. Gehen Sie dazu auf die Seite cobi.de/go/antispy, geben Sie dort Ihre E-Mail-Adresse an, aktivie-

ren Sie die beiden Häkchen, und bestätigen Sie die Eingabe. In der folgenden Mail klicken Sie auf **OK**. Sie bekommen den Schlüssel angezeigt und nochmals zugesandt. Installieren Sie Anti-Spy, und geben Sie den Schlüssel nach dem Start in das Eingabefenster ein – fertig. Sie sehen nun das Programmfenster von Anti-Spy. Die Bedienung ist selbsterklärend: Klicken Sie einfach auf einen der Einträge, um die betreffende Spionagefunktion an- oder abzuschalten. Sind Sie mit Ihrer Auswahl fertig, klicken Sie zur Bestätigung auf **Übernehmen**.

INTERNET: anti-spy.net/



GRATIS
AUF HEFT-DVD
STATT
19,99 EURO*



Spionagestopp: Per Klick schalten Sie über 80 Spionagefunktionen in Windows einfach ab!

SMARTE WACH



Überraschung:
Ein Außenseiter
baut die **beste**
Überwachungs-
kamera.

Die Ferienzeit beginnt, viele Häuser sind wochenlang verlassen. Hochsaison auch für Langfinger, die sich schon darauf freuen, die verwaisten Wohnungen auszuräumen. Gegenmaßnahme: WLAN-Überwachungskameras, die Nutzer übers Smartphone warnen und direkt zeigen, was gerade vor der Linse passiert. Streift Nachbars Waldi gerade durch den Garten, oder hebelt ein Einbrecher bereits die Terrassentür auf? Smarte Wächter haben alles im Blick und können je nach Modell auch Laute von sich geben. Damit vertreiben sie Täter und alarmieren die Nachbarn gleich mit. COMPUTER BILD hat vier Überwachungskameras von 70 bis 240 Euro genau unter die Lupe genommen. Überraschung: Ein 70-Euro-Modell machte im Test den Wächter-Job am besten!

Was will ich überwachen?

Die Überwachungskamera muss ein Gehäuse und eine Ausstattung mitbringen, die zu ihrem Einsatzort passen. Nicht jeder smarte Wächter eignet sich für alle Bereiche eines Grundstücks. Möchte der Besitzer etwa seinen Garten im Blick haben, muss die Kamera Wind und Wetter trotzen. Zu den Outdoor-Modellen, die das können, zählt etwa die Arlo Pro 4 – ihr wetterfestes Gehäuse soll laut Hersteller Regen und Temperaturen bis -20 Grad überstehen.

Ebenfalls mit einem wetterfesten Gehäuse wirbt Logitech bei der Circle View, allerdings ist nur die Kamera gegen Regen und Staub geschützt (Schutzstufe IP64). Das fest verbaute Kabel

muss hingegen zu einer wetterfesten Steckdose führen. Denn einen Akku wie die Konkurrenz hat die Circle View nicht.

Schade: Die getesteten wetterfesten Kameras kosten allesamt mehr als 100 Euro, die günstigeren Modelle sind also nicht für den Außeneinsatz geeignet.

In Position bringen

Der kleine Wächter sollte so positioniert sein, dass er die Umgebung optimal einfängt – etwa die Eingangstür oder bestimmte Bereiche auf dem Grundstück. Tipps dazu, wie Sie Ihre Überwachungskamera positionieren, erhalten Sie auf Seite 107.

Mit nur wenigen Handgriffen schrauben Nutzer die Überwachungskamera an die (Haus-) Wand oder stellen sie auf. Alle Kameras ließen sich im Test optimal positionieren, sodass die Linse den gewünschten Bereich korrekt erfasste. Bei einigen Modellen war es aber nötig, ein Strom-



* Daten aus der Polizeilichen Kriminalstatistik (PKS 2021), Grundtabelle V1.0

TER FÜR ALLE

ALLES IM BLICK!

1 HAUSTÜR

Hier lassen sich Einbrecher als Erstes erspähen und mit der richtigen Kamera abwimmeln.

3 TERRASSENTÜR

Terrassentüren sind meist weniger gut gesichert als Haustüren. Hier lohnt sich eine Kamera.

2 ERSTER STOCK

Ein großer Vorgarten lässt sich aus einer erhöhten Position am besten beobachten.

4 GARTEN

Was für den Vorgarten gilt, ist auch für das übrige Grundstück gültig: Höhe bringt Weitblick.

CANARY
VIEW
99 EURO

YALE
SV-DPFX-B
70 EURO

ARLO
PRO 4
210 EURO

kabel zu verlegen. Die Nest Cam und die Arlo Pro 4 laufen per Akku; der muss in regelmäßigen Abständen ans Netz. Die Amazon-Tochter Blink verfolgt einen hybriden Ansatz: Zwar läuft die Kamera selbst über zwei AA-Batterien, der kabellos gekoppelte Hub

benötigt jedoch Strom aus der Steckdose.

Handliches Sicherheitszentrum

Für die Einrichtung setzen alle Kameras ein Smartphone voraus. Ebenfalls Pflicht ist ein kostenloser Account beim jeweiligen Hersteller. Bedenklich: Die Online-Dienste verlangen viele Daten, zum Beispiel die Adresse oder auch die Telefonnummer.

Die Einrichtungen führen mit leicht verständlichen Hinweisbildern durch die Installation. Kein Hersteller leistet sich in diesem Punkt grobe Schnitzer oder führt den Nutzer in die Irre. Mit wenigen Wischern lässt sich etwa der Überwachungszeitraum bestimmen oder die Empfindlichkeit einstellen.

Das klappte im Test am einfachsten mit der Logitech-App, die bei der Circle View zum Einsatz kommt. Die Menüs sind schön aufgeräumt und alle wichtigen Optionen lassen sich schnell finden. Auch per Sprache lässt sich die Circle View bedienen, aller-

dings versteht sie sich nur mit Apples Siri und einem verbundenen HomeKit-System.

Mit dem Großteil der anderen Überwachungskameras kommunizieren Nutzer per Alexa von Amazon oder Google Assistant. Auf Zuruf lässt sich der Wächter beispielsweise scharf schalten. Das ist wirklich smart. Besitzer eines smarten Displays wie eines Amazon Echo Show 5 (ab 90 Euro) können sich das Livebild anzeigen lassen. Das klappte im Test unter anderem mit den Geräten von Arlo sowie der Google Nest.

Wolkige Aussichten

Klasse: Die kleinen Wächter nehmen Bewegungen wahr, filmen das Geschehen und schicken auf Wunsch auch eine Nachricht an das Smartphone des Nutzers.

Diese essenzielle Funktion stellt Gigaset leider teilweise hinter eine Bezahlschranke. Ohne Abo entdeckt die kompakte Überwachungskamera zwar Bewegungen und schickt eine Nachricht ans Smartphone des Hausherrn;



Die Nachtaufnahmen der Arlo Pro 4 können sich sehen lassen. Im Infrarotmodus (links) wie auch mit zugeschaltetem Flutlicht (rechts) sind viele Details erkennbar.

soll jedoch im entscheidenden Augenblick eine Aufnahme erfolgen, müssen Nutzer extra zahlen. Mindestens 99 Cent monatlich sind für diese grundlegende Funktion fällig. Die gibt es im Paket mit weiteren Funktionen wie dem Festlegen von Zonen für die Bewegungsüberwachung und einem einwöchigen Speicher in der Cloud.

Da schnürt Arlo für monatlich rund 3 Euro ein teureres, aber dafür umfangreicheres Paket und

macht seine Überwachungskameras sogar smarter. So unterscheidet die Überwachungskamera zwischen Tieren, Menschen und Fahrzeugen. Ein 30-tägiger Cloud-Speicher ist im Paket ebenfalls enthalten.

Ganz ohne Abo geht es aber auch – Yale liefert zum Beispiel alle Funktionen ohne Zusatzkosten. Zudem speichert die Kamera Aufnahmen auf einer microSD-Karte. Damit landen die Videos allerdings auch nicht mehr in der

MEHR SMARTE HELFER

HAUSTÜR

Für die Haustür bieten Arlo, Yale, Blink und Google smarte Türklingeln und Türspione an. Damit lässt sich sehen, wer um Einlass bittet – und mit dem Besucher sprechen, ohne dass er das Zuhause betritt. Preis: ab 90 Euro.

FENSTER

Für mehr Sicherheit haben Gigaset und Yale smarte Fensterkontakte im Sortiment. Löst einer der Sensoren aus, starten Kameras beispielsweise die Aufnahme und alarmieren gleichzeitig die Hausbewohner. Preis: ab 35 Euro.

ALARM

Wer sich komplett sicher fühlen will, greift zu einem Alarmsystem, das verschiedene Sensoren und Kameras verbindet. Gigaset und Yale bieten diese Rundumschutz-Pakete an. Preis: ab 200 Euro.





Klasse: Dank ihres magnetischen Kugelgelenks lässt sich die Gigaset Camera 2.0 optimal ausrichten.

Cloud – wenn ein Dieb auch die Kamera mitgehen ließe, so wären auch die Videos weg.

Hingeschaut und hingehört

Alle Kameras filmen mindestens in Full HD (1920 x 1080 Pixel). Sie filmten im Test sowohl am Tag als auch nachts ohne Probleme. Der Nutzer kann sich die Videos nach ihrer Aufnahme anschauen, oder er schaltet per Smartphone-App live ins Wohnzimmer.

Die mit Abstand beste Bildqualität bot im Test der Zweitplatzierte: Die Arlo Pro 4 lieferte flüssige Videos mit einer maximalen Auflösung von 2560 x 1440 Pixeln. Die Clips sind scharf und reich an Details. Einziges Manko: Im Bild stören kleine Klötzchen (Artefakte). Gut hingegen: Auch bei wenig Licht gelingen der Pro 4 ordentliche Aufnahmen. In solchen Situationen aktiviert sie ihre Infrarotlinsen und erfasst das Geschehen in Schwarz-Weiß. Oder sie schaltet das eingebaute Flutlicht ein und nimmt in Farbe auf.

Die schlechtesten Videos lieferte die Blink. Dass gerade ein Einbrecher im Wohnzimmer steht, ist noch erkennbar. Insgesamt wir-



Über das Sync-Modul (rechts) speichert die Blink ihre Aufnahmen auch lokal – und nicht nur in der Cloud.

ken die Aufnahmen aber verwaschen, in der Nacht entstandene Videos sind zudem zu dunkel.

Außer mit einer Linse sind die kleinen Wächter zur Beweissicherung auch mit Mikrofonen ausgestattet. Den besten Ton gibt's mit der Logitech. Sie fing im Test Umgebungsgeräusche recht klar und laut ein. Am schlechtesten klangen die Clips der Gigaset Camera 2.0 – hier war die Tonwiedergabe blechern und rauschend.

Die eingebauten Mikros haben noch einen weiteren Zweck: Sie ermöglichen zusammen mit den integrierten Lautsprechern eine Zwei-Wege-Kommunikation. Wollen Nutzer während ihrer Abwesenheit das Haustier vom Sofa scheuchen, klappt das mit allen Testkandidaten so ganz einfach. Canary bietet diese Funktion bei der View allerdings nicht kostenlos, sondern nur bei Abschluss eines Abos (rund 10 Euro je Monat).

Wer sich gern die Clips im Großformat anschauen will, lädt sie entweder herunter oder öffnet sie direkt im Internet-Browser. Die Testkandidaten von Gigaset und Arlo bieten entsprechende Oberflächen, die denen der jeweiligen Apps ähneln und auch Einstellungen erlauben.

Klasse: Mithilfe von Alarmierungskontakten weiß nicht nur der Nutzer im Ernstfall Bescheid, die Kameras senden etwa Meldungen auch an Familienmitglieder. Die Yale SV-DPFX-B ist besonders mitteilungsfreudig: Bis zu sechs Personen lassen sich mit dieser Kamera verknüpfen.

Einbrecherschreck inklusive

Als Warnung und für die Beweissicherung lassen sich alle Testkan-



Die Logitech versteht sich mit Apples Smarthome-System HomeKit. Aus diesem Grund ist die Kamera per Sprachassistentin Siri steuerbar.

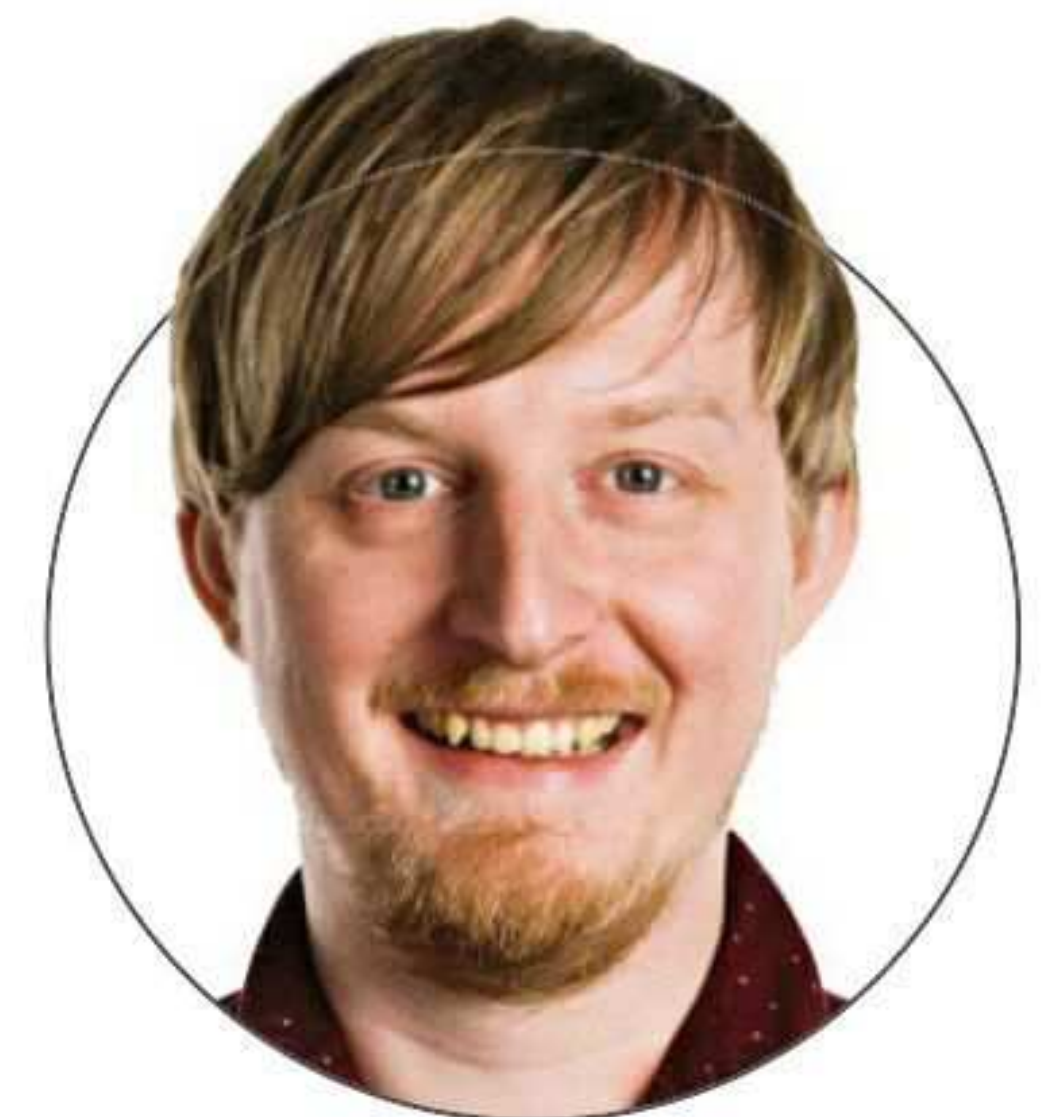
didaten ohne Schwierigkeiten nutzen. Arlo setzt aber noch eins drauf: Der Hersteller stattet die Pro 4 mit einem Flutlicht sowie einer Sirene aus. Das grelle Licht dient nicht nur für 1-a-Nachtaufnahmen, sondern soll auch unbetenen Besuch – im besten Fall – vertreiben. Die Sirene tut ihr Übriges und alarmiert, wenn's gut läuft, auch die Nachbarn.

Die Yale bietet ebenfalls eine Sirene, die ist jedoch alles andere als laut – die schreckt den Langfinger nicht ab, sondern macht ihn auf sich aufmerksam. [r/]

FAZIT

Ein smarter Wächter muss nicht teuer sein. Das beweist die Yale mit einem Preis von 70 Euro, die knapp vor der mit 210 Euro dreimal so teuren Arlo Pro 4 den Testsieg holt! Die Yale macht bei Tag und Nacht solide Aufnahmen von Langfingern. Außerdem verfolgt sie den Dieb mit der automatisch schwenkbaren Linse auf Schritt und Tritt (siehe Infos unten). Wer allerdings richtig gute Auf-

nahmen will, greift besser zur Arlo Pro 4. Deren Videos sind knackscharf und flüssig, wenn auch nicht frei von kleinen Fehlern. Schade: Zum hohen Anschaffungspreis kommen noch weitere Kosten. Den vollen Funktionsumfang samt Cloud-Speicher gibt es nur mit Abo.



„Die günstige Yale überraschte mit vielen Funktionen und ordentlichen Videos.“

Robert Ladenthin
Redakteur



AUF SCHRITT UND TRITT

Der Testsieger von Yale ist der einzige Testkandidat mit kleinem Motor. Der kann die Kameralinse in fast jede Richtung bewegen. Per Smartphone lässt sich die Cam ausrichten und ein Verfolger-Modus aktivieren, etwa um der Bewegung des Einbrechers zu folgen. ➤



1 YALE SV-DPFX-B
Preis: 70 Euro
Abo: nicht vorhanden



2 ARLO PRO 4
Preis: 210 Euro
Abo: ab 2,99 Euro pro Monat



3 ARLO ESSENTIAL INDOOR
Preis: 99 Euro
Abo: ab 2,99 Euro pro Monat

ÜBERWACHUNGSKAMERAS IM VERGLEICH

An die Spitze der WLAN-Wächter setzt sich die recht unbekannte Yale. Die günstige Kamera überrascht mit einer ordentlichen Aufnahmequalität sowie einer guten Bedienung. Dank ihres Motors folgt sie Dieben automatisch. Alternativ legt der Nutzer selbst Hand an und richtet die Linse per App aus. Ihre Aufnahmen sichert die Yale lokal auf einer microSD-Karte.

+ Schwenkbar, sichert auf SD-Karte, einfache Bedienung.

- Etwas dunkel, wenige Aufzeichnungsmodi, Klang mäßig.

Die Pro 4 vereint Alarmanlage und Überwachungskamera. Zudem bietet sie die beste Videoqualität im Test. Sie liefert Aufnahmen am Tag sowie in der Nacht in guter Qualität mit nur kleinen Schwächen. Per Sirene und Flutlicht schreckt die Arlo Diebe ab. Wer den vollen Funktionsumfang und Zugriff auf gespeicherte Videos will, muss allerdings für das Abo extra bezahlen.

+ Gute Aufnahmen, smarte Zusatzfunktionen, Akkubetrieb.

- Hoher Zeitversatz zum Livebild, viele Funktionen im Abo.

Die Essential Indoor gefällt mit guten Aufnahmen am Tag. Nachts zeigt sie Bewegungen etwas stockend. Sie lässt sich einfach bedienen, speichert ihre Videos aber nur in der Cloud. Die gibt's wiederum nur bei Abschluss eines Abos. Wer etwas mehr zahlt, bekommt jedoch auch viele Zusatzfunktionen wie eine Paketerkennung. In der Grundausstattung leistet sie auch gute Arbeit.

+ Gute Tagaufnahmen, Bedienung per Browser und App.

- Viele Funktionen nur mit Abo, ruckelt bei wenig Licht.

TESTERGEBNISSE

		Einsatzgebiet: innen Sprachassistenten: Amazon Alexa, Google Assistant	Einsatzgebiet: innen und außen Sprachassistenten: Amazon Alexa, Google Assistant, Apple Siri (nur mit Basisstation)	Einsatzgebiet: innen Sprachassistenten: Amazon Alexa, Google Assistant, Apple Siri (nur mit Basisstation)
Wie gut ist die Videoqualität?	55 %	Gut, nur leichte Schwächen	Beste Videoqualität im Test	Teilweise sehr helles Bild
Sichttest: bei Tageslicht / Sichttest: bei Dunkelheit		gut, recht scharf, etwas dunkel / sichtbares Rauschen, kein Ruckeln	gut, flüssig, aber Artefakte sichtbar / hell, viele Details	gut ausgeleuchtet, teils überstrahlt / leicht ruckelig
Video: Pixelzahl / Bildwinkel / Nachtmodus		1920 x 1080 (1080p) / etwas klein, nicht veränderbar / vorhanden	2850 x 1440 (1440p) / sehr groß, veränderbar / vorhanden	1920 x 1080 (1080p) / sehr groß, veränderbar / vorhanden
Tonqualität / Zeitversatz im Video		blechern und recht hohl, aber verständlich (mono) / 0,8 Sekunden	hörbares Rauschen, Stimmen nasal (mono) / 3,79 Sekunden	etwas dumpf und blechern, aber verständlich (mono) / 2 Sekunden
Wie gut klappt die Überwachung?	10 %	Speichert auf Speicherkarte	Sehr viele Funktionen	Speichert nur in der Cloud
Überwachungsfunktionen: zu überwachende Bereiche / Zeitfenster / Bewegungsmelderempfindlichkeit einstellbar / Benachrichtigung / Alarmierungskontakte (Anzahl)		ja, einstellbar / ja, eingrenzbar / ja / ja, per App / ja (6)	ja, eingrenzbar / ja einstellbar / ja / ja, per E-Mail und App / ja (3)	nein / ja, eingrenzbar / ja / ja, per App / ja (3)
Aufzeichnungsmodi: Vorlauf / Nachlauf / Video / Foto / Loop / automatische Löschung einstellbar / Speicherung im Gerät / auf Speicherkarte / Cloud (Dauer maximal)		ja / ja / ja / ja / nein / nein / nein / ja / nein (keine)	nein / ja / ja / ja / nein / nein / nein / nein / ja (60 Tage, nur im Abo)	ja / ja / ja / ja / nein / nein / nein / nein / ja (30 Tage, nur im Abo)
Wie einfach lässt sich die Kamera bedienen?	21 %	Einfachste Bedienung im Test	Gute Beweissicherung	Gute Menüs, übersichtlich
Gedruckte Bedienungsanleitung		nur Kurzanleitung	nur Kurzanleitung	nur Kurzanleitung
Inbetriebnahme		einfach	einfach	einfach
Bedienung: per App / per PC-Programm / per Webbrowser		ja / nein / nein	ja / nein / ja	ja / nein / ja
Einfachheit der Bedienung: Video abrufen / Videos versenden / Bilder abrufen / Bilder versenden / Kamera scharf schalten / Benachrichtigungsfunktion benutzen / Bewegungsereignis kontrollieren		einfach / einfach / etwas umständlich / einfach / einfach / etwas umständlich / einfach	einfach / einfach / einfach / einfach / etwas umständlich / einfach / einfach	einfach / einfach / einfach / einfach / einfach / einfach / einfach
Funktionen für Beweissicherung / Funktionen im Abo		sehr umfangreich / keine	umfangreich / Erkennung Pakete, Personen und mehr, Notfallkontakte, individuelle Benachrichtigungen	umfangreich / Erkennung Pakete, Personen und mehr, Notfallkontakte, individuelle Benachrichtigungen
Anschluss: LAN-Kabel / USB / WLAN / Bluetooth / Mobilfunk / Spezialkabel		ja / nein / ja / nein / nein / nein	nein / nein / ja / nein / nein / nein	nein / ja / ja / nein / nein / nein
Wie sicher und sparsam ist die Cam?	14 %	Geringster Stromverbrauch	Akkuladung frisst viel Strom	Etwas hoher Verbrauch
Sicher vor unbefugtem Zugriff: auf Videos / auf Einstellungen		sehr sicher / sehr sicher	etwas unsicher / etwas unsicher	etwas unsicher / sehr sicher
Stromverbrauch: Bereitschaft bei eingeschalteter Videofunktion und WLAN-Übertragung (Kosten pro Jahr)		2,2 Watt (4,82 Euro pro Jahr)	5,3 Watt (11,61 Euro pro Jahr)	3,2 Watt (7,01 Euro pro Jahr)
Abwertung		keine	keine	keine
TESTERGEBNIS		gut 2,1	gut 2,2	gut 2,4



4 LOGITECH CIRCLE VIEW

Preis: 150 Euro
Abo: ab 0,99 Euro pro Monat

Wer ohnehin im Apple-Universum zu Hause ist und iCloud-Speicher gebucht hat, ergänzt sein Smarthome mit dieser Cam perfekt. Die Kamerabilder gehen in Ordnung, Bedienung und Tonqualität überzeugten im Test. Bei den Funktionen ist mehr drin – sobald Apple dies in HomeKit einbaut. Aufnahmen landen verschlüsselt in der iCloud, die Abogebühren gehen an Apple.

+ Lokale Bildanalyse, Aufnahmen gut verschlüsselt.

- Wenige Funktionen, Apple-Gerät und -Cloud-Abo nötig.



5 GOOGLE NEST CAM

Preis: 180 Euro
Abo: ab 5 Euro pro Monat

Viele Funktionen gibt's nur mit Abo, deshalb landet die Nest nur auf Rang fünf. Bei der Bildqualität gehört sie aber zur Spitzengruppe. Am Tag liefert sie ansprechendes, wenn auch etwas dunkles Material. Bei wenig Licht zeigt sie viele Details. Dank ihres Akkus, der flexiblen Halterung sowie des wetterfesten Gehäuses fühlt sie sich sowohl drinnen als auch draußen wohl.

+ Gute Aufnahmen, innen und außen nutzbar, Akkubetrieb.

- Viele Funktionen nur mit Abo, keine Fotos möglich.



6 BLINK INDOOR

Preis: 70 Euro
Abo: 3 Euro pro Monat

HD-Aufnahmen, Videoaufzeichnung bei Bewegung, Nachtlicht und Gegensprechen: Die kabellose und kompakte Innenkamera liefert viele wichtige Funktionen ohne Aufpreis. Die Kamerabilder könnten aber besser und vor allem nachts heller sein. Cloudspeicher gibt's ab 3 Euro im Monat. Alternative: Aufnahmen lokal sichern per Sync-Modul (40 Euro extra) oder USB-Stick (ab 5 Euro).

+ Günstig, Akkubetrieb (2 AA-Batterien).

- Videos ruckeln mitunter, nachts etwas dunkel.



7 CANARY VIEW

Preis: 99 Euro
Abo: ab 9,99 Euro pro Monat

Canary liefert mit der View eine passable Kamera für Innenräume. Ihre Full-HD-Aufnahmen haben sowohl am Tag als auch in der Nacht leichte Schwächen – für die Beweissicherung reicht es aber problemlos aus. Ohne Abo speichert sie Videos gerade mal für einen Tag in der Cloud, immerhin lassen sich die Aufnahmen auf dem Handy sichern. Ebenfalls negativ ist der hohe Stromverbrauch.

+ Flüssige Videos, Benachrichtigung per App & Mail.

- Sichtbare Artefakte, mauler Tonqualität, hoher Verbrauch.



8 GIGASET CAMERA 2.0

Preis: 160 Euro
Abo: ab 0,99 Euro pro Monat

An die frische Luft möchte die Gigaset Camera 2.0 nicht. Sie fühlt sich wohler in Innenräumen. Dort macht sie brauchbare Aufnahmen, die jedoch hinter denen der Konkurrenz zurückbleiben. Einen Schnitzer leistet sich Gigaset beim Abo-System. Bei Bewegungen filmt die Camera 2.0 nämlich nur, wenn Nutzer monatlich zahlen. Die Einrichtung und Bedienung sind okay.

+ Einfach Einrichtung, Steuerung per App und Browser.

- Grundfunktionen nur mit Abo, unscharfe Aufnahmen.

Einsatzgebiet: innen und außen
Sprachassistent: Apple Siri

Einsatzgebiet: innen und außen
Sprachassistent: Google Assistant

Einsatzgebiet: innen
Sprachassistent: Amazon Alexa

Einsatzgebiet: innen
Sprachassistenten: Amazon Alexa, Google Assistant

Einsatzgebiet: innen
Sprachassistenten: Amazon Alexa, Google Assistant

Beste Tonaufnahme im Test	2,4	Deutliche Aufnahmen	2,3	Detailarm und verwaschen	3,0	Bild flüssig, mit Klötzchen	2,8	Etwas unscharf, Farben mau	3,0
detailliert, teilweise etwas pixelig / unscharf und verwaschen	2,8	gut, aber etwas dunkel / viele Details erkennbar, ruckelig	2,4	etw. detailarm, stark verwaschen / ruckelig	3,6	sichtbare Artefakte bei Bewegungen / recht hell	3,0	etwas unscharf, Farben wirken grell / sichtbare Artefakte, ruckelig	3,2
1920 x 1080 (1080p) / sehr groß, nicht veränderbar / vorhanden	1,2	1920 x 1080 (1080p) / sehr groß, nicht veränderbar / vorhanden	2,4	1920 x 1080 (1080p) / sehr groß, nicht veränderbar / vorhanden	1,0	1920 x 1080 (1080p) / groß, nicht veränderbar / vorhanden	1,8	1920 x 1080 (1080p) / etwas klein, nicht veränderbar / vorhanden	2,1
recht klar und ordentlich laut, gut verständlich (mono) / 1 Sekunde	1,7	etwas blechern, aber gute Sprachwiedergabe (mono) / 0,8 Sekunden	2,3	etwas dumpf und blechern, aber verständlich (mono) / 2 Sekunden	2,4	leichtes Rauschen, Stimme klingt abgehackt (mono) / 1,55 Sekunden	3,0	halbwegs deutlich, rauscht, blechern und dumpf (mono) / 1 Sekunde	3,1
Wenige Funktionen	3,5	Sehr wenige Funktionen	3,5	Wenige Videofunktionen	2,7	Wenige Aufnahmemodi	3,2	Sehr wenige Funktionen	3,2
ja / ja, einstellbar / nein / ja, per App / nein (keine)	2,8	ja, eingrenzbar / ja, einstellbar / nein / ja, per App / nein (keine)	3,0	ja, einstellbar / ja, eingrenzbar / ja / ja / nein (keine)	2,0	ja, eingrenzbar / ja, einstellbar / nein / ja, per E-Mail & App / ja (4)	2,0	ja, nur im Abo / nein / ja / ja, per App einstellbar / nein (keine)	3,4
ja / ja / ja / ja / nein / nein / nein / nein / ja (10 Tage, nur im Abo)	4,2	nein / ja / nein / nein / nein / ja / ja / nein / ja (60 Tage, nur im Abo)	3,9	ja / ja / ja / ja / nein / nein / nein / ja / ja (30 Tage, nur im Abo)	3,3	ja / ja / ja / nein / nein / nein / nein / nein / ja (30 Tage, nur im Abo)	4,3	nein / nein / ja / nein / nein / nein / nein / nein / ja (30 Tage, nur im Abo)	4,9
Einfache Bedienung	2,5	Keine Fotos möglich	2,5	Beweissicherung eingeschränkt	2,6	Wenige Funktionen	3,0	Viele Funktionen nur per Abo	2,9
nur Kurzanleitung	4,5	nur Kurzanleitung	4,5	nur Kurzanleitung	4,5	nur Kurzanleitung	4,5	nur Kurzanleitung	4,5
sehr einfach	1,0	sehr einfach	1,0	einfach	2,0	einfach	1,5	einfach	2,0
ja / nein / nein	2,3	ja / nein / nein	2,3	ja / nein / nein	2,3	ja / nein / nein	2,3	ja / nein / ja	1,3
sehr einfach / einfach / einfach / einfach / sehr einfach / einfach / einfach	1,8	sehr einfach / sehr einfach / nicht möglich / nicht möglich / sehr einfach / sehr einfach / sehr einfach	2,7	einfach / einfach / einfach / einfach / einfach / einfach / einfach	2,0	sehr einfach / einfach / nicht möglich / nicht möglich / sehr einfach / einfach / sehr einfach	3,1	einfach / umständlich / nicht möglich / nicht möglich / nicht möglich / einfach / einfach	3,6
etwas eingeschränkt / Aufnahme	2,7	etwas eingeschränkt / lückenloser Videoverlauf	2,7	etwas eingeschränkt / Aufzeichnung und Fotoaufnahme, Freigabe von Videos	2,9	eingeschränkt / Personenerkennung, unbegrenzte Video-Downloads, Gegensprechfunktion	3,7	etwas eingeschränkt / Aufnahme bei Bewegungsalarm, Videos freigeben, Bewegungszonen	3,9
nein / nein / ja / nein / nein / nein	2,3	nein / ja / ja / nein / nein / nein	1,9	nein / ja / ja / nein / nein / nein	1,9	nein / nein / ja / nein / nein / nein	2,3	nein / nein / ja / nein / nein / nein	2,3
Sicher und sparsam	2,3	Geringer Stromverbrauch	3,2	Geringer Stromverbrauch	2,3	Etwas hoher Verbrauch	3,3	Etwas hoher Stromverbrauch	2,4
etwas unsicher / sehr sicher	2,3	etwas unsicher / etwas unsicher	3,5	etwas unsicher / sehr sicher	2,3	etwas unsicher / etwas unsicher	3,5	sehr sicher / etwas unsicher	2,3
3 Watt (6,57 Euro pro Jahr)	2,3	2,4 Watt (5,26 Euro pro Jahr)	2,4	3 Watt (6,57 Euro pro Jahr)	2,3	2,7 Watt (5,91 Euro pro Jahr)	2,7	2,7 Watt (5,91 Euro pro Jahr)	2,7
keine				keine		keine		Grundfunktionen nur im Abo	+0,1

befriedigend 2,5

befriedigend 2,6

befriedigend 2,8

befriedigend 2,9

befriedigend 3,1

Die Marktpreise (letzter Stand: 19.05.2022) ermittelt COMPUTER BILD über idealo.de

TIPPS

SO NUTZEN SIE IHRE SMARTE CAM OPTIMAL

ACHTUNG, AUFNAHME! NUR ERLAUBTES FILMEN

Smarte Überwachung ist legal, aber: Kameras dürfen nur den Bereich filmen, der unmittelbar vor der eigenen Haustür liegt, nicht den öffentlichen Raum, etwa den Bürgersteig, oder den Privatbereich anderer, wie zum Beispiel das Nachbargrundstück. Um Ärger zu vermeiden, legen Sie in den Einstellungen der Cam-App Aufnahmebereiche fest: Je nach Anbieter markie-

ren Sie dazu ein Raster oder ziehen einen Rahmen um die Bereiche, die Ihre Cam erfassen soll. Ein weiterer Vorteil solcher Aktivitätszonen: Sie verhindern, dass die Cam zu oft Alarm schlägt, etwa weil sich ein Baum im Wind wiegt. Meist sind auch Empfindlichkeit und Reaktionszeiten justierbar. So gibt's nur noch Meldungen, wenn sich in den Zonen was Bedenkliches tut.



Foto aktualisieren

Zonen zurücksetzen

Einfach

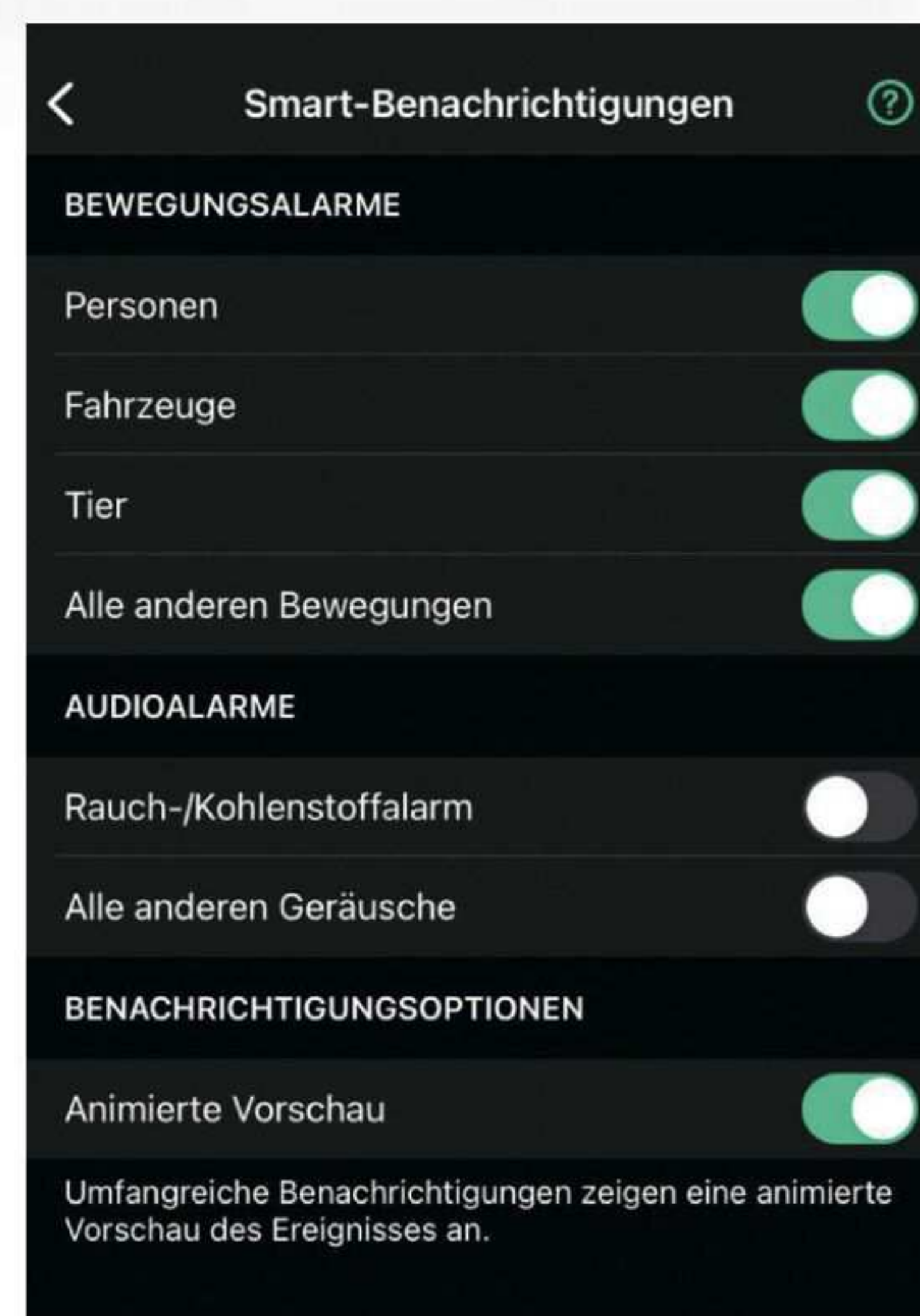
Erweitert

Änderungen der Lichtverhältnisse (z. B. Scheinwerfer, Schatten, Spiegelungen etc.), die außerhalb von deaktivierten Bereichen liegen, können zu Fehlalarmen führen.

In den Apps sind Aktivitätszonen fix angelegt. Bei Blink markieren Sie ein Raster (siehe oben), bei Arlo „malen“ Sie Rahmen ins Kamerabild.

FREUND ODER FEIND?

Die Kameras von Arlo und Canary können speziell menschliche Bewegungen erkennen. Daher startet die Aufnahme nur, wenn das Gerät eine Person erfasst. Die Google-Cam kann sogar Gesichter erkennen. Bekannte Gesichter lassen sich in der App benennen und Personen zuordnen. Auch das vermeidet lästige Fehlalarme. Einige Cams gehen noch einen Schritt weiter: Sie erkennen auch Haustiere, Arlo meldet sogar Pakete vor der Haustür. In den Einstellungen der Apps lässt sich genau einstellen, worauf die Kameras reagieren sollen.

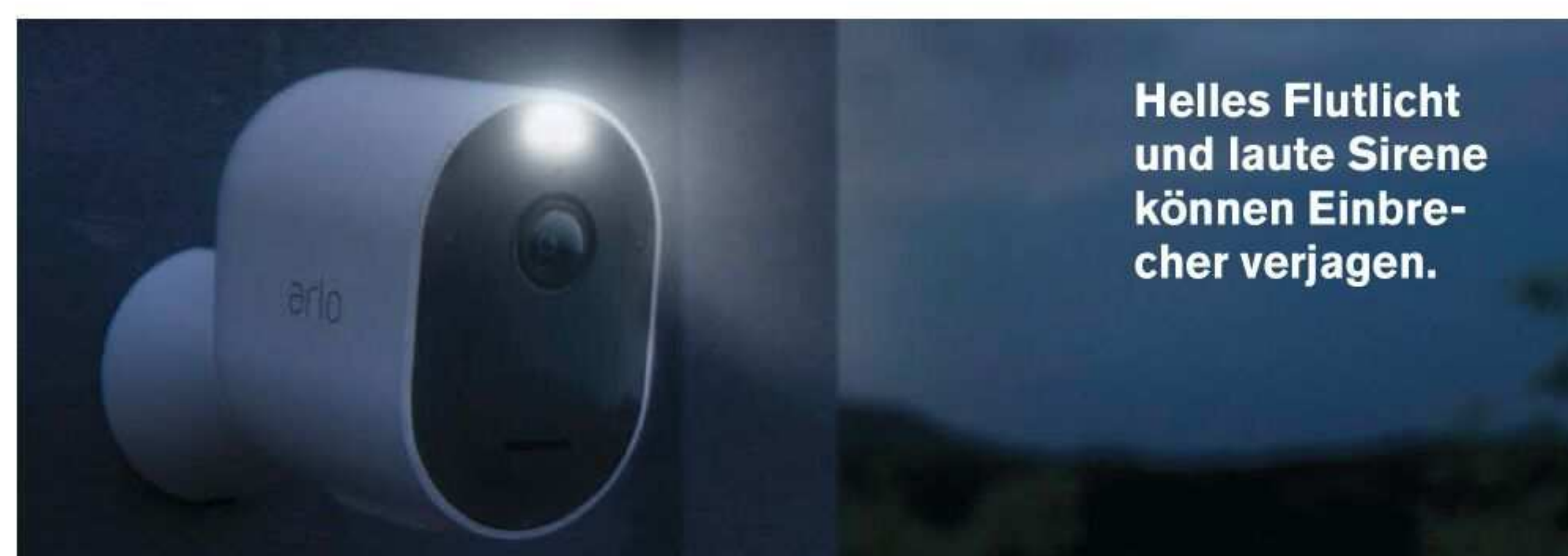


In der Arlo-App lässt sich regeln, wann es Benachrichtigungen gibt. Dafür brauchen Nutzer aber das Bezahl-Abo.

EINBRECHERSCHRECK

Bei Dunkelheit hellen die meisten getesteten Cams mit Infrarot-Leuchten die Umgebung auf und sorgen für erkennbare Aufnahmen. Videos wirken zwar verwaschener als am Tag, zeigen aber das Wichtigste. Besser: Die Arlo Pro 4 hat eine leuchtstarke LED-Lampe an Bord. So ein „Strahlemann“

macht die Nacht zum Tag. Neben der Beleuchtung dient auch ein schriller Alarmton zur Abschreckung unerwünschter Besucher. Licht und Alarmton steuern Sie in der Arlo-App: Die Sirene aktivieren Sie mit dem roten Symbol im Vorschaubild, das Flutlicht in den **Videoeinstellungen**.



DAS KAMERABILD AUF FERNSEHER ODER SMART DISPLAY HOLEN

Wer gerade auf dem Sofa eine Serie guckt oder in der Küche das Abendessen zubereitet, will nicht immer das Handy zücken, um einen Blick aufs Livebild der Cam zu werfen. Besser: Holen Sie die Videos auf den großen Bildschirm Ihres Fernsehers oder auf Smart Displays wie den Amazon Echo Show. Hier die drei Möglichkeiten:

Ring und Blink mit Alexa-Skill

Überwachungskameras der Amazon-Töchter Blink und Ring arbeiten mit Echo Show oder Fernsehern samt Fire TV Stick

zusammen. Dazu braucht's einen Alexa-Skill, den Sie per Alexa-App am Handy installieren. Sie heißen Blink SmartHome oder Ring. Den Skill mit Blink- oder Ring-Konto verknüpfen, nach Kameras suchen, fertig! Sobald sich etwas tut, erscheint auf TV oder Smart Display eine Benachrichtigung, um das Livebild einzublenden. Per Sprachkommando wie „Alexa, zeige Haustür!“ klappt's auch auf Zuruf.

HomeKit-Kameras und Apple TV

Apple-Fans blenden beim Schauen von Filmen und Serien

auf dem Apple TV das Livebild ihrer Kameras ein. Das klappt mit Apples Smarthome-Steuerung HomeKit (siehe unten), mit der etwa Arlo Pro 4 und Logitech Circle View funktionieren. Ist die Cam in der Home-App auf iPhone oder iPad als Kamerafavorit markiert, erscheint der Videostream im Kontrollzentrum des Apple TV. Zum Aufruf reicht ein Druck auf die Home-Taste der Siri-Remote-Fernbedienung.

Google Nest mit SmartThings

Auf neueren Samsung-TVs (ab 2018) gibt es die Heimsteuerung SmartThings. Die kennt auch Überwachungskameras von Ring und Google Nest: Wer die Cams in der SmartThings-App koppelt, holt das Livebild per Fernbedienung aufs TV-Gerät und sieht jederzeit, wer da ums Haus schleicht oder vor der Tür steht. Das gelingt auch auf dem Display kompatibler Samsung-Family-Hub-Kühlschränke.

Hängt die Apple-TV-Box am Fernseher und eine HomeKit-Kamera im selben WLAN, lässt sich das Kamerabild in einer Seitenleiste anzeigen.



KAMERAS RICHTIG PLATZIEREN



Bestes Blickfeld

Eine Kamera kann nur dann gut überwachen, wenn sie alles Wesentliche überblickt. Bringen Sie die Cam daher leicht erhöht an, und sorgen Sie so für ein freies Blickfeld, ohne direkt vor der Linse befindliche Hindernisse.



Kein Gegenlicht

Ein Fenster gegenüber der Kamera bringt Licht, kann aber die Aufnahme erschweren. Vermeiden Sie daher starke Lichtquellen und auch Spiegelflächen im Bild, die die Optik blenden und bei der Ausleuchtung irritieren.



Bewegungen im Blick

Richten Sie die Kamera möglichst so aus, dass sie etwa den Weg vor der Haustür seitlich filmt – und die Bewegung damit „aus der Flanke“ erfassen kann. Das erleichtert dem Sensor die Bewegungserkennung. Auch der Abstand zwischen Kamera und Bewegung sollte passen: Optimal gelingt die Erkennung bei 1,5 bis 6 Meter Entfernung.

Fotos: iStock, Arlo, Blink/Amazon, Eufy; Montage: COMPUTER BILD



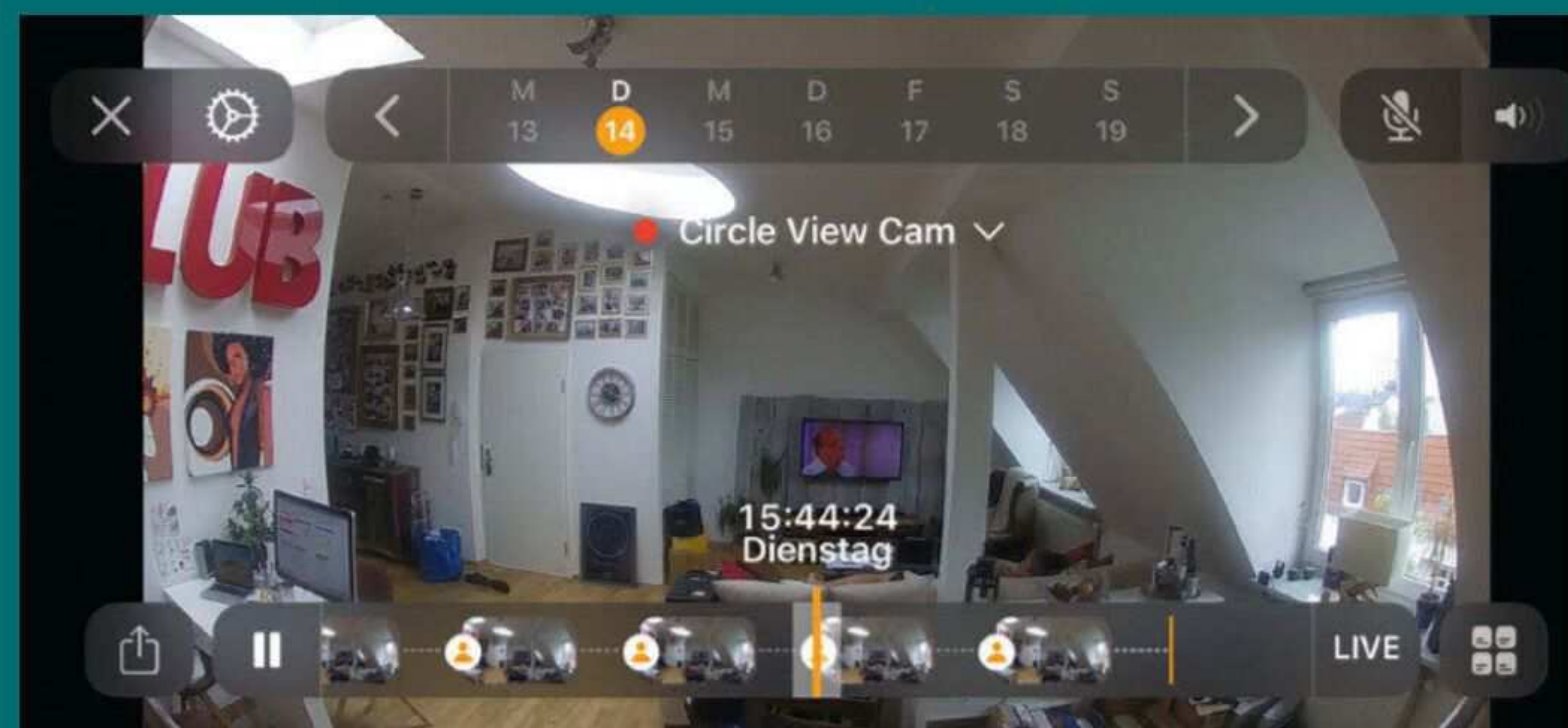
FÜR APPLE-NUTZER: IN HOMEKIT EINBINDEN

Nutzer im Apple-Smarthome verwenden am besten HomeKit-Kameras wie Arlo Pro 4 oder Logitech Circle View. Vorteil: Sensible Überwachungsdaten gelangen nicht auf die Server der Kamerahersteller, sondern übers heimische WLAN direkt aufs iPhone oder iPad. Sogar bei Bewegungserkennung bleibt die Bildanalyse eine lokale Angelegenheit. Apple nennt das „sicheres HomeKit-Video“. Auf Wunsch wandern Videos für zehn Tage in Apples iCloud. Obwohl HomeKit-Clips nicht das Speicherlimit belasten, ist

Per Datumsleiste und Schieberegler können Nutzer in den Aufnahmen der HomeKit-Cam stöbern.

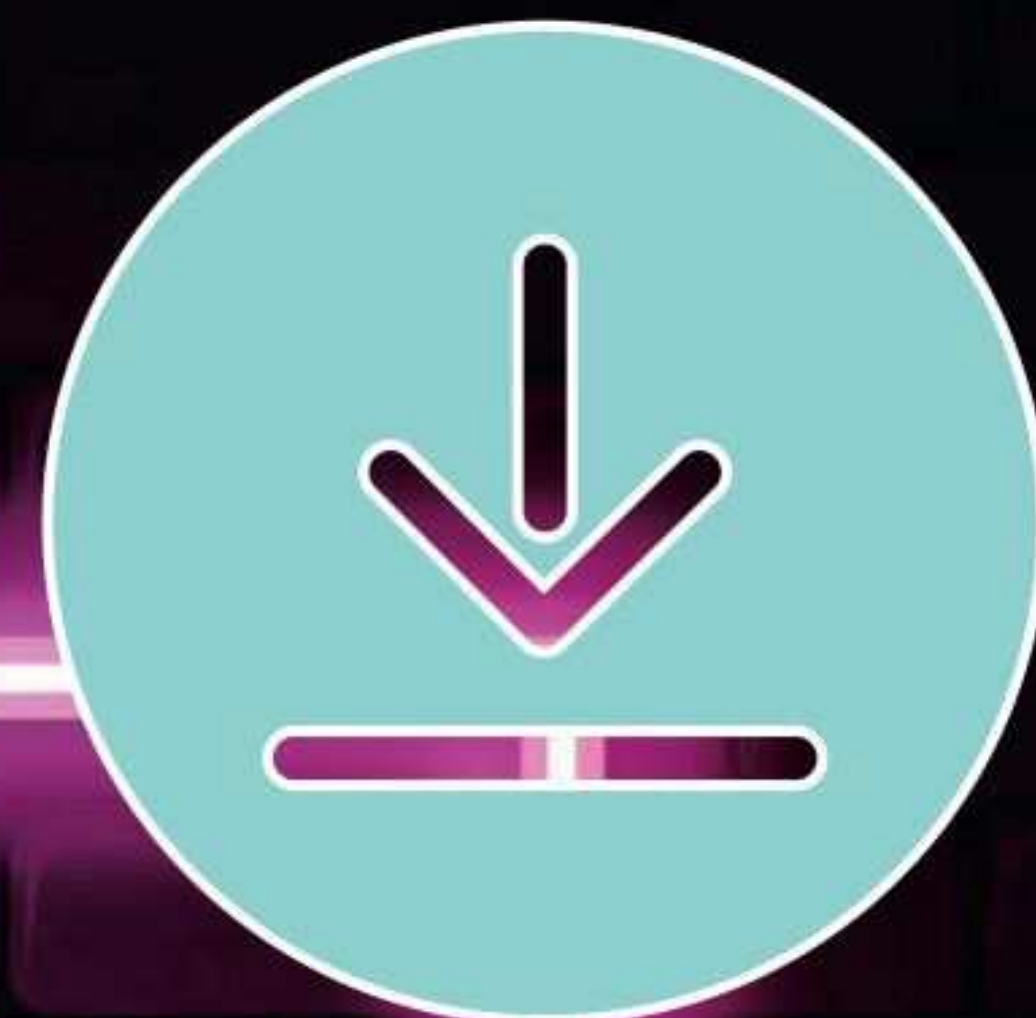
mindestens das 50-Gigabyte-Paket Pflicht. Kostenpunkt: 1 Euro pro Monat. Das Einrichten und Steuern übernimmt Apples Home-App. Tippen Sie auf **+** und **Gerät hinzufügen**. Per iPhone- oder iPad scannen Sie den speziellen QR-Code, den Sie direkt auf

der Cam oder der Verpackung finden. Legen Sie noch fest, ob Sie Videos nur sehen oder auch aufnehmen wollen. Als **Favorit** markiert, erscheinen Cam und Bild gleich im Kontrollzentrum der Home-App. Benachrichtigungen und Vorschaubild führen per Tipp zur Live-Ansicht.



COMPUTERBILD.DE

DIE BESTEN DOWNLOADS


**KOSTENLOSE
VOLLVERSIONEN**
**SICHERHEITS-
PROGRAMME**
**DIE BESTE SOFTWARE
FÜR JEDE AUFGABE**


Sie sind auf der Suche nach Software? Dann schauen Sie doch im großen Download-Bereich von www.computerbild.de vorbei – dort finden Sie mehr als 12000 Programme übersichtlich sortiert zum Runterladen. Vom einfachen Malprogramm über umfangreiche Office-Pakete bis hin zum ausgefeilten Schutzprogramm für Ihren PC: Im Download-Bereich auf cobi.de/download gibt es für jede Aufgabe die passende Software!

Exklusive Vollversionen

Und damit nicht genug: Neben Unmengen an Freeware finden Sie dort auch exklusive Vollversionen. Software für PC-Tuning, Sicherheits-Tools und Programme zur Bildbearbeitung kosten im Handel meist viel Geld, bei www.computerbild.de erhalten Sie die Software gratis.

Einige Programme gibt es sogar als spezielle CBE-Versionen mit einem exklusiven Funktionsumfang, und der kostet Sie ebenfalls

keinen Cent. Schauen Sie einfach selbst – auf www.computerbild.de/10701 ist sicher was Passendes für Sie dabei.

Praktische Download-Specials

Sie suchen einen bestimmten Typ Software? Dann sind die Download-Specials die perfekte Anlaufstelle für Sie. Dort finden Sie für die unterschiedlichsten Themen Download-Pakete mit den wichtigsten und besten Programmen, aber auch Geheimtipps. Egal ob

Sie ein neues Wallpaper suchen, Firefox erweitern oder Windows optimieren möchten – reinschauen lohnt sich: www.computerbild.de/downloads/specials

Perfekt abgesichert

Passwort-Manager, Verschlüsselungsprogramme, Datensafes: Auf www.cobi.de/sicherheitscenter finden Sie nicht nur Programme, die Ihren PC schützen, sondern auch Sicherheits-News, Hinweise auf Sicherheitslücken und vieles mehr.

Fotos: iStock; Montage: COMPUTER BILD

IMPRESSUM

Chefredakteur: Dirk General-Kuchel (dgk)

Stellv. Chefredakteure: Georg Oevermann, Felix Disselhoff

Geschäftsführender Redakteur: Florian Rüttinger

Ressortltg. Sonderpublikationen: Marco Häntsch (mc)

Textredaktion: Martin Seigel (Lt.), Rüdiger Kopp

Ressortltg. Layout / Head of Editorial Design: Kristina Münster

Chefs vom Dienst: Frank Schaper, Alexander Petrovic

Autoren: Marco Engelin (me), André Hesel (hes), Robert Ladenthin (rl), Hubert Popiolek (hp), Andreas Sauerland (asa), Rainer Schuldt (rs), Thomas Vattrodt (tv), Andy Voß (av)

Layout: Sabrina Pompe-Roß, Tanja Steenbuck, Alexander Blancke, Timo Knorst, Urs Höer, Birte Holländer

Fotoredaktion: Cornelius Braun

Schlussredaktion: Stephan Arweiler, Thomas Meins, Thomas Schlüter, Ilka Weihmann

Redaktionsanschrift: COMPUTER BILD,

Brieffach 5610, 20350 Hamburg

Geschäftsführer: Dirk General-Kuchel,

Frank Mahlberg (Vorsitz), Christian Wolf

General Manager: Andrea Starke

Anzeigenvertretung: B&M Marketing GmbH,

www.bm-marketing.de, Geschäftsführer: Stefan Müller

Gesamtanzeigenleiter: Benjamin Schweppe

(verantwortlich für den Inhalt der Anzeigen)

Vertrieb (Einzelverkauf): DMV Der Medienvertrieb

GmbH & Co. KG, www.dermedienvertrieb.de

Vertriebsleitung: Benjamin Frank

Druck: Prinovis GmbH & Co. KG, Betrieb Ahrensburg, Alter Postweg 6, 22926 Ahrensburg

Verlag: COMPUTER BILD Digital GmbH, Axel-Springer-Platz 1,

20350 Hamburg; Tel. 040-347 00; www.axelspringer.de

Informationen zum Datenschutz finden Sie auf der Webseite www.computerbild.de/datenschutz – Sie können sie auch schriftlich unter Axel Springer SE, Datenschutz, Axel-Springer-Straße 65, 10969 Berlin, anfordern.

Das Papier von COMPUTER BILD ist umweltfreundlich und recycelbar. Zur Herstellung wird ausschließlich chlorfrei gebleichter Zellstoff genutzt.

Für unverlangt eingesandte Manuskripte und Fotos wird keine Haftung übernommen. COMPUTER BILD wird als Print- und Online-Ausgabe verbreitet und ist per Internetdatenbank recherchierbar. Alle Rechte vorbehalten.

DIE MÄNNERBOX

POWERED BY:



Computer
Bild



SO GENIESST MANN DEN SOMMER

WARENWERT ÜBER 100 €

NUR
34,90 €

MIT DEM CODE:
BILD5



UNSERE HIGHLIGHT-PRODUKTE FÜR DIE GRILLSAISON

INHALT DER MÄNNERBOX SOMMER-EDITION 2022: AMERICAN CREW DEFINING PASTE, ULTRASUN BRIGHTENING UND ANTI-POLLUTION FLUID SPF 50+, BBQ DAS ORIGINAL, GORBATSCHOW HARD SELTZER FIZZY GRAPEFRUIT, TEFAL OPTIMAL GRILLEN KOCHBUCH, ÖLMÜHLE HARTMANN GRILLÖL BBQ, BALLISTOL GRILL-REINIGER, SIX MÄNNERSONNENBRILLE, SPREEWALDHOF UNSERE KLEINEN SPREELINGE, BREWDOG HAZY JANE, COOK IN WOOD FOODIE POWER BLOCK

JETZT SICHERN UNTER WWW.MAENNERBOX.DE

* Der Gutscheincode kann nicht mit anderen Gutscheincodes oder Rabattaktionen kombiniert werden. Eine nachträgliche Gutschrift ist nicht möglich. Der Gutscheincode kann nur einmal je Kunde eingelöst werden. Es handelt sich um eine Beispielabbildung. Die Produktzusammenstellung kann abweichen. Der Gutscheincode ist bis zum 05.09.2022 gültig.



Deine Privatsphäre: unbezahlbar

Avast One

Hurra, Ihr Smart-Scan ist abgeschlossen!

Wir empfehlen, regelmäßig einen Smart-Scan auszuführen, um sicher und privat zu bleiben.

Fertig

Computer Bild

„BESTER IM PRAXISTEST“

Avast One

NOTE **2,0**

Ausgabe 6/2022
8 PRODUKTE IM VERGLEICH **

Avast One

13:58

WILLKOMMEN BEI AVAST ONE

Lassen Sie uns Ihren ersten Smart-Scan ausführen

Finden und entfernen Sie Sicherheitsbedrohungen und verbessern Sie Ihre Privatsphäre mit diesem optimierten Scan.

Smart-Scan ausführen

Das dauert nur einen Moment

Start Entdecken Profil



**Jetzt auch
kostenlos*
herunterladen:
avast.com/cobi**

Dein Cyber-Schutz: **kostenlos**



Sicherheit, Privatsphäre & Performance in One.



Wir schützen die digitale Freiheit für alle.

* Der kostenlose Download über den angegebenen Link beinhaltet Avast One Essential mit dem Basisschutz für ein Endgerät. (PC, MAC, Android und iPhone/iPad). Es können zusätzliche Kosten für den Download durch den jeweiligen Internetanbieter entstehen.

** Auszeichnung für Avast One Individual/Family mit erweiterten Schutzfunktionen für bis zu 5 Endgeräte. 2022 Copyright Avast Deutschland GmbH.

ONE.de empfiehlt



Erhalte beim Kauf eines Systems ein **GRATIS** Jahresabo Norton 360 für 3 Geräte.

- ✓ Passwort-Manager
- ✓ Cloud-Backup für PC
- ✓ Dark Web Monitoring
- ✓ Bedrohungsschutz in Echtzeit
- ✓ Secure VPN für deine Online-Privatsphäre
- ✓ Schutz vor Viren, Malware, Spyware und Ransomware

Und vieles mehr!

Norton 360



Umfassende Gerätesicherheit sowie ein VPN für deine Online-Privatsphäre. Es ist leicht, online unvorsichtig zu sein – aber es ist auch leicht, sich zu schützen!

Norton ist nicht vorinstalliert, löse dazu den mitgelieferten Key ein!

Deluxe:



ONE BUSINESS ADVANCED A006

AMD **Ryzen 5 PRO 4650G** mit 6x 4.20 GHz

AMD Radeon Vega 7

16 GB DDR4 mit 2666 MHz GoodRam

500 GB M.2 PCIe WD Blue NVMe SSD

36 MONATE GARANTIE
499,99€¹
oder Finanzkauf² z. B. **9,96 €**
mtl. Laufzeit: 60 Monate



MSI B450M Pro-VDH Max
350 W FSP Fortron/Sourc
inkl. Windows 11 Home
inkl. Norton 360 Deluxe

Art-Nr. 65019

Für Gamer:



ONE GAMING ULTRA A002

AMD **Ryzen 5 5600X** mit 6x 4.60 GHz

RTX 3080 Ti mit 12 GB GDDR6X KFA²

32 GB DDR4 mit **3200 MHz** CORSAIR

1 TB M.2 PCIe WD Blue NVMe SSD

36 MONATE GARANTIE
2.249,99€¹
oder Finanzkauf² z. B. **38,63 €**
mtl. Laufzeit: 72 Monate



MSI B450M Pro-VDH Max
850 W GIGABYTE P850GM
inkl. ONE GAMING GPU-Halterung
inkl. Windows 10 Home
inkl. Norton 360 für Gamer

Art-Nr. 24040

ONE THIN & LIGHT V3 I002



14.1" 35.81 cm

THIN & LIGHT

Intel **Pentium N5030** mit 4x 3.10 GHz

Intel **UHD Graphics**

8 GB LPDDR4

256 GB M.2 SSD

24 MONATE GARANTIE
415,00€¹
oder Finanzkauf² z. B. **9,98 €**
mtl. Laufzeit: 48 Monate



Full HD IPS Display
16 mm dünn, 1.30 Kg leicht
ac WLAN, BT 4.2, 2x USB 3.1
Mini HDMI, Kopfhörer
inkl. Windows 11 Home
inkl. Norton 360 Deluxe

Art-Nr. 65034

ONE GAMING K56-11NB-NH4



15.6" 39.62 cm

one GAMING

RGB TASTATUR

Intel Core **i5-11400H** mit 6x 4.50 GHz

RTX 3060 mit 6 GB GDDR6

8 GB DDR4 - SO-DIMM mit **3200 MHz**

500 GB M.2 PCIe WD Blue NVMe SSD

24 MONATE GARANTIE
1.219,00€¹
oder Finanzkauf² z. B. **20,93 €**
mtl. Laufzeit: 72 Monate



Full HD 144 Hz IPS-Level Display
Wi-Fi 6 AX, BT 5.2, USB 2.0, 2x USB 3.2
2x USB 3.2 (Typ-C), HDMI, Mini DP, DP
Kopfhörer + Mikrofon (Kombianschluss)
inkl. Windows 11 Home
inkl. Norton 360 für Gamer

Art-Nr. 25024



one.de
0 44 61/74 87-4 00



ONE.de IT-Handelsgesellschaft mbH, Nordfrost-Ring 16, 26419 Schortens
Informationen zu den Versandkosten findest du unter: www.one.de/versandkosten

Technische Änderungen, Irrtümer und Druckfehler vorbehalten. Produktabbildungen können farblich und von der gewählten Konfiguration abweichen und dienen nur zur reinen Darstellung. 1) Alle genannten Preise inkl. MwSt. zzgl. Versandkosten. Abbildung enthält Sonderausstattung. Der Käufer erhält ein 14-tägiges Widerrufsrecht. Es gilt das Widerrufsrecht gemäß EGBGB. 2) Barzahlungspreis entspricht dem Nettodarlehensbetrag. Finanzierungsbeispiel: Nettodarlehensbetrag von 499€. Effektiver Jahreszins von 9,9% bei einer Laufzeit von 36 Monaten entspricht einem gebundenen Sollzins von 9,47% p. a. Bonität vorausgesetzt. Partner ist die BNP Paribas S.A. Niederlassung Deutschland, Standort München: Schwanthalerstr. 31, 80336 München. Die Angaben stellen zugleich das 2/3 Beispiel gem. § 17 a Abs. 4 PAngV dar.