

Europas größtes IT- und Tech-Magazin

# Photovoltaik installieren

**Statt zu warten: Mit Selbstbau Geld und Zeit sparen****Balkonkraftwerk und Dachanlage: Was Sie dürfen, wie es klappt****TEST**

- Raspi-Alternative OKdo Rock 4 SE
- Desktop-Virtualisierer VMware Workstation 17
- Senioren-Smartphone Gigaset GS5
- Die eigene Filmsammlung verwalten

## Endlich effiziente Ryzen-CPUs

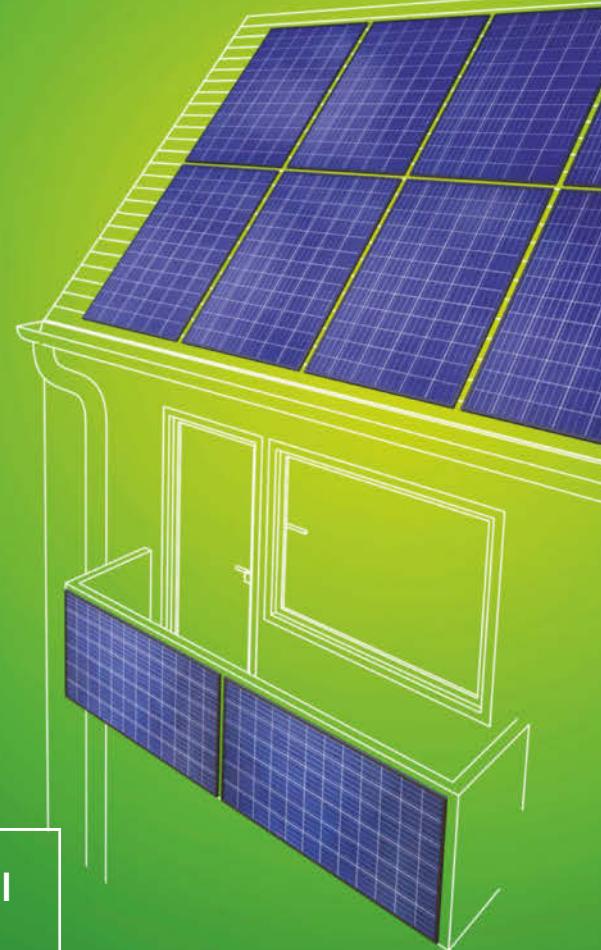
Stromspartipps und Test: AMD Ryzen 7000 mit 65 Watt

## Digitalisierung: 32 Städte im ct-Ranking

Von Augsburg bis Wuppertal: Was geht online?

**FOKUS**

- Online-Payment: Was Giropay besser macht als PayPal
- Malware filtern per TLS-Inspektion in der Firewall
- ChatGPT: Wie KI die Internetsuche revolutioniert
- Linux-Desktop Gnome für große Bildschirme einrichten



€ 5,90

AT € 6,50 | LUX, BEL € 6,90

NL € 7,20 | IT, ES € 7,40

CHF 9,90 | DKK 64,00

# Praxisleitfaden Verschlüsselung

Test: Selbstverschlüsselnde USB-Speicher • Sicher unterwegs

Tipps zu BitLocker, VeraCrypt &amp; Co.



MACH, WAS WIRKLICH ZÄHLT.



Torben B., Hauptfeldwebel

# DIGITAL GUARD

Werde Teil der Truppe als **IT-Administrator/in (m/w/d)**

[bundeswehrkarriere.de](http://bundeswehrkarriere.de)



BUNDESWEHR



## Digitalisierung der Verwaltung: Gegen jede Logik

Stellen Sie sich vor, jedes Amazon-Logistikzentrum würde seine eigene Bestellwebseite und sein eigenes Warenwirtschaftssystem entwickeln: Genau nach diesem Muster läuft die Digitalisierung der Verwaltung ab. Das Rad wird gegen jede Logik zigfach neu erfunden – mit entsprechend holprigen Ergebnissen.

In Deutschland sind die 300 Landkreise und 11.000 Kommunen für 75 Prozent aller Verwaltungsaufgaben zuständig. Von Flensburg bis Kempten muss jede Stadt selbst Webdienste entwickeln und Server betreiben, selbst dann, wenn der Bund die Abläufe bundesweit einheitlich vorschreibt, wie bei Führerschein- und Perso-Antrag und vielem mehr.

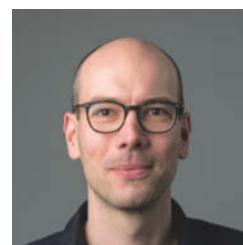
Dass dabei Milliarden verschwendet werden, ist das eine. Das andere ist, dass dabei einfach nichts Gutes herauskommen kann. Vor allem kleine Städte sind überfordert. Deshalb floppte das Onlinezugangsgesetz, das bis Ende 2022 eigentlich für flächendeckende Onlinedienste sorgen sollte.

Unsere Analyse auf Seite 116 zeigt: Es gibt zwar Vorreiter wie Nürnberg und München, doch in den meisten Städten muss man auch 2023 selbst für Kleinigkeiten persönlich zum Amt. Falls doch was digital geht, dann meist rumpelig, mit irrwitzigen Formularen, auf Webseiten, die aussehen wie von 2003.

Die verantwortlichen Politiker beim Bund und in den Ländern klopfen sich trotzdem auf die Schultern. Die Städte könnten ja Webdienste von anderen Städten übernehmen. Doch in der Praxis scheitert dieses "Einer-für-alle-Prinzip" oft an fehlenden Schnittstellen und anderen Hürden.

Sinnvoller wäre es, einheitliche Aufgaben stärker zu zentralisieren. Dafür müsste man nicht den Föderalismus über Bord werfen. Es muss nicht alles beim Bund liegen, schon Länderdienste wären besser als das Chaos in den Kommunen.

Dabei geht es nicht nur um Effizienz. Eine digitale, bürgerfreundliche Verwaltung ist auch wichtig für den sozialen Zusammenhalt, wie man aktuell am Beispiel Wohngeld sieht: Der Bund verspricht Hilfe für Energiekosten, doch die Kommunen kommen beim Abarbeiten der Anträge nicht hinterher, und die Menschen warten monatelang auf das Geld – wenn sie nicht ohnehin vor den Formularen kapituliert haben.



Christian Wölbert

Christian Wölbert

## Titelthemen

### Photovoltaik installieren

- 14 **Rahmenbedingungen** für die eigene PV-Anlage
- 20 **Balkonkraftwerke** allmählich geht mehr
- 24 **Photovoltaik** mit Eigenleistung installieren
- 32 **Solarwechselrichter** Technik und Arbeitsweise

### Praxisleitfaden Verschlüsselung

- 62 **Verschlüsselung** Daten komfortabel schützen
- 70 **Tragbare Laufwerke** selbst verschlüsseln
- 74 **Test** 3 USB-Speicher mit Verschlüsselung
- 78 **IT-Sicherheitsanalysen** für USB-Speicher

### Endlich effiziente Ryzen-CPUs

- 84 **Effiziente Ryzen-7000-CPUs** im Test
- 152 **Stromspartipps** für AMDs Ryzen 7000

### Digitalisierung: 32 Städte im c't-Ranking

- 116 **Digitale Verwaltung** Was online geht

## Test & Beratung

- 86 **Mac-Eieruhr** Horo
- 86 **Leichte In-Ear-Kopfhörer** Nothing Ear (stick)
- 87 **Datenvisualisierer** JSON Crack
- 88 **Schneller Flachbettscanner** Avision FB25
- 89 **Spiegellose Systemkamera** Fujifilm X-T5
- 90 **Alternativer Spiele-Launcher** für Epic und GOG
- 91 **Synthesizer-Emulation** Cherry Audio
- 92 **Desktop-Virtualisierer VMware Workstation 17**
- 93 **Raw-Entwickler** Capture One Pro 23
- 94 **Raspi-Alternative OKdo Rock 4 SE**
- 98 **Senioren-Smartphone Gigaset GS5**
- 100 **Vernetztes Musiksystem** von Braun
- 104 **Apple Freeform** ausprobiert
- 106 **Die eigene Filmsammlung verwalten**
- 179 **Bücher** Comic über KI, Mediennutzung in Kitas

## Aktuell

- 12 **Wie ChatGPT die Internetsuche revolutioniert**
- 36 **Meta** EU zwingt Aufsicht zu schärfere Vorgehen
- 37 **Anonymer Digital-Euro** EU-Minister dagegen
- 38 **Interview:** Souveräne Verwaltungscloud Delos
- 40 **Bit-Rauschen** Intel spart, Ryzen 7000, UEFI
- 41 **Datenschutz** EuGH stärkt Auskunftsanspruch
- 42 **Hardware** Neue High-End-Prozessoren
- 44 **Hardware** Raspi-Kameras mit Autofokus
- 45 **Server & Storage** Ryzen 7000 Boards
- 46 **DNS4EU** Europas eigene Namensauflöser
- 48 **Netzwerke** Mobiler 5G-Router Nighthawk M6 Pro
- 49 **Forschung** Handschuh liest Blindenschrift
- 50 **iPhone** Preiserhöhung für Akkuwechsel
- 51 **YouTube** Neue Umsatzregeln
- 52 **Anwendungen** Microsoft-365-Einsteiger-Abo
- 53 **Open Source** Quelloffener Nvidia-Treiber NVK
- 54 **Kopfhörer** Sennheiser Conversation Clear Plus
- 56 **Leser helfen Lesern** Mülltonnenampel
- 58 **Web-Tipps** Geografie, Energie, Gesprächscoach

### 14 Photovoltaik selbst installieren



Hohe Strompreise machen Photovoltaikanlagen interessant. Doch was tun, wenn Installateure auf Monate ausgebucht sind? Wir zeigen, wo Sie beim Aufbau Ihres Sonnenkraftwerks selbst Hand anlegen können.

## Wissen

- 82 40 Jahre c't: Wir verlosen eine Teufel Power HiFi**
- 112 Zahlen, Daten, Fakten** Elektroschrott
- 122 Online-Payment: Was Giropay besser macht**
- 136 Neuromorphe Computer** Das Gehirn als Vorbild
- 140 Spiele** Die besten (weniger bekannten) in 2022
- 146 Interview** Mastodon chaos.social-Admin
- 150 40 Jahre c't** Das Jahr-2000-Problem
- 174 Personalausweis-Kopien** Tipps zur Weitergabe

## Praxis

- 128 Malware filtern per TLS-Inspektion in der Firewall**
- 132 OPNsense-Firewall** als TLS-Inspektor einrichten
- 152 Energiesparen** bei Ryzen-7000-Prozessoren
- 156 Android** Fitnessdaten synchronisieren
- 160 Notizprogramme** Daten exportieren und sichern
- 166 Linux-Desktop Gnome auf großen Displays**

## Immer in c't

- 3 Standpunkt** Digitalisierung der Verwaltung
- 6 Leserforum**
- 11 Schlagseite**
- 60 Vorsicht, Kunde** MediaMarkt-Reklamation
- 176 Tipps & Tricks**
- 180 FAQ** BitLocker
- 182 Story** Bergungsmision
- 191 Stellenmarkt**
- 192 Inserentenverzeichnis**
- 193 Impressum**
- 194 Vorschau 5/2023**

## 62 Praxisleitfaden Verschlüsselung



Verschlüsselte Daten sind in fremden Händen nutzlos. Daheim am PC schützen BitLocker & Co., zum Anstöpseln unterwegs gibt es sichere USB-Speicher. Wir haben getestet, ob sie halten, was sie versprechen.

Frisch aus  
**c't Nerdistan**

- 94 Raspi-Alternative** Einplatinencomputer OKdo Rock 4 SE

**c't Hardcore**

- 32 Solarwechselrichter** Technik und Arbeitsweise
- 128 Malware filtern** per TLS-Inspektion
- 132 OPNsense-Firewall** als TLS-Inspektor einrichten

# Leserforum

## Nicht alles aufs Smartphone

*Karten digitalisieren für mehr Platz im Portemonnaie,*  
c't 3/2023, S. 18

Ist schon eine tolle Sache, was alles möglich ist. Das Smartphone entwickelt sich zu einem universellen Allroundgerät. Ich finde das auch gut, so eine Zentrale für fast alles zu haben. Wenn wir nun vieles aufs Handy verlagern, werden wir dann nicht vielleicht noch (fast hätte ich „total“ gesagt) abhängiger davon? Ich finde, man sollte einige parallele Wege dazu bestehen lassen, wenigstens in sicherheitsrelevanten Angelegenheiten.

Notizen 

## Leerer Akku, was dann?

Was Sie gegenüber allen Vorteilen des Smartphones überhaupt nicht erwähnen, ist dessen Nachteil: Wenn der Akku leer ist, kann ich damit nicht mehr bezahlen, mit der Plastikkarte immer. Deswegen sollte man meinem Ermessen nach immer eine Plastikkarte dabeihaben, sonst könnte es peinlich werden an der Kasse. Wenn das Smartphone in einem Cover steckt, kann man darin meist eine Plastikkarte unterbringen, dann wäre der Fallback auch immer dabei.

Benno Kardel 

## Wunschdenken

*Die elektronische Krankschreibung läuft holprig an,*  
c't 3/2023, S. 34

Irgendwelche Schönschwätzer stellen sich hin und verlautbaren die schöne neue Welt der Digitalisierung. Wir haben täglich damit zu tun und stellen immer wieder fest, dass dieses Schöne-neue-Welt-Konstrukt zu einem großen Teil nur aus Wunschdenken auf dem Papier besteht.

Ich mag schon gar nicht mehr zählen, wie oft der Start der einen oder anderen „Killerapplikation“, die den absoluten Arbeitersparnis-Durchbruch für Krankenkassen und Ärzte bringen sollte, verschoben wurde, weil weder die technischen Voraussetzungen gepasst haben noch die entsprechende Infrastruktur stabil vorhanden war.

Zum Schluss ist bis jetzt immer nur eines dabei herausgekommen: noch mehr

Verwaltungsaufwand für den Arzt, noch mehr Kosten für die einzelne Praxis, noch mehr Richtlinien und Gesetze zur Erzwingung der Umsetzung, noch mehr Bürokratie. Noch mehr Kosten für die Versicherten und Steuerzahler, die den ganzen unausgegorenen Unfug mit ihren Beiträgen finanzieren müssen.

Dieter Hoffmann 

## Besser direkt

*Web-Tipps: Spende statt Schokolade,* c't 3/2023,  
S. 48

Ich verstehe den Hinweis auf ThankU nicht. Warum brauche ich einen Zwischenhändler, der bis zu 20 Prozent von der Spende einbehält, statt direkt auf die entsprechende Organisation zu verweisen? Ein entsprechender Mehrwert fehlt eindeutig. Viele Organisationen bieten eigene Online-Spendenaktionen an. Einen Link oder eine Bankverbindung kann ich auch so posten.

Andreas Linnemann 

## SSD gerettet

*Zwanzig M.2-SSDs mit PCIe 3.0 und 4.0 im Test,*  
c't 2/2023, S. 116

Der Artikel war für mich extrem hilfreich, insbesondere die Informationen zu „Read Rate Degradation“. Meine Frau klagte seit einigen Wochen darüber, dass ihr PC häufig sehr langsam reagiert.

Meine Untersuchungen ergaben teilweise sehr geringe Transferraten der System-SSD. Die SMART-Werte sahen nach meiner Einschätzung gut aus. Da die Performancewerte nach H2testw-Lesetest jedoch teils sehr geringe Leseraten zeigten, plante ich den Ersatz der SSD. Mit den Informationen aus dem Artikel und der Anwendung von DiskFresh auf die gesamte SSD konnte ich das Problem stattdessen schnell, einfach und kostenlos beheben.

Jürgen Dreßler 

## Wie bei den Musikdiensten

*Abo-Videostreamingdienste im Vergleich,* c't 3/2023,  
S. 52

Mich erinnern die Dienste – und vor allem auch die Vielfalt – mittlerweile an die

Musikdienste, welche in den Nullerjahren vorhanden waren. Getrieben vom illegalen Download über Napster in den 90ern hatte jedes Musikstudio seinen eigenen Dienst etabliert, sodass Künstler A bei Anbieter X und Künstler B bei Anbieter Y vorhanden war. Über eine Dekade später gibt es Dienste, welche alle Künstler und Kataloge mit 100 Millionen Titeln für rund 10 Euro anbieten.

Ich werde dem Verwertungswahnsinn der Dienste nicht hinterherlaufen. Wer ein mittlerweile normales 4K-TV-Gerät voll ausnutzen will und eine breite Auswahl möchte, muss 200 Euro im Monat berappen. Sinnvoll wäre ein Metadienst für viele oder alle Studios mit globaler Suche über alle Inhalte, in einer schicken Oberfläche verpackt.

Mit dem würde endlich aus dem Streaminganbieter wieder ein Streaminganbieter (und kein Contentlieferant). Dann würden nur noch Aufmachung, leichte Zugänglichkeit und der Preis zählen, da der Katalog überall gleich ist. Außerdem würde illegalen Downloadportalen damit der Boden entzogen. Es dauert noch etwas, aber ich kann warten.

Marco Hoh 

## Keine Begeisterung

*Affinity V2: Bildbearbeitung, Grafikdesign und DTP,*  
c't 3/2023, S. 74

Ich nutze Affinity Photo und Designer seit 2016 sowie Publisher seit 2019, alles insgesamt mit recht guter Zufriedenheit. Begeisterung für Version 2 ist allerdings keine aufgekommen. Die funktionalen Fortschritte rechtfertigen eigentlich kein Major Release, und die Vorteile der inneren Programmstruktur sind bislang nach außen kaum aufgefallen. Im Gegenteil, an einigen Stellen hat es sogar funktionale Rückschritte gegeben.

## Fragen zu Artikeln

 Mail-Adresse des Redakteurs  
am Ende des Artikels

 Artikel-Hotline  
jeden Montag 16-17 Uhr  
05 11/53 52-333



# LIQUID FREEZER II SERIE

Am 23. August 2022 informierten wir durch eine Pressemitteilung, dass wir im Rahmen unserer routinemäßigen Qualitätskontrollen bei bestimmten Liquid Freezer II ein möglich auftretendes Problem festgestellt haben. Jeder betroffene Kühler muss umgebaut werden. Der Umbau beinhaltet das Austauschen der Kupferkühlplatte sowie der Dichtung.

[VIDEO](#)

Weiterhin ist es uns sehr wichtig, dass so viele betroffene Kunden wie möglich davon erfahren und ihren Kühler entsprechend umrüsten können.

Jeder betroffene Kunde erhält kostenfrei ein Service-Kit für den Umbau.

Der Austausch erfolgt in wenigen Schritten, bedarf keinerlei technische Fähigkeiten und ist in diesem Video zu sehen:



youtu.be/09ryTvguaw8

Wir bitten darum, dass Kunden, die einen Liquid Freezer II im Zeitraum Mai 2021 bis Mai 2022 erworben haben, das Formular auf unserer Webseite nutzen. Mit dem Formular kann schnell und einfach überprüft werden, ob ein Modell betroffen ist sowie das kostenlose Service-Kit angefordert werden.



arctic.de/lf-service-kit



[Hier geht es zum Formular, um das kostenfreie Service-Kit zu erhalten:](#)

Gerne hilft unser Service-Team beim Umbau und jeglichen Fragen.

Bitte kontaktieren Sie uns unter [lf-service@support.arctic.de](mailto:lf-service@support.arctic.de)

Uns ist bewusst, dass die Lösung des Problems ohne die Mitarbeit unserer Kunden in den letzten Monaten so nicht möglich gewesen wäre. Dafür möchten wir uns bedanken!



Gravierend ist allerdings die Schwäche in der Produktstrategie von Serif. Wenn man sich die Software-Suite von Adobe als Referenz ansieht, kommt man nicht daran vorbei, dass für den Fotografen stets Lightroom mit der Bilderverwaltung der Dreh- und Angelpunkt ist. Man kommt – zumindest, wenn man mehr als ein Foto macht – auch mit Affinity Photo nicht ohne Lightroom aus, denn Serif hat dazu bislang nichts Vergleichbares zu bieten und in dem Bereich offensichtlich auch nichts vor.

Da das letzte Update einer Lightroom-Kaufversion von 2017 stammt, ist das Ende absehbar: Man muss auf das Adobe-Abo wechseln und da ist Photoshop schon dabei und somit Affinity Photo entbehrlich.

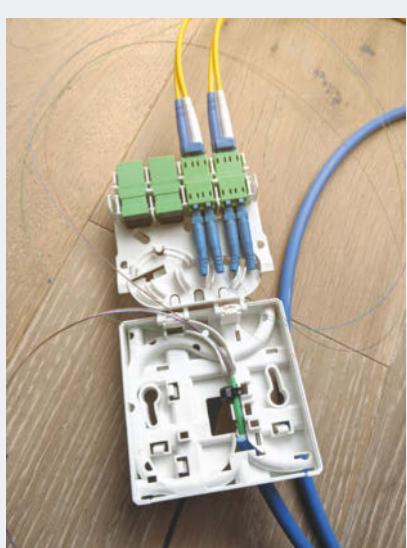
Rainer Böhm

## Das entfritzte Heim

*Erfahrungsbericht: Abschied von der Fritzbox, c't 3/2023, S. 146*

Manche Punkte aus dem Bericht kommen mir von meinem Netzwerk bekannt vor. Und wenn dann die Bandbreite im Haus für manche Netzwerktätigkeiten zu knapp wird, kann man mit Glasfaser, dem Leerrohr vom Telefonkabel und ein bisschen Werkzeug aus China größere Verbesserungen schaffen.

Thomas Genser



c't-Leser Thomas Genser hat bei sich im Haus Glasfaser gelegt, um mehr Bandbreite zu erreichen.

## Alternative

Ich benutze seit mehreren Jahren [Anm. d. Red.: die Firewall] Sophos UTM mit dahinter geschalteter Fritzbox 7530 und bin sehr zufrieden mit dieser Lösung. Für private Nutzer gibt es die Lizizenzen ohne Kosten. Man muss allerdings in die Hardware investieren. Ich habe dafür ein von PC Engines angebotenes APU.2E4-Board (als Bundle) eingesetzt, das mit einigen Extras circa 250 Euro kostete. Sophos UTM arbeitet als professionelle Firewall, die Fritzbox dahinter für die Telefonie (SIP) und den WLAN-Zugang.

Reinhard Trebbow

## Auch per Internet

*PlayStation-Spiele auf das Steam Deck streamen, c't 3/2023, S. 164*

Man kann PlayStation Remote Play sogar über das Internet verwenden, also die Heimkonsole überallhin streamen. Das funktioniert auch mit Chiaki und dem Steam Deck. Auf Reddit hat sich jemand die Mühe gemacht, eine Anleitung abzutippen: Ganz einfach die von der PS für Remote Play verwendeten Ports in den Routereinstellungen weiterleiten.

audio pathikz

## Vorsicht bei FreeBSD

*Der Einplatinencomputer Hardkernel Odroid-H3 mit Intel Celeron N5105, c't 3/2023, S. 66*

Im Artikel wird unter anderem FreeBSD als mögliches Betriebssystem erwähnt. Allerdings hat FreeBSD seine Probleme mit Realtek-Netzwerkschnittstellen, sodass es bei höherer Netzwerklast gelegentlich geschieht, dass der gesamte Rechner stehenbleibt.

In der Praxis mag das selten auftreten, aber ich habe es mittlerweile bei zwei Rechnern beobachtet und durch Tausch gegen Intel-Karten beheben können. Und es wird in der FreeBSD-Community auch konkret von Realtek abgeraten.

Thomas Mack

## Bastellösung für Anschluss

In der Beschreibung zum Hardkernel Odroid H3 monieren Sie, dass die SATA-Stromanschlüsse proprietär seien. Das sind stinknormale 4-polige JST-XH-Anschlüsse, passende Gegenstücke bekommt man bei den

## Wir freuen uns über Post

✉ redaktion@ct.de

✉ c't Forum

✉ c't Magazin

✉ @ctmagazin

Ausgewählte Zuschriften drucken wir ab. Bei Bedarf kürzen wir sinnwährend.

Antworten sind kursiv gesetzt.

👤 **Anonyme Hinweise**  
<https://heise.de/investigativ>

meisten einschlägigen Elektronikanbietern und Auktionshäusern für wenige Cent.

Stephan

*Die Formulierung „proprietary Anschlüsse“ war irreführend. Aber auch wenn das standardisierte Steckverbinder sind, liefert außer Odroid keine andere Firma Kabel mit diesen JST-XH-Steckern auf der einen und SATA-Stromsteckern auf der anderen Seite. Mit Ihrem Hinweis kann man sich aber aus einem billigen SATA-Stromkabel mit Molex- oder Floppy-Stecker auf der anderen Seite ein passendes Kabel basteln, indem man einen JST-XH-Stecker anlötet oder ancrimpt.*

## Ergänzungen & Berichtigungen

### Erstattung nur bei Privatpatienten

*Die elektronische Krankschreibung läuft holprig an, c't 3/2023, S. 34*

Ärzte erhalten nur bei Privatpatienten eine Erstattung von 5,36 Euro pro Arbeitsunfähigkeitsbescheinigung. Bei den gesetzlichen Krankenkassen bekommen Ärzte keine gesonderte Vergütung. Dort sind die Bescheinigungen in den sogenannten Behandlungspauschalen enthalten.

### Intel-Xeon-CPUs mit AMX

*Intels neue Xeon-Prozessoren für Server und Rechenzentren, c't 3/2023, S. 40*

Die Advanced Matrix Extensions heißen abgekürzt AMX und nicht AMD, wie wir versehentlich schrieben.

- Komponieren Sie Ihren eigenen Code
- Orchestrieren Sie Ihre Lizenzstrategie
- Stimmen Sie Ihren IP-Schutz genau ab
- Verbreiten Sie Ihr gestaltetes Werk

Klingt einfach, oder?  
Und das ist es auch  
mit CodeMeter

CM  
Dongle

CM  
LC

CM  
Certificate  
Vault

CM  
Embedded

CM



Starten Sie jetzt  
und fordern Sie Ihr  
CodeMeter SDK an  
[wibu.com/de/sdk](http://wibu.com/de/sdk)

+49 721 931720  
[sales@wibu.com](mailto:sales@wibu.com)  
[www.wibu.com](http://www.wibu.com)



SECURITY  
LICENSING  
PERFECTION IN PROTECTION



29.03.23

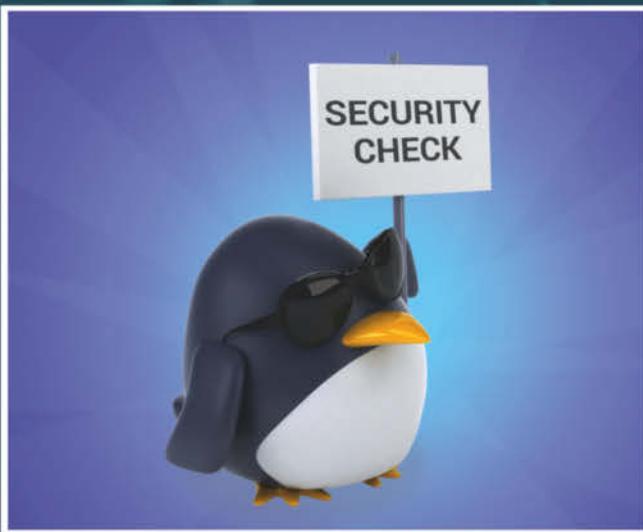
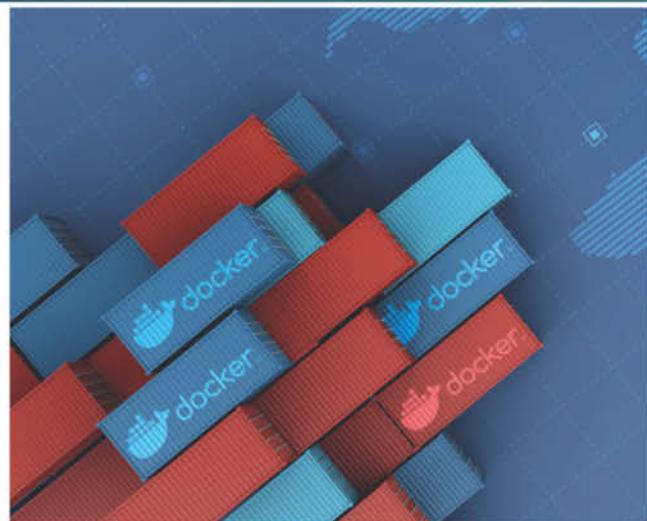
## Einführung in den Kea DHCP Server

Der Workshop gibt eine vollständige Einführung in die neue Kea-DHCP-Software auf Unix- und Linux-Systemen. Sie lernen, wie man das Kea-DHCP-System installiert, konfiguriert und wartet. Der Workshop beinhaltet auch eine Auffrischung des DHCPv4-Protokolls und erklärt DHCPv6 für IPv6-Netzwerke.

09. - 10.05.23

## Docker und Container in der Praxis

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



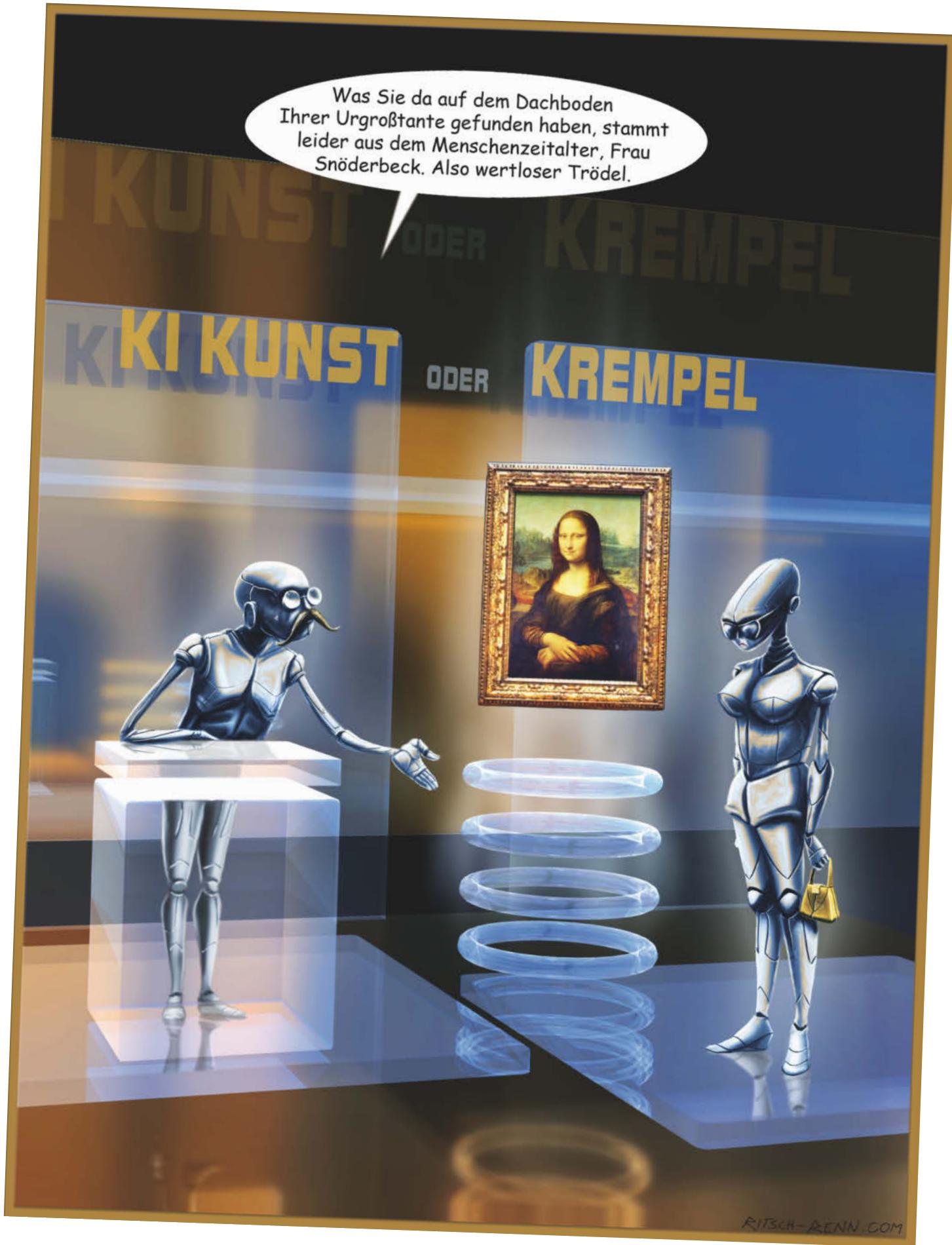
20. - 21.11.23

## Dienste mit SELinux absichern

SELinux einfach abzuschalten, wenn es Probleme gibt, ist üblich, aber unklug. Der zweitägige Workshop zeigt, wie man das System stattdessen so nutzt, dass alles besser abgesichert ist und trotzdem funktioniert.

Sichern Sie sich Ihren Frühbisher-Rabatt:  
[www.heise-events.de/workshops](http://www.heise-events.de/workshops)

Was Sie da auf dem Dachboden  
Ihrer Urgroßtante gefunden haben, stammt  
leider aus dem Menschenzeitalter, Frau  
Snöderbeck. Also wertloser Trödel.



Weitere Schlagseiten auf [ct.de/schlagseite](http://ct.de/schlagseite)

# Das Ende der Trefferlisten?

## Suchmaschinen beantworten Fragen mithilfe von KI

**Sprachmodelle wie ChatGPT beantworten viele Fragen – aber nicht immer korrekt. Trotzdem will Microsoft seine Suchmaschine Bing mit ChatGPT verheiraten. Einige Suchdienste liefern schon heute mit Sprachmodellen maßgeschneiderte Antworten auf Anfragen.**

Von Jo Bager

**M**icrosoft will laut Medienberichten zehn Milliarden US-Dollar in das Unternehmen OpenAI investieren, unter anderem, um dessen KI-Sprachmodell ChatGPT in seine Suchmaschine Bing zu integrieren. Auch wenn sich Microsoft bisher in Schweigen darüber hüllt, wie es in die Suchmaschine eingebettet werden soll, führt die Meldung unter Beobachtern zu angeregten Diskussionen: Kann Google nun einpacken oder ist eine solche Integration Unfug?

Zunächst spricht einiges dagegen, Sprachmodelle für die Internetsuche zu nutzen. So liefern ChatGPT & Co. gerne mal frei erfundenes statt Fakten. Und sie ermöglichen es den Nutzern nicht einmal, die Angaben zu prüfen, weil sie für gewöhnlich nicht ihre Quellen nennen. Abgesehen davon ist ihr Wissensstand nicht aktuell. Sprachmodelle werden bis zu einem bestimmten Zeitpunkt mit Texten gefüttert, danach nicht mehr. Zu allem, was sich danach ereignet, können sie keine Angaben machen.

Der Datenbestand von ChatGPT zum Beispiel ist laut OpenAI auf dem Stand von Anfang 2022. Wenn ChatGPT vereinzelt Informationen kennt, die es später gelernt haben muss – etwa, dass Elon Musk der CEO von Twitter ist –, so ist das nur eine Ausnahme von dieser Regel. Wer den Dienst nach dem brasilianischen Präsidenten fragt, erhält die falsche Antwort Jair Bolsonaro.

Suchmaschinen funktionieren seit über zwanzig Jahren mehr oder weniger nach dem gleichen Prinzip: Auf eine Suchanfrage hin stellen sie eine Liste von Links zusammen, von denen sie annehmen, dass diese für die Anfrage relevant sind. Diese Links stammen aus einem Index, den sie mit sogenannten Crawler-Programmen angelegt haben. Ein solcher Index ist viel aktueller als der Datenbestand eines Sprachmodells.

### Crawler, Index, Liste

Auch Suchdienste versuchen, Anfragen direkt zu beantworten, wo das für sie möglich ist. Dazu bauen sie sogenannte One-Boxes auf den Suchergebnisseiten ein, besondere Suchergebnisse für bestimmte Fragen. Allerdings gibt es solche Boxen nur für einen Bruchteil der Suchanfragen.

Könnte eine Suchmaschine die Vorteile der beiden Welten vereinen – maßgeschneiderte, ausformulierte Antworten einerseits, Aktualität und Überprüfbarkeit andererseits – käme das einer Revolution der Internetsuche gleich. Mehrere Suchdienste zeigen, dass das möglich ist. Perplexity AI, You.com und Neeva.com liefern ausformulierte Antworten im ChatGPT-Stil, zu denen sie ihre Quellen mit angeben. Der Benutzer kann so die Herkunft der Informationen überprüfen.

Die drei Suchdienste sind allesamt noch nicht ausgereift und funktionieren derzeit nur für englische Suchanfragen. Perplexity AI und You.com betreiben ihre Antwortmaschinen zudem losgelöst von ihren normalen Suchergebnisseiten. Perplexity AI präsentiert nur Freitextantworten und überhaupt keine klassischen Link-

The screenshot shows a search interface for 'Who is the brasilian president?'. The results are categorized under 'PERPLEXITY'. The main text states: 'Jair Bolsonaro is the current President of Brazil<sup>[1]</sup>. He was elected in 2018<sup>[2]</sup> and took office in 2019<sup>[1]</sup>. Prior to him, Luiz Inácio Lula da Silva served as President from 2003–2010<sup>[3]</sup>.'. Below this, under 'SOURCES', are links to britannica.com, npr.org, and go.com. At the bottom, there are 'CONTINUE READING' links for 'Brasil president election', 'Brasil president impeachment', and 'who is the current president of Brasil'.

Perplexity AI liefert maßgeschneiderte Antworten inklusive der Quellen – die Antworten sind aber nicht immer up to date.

listen. In unseren Versuchen lieferte der Suchdienst außerdem teilweise veraltete Angaben, etwa über den aktuellen Präsidenten von Brasilien. You.com ist eine noch recht neue, „klassische“ Suchmaschine. Zusätzlich ist im Dezember You-Chat gestartet, das Antworttexte mit einem Sprachmodell generiert. Es läuft alternativ zur althergebrachten Suche.

## Index füttert Sprachmodell

Am stimmigsten hat Neeva seine Chat-GPT-artige Antwortmaschine in seinen Suchdienst integriert. Bei vielen Suchanfragen zeigt deren Funktion NeevaAI auf der Ergebnisseite eine Box mit der dynamisch von einer KI verfassten Antwort mitsamt der Quellen an. Wer zum Beispiel nach „Twitter Files“ sucht, erhält als Antwort: „The Twitter Files are a series of documents released by Twitter owner Elon Musk that provide insight into the company’s content moderation decisions. The documents have revealed that the CIA has been meddling in Twitter’s internal content moderation for years. They have also shown that the U.S. military has been directly assisted by Twitter.“ Dazu verlinkt NeevaAI die Quellen CBS News, MSN.com, Fox News und NY Post.

Welche Fragen Neeva mit Freitext beantwortet und wo es den NeevaAI-Text platziert, entscheidet der Dienst automatisch, genauso wie für andere Inhalte, die es in die Suchergebnisseiten integriert – Bilder, Videos und Wikipedia-Kästen. Wer zum Beispiel „Eiffel Tower“ ins Suchfeld tippt, erhält zuerst einen Link auf die offizielle Homepage des Turms, dann eine Karte und dann erst die KI-Antwort. Einen Auszug aus dem Wikipedia-Eintrag über den Eiffelturm stellt Neeva rechts daneben.

Anders als viele andere Suchdienste, die nur Ergebnisse von Google oder Bing durchreichen, betreibt Neeva einen eigenen Suchindex. Offenbar ist dieser eigene Index eine der Grundlagen dafür, NeevaAI so nahtlos in die Suche zu integrieren. Zum Beantworten einer Anfrage verwendet Neeva gleich mehrere Sprachmodelle, wie Sridhar Ramaswamy, CEO des Dienstes, im Gespräch mit c’t erklärte. Nach der Eingabe der Suchanfrage bestimmt zunächst ein Sprachmodell die Absicht des Nutzers und ergänzt die Anfrage mit Synonymen, rechtschreibkorrigierten Wörtern und verwandten Ausdrücken. In seinem Blog beschreibt Neeva die Anpassung der Anfrage und NeevaAI im Detail und

The screenshot shows the Neeva search interface for the query "Reichstag". The results page includes a sidebar with "Related Searches" and a "Get Neeva for Vivaldi" button. The main content area shows a summary of the Reichstag building, a map of its location in Berlin, and a snippet from Wikipedia.

**NeevaAI verfasst einen maßgeschneiderten Text, den die Suchmaschine mit den anderen Inhalteboxen auf der Suchergebnisseite anzeigt.**

bietet Feedback-Möglichkeiten, falls man Fehler findet.

Nachdem NeevaAI die Anfrage des Nutzers analysiert und umgeschrieben hat, ruft es die Inhalte der relevantesten Seiten ab und baut daraus eine Antwort zusammen – meist einen Absatz lang. Die von der KI generierte Antwort lädt in der Regel ein wenig langsamer als der Rest der Suchergebnisseite – aber meist deutlich schneller als bei der derzeit arg überlasteten ChatGPT-Homepage. NeevaAI ist im Moment nur für Nutzer mit einem US-amerikanischen Account verfügbar – wer hierzulande NeevaAI ausprobieren möchte, kann seinen Account in den Einstellungen einfach entsprechend umschalten.

## Werbefrei und abofinanziert

Dass Neeva eine derart ausgefeilte Antwortmaschine betreibt, ist umso erstaunlicher, als dass Neeva als junges Suchmaschinen-Start-up gerade einmal 50 Mitarbeiter beschäftigt. Neeva soll in einer Basisversion inklusive NeevaAI dauerhaft werbefrei und kostenlos bleiben. Geld verdienen will das Unternehmen mit kostenpflichtigen Accounts. Diese sollen auch bei Clouddiensten liegende Daten durchsuchen, außerdem gehören Dienste von Fremdanbietern dazu, etwa das Bitdefender-VPN und der Passwortmanager Dashlane.

Google ist mit Sicherheit eines der Unternehmen mit der größten Expertise in KI. Der Branchenprimus verfolgt mehrere Ansätze, KI in seine Suche zu integrieren. Das BERT-Sprachmodell (Bidirektionale Encoder Darstellungen von Transformers) etwa, das Neeva für die Vorbehandlung der Suchanfragen verwendet, ist ursprünglich von Google entwickelt worden und bearbeitet auch dort Anfragen vor. Und auch Google hat einen Chatbot: LaMDA – Language Model for Dialogue Applications. Eine derart stimmige Integration der Sprachmodelle in die Suchmaschine wie Neeva hat Google aber bisher nicht gezeigt.

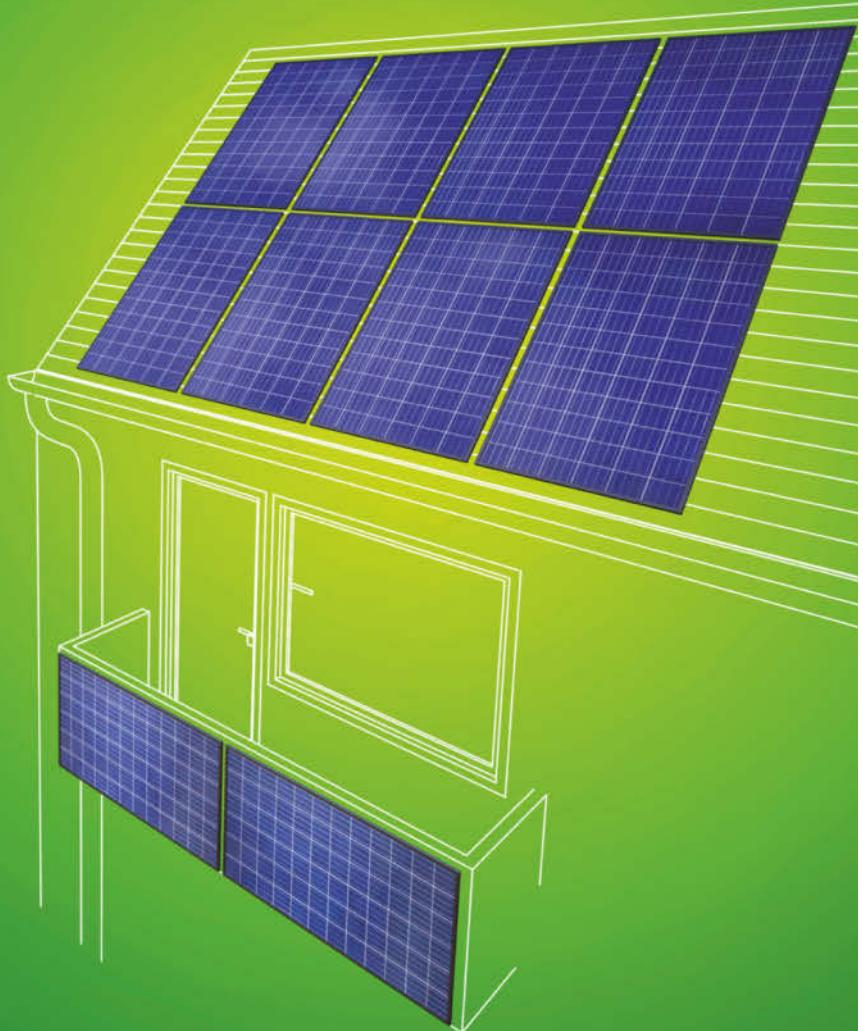
Google steht ohnehin unter Druck in seinem zentralen Geschäftsfeld, der Suche. So kommen junge Menschen immer seltener auf die Idee, bei Google zu suchen, sondern nutzen stattdessen TikTok oder Instagram. Das habe eine interne Studie ergeben, wie ein Google-Manager erklärte (siehe c’t 18/22, S. 40). Und jetzt erwächst zusätzlich noch Konkurrenz durch andere Suchdienste, die statt einer Liste von Links eine fertig ausformulierte Antwort zur Suchanfrage präsentieren können: 2023 könnte das Jahr werden, in dem sich Suchmaschinen so stark verändern wie lange nicht mehr.

(jo@ct.de) ct

**Blog-Posts zu NeevaAI: ct.de/yx4d**

# Solarstrom für alle

Rechtliche, technische und finanzielle  
Rahmenbedingungen für die eigene PV-Anlage



<b>Solarstrom für alle .....</b>	<b>Seite 14</b>
<b>Balkonkraftwerke: Der aktuelle Stand .....</b>	<b>Seite 20</b>
<b>Ab aufs Dach .....</b>	<b>Seite 24</b>
<b>Wie Solarwechselrichter arbeiten .....</b>	<b>Seite 32</b>

# Die Anschaffung einer Photovoltaikanlage lohnt sich immer. Doch aktuell ist es schwer, jemanden zu finden, der sie aufbaut. Warum also nicht selbst zum Installateur werden? Selber bauen ist nicht Ihr Ding? Hier lernen Sie auch alles Wissenswerte, um dem Profi auf die Finger zu schauen oder ihm Arbeit abzunehmen.

Von Georg Schnurer

**J**etzt dürfte nahezu jeder Post vom Energieversorger bekommen haben: Der alte Tarif läuft aus und Strom wird teurer. Begründet wird das in der Regel mit gestiegenen Einkaufspreisen an den Strombörsen. Deshalb – so schreibt mir etwa mein aktueller Stromlieferant, die Naturstrom AG – steigt der Preis für die Kilowattstunde nachhaltigen Ökostroms von ehemals 37 auf stolze 57 Cent.

Tatsächlich ist der mittlere Strompreis für Privathaushalte seit Oktober 2021 stark gestiegen. Zahlte man im Oktober 2021 noch durchschnittlich 32 Cent pro Kilowattstunde (ct/kWh), waren es im Mai 2022 bereits 39 ct/kWh und im Oktober 2022 folgte dann das Allzeithoch von 54 ct/kWh. Für Sparfüchse lautet das Gebot der Stunde: Preise vergleichen und Strom sparen. Ein Blick auf die Strompreisvergleichsportale gibt erste Orientierung, sollte aber nicht die einzige Basis für die Wahl des Stromlieferanten sein. Mitunter fehlen dort die Tarife der örtlichen Grundversorger, die inzwischen durchaus konkurrenzfähig sein können. Auch wichtig: Vertragslaufzeiten und Preisgarantien im Auge behalten und sich nicht von einmaligen Boni blenden lassen.

Meine Empfehlung für den Tarifwechsel in turbulenten Zeiten wäre ein Vertrag mit einer einjährigen Preisgarantie und idealerweise der gleichen Laufzeit. Kürzere Preisgarantien schützen nicht vor Kapriolen am Strommarkt. Längere Preisgarantien gibt es nur selten und man bezahlt dafür meist einen erheblichen Aufpreis. Tarife mit Vorkasse oder Kautionskasse sollte man grundsätzlich meiden – die

Vergangenheit hat gezeigt, dass das Geld weg ist, wenn der Anbieter plötzlich in die Pleite schlittert.

## Eigener Strom

Nach der Tarifoptimierung lohnt es sich, über die Anschaffung einer eigenen Photovoltaikanlage nachzudenken. Das kann ein kleines Balkonkraftwerk, aber natürlich auch eine größere Anlage sein. Überall, wo die Sonne weitgehend ungehindert scheinen kann, lässt sich meist auch ein Solarpanel unterbringen. Ideal sind Flächen mit Südausrichtung, aber auch Dächer und Balkone mit Ost- oder West-Ausrichtung eignen sich fürs eigene Solar-kraftwerk.

Sind passende Flächen verfügbar, folgt die Kosten-Nutzen-Analyse. Eine moderne PV-Anlage in Deutschland erzeugt übers Jahr gerechnet zwischen 800 und 1000 kWh pro installierter Nennleistung. Diese wird in der Einheit „kW Peak“ gemessen und in der PV-Szene physikalisch nicht korrekt als kWp abgekürzt. Ein typisches Balkonkraftwerk mit einer Nennleistung von 600 Wp sammelt in einem Jahr zwischen 480 und 600 kWh elektrischer Energie ein. Wird der Strom komplett im Haushalt verbraucht, ent-

spricht das einer Jahresersparnis von 192 bis 240 Euro (Strompreis 40 ct/kWh). Ein Balkonkraftwerk besteht in der Regel aus zwei PV-Modulen für etwa 400 Euro. Hinzu kommt noch ein 600-Watt-Wechselrichter (120 bis 180 Euro) sowie Kabel und Installationsmaterial für etwa 80 Euro. Komplettsysteme werden für knapp 700 Euro angeboten. Die Investition in Höhe von 600 bis 700 Euro hat sich in zweieinhalb bis dreieinhalb Jahren amortisiert. Wer die Möglichkeit hat, sollte sich deshalb so ein Mini-Kraftwerk zulegen.

Der Installationsaufwand ist überschaubar und auch die vorgeschriebene Anmeldung beim Marktstammdatenregister geht leicht von der Hand. Etwas mehr bürokratischen Aufwand verursacht die Anmeldung beim Netzbetreiber. Doch hier bröckelt die Front der Verhinderer so langsam – mehr zu Balkonkraftwerken, deren Installation und den sich anbahnen den Erleichterungen bei der Inbetriebnahme finden Sie im nachfolgenden Artikel ab Seite 20.

## Groß denken

Wer Platz für eine größere PV-Anlage hat, muss seine Investition sorgfältiger planen. Auch bei einer typischen Dachanlage rechnet man mit einem jährlichen Ertrag von 800 bis 1000 kWh pro kWp. Der Installationsaufwand ist hier aber höher. Zudem muss bei der Inbetriebnahme ein Elektriker mithelfen. In der Regel beauftragt man deshalb eine spezialisierte Firma mit der Installation der Anlage. Blind auf die Empfehlungen des Solaranlagenbauers verlassen sollte man sich aber nicht. Deshalb lohnt es sich, selbst einige grundlegende Dinge über moderne PV-Anlagen zu wissen.

Das geht schon mit der Wirtschaftlichkeitsrechnung los: So erzeugt eine typische private PV-Anlage mit einer Leistung von knapp 10 kWp zwar im Jahr bis zu 10 MWh (10.000 kWh) Energie, doch diese selbst zu verbrauchen, klappt kaum. Gerade im

**Nach dem Allzeithoch im Oktober 2022 pendelt sich der mittlere Strompreis für Privathaushalte mit einem jährlichen Verbrauch von 4000 kWh aktuell bei etwa 48 ct/kWh ein.**

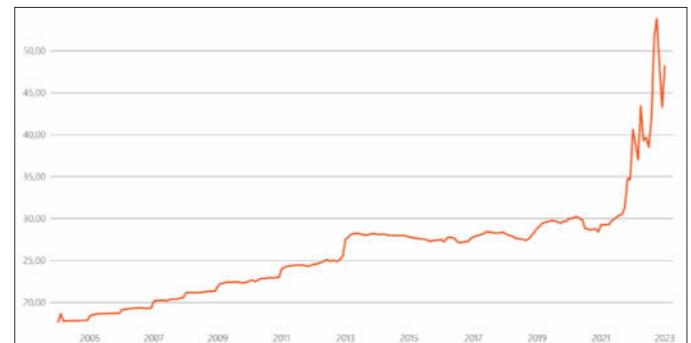
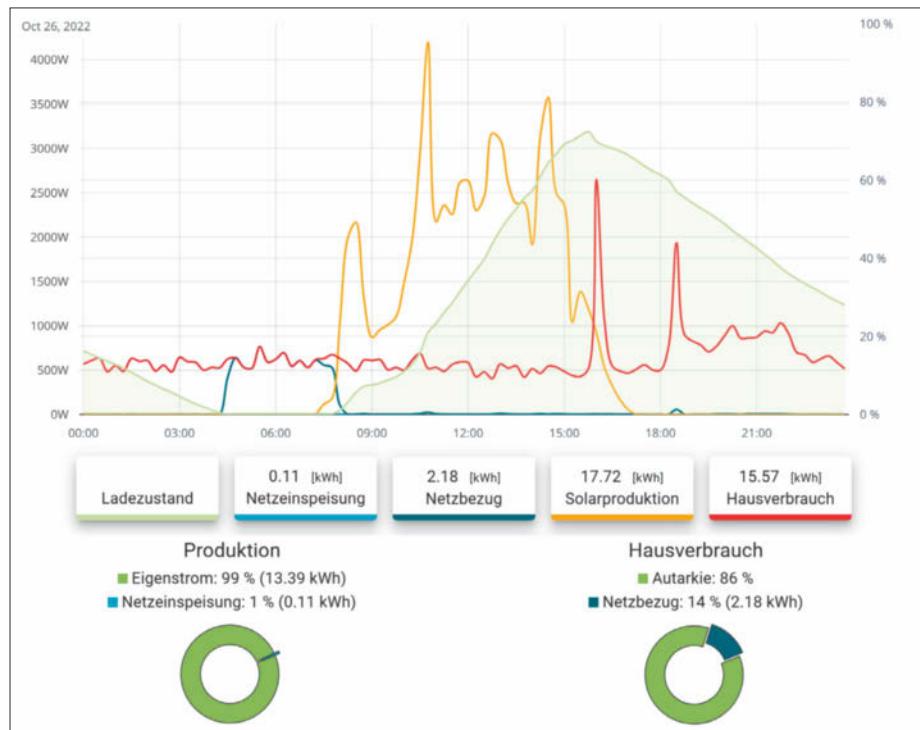


Bild: Verivox



**Ein typischer Tag im Oktober: Die Sonne wurde teilweise von Wolken verdeckt, deshalb füllte sich der Speicher über den Tag nur zu gut 70 Prozent.**

Sommer, wo die Anlage etwa 80 Prozent ihrer Energie produziert, fließt ein großer Teil des über den Tag gewonnenen Stroms ins öffentliche Netz. Dieser wird aber für neue Anlagen nur mit 8,2 ct/kWh vergütet.

Es lohnt sich deshalb fast immer, der PV-Anlage auch noch einen Speicher zu spendieren. Dieser speichert die tagsüber produzierte überschüssige Energie und gibt sie nach Sonnenuntergang wieder ab. Solarspeicher sind aber ein teurer Spaß – pro kWh Kapazität muss man mit Kosten zwischen 700 und 1200 Euro rechnen. Zu groß heißt deshalb meist auch zu teuer. Über den Daumen gepeilt, sollte ein PV-Speicher knapp die halbe Nennkapazität der PV-Anlage haben. Wer seinen Bedarf genauer berechnen will, ermittelt zunächst den Grundverbrauch von Haus oder Wohnung und wählt den Akku so groß, dass dieser 12 Stunden lang Strom liefern kann.

Zu theoretisch? Nun, in meinem Haushalt mit sieben Personen haben wir uns für eine PV-Anlage (Ost-West-Dach) mit einer Maximallistung von knapp 16 kWp entschieden. Dieser steht ein Akku mit 10 kWh zur Seite. Unser nächtlicher Grundverbrauch liegt bei gut 600 Watt. Rechnerisch würde also ein Akku mit 7,2 kWh ausreichen, um die sonnenlose Zeit zu überbrücken. Trotzdem schaffen wir es auch im Sommer immer mal wieder, den 10-kWh-Akku leer zu saugen – da wird abends aus-

giebig gekocht, der Server läuft und wenn dann auch noch alle Mitbewohner ihre PCs einschalten, sind die 10 kWh schon vor Sonnenaufgang verbraucht. Trotzdem lohnt sich kein größerer Akku, denn für den zusätzlichen Puffer entstünden uns, verglichen mit dem eingesparten Strom vom Energieversorger, unverhältnismäßig hohe Kosten.

PV-Akkus gibt es in zwei grundverschiedenen Ausführungen: AC- oder DC-gekoppelt. DC-gekoppelte Speichersysteme hängen in der Regel direkt am Wechselrichter und werden von der Gleichspannung der PV-Anlage versorgt. Oft sind sie schon in den Wechselrichter integriert – der heißt dann „Hybrid-Wechselrichter“, weil er auch noch den Akku verwaltet. Die Integration des Akkus bringt den Vorteil, dass der Wechselrichter den Akku direkt und ohne große Verluste be- und entladen kann. Dafür sind DC-gekoppelte Akkus nur erweiterbar, wenn der Wechselrichterhersteller entsprechende Vorkehrungen getroffen hat.

AC-gekoppelte Speicher hängen hingegen im Wechselspannungskreis des Hauses. Deshalb eignen sie sich sehr gut, um PV-Anlagen nachträglich mit einem Speicher auszustatten. Sie enthalten einen eigenen Wechselrichter, der sowohl Energie aus dem Akku ins Hausnetz speist als auch bei Energieüberschuss im Hausnetz die Wechselspannung gleichrichtet und den Akku lädt. Damit beides stets zur rechten Zeit

passiert, muss der AC-gekoppelte Wechselrichter mit dem Wechselrichter der PV-Anlage kommunizieren. Durch die mehrfach entstehenden Wandlungsverluste haben PV-Anlagen mit AC-gekoppeltem Akku meist einen etwas schlechteren Wirkungsgrad als Anlagen mit Hybridwechselrichter.

### Viel hilft viel

Wie viele PV-Module man installiert, hängt von Platzangebot und Geldbeutel ab. Generell gilt hier: Viel hilft viel. Das liegt vor allem daran, dass Solarmodule in der trüben Jahreszeit gerade mal 20 Prozent ihrer Jahresleistung produzieren. Je mehr PV-Module vorhanden sind, desto höher ist die Autarkie auch im Winter.

Auch hier einige Zahlen aus meiner Praxis: Der Oktober 2022 war „golden“ und die PV-Anlage verhalf uns zu einem Autarkiegrad von 93 Prozent. Wir mussten also lediglich sieben Prozent Energie (42 kWh) zukaufen. Im Dezember sank der Autarkiegrad auf 17 Prozent, was uns zum Zukauf von 543 kWh zwang. Für den Januar sieht es mit einer Autarkie von 20 Prozent schon besser aus.

### String oder nicht?

Dach-PV-Anlagen arbeiten meist mit großen Wechselrichtern, die Anschluss für ein oder zwei sogenannte Strings bieten. Ein String besteht aus mehreren in Reihe geschalteten PV-Modulen. Dadurch addieren sich die Ausgangsspannungen der angeschlossenen Module und es entstehen schnell gefährlich hohe Gleichspannungen. Für jeden String bringt der Wechselrichter einen sogenannten MPP-Tracker (Maximum Power Point) mit. Dieser sucht kontinuierlich den optimalen Arbeitspunkt der angeschlossenen PV-Module, um den Ertrag zu maximieren. Alle an einem String angeschlossenen PV-Module sollten die gleiche Ausrichtung zur Sonne haben.

Die maximale Eingangsspannung eines Wechselrichters bestimmt, wie viele Module an einem String hängen dürfen. Um dennoch auch Anlagen mit vielen PV-Modulen zu bauen, bieten einige Wechselrichter die Möglichkeit, zwei Strings parallel auf einen MPP-Tracker zu schalten. Damit das funktioniert, müssen die parallel geschalteten Strings aber aus gleich vielen PV-Modulen bestehen – also die gleiche Maximalspannung aufweisen – und zusätzlich die gleiche Ausrichtung haben. Wer tiefer in die Arbeitsweise von Wechselrichtern und MPP-Trackern einsteigen will, kann das mit dem Beitrag ab Seite 32.

## Mikrowechselrichter

Der Gegenentwurf sind sogenannte Mikrowechselrichter, die bis zu sechs PV-Module ansteuern und im Idealfall für jedes Modul einen eigenen MPP-Tracker mitbringen. Mikrowechselrichter gibt es mit Wechsel- und Drehstromausgang (einphasig und dreiphasig). Sie lassen sich auf der AC-Seite einfach parallel schalten, was auch den Aufbau größerer PV-Anlagen erlaubt. Das ist freilich nur sinnvoll, wenn die Anlage sehr inhomogen ist. Je mehr PV-Module es mit gleicher Ausrichtung und Beschattung gibt, desto eher rentiert sich der Griff zum String-Wechselrichter. Zudem kosten viele Mikrowechselrichter in Summe mehr als ein großer String-Wechselrichter und haben einen schlechteren Wirkungsgrad. Bei kleineren Anlagen bieten die kleinen Geräte aber den Vorteil, dass man es beim Installieren nie mit hohen Gleichspannungen zu tun hat. Wie man so eine PV-Anlage mit zwei Mikrowechselrichtern selbst aufs Dach bringt und welche Tücken dabei lauern, beschreibt der Artikel auf Seite 24 ganz praktisch.

## Modultypen

PV-Module gibt es in sehr unterschiedlicher Ausprägung. Am günstigsten sind polykristalline Module. Ihr Wirkungsgrad liegt aber bei lediglich 15 bis 20 Prozent. Teurer, aber auch ertragreicher sind monokristalline Module mit einem Wirkungsgrad von bis zu 22 Prozent. Noch höhere Wirkungsgrade erreichen teure Tandem-Solarzellen. Sie bestehen aus mehreren Schichten, die jeweils andere Wellenlängen des Lichts in Energie umwandeln können. In der Summe sind mit dieser Technik Wirkungsgrade von bis zu 41 Prozent erreichbar, serienreife Tandem-Solarzellen liegen aktuell bei etwas über 30 Prozent Wirkungsgrad.

Neben starren PV-Modulen gibt es auch flexible und semiflexible Varianten. Sie eignen sich gut, um etwa Fahrzeuge zu bekleben, bieten aber einen Wirkungsgrad von nur zehn bis dreizehn Prozent. Ihre Lebensdauer ist mit 10 Jahren auch gering.

Im Massenmarkt dominieren derzeit PV-Module mit monokristallinen Solarzellen. Sie sind nur noch wenig teurer als polykristalline Modelle, bieten aber bei beschränktem Platzangebot eine höhere Energieausbeute. Die Lebensdauer eines aktuellen monokristallinen PV-Moduls wird auf bis zu 30 Jahre geschätzt.

Unterschiedliche Bauformen ermöglichen den flexiblen Einsatz von PV-Modulen. Auf dem Dach und am Balkon kommen



## Trauriger Solar-Sonntag: Kaum Sonne am Himmel und die halbe WG ist am Kuchenbacken.

typischerweise Module mit Aluminiumrahmen zum Einsatz. Sie sind robust, preiswert und leicht zu handhaben. Geht es um die Bedachung etwa von Carports, bieten sich Glas-Glas-PV-Module an. Hier befinden sich die PV-Zellen zwischen zwei gehärteten Glasscheiben. Die Stärke der beiden Glasscheiben variiert je nach Einsatzszenario zwischen 4 und 10 Millimeter. Glas-Glas-PV-Module sind deutlich schwerer und auch kostspieliger als Module mit Rahmen. Neben nahezu undurchsichtigen Modulen gibt es auch solche, die zwischen 30 und 40 Prozent Licht durchlassen. Sie eignen sich etwa als Terrassenüberdachung und werden von verschiedenen Herstellern angeboten. Für Wintergärten gibt es auch Glas-Glas-PV-Module als Isolierglas.

## Zweigesichtig

Eine weitere Variante monokristalliner PV-Module sind sogenannte bifaziale Module. Die arbeiten beidseitig und nutzen auch das Licht, das auf die Modulrückseite fällt. Dadurch erhöht sich der Wirkungsgrad um fünf bis 30 Prozent. Die Herstellung bifazialer Module erfordert aber zusätzliche Arbeitsschritte. So muss die Zellenrückseite poliert und passiviert werden. Dazu kommt ein Metallisierungsgitter mit ähn-

licher Struktur wie auf der Vorderseite. Da immer mehr Hersteller ihre Anlagen auf bifaziale Zellen umstellen, verringert sich der Preisunterschied zwischen monofazialen und bifazialen PV-Modulen aber stetig.

Ideale Bedingungen für bifaziale Module bieten Solarzäune, aber auch Carport-Dächer profitieren von dieser Technik. Bei einer typischen Dach- oder Fassadeninstillation ist der Zugewinn durch den Einsatz bifazialer Module eher gering.

Eine weitere Entwicklung bei monokristallinen Solarzellen sind Halbzellen. Sie bestehen aus den gleichen Materialien wie normale Solarzellen, werden nach der Produktion aber in zwei Hälften geschnitten. Das Teilen der Zellen halbiert den durch die Zelle fließenden Strom. Dadurch verringern sich die Leistungsverluste in einer Halbzelle um den Faktor 4 ( $P_v = R \times I^2$ ). Die geringere Verlustleistung innerhalb der Zellen verbessert den Temperaturkoeffizienten, sodass Halbzellenmodule bei hohen Temperaturen bessere Leistungen erbringen können. Ein Halbzellen-Solarmodul besteht dann aus 120 statt der sonst üblichen 60 Solarzellen. Der zusätzliche Raum zwischen den Zellen verstärkt Reflexionen innerhalb des Laminats und erhöht so die Lichtnutzung

in der Zelle. Unterm Strich sind PV-Module mit Halbzellen bei gleicher Größe etwa zwei bis drei Prozent leistungsfähiger als Module mit Vollzellen. Weil Halbzellenmodule inzwischen bereits günstiger sind als Vollzellenmodule werden diese langsam aus dem Markt gedrängt.

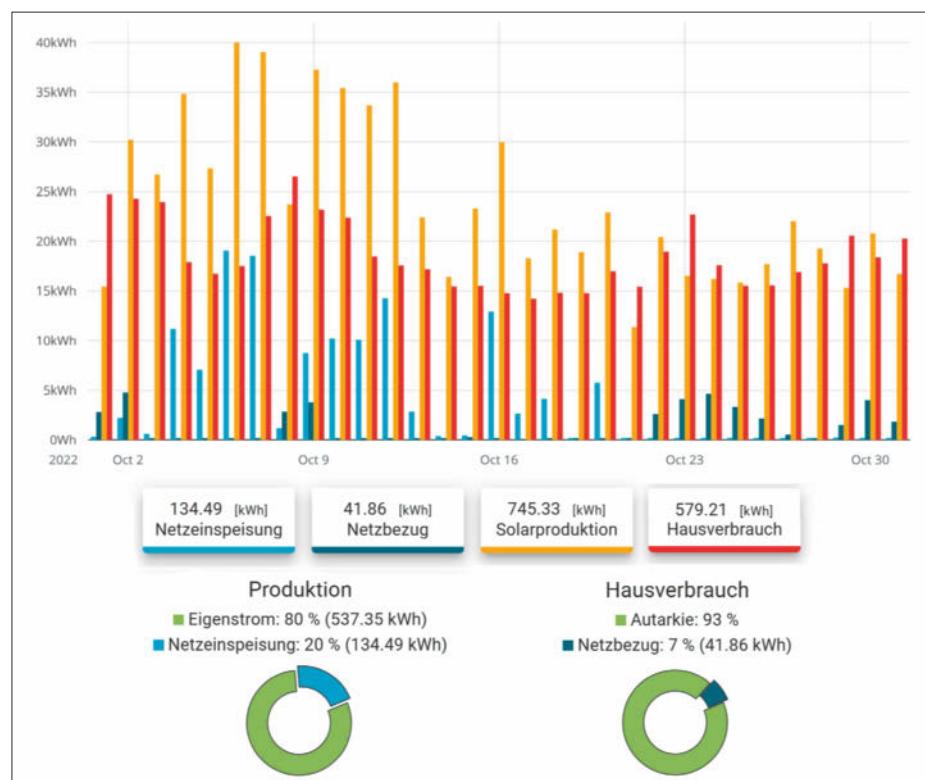
## Hürdenlauf

Auch wenn die Ampelkoalition inzwischen einiges getan hat, um den Bau privater PV-Anlagen zu unterstützen, gibt es nach wie vor einige Stolpersteine. So hat der Wegfall der Mehrwertsteuer für PV-Komponenten zum 1. Januar zwar die Preise gesenkt, doch nach wie vor gibt es lange Wartezeiten, bis die Anlage auf dem Dach liegt und in Betrieb gehen kann. Wer heute ein Angebot einholt, sollte mit mehreren Monaten Wartezeit bis zum Baubeginn rechnen.

Steht die Anlage, muss man sie im Marktstammdatenregister der Bundesnetzagentur eintragen und beim örtlichen Netzbetreiber anmelden. Die Registrierung im Marktstammdatenregister ist mit etwas Schützenhilfe vom Errichter keine große Hürde. Die Registrierung beim Netzbetreiber kann aber ein echter Alptraum werden. Jeder Betreiber kocht da sein eigenes Süppchen.

Zu weiteren Verzögerungen führt oft der fällige Zählerwechsel: Alte Ferraris-Zähler – die schwarzen Kästchen mit mechanischem Zählwerk und Drehrad – würden beim Einspeisen ins Stromnetz rückwärts laufen. Das ist verboten, da man ja für die bezogene Energie viel mehr zahlt, als man für die Einspeisung bekommt. Dreht der Zähler rückwärts, betrügt man also den Energieversorger, und das ist böse ... Bei moderneren Digitalzählern mit Rücklaufsperrre besteht diese Gefahr nicht, trotzdem bestehen die Energieversorger hier auf den Austausch gegen einen Zweirichtungszähler. Für den Wechsel wiederum braucht es Personal und mitunter sind auch die Zähler nicht sofort verfügbar. So kann es vorkommen, dass die betriebsbereite PV-Anlage monatelang im Dornröschenschlaf verbringt, weil der Netzbetreiber nicht in die Pütte kommt. Zwar gibt es auch hier Bestrebungen, das Verfahren zu vereinheitlichen, doch bis das in der Praxis zur schnelleren und einfacheren Inbetriebnahme von privaten PV-Anlagen führt, wird es noch eine Weile dauern.

Immerhin: Der bereits erwähnte Wegfall der Mehrwertsteuer beim Kauf der PV-Anlage und Änderungen im Erneuerbare-Energien-Gesetz (EEG) bringt eine



**Der goldene Oktober 2022: Die PV-Anlage auf dem Dach sammelte 745 kWh Energie ein, trotzdem mussten noch 42 kWh Energie zugekauft werden.**

weitere Erleichterung für 2023 neu errichtete PV-Anlagen mit sich. Speist man die nicht selbst verbrauchte Energie ins Netz ein, erhält man dafür ja eine Vergütung. Damit galt man nach alter Rechtsprechung als Unternehmen und musste die Einkünfte aus dem Stromverkauf beim Finanzamt melden und dafür Steuern entrichten. Auch für die selbst verbrauchte Energie aus der PV-Anlage fielen Steuern an (Selbstentnahme). Im Gegenzug konnte man die Investition für die Solaranlage über mehrere Jahre abschreiben und sich im ersten Jahr die beim Kauf gezahlte Mehrwertsteuer erstatten lassen. Das ist zwar mit einem Aufwand verbunden, rentierte sich aber zumindest im Jahr der Anschaffung der PV-Anlage. Nach zwei Jahren konnte man dann versuchen, dem Finanzamt glaubhaft zu machen, dass mit der PV-Anlage keine langfristige Gewinnerzielungsabsicht einhergeht.

Seit Januar 2023 hat man nun bei privaten PV-Anlagen mit einer Nennleistung von weniger als 30 kWp die Möglichkeit, unkompliziert die sogenannte Kleinunternehmerregelung in Anspruch zu nehmen. Das erspart einem die Notwendigkeit, eine Umsatzsteuervoranmeldung abzugeben. Zusätzlich stellt das EEG Einnahmen aus privaten PV-Anlagen mit weniger als 30

kWp ab dem Steuerjahr 2022 steuerfrei. Damit sind keine Einkommensteuern mehr auf die Einnahmen aus dem Energieverkauf an den Netzbetreiber zu entrichten und auch die Versteuerung der Selbstentnahme entfällt. Beim Finanzamt anmelden muss man die PV-Anlage aber nach wie vor.

Für Selbstständige lauert hier aber eine Falle: Das Finanzamt betrachtet Sie als eine Steuerperson. Das bedeutet, die Umsätze aus einer selbstständigen Tätigkeit oder auch weiteren unternehmerischen Einnahmen werden zusammen betrachtet. Überschreitet die Summe den Freibetrag von 22.000 Euro, können Sie die Kleinunternehmerregelung nicht mehr in Anspruch nehmen. Das gilt auch nach der EEG-Neuregelung. Selbstständige sollten daher die PV-Anlage nicht selbst kaufen, sondern dies an den Partner oder die Partnerin delegieren.

## Ans Werk!

Doch nun genug der Theorie – in den nachfolgenden Artikeln finden Sie praktische Beispiele rund um das Thema Balkonkraftwerke und den – zumindest teilweise – Selbstbau einer Dach-PV-Anlage. Vielleicht ermutigen Sie unsere Tipps ja zum Bau einer eigenen PV-Anlage. (gs@ct.de)

UNSERE PREISE

# DER BESTE SCHUTZ VOR HOHEN KOSTEN



The best part of your project: [www.reichelt.de](http://www.reichelt.de)

## Mit reichelt holen Sie mehr aus Ihrem Budget

Dank effizienter, selbstentwickelter Logistik und IT und der Bündelung unserer Einkaufsleistung auf ausgesuchte Qualitätsprodukte, liefern wir Kleinstmengen zu Top-Preisen. Dadurch sind wir bei Entwicklungsprojekten, Instandhaltung und Kleinserien trotz Versandkosten meist die bessere Wahl.

### The best part of your project

Ganz gleich ob es um die Automatisierung Ihrer Produktionsprozesse oder um smarte Energieversorgung geht, mit passender Technik aus unserem Sortiment können Ihre Projekte weiterhin effizient geplant und durchgeführt werden.



Portenta Breakout  
Erweiterungsboard

Bestell-Nr.:  
ARD SHD ASX00031

45,95



NVIDIA Jetson Nano  
Modul

Bestell-Nr.:  
JETSON NANO

177,50



Mobiler Business-  
Scanner

Bestell-Nr.:  
EPSON DS310

249,00



Jetzt entdecken ► [www.reichelt.de/best-part](http://www.reichelt.de/best-part)

EFFIZIENT. NACHHALTIG. KOSTENGÜNSTIG.  
BEDARFSGERECHTES  
ENERGIEMANAGEMENT

Jetzt entdecken ►  
<https://rch.lt/em>



#SAVEENERGY



THE BEST PART OF YOUR PROJECT  
DIGITALE  
TRANSFORMATION

Jetzt entdecken ►  
<https://rch.lt/digi>



#DIGITALE  
TRANSFORMATION



Top Preis-Leistungs-Verhältnis

über 130.000 ausgesuchte Produkte

zuverlässige Lieferung – aus Deutschland in alle Welt

[www.reichelt.de](http://www.reichelt.de)

Bestellhotline: +49 (0)4422 955-333

 **reichelt**  
elektronik - The best part of your project

Es gelten die gesetzlichen Widerrufsregelungen. Alle angegebenen Preise in € inklusive der gesetzlichen MwSt., zzgl. Versandkosten für den gesamten Warenkorb. Es gelten ausschließlich unsere AGB (unter [www.reichelt.de/agb](http://www.reichelt.de/agb), im Katalog oder auf Anforderung). Abbildungen ähnlich. Druckfehler, Irrtümer und Preisänderungen vorbehalten. reichelt elektronik GmbH & Co. KG, Elektronikring 1, 26452 Sande, Tel.: +49 (0)4422 955-333

TAGESPREISE! Preisstand: 9. 1. 2023



**Kleine 600-Watt-Photovoltaikanlagen, die den Strombezug von Haus oder Wohnung senken, sind im Massenmarkt angekommen und keine Spielerei exklusiv für Technikinteressierte mehr. Bürokratische Hürden stehen noch immer im Weg, doch in zentrale Diskussionen kam zum Jahreswechsel frischer Wind. Zeit für eine Bestandsaufnahme.**

**Von Jan Mahn**

**V**ierzig Millionen Haushalte gibt es laut Statistischem Bundesamt in Deutschland, also schätzungsweise auch so viele Kühlschränke. Ähnlich hoch ist die Anzahl an Breitbandanschlüssen – laut Daten der Bundesnetzagentur dürften an 37 Millionen Internetzugängen ungefähr so viele Router rund um die Uhr laufen. Zusammen mit Smart-Home-Gerätschaften und Standby-Verbrauchern, vor allem aus dem Hi-Fi- und Unterhaltungsbereich, machen sie den Grundverbrauch privater Haushalte aus – in großen Häusern kommen weitere Kleinverbraucher wie Klingeltrafos dazu. Selbst in einer einfach ausgestatteten Wohnung kommen schnell 100 Watt zusammen, die sie zu jeder Tages- und Nachtzeit aus dem Netz bezieht. Im Jahr sammeln sich so 875 Kilowattstunden an. Energie, für die man nach der letzten Preiserhöhungsrunde der Versorger bei 45 Cent pro Kilowattstunde knapp 400 Euro bezahlen muss.

Im Jahr 2022, das sicher noch lange wegen der rapiden Energiepreissteigerungen in Erinnerung bleiben wird, erlebte deshalb eine Idee ihren Durchbruch, die vorher nur einer an Umweltschutz und Energiethemen interessierten Minderheit ein Begriff war: Das Balkonkraftwerk schaffte den Sprung aus der Nische in den Massenmarkt. Im Amtsdeutsch heißen die Geräte „steckerfertige Erzeugungsanlage“, anderen sind sie als Mini-PV oder Guerilla-PV bekannt.

Gemeint sind Photovoltaikanlagen mit einer maximalen Wechselrichterleistung von 600 Watt. Die Besonderheit:

# Ich habe steckerfertig

**Balkonkraftwerke: der aktuelle Stand**

Anders als große Anlagen (wie jene, die wir auf S. 22 vorstellen), braucht man keinen Elektrofachbetrieb, um sie anzuschließen. Typischerweise besteht eine Mini-PV-Anlage aus einem oder zwei Photovoltaikmodulen und einem Mikrowechselrichter. Ihr natürliches Habitat ist nicht allein das Dach: Die beiden Module können auch am Balkon hängen (wie auf dem Bild rechts), im Garten stehen, an der Fassade installiert werden oder das Dach der Gartenhütte bedecken – aber auch Installationen auf dem Hausdach sind erlaubt. Insgesamt wird die Zielgruppe dadurch größer: Nicht nur Hausbesitzer können mit Sonnenenergie einen Teil des selbst verbrauchten Stroms erzeugen, auch wer in einer Wohnung zur Miete wohnt, kann den Strombezug aus dem Netz reduzieren und damit die Stromrechnung. Module aufhängen, Wechselrichter dahinter schrauben und Kabel in die Steckdose gesteckt.

Ganz so einfach ist es nicht, denn gleich auf mehreren Ebenen haben verschiedene Akteure Hürden errichtet und teilweise heftige Debatten angezettelt. Mitte 2022 haben wir zuletzt eine Übersicht über die Hindernisse veröffentlicht [1] und im Anschluss viele Leserfragen beantwortet [2]. Doch in der Zwischenzeit hat sich die Lage verändert, große Vereinfachungen sind in Sicht und unerwartete Akteure sind auf der Bühne aufgetaucht.

## PV für alle

Dass die Klein-PV-Anlagen Massenware sind, kann man an gleich mehreren Indizien festmachen. Zunächst ist da das Marktstammdatenregister der Bundesnetzagentur. Unter [www.marktstamm](http://www.marktstamm)

**Jeder Balkon ist anders. Damit das Modul sicher hält, wird es oben eingehängt und unten auf einer Profilschiene mit Endklemmen befestigt.**



[datenregister.de](http://www.datenregister.de) (ohne vorangestelltes www. funktioniert es zurzeit nicht) muss sich jeder Betreiber einer Energieerzeugungsanlage eintragen. Das ist kein abschreckend bürokratischer Schritt, das Onlineformular ist recht übersichtlich und benutzerfreundlich, Erklärungen stehen jeweils direkt neben den Eingabefeldern. In dieser Datenbank kann man auch suchen und Daten exportieren. Und die haben es in sich: Setzt man einen Filter auf aktive PV-Anlagen unter 1 Kilowatt Spitzenleistung (Peak), spuckt die Datenbank ganze 103.000 Anlagen aus. Trägt man die installierte Leistung über die Zeit in einem Diagramm ab, entsteht die Kurve mit einem steilen Anstieg, die Sie auf Seite 20 sehen. Sie geht stark in Richtung einer Exponentialfunktion, ein Abflachen ist nicht erkennbar. Auch die installierte Gesamtleistung ist stattlich: 65.500 kW Peak (65 Megawatt) kommen zusammen. Über 50 Megawatt davon wurden allein 2022 in Betrieb genommen. Bei dieser Betrachtung darf man nicht außer Acht lassen, dass längst nicht jeder Betreiber seine Anlage angemeldet hat. Um Ärger und Bürokratie beim Kontakt mit den Netzbetreibern zu vermeiden, lassen viele diesen Schritt weg.

Mit den vorliegenden Daten sind auch andere Auswertungen möglich. Jeder Anlagenbetreiber darf sich einen Namen ausdenken, der ebenfalls in den exportierbaren Daten liegt. Neben kreativen Namen wie „Sonnenoby“ schreiben viele Begriffe in den Namen, die Rückschlüsse auf die Installationsart zulassen. 31.000-mal fanden wir das Wort Balkon, 7000-mal Garage und 10.000-mal Dach. Wenn Sie sich selbst an die Anmeldung machen, achten Sie auf Datenschutz und schreiben

Ihren Namen, Ihre Adresse oder die Mailadresse nicht in das öffentlich einsehbare Freitextfeld – auch das haben einige Betreiber getan.

Das zweite Indiz für ein Massenphänomen: Balkonkraftwerke gibt es nicht mehr nur in darauf spezialisierten PV-Webshops im Internet, auch große Händler haben das Potenzial erkannt. Ende Dezember fiel uns ein Photovoltaikregal in einem Obi-Baumarkt auf, ausgestattet mit fertigen Kleinanlagen und Kabeln. Im Januar stieg dann Discounter Netto ins Geschäft ein. Unter dem Markennamen Juskys gibt es im Netto-Onlineshop (nicht im Markt) ein Komplettspaket aus 600-Watt-Wechselrichter und zwei 410-Watt-Modulen für 899 Euro. Wenn Sie neu im Thema sind, mag das falsch klingen: Zwei Module à 410 Watt können schließlich mehr liefern als die erlaubten 600 Watt. Entscheidend bei der sogenannten Bagatellgrenze ist jedoch nur die Ausgangsleistung des Wechselrichters. Der kann die vollen 410 Watt der Module nicht aus schöpfen und damit bleibts legal.

Zwei Haken hat das Netto-Angebot: Zum einen ist es Stand 17. Januar bereits ausverkauft (mit 38 Tagen Wartezeit). Zum anderen legt Netto als Wechselrichter einen problematischen alten Bekannten bei: Der stammt vom Hersteller Deye aus China, wird in Deutschland auch von Pearl und Bosswerk vertrieben und bietet als einziges Gerät seiner Klasse eine WLAN-Schnittstelle – mit einem schweren Sicherheitsproblem. Mehr dazu im Kasten auf Seite 21.

## Steuererleichterung

Die größte Veränderung bescherten zum Jahreswechsel Bundestag und Bundesrat:

## c't kompakt

- Photovoltaikanlagen bis 600 Watt dürfen auch Laien anschließen – jetzt fordert auch der VDE, die Grenze auf 800 Watt zu erhöhen.
- Im Jahr 2022 wurden die Geräte zum Massenphänomen. Über 100.000 Anlagen sind bereits bei der Bundesnetzagentur angemeldet.
- Zum Jahreswechsel entfiel die Umsatzsteuer auf die Anschaffung, der Kauf lohnt sich jetzt schneller.



**Es muss nicht immer Süden sein: Die zwei Module stehen in Ost-/West-Ausrichtung. Die Aufstände rung ist mit Waschbetonplatten ballastiert.**

Kurz vor der Weihnachtspause verabschiedeten sie umfangreiche Steuerreformen, unter anderem eine Reform des Umsatzsteuergesetzes. Eingeführt wurde zum 1. Januar der Nullsteuersatz für Photovoltaikanlagen, Installationsmaterial und die Installation unter bestimmten Voraussetzungen: Die Anlage muss von Privatpersonen gekauft werden und darf nicht größer als 30 kW Peak sein. Ausdrücklich fallen auch Balkonkraftwerke unter diese Steuersenkung. Ganz konkret heißt das: Die Geräte werden mit 0 Prozent Mehrwertsteuer verkauft. Stand 12. Januar konnten wir noch nicht beobachten, dass große Händler die Differenz heimlich draufgeschlagen haben. Die Komponenten sind derzeit wirklich günstiger als Ende 2022. Weil Bund und Länder nicht pünktlich zu Neujahr alle Fragen zur Umsetzung klären konnten, sind die Händler unterschiedlich ins Jahr 2023 gestartet. Einige weisen den Preis direkt mit 0 Prozent in ihren Webshops

aus, andere haben kurz vor dem Ende des Verkaufsprozesses eine Frage eingebaut, mit deren Antwort man bestätigt, dass man die Voraussetzungen für den Nullsteuersatz erfüllt. Klarheit soll ein gemeinsames Schreiben von Bundesfinanzministerium und Ländern bringen. Gegenüber c't erklärte das Bundesministerium Ende Dezember, dass das bald erscheinen solle.

Wer günstig kaufen will, sollte die Gunst der Stunde nutzen und jetzt zuschlagen. Bleibt die Nachfrage so hoch, ist es nicht ausgeschlossen, dass die Händler in einigen Monaten die durch die Steuersenkung gefühlten günstigen Preise ausnutzen und erhöhen.

### Auftritt Bundesnetzagentur und VDE

Kam die Mehrwertsteuersenkung schon recht unerwartet, so gab es rund um den Jahreswechsel zwei Ereignisse, die noch mehr überraschten: Nach Weihnachten

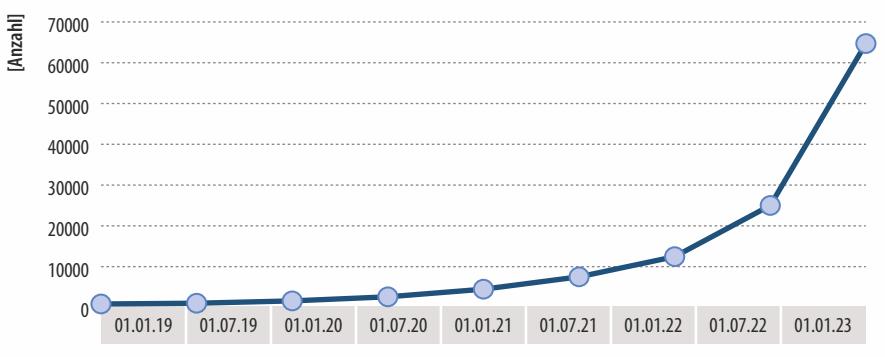
mischte sich Klaus Müller, der Präsident der Bundesnetzagentur (BNetzA), in den wohl größten Streit ein, der seit Beginn des Balkonkraftwerkszeitalters geführt wird: in die Steckerdiskussion. Im Kern geht es um die Frage, wie ein steckerfertiges Gerät mit dem Stromnetz verbunden werden darf. Mit einem speziellen Steckverbinder, der berührungslose Kontakte hat und der nur mit Werkzeug aus der zugehörigen Steckdose entnommen werden kann, sagen die einen. Mit einem ganz ordinären Schukostecker sagen die anderen. Aufeinander trafen die beiden Lager in Sitzungen der Deutschen Kommission Elektrotechnik (DKE), der Organisation, die für den Verband der Elektrotechnik (VDE) die Normen erarbeitet. Entstehen soll dort eine Produktnorm für steckerfertige PV-Anlagen. Im Mai 2022 gab es das erste Zwischenergebnis: Die Schukobefürworter konnten sich nicht durchsetzen, eine Abstimmung endete mit einem Patt und nur der Einspeisestecker (in der Praxis fast ausschließlich vom Hersteller Wieland) landete in der Vornorm. Das große Problem für Kunden: Um die Norm zu erfüllen, müssten sie einen Elektriker beauftragen, der die Steckdose tauscht. Das ist für die sowieso schon gut ausgelastete Branche aber nur ein vergleichsweise kleiner Auftrag, der dementsprechend ins Geld geht und so die Amortisationszeit der Anlage nach hinten verschiebt.

Die Argumentation der Schuko-Gegner: An den blanken Kontakten könne man einen Schlag erleiden, wenn man den Wechselrichter bei Last abzieht. Außerdem seien Haushaltssteckdosen per se nicht geeignet, weil die 600 Watt des Wechselrichters nicht am Sicherungsaufschmelzen (Leitungsschutzschalter) vorbeifließen und der dadurch zu spät auslöse. Das Pro-Schuko-Lager hielt dagegen, dass die Leitungen durch die zusätzlichen 2,5 Ampere nicht unzulässig erwärmt werden und dass der sogenannte NA-Schutz in den Wechselrichtern so schnell abschalte, dass man unmöglich die Kontakte des Schukosteckers schnell genug berühren könne, um einen Schlag zu erleiden. Im Wechselrichtertest [3] haben wir diese Behauptung getestet und extrem niedrige Abschaltzeiten gemessen, die die Argumentation der Schukobefürworter stützen.

Zum Lager der Befürworter bekannte sich dann auch Klaus Müller, seines Zeichens nicht Elektroingenieur, son-

## Balkonkraftwerke in Deutschland

Allein im Marktstammdatenregister der Bundesnetzagentur sind Anfang Januar 2023 über 103.000 Photovoltaikanlagen unter 1 kW Peak-Leistung mit zusammen über 65.000 kW Leistung registriert.



dern Volkswirt, ehemaliger Umweltminister und Verbraucherzentralen-Vorstand. Per Twitter und in einem Brief verkündete er, dass nach Einschätzung der Bundesnetzagentur der Schukostecker ausreicht. Die BNetzA wolle sich außerdem im Normungsprozess für ihn einsetzen. Das sind ungewöhnliche Töne für eine Behörde.

Der nächste Paukenschlag folgte am 11. Januar: Der VDE höchstselbst veröffentlichte ein Positionspapier über Balkonkraftwerke, das es in sich hatte. Darin forderte der Verband umfangreiche Änderungen. Die Bagatellgrenze von 600 Watt solle auf 800 Watt angehoben werden, schließlich handhaben das andere europäische Länder auch so. Geduldet werden solle auch der Schukostecker – eine bemerkenswerte Aussage des Verbands, die Folgen für die Beteiligten des eigenen Normungsprozesses haben dürfte. Und noch eine Überraschung hatte der bisher eher konservative Verband: Auch der Betrieb an einem alten schwarzen Ferrariszähler solle erlaubt werden. Aktuell ist das illegal, weil sich dieser Zählertyp auch rückwärts drehen kann. Auf diese Weise kann man das gesamte europäische Verbundnetz als riesigen Speicher nutzen, tagsüber Überschuss einspeisen und nachts kostenlos wieder abrufen. Sollte der VDE sich damit durchsetzen, wäre das für Betreiber durchaus attraktiv. Jedoch: Wer schon einen digitalen Zähler hat, kann nicht

mehr zurückwechseln, bis 2032 sollen die alten schwarzen Zähler flächendeckend verschwunden sein.

Eine weitere Forderung des VDE betrifft die Anmeldeprozedur. Statt wie bisher auf der Homepage des lokalen Netzbetreibers ein Formular zu suchen (das jeder Netzbetreiber selbst entwirft), per Post oder Mail einzureichen und auf Reaktion zu warten, solle man die Anlage nur noch bei der Bundesnetzagentur anmelden – der Netzbetreiber würde dann eine Information erhalten und keine eigenen Formulare mehr pflegen.

### Zwischenstand

Kaum ein Bereich entwickelt sich derzeit so dynamisch wie kleine Photovoltaikanlagen. Mit der Steuernsenkung und Stellungnahmen von BNetzA und VDE kommt Bewegung in lange festgefahrenen Debatten. Auch die Liefersituation bei Wechselrichtern und Modulen hat sich im Winter deutlich entspannt. Gut entwickelt hat sich auch das Angebot an Befestigungssystemen für die Balkon- und Fassadenmontage. Für viele Balkongitter findet man mit etwas Recherche im Netz passendes Befestigungsmaterial.

Ganz so rosig ist es noch nicht überall. Für viele Mieter bleibt ein großes Ärgernis: Wollen sie die zwei Module von außen ans Balkongitter hängen, müssen sie den Eigentümer um Erlaubnis fragen. Und da stoßen viele, so berichten es uns Leser,

noch immer auf Unverständnis und Ablehnung. Selbst wenn der Vermieter selbst einverstanden ist, gibt es vielerorts noch die Eigentümersammlung als ultimative Endgegner. Einen Konsens für Balkonkraftwerke und gegen das gern zitierte „einheitliche Erscheinungsbild“ zu finden, scheitert allzu oft.

Wer seinen Vermieter überzeugt hat und aktuell über eine Anschaffung nachdenkt, steht vor schweren Entscheidungen: Darauf warten, ob sich die 800-Watt-Grenze wirklich durchsetzt? Oder lieber jetzt kaufen, günstige Preise nach der Steuernsenkung mitnehmen, bevor die Preise anziehen? Vieles spricht für die letzte Option – denn ob und wann der VDE mit der Idee Gehör findet, ist offen. Ganz leicht ist die Entscheidung für alle, die ohnehin nicht planen, ihrer Verpflichtung nachzukommen und die Anlage dem Netzbetreiber zu melden. Sie kaufen einfach schon heute einen 800-Watt-Wechselrichter und installieren eine Guerilla-Anlage.

(jam@ct.de) 

### Literatur

- [1] Jan Mahn und Andrijan Möcker, Heimkleinkraftwerk, Mit Balkonsolaranlagen die Stromrechnung senken, c't 15/2022, S. 20
- [2] Jan Mahn, Pina Merkert und Andrijan Möcker, FAQ Balkonkraftwerke, c't 23/2022, S. 178
- [3] Jan Mahn und Andrijan Möcker, Sonnenwandler, Mikrowechselrichter für Balkonkraftwerke: Grundlagenwissen und Marktübersicht, c't 17/2022, S. 104

## Netto, Bosswerk, Pearl: Sicherheitslücke per WLAN

Wechselrichter von Deye mit 600 Watt, die auch im Netto-Set stecken, tauchen in Deutschland unter mehreren Namen auf, unter anderem findet man sie als Bosswerk MI600 und beim Händler Pearl unter dem Namen revolt. Nach unserem Stand steckt in jedem aktuell erhältlichen 600-Watt-Wechselrichter mit WLAN-Schnittstelle der Deye 600. Übers Internet funkts er seine Leistungsdaten an die Cloud des Anbieters Solarman, per App kann man die Daten auswerten.

Für unseren ausführlichen Wechselrichtertest [3] hatten wir ihn in der Pearl- und Bosswerk-Verpackung im Labor und bereits auf ein Sicherheitsproblem hingewiesen. Das Gerät öffnet einen WLAN-Access-Point mit dem Schlüssel 12345678. Eigentlich soll man ihn darüber nur ein-

richten, mit dem eigenen WLAN verbinden und den Access Point dann abschalten oder zumindest dessen Zugangsdaten ändern. Der Speichern-Button ist aber ohne Funktion, der Access Point bleibt immer offen, der Schlüssel bleibt unverändert. Wer in der Nähe ist, kann sich mit dem Access Point verbinden und mit minimalem Aufwand über AT-Befehle die WLAN-Zugangsdaten zum heimischen WLAN ausspähen und Einstellungen verändern. Leser berichteten, der Hersteller könnte ein Firmware-Update auslösen, das den Fehler behebt, wenn man den Deye-Support per Mail kontaktiere. Bis Redaktionsschluss erhielten wir aber keine Reaktion. Sobald wir einen Weg kennen, die Geräte zu aktualisieren, werden wir darüber berichten.



**Ein Wechselrichter, viele Namen:**  
Hersteller Deye hat einen Wechselrichter mit WLAN-Schnittstelle im Sortiment, der in Deutschland unter vielen Namen vertrieben wird.



# Ab aufs Dach

## Photovoltaik auf dem Dach mit Eigenleistung

**Balkonkraftwerke baut man selbst, Aufdachanlagen lässt man vom Fachbetrieb installieren. Aber was tun, wenn kein Installateur verfügbar ist? Wir haben ausprobiert, wie man die Solaranlage einfach selbst aufs Dach schrauben kann.**

**Von Jan Mahn, Pina Merkert und Andrijan Möcker**

**D**as hören viele seit Monaten: „Gerne bauen wir Ihnen eine Photovoltaikanlage. Aber nicht vor dem vierten Quartal 2023.“ Mancherorts, so schilderten uns Leser, waren Fachbetriebe für die Montage nicht mal persönlich zu erreichen – wegen der riesigen Nachfrage hatten viele Betriebe nur noch einen Anrufbeantworter aktiviert, der Neukunden vertröstete.

Das Problem hatten wir selbst auch: Das Garagendach von Redakteurin Pina Merkert lockte mit 25 Quadratmeter Zie-

geldach in optimaler Südausrichtung, doch es fand sich niemand, der es mit Photovoltaik belegen wollte. Dabei könnte die Dachfläche die winterliche Solarstromknappheit im daneben stehenden Wohnhaus lindern. Letzteres besitzt bereits seit 2021 eine Ost-West-Photovoltaikanlage mit Stromspeicher. Da wir in der Redaktion inzwischen einige Erfahrungen mit Balkonkraftwerken gesammelt hatten [1], fragten wir uns, ob wir die Garage nicht einfach selbst mit Solarmodulen bestücken könnten. Das Grundprinzip aus

## c't kompakt

- Viele Arbeitsschritte beim Aufbau einer Solaranlage kann und darf man selbst ausführen.
- Mit einem Gerüst und dem richtigen Werkzeug setzt man selbst Dachhaken, klinkt Ziegel aus und klemmt Module fest.
- Die Elektrik kann man nur vorbereiten: Solaranlagen über 600 Watt muss ein zertifizierter Elektrobetrieb ans Stromnetz anschließen.

Modulen, Wechselrichter, DC- und AC-Verkabelung ist gleich; es ist nur alles etwas größer und statt des Balkons sind Dachziegel unter den Modulen.

Kaum saßen wir – die drei Autoren dieses Artikels – zusammen, wurde aus der fixen Idee ein konkretes Projekt. Das Garagendach eignet sich perfekt als Lehrstück für Einsteiger, denn es ist vergleichsweise klein ( $4 \times 6,2$  Meter), nicht besonders hoch über dem Boden und es gibt keinen störenden Schornstein. Unter den um 40 Grad geneigten Ziegeln befindet sich zudem eine Unterkonstruktion wie sie auch viele Hausdächer haben, sodass unsere Erfahrungen auf große Dächer übertragbar sind.

Im Keller des Haupthauses steht bereits ein Speichersystem mit einer Kapazität von 5,4 Kilowattstunden, das bislang von zwei AC-gekoppelten Wechselrichtern gespeist wurde. Diese Art der Kopp lung macht es leicht, ein weiteres AC-gekoppeltes System zu ergänzen – oder anders formuliert: Die zusätzliche Anlage hängt einfach als negativer Verbraucher im Hausnetz. Die Aufgabe: Das Dach so effizient wie möglich ausnutzen. Die Hoffnung: Zu Spitzenzeiten im Frühjahr und Sommer kann das Haus mehr Strom verkaufen und im Winter hilft die Anlage auf der Garage, den Akku vollzuladen und ohne Stromnachschub aus dem Versorger netz über die Nacht zu kommen. Insgesamt sollen möglichst viele Tage im Jahr ganz ohne Netzbezug vergehen. Die Aus sicht, durch Eigenleistung merklich gerin gere Baukosten für die Anlage zu haben, ließ die Wirtschaftlichkeitsabschätzung von „lohnt sich“ auf „lässt die Kasse klin geln“ springen.

## Quartettspiel für die Planung

Los ging die Planung mit Recherche – eine machbare Aufgabe, wenn sich drei Technikjournalisten in einer Videokonferenz treffen. Zunächst klärten wir Grundlegendes: Dürfen wir das überhaupt? Wie sieht es bei Aufdachanlagen unter den Modulen genau aus? Welches Werkzeug benötigen wir und wie sichern wir uns auf dem Dach? Die Antworten: Vieles dürfen wir auf eigene Verantwortung selber erledigen und gemeinsam haben wir genug Werkzeug – Schlag- und Akkuschrauber, Trennschleifer, Seitenschneider, Crimpzangen für MC4-Stecker und Aderendhülsen – und Fallschutzgurte, um nicht vom Dach zu stürzen. Außerdem zeigte die Recherche einen praktischen Umstand auf: Die Anlage auf dem Hausdach war noch kein ganzes Jahr alt und deswegen kann die Erweiterung auf dem Garagendach einfach mit der gleichen Einspeisevergütung ab gerechnet werden.

Mit diesen guten Nachrichten starten wir die Anlagenplanung. Wie bei einem Quartettspiel ging es zu: Werte aus Datenblättern wurden in den Ring geworfen, Modulgrößen mit dem Platz auf dem Dach verrechnet. Gesucht wurde eine Kombination aus Modulen und Wechselrichtern, die aufs Dach passt und die größtmögliche Gesamtleistung bringt. Lieber wenige und dafür große 500-Watt-Module oder kleine 300-Watt-Panels, dafür eine zusätzliche Reihe quer? Lieber ein großer String-Wechselrichter oder mehrere Mikrowechselrichter? String-Wechselrichter arbeiten meist etwas effizienter, mit Mikrowechselrichtern bekommt man ohne Aufpreis mehr Leistungspunktsucher (MPPT), die bei Verschattung das Optimum herausholen.

## Kosten

Posten	Preis
Wechselrichter: 2 x Hoymiles HMT2250 6T	973,90 €
Module: 12 x Trina Solar TSM-DE09.08	2.271,60 €
Dachhaken und Profile: Novotegra Klemmsystem top-fix	686,40 €
100 Meter DC-Solarkabel 4mm <sup>2</sup>	125,44 €
100 MC4-Stecker	44,99 €
AC-Anschlusskabel: NYM 5x2,5mm <sup>2</sup> Mantelleitung	34,39 €
Sicherungsautomaten (3x16A B-Typ plus Automaten für Licht und Steckdosen)	91,92 €
Mini-Sicherungskasten 12 Elemente breit	24,99 €
10 Feuchtraum-Abzweigdosen	9,99 €
WAGO-Klemmen	13,95 €
Elektrische Prüfung	700,00 €
<b>Summe</b>	<b>4977,57 €</b>

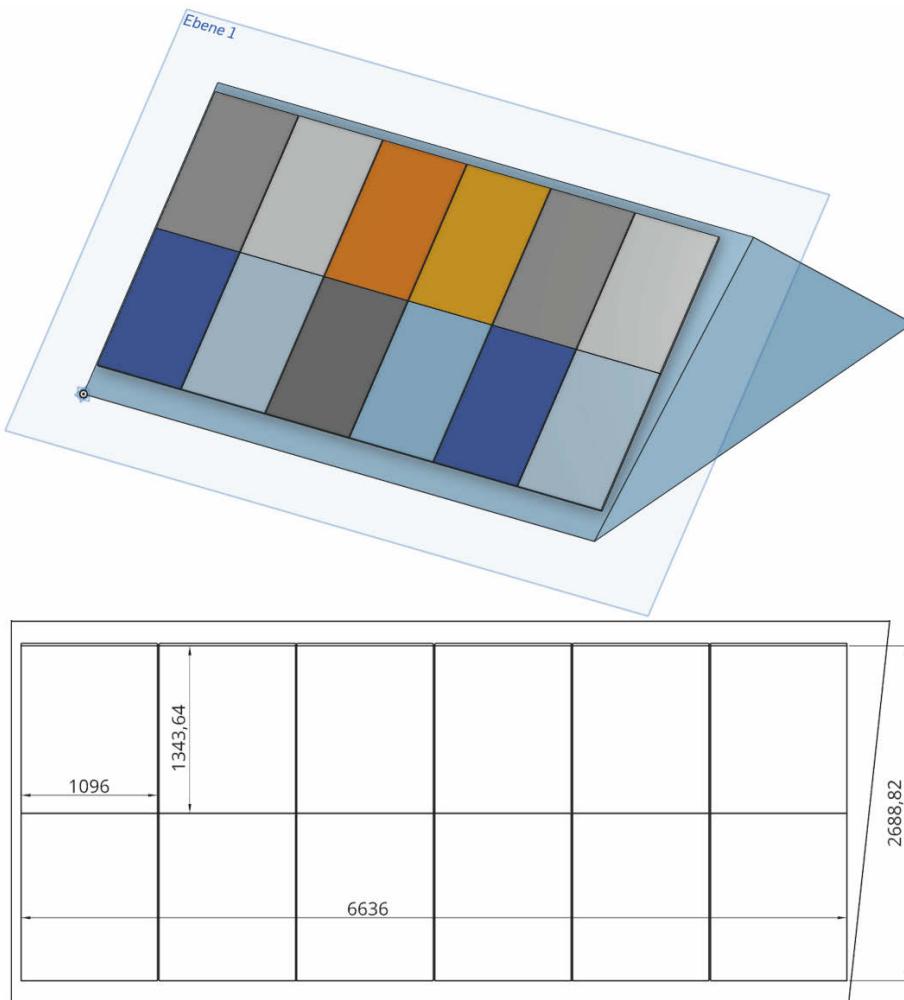
## Werkzeugempfehlung

- Winkelschleifer mit Diamantscheibe
- Edding für Markierungen auf den Ziegeln
- Schlagschrauber (Impact Driver) mit Torx T20-Bit
- Metallsäge zum Ablängen der Schienen
- Akkuschrauber mit 8-mm-Nuss für die Modulklemmen
- Ratsche und 19-mm-Nuss für die Verbindung zwischen Dachhaken und Schienen
- 19-mm-Gabelschlüssel für die Höheneinstellung der Dachhaken
- Crimpzange für MC4-Stecker
- Seitenschneider
- Cuttermesser
- Abisolierzange
- Crimpzange für Aderendhülsen
- Stufenbohrer für Kabeldurchführungen in die Verteilerdosen
- Bohrhammer für Dübellöcher

Klarer Sieger: Eine Kombination aus zwölf 400-Watt-Modulen und zwei Mikrowechselrichtern.

## Drei Phasen

Wer bei Mikrowechselrichtern nur an Balkenkraftwerke mit 600 Watt denkt, ist aber auf der falschen Spur: Die ausgewählten Geräte – zwei Hoymiles HMT-2250-6T – liefern jeweils 2250 Watt und haben sechs Eingänge mit sechs Leistungspunktsuchern – ein großer Vorteil, weil das Wohnhaus und die benachbarte Scheune die Fläche zum mindest teilverschatten. Die HMT-2250-6T werden AC-seitig einfach parallel geschaltet mit den drei Phasen vom Hausanschluss verbunden. Maximal 4500 Watt kann die Anlage so leisten; die Module können in der Spur kaum mehr erreichen und wir verschenken unter optimalen Bedingungen nur rund 300 Watt. Insgesamt ist das die optimale Kombination: Das Dach wird ganz voll und die Gesamtkosten dieser Zusammenstellung liegen mit 5000 Euro deutlich unter einer Variante mit großem Wechselrichter. Die Module (Trina Solar TSM-DE09.08) bot uns der lokale Solarzulieferer an, sodass wir uns hohe Speditionsversandkosten gespart haben. Die gesamte Kalkulation für unser Projekt finden Sie in der Tabelle links.



Im CAD-Programm Onshape konnten wir leicht das Dach modellieren und die Module auf die verfügbare Fläche „puzzeln“. Die hintere Wand der Garage ist schräg, weil sie der Grundstücksgrenze folgt.

Von einem solchen Solarquartettspiel mit Datenblättern, die im Internet leicht zu finden sind, können auch Kunden profitieren, die nicht selbst aufs Dach möchten. Es lohnt sich durchaus, das Dach genau zu vermessen und verschiedene Kombinationen durchzurechnen, bevor man einen Fachbetrieb kontaktiert. Was möglich ist, muss am Ende der Installateur beurteilen, aber es kann nicht schaden, wenn man ein paar Vorschläge zum Diskutieren dabei hat – besonders bei teilverschatteten Dächern und Dachgauben können Ergänzungen mit Mikrowechselrichtern sinnvoll sein, damit am Ende möglichst wenig nutzbare Fläche brachliegt.

CAD-Programme erweisen sich dafür als nützliches Werkzeug. Hat man wie wir eine bemaßte Aufsicht auf den Sparrenplan (auf Papier aus dem Jahr 1982), sind die Maße schnell in ein CAD-Programm übertragen. Wir verwendeten dafür das browsergestützte Onshape [2], das kosten-

los nutzbar ist, solange man die Planung öffentlich teilt. In Onshape konstruierten wir das Dach in 3D und erstellten eine Skizze in der Ebene der Dachfläche. In der kann man dann sehr schnell verschiedene Modulgrößen ausprobieren. Unser Design können Sie online nachschauen. Den Link finden Sie über [ct.de/yemv](http://ct.de/yemv).

### Nicht ganz ohne Fachbetrieb

Der famose Plan hatte allerdings ein entscheidendes Problem: Dreiphasige Wechselrichter mit 2,25 Kilowatt dürfen wir nicht selbst ans Stromnetz anschließen. Ganz ohne Fachbetrieb geht es also nicht. Genau wie alle Anlagen über 600 Watt muss jede Anlagenerweiterung beim Netzbetreiber angemeldet und von diesem abgenommen werden. Voraussetzung dafür ist, dass ein beim Netzbetreiber eingetragener Elektrobetrieb als Errichter der Anlage auftritt und gegenüber dem Netzbetreiber bestätigt, dass die Anlage auf der

Wechselspannungsseite nach dem Stand der Technik installiert ist und dass die Wechselrichter die VDE-Anschlussregel AR-N 4105 erfüllen – nachgewiesen mit Prüfzertifikaten des Herstellers.

Als handwerklich erfahrener Laie kann man selbst die Dachhaken anschrauben, die Ziegel ausklinken, Aluprofile als Unterkonstruktion anbringen, die Module befestigen und die Verkabelung vorbereiten. Auch die Formulare für die Anmeldung kann man selbst ausfüllen. Nur die Verbindung zum Stromnetz stellt der Solarteurbetrieb her.

Für unser Projekt hatten wir mit dem Betrieb, der die Anlage auf dem Dach des Wohnhauses gebaut hat, einen Deal geschlossen: Er lieferte uns nicht nur die Solarmodule und das Montagematerial, sondern übernahm auch die Ab- und Inbetriebnahme sowie die Anmeldung beim Netzbetreiber. Wir leisteten die schwere Arbeit auf dem Dach und bereiteten alles vor, schalteten aber noch keine Verbindung zum Netz. Der Elektriker sollte unsere Arbeit prüfen und die Anlage in Betrieb nehmen. In den Formularen für die Anmeldung beim Netzbetreiber konnten wir so den Fachbetrieb als Errichter eintragen. Für diese Arbeiten veranschlagten die Profis 700 Euro. Der Erfolg dieses Deals hing aber natürlich davon ab, dass wir professionell genug arbeiten würden, damit der Fachbetrieb nicht nachbessern muss.

### Hakenarbeit

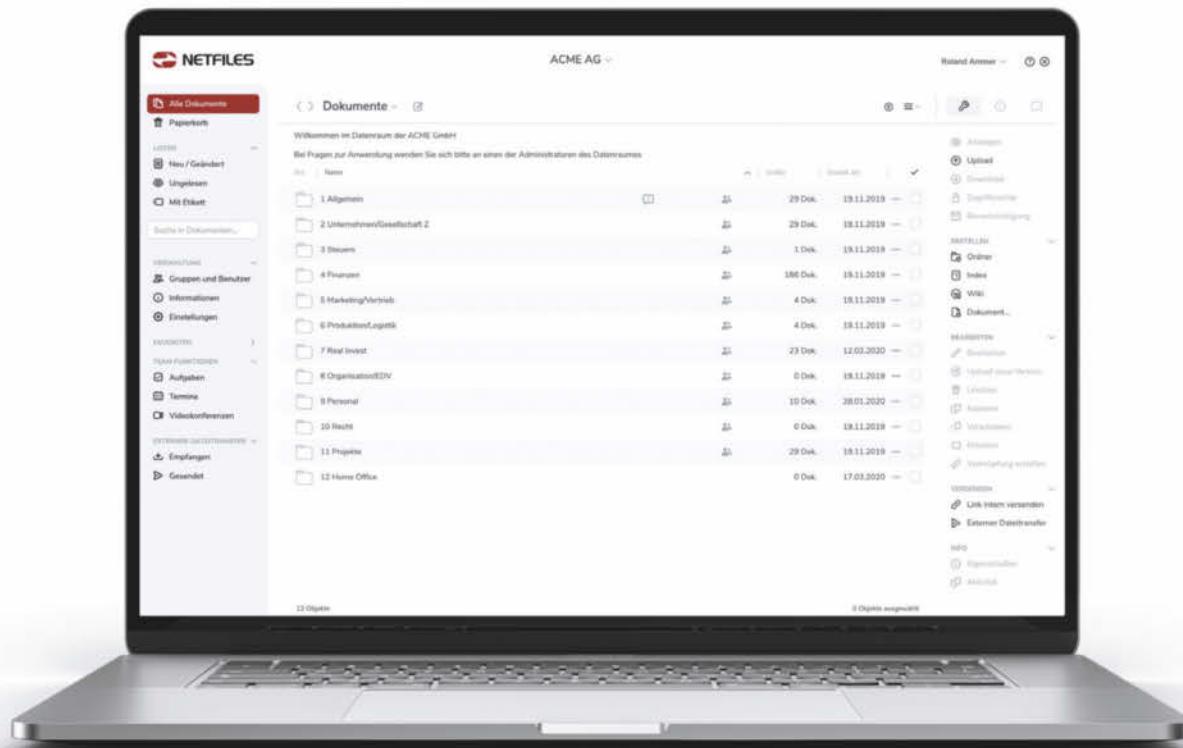
Im Nieselregen ging es damit los, ein geliehenes Gerüst aufzubauen. Ohne geht es nicht. Spätestens beim Hochwuchten der Solarmodule würde man auf einer Leiter verzweifeln. Der Himmel klarte glücklicherweise etwas auf, als wir von der Gerüstplattform aus die ersten Ziegel ausklinkten und die Sparren freilegten. Auf die schraubten wir mit langen Tellerkopfschrauben die erste Reihe Dachhaken. Der



Die Dachhaken, Profile und Module lieferte uns der Solarteur, mit dem wir handelseinig wurden.

# Sichere Cloud-Lösungen

## für Datenaustausch und Collaboration



### Einfach

Der netfiles Datenraum ist besonders einfach zu bedienen, bietet umfangreiche Funktionalität und steht Ihnen sofort, ohne Installation von Software oder Plugins zur Verfügung. Ein Webbrowser genügt.

### Sicher

Im netfiles Datenraum sind Ihre Daten sowohl bei der Speicherung als auch Übertragung durch 256-bit Verschlüsselung sicher und Compliance-gerecht geschützt.

### Bewährt

netfiles gibt es seit mehr als 20 Jahren. Profitieren auch Sie von unserer langjährigen Erfahrung und dem zuverlässigen Betrieb. Wir sind ein deutsches Unternehmen und hosten ausschließlich in Deutschland.

[www.netfiles.com](http://www.netfiles.com)

Testen Sie jetzt netfiles 14 Tage kostenlos  
oder vereinbaren Sie einen Termin für eine Online-Präsentation.



**Ein Gerüst ist für die Installation einer Aufdachanlage unverzichtbar. Ohne hätten wir die Module nicht auf die Profile wuchten können.**

Akkuschlagschrauber prügelte die langen Schrauben, die der Hersteller des Befestigungsmaterials vorgesehen hat, handgegenfreundlich ins Holz.

Es gibt zwar verschiedene Dachhaken, sie werden aber immer mit einer gelochten Platte angeschraubt. Die Hakenform ist nötig, weil sie zwischen der unteren Kante eines Ziegels und der oberen Kante des darunterliegenden Ziegels hindurchgeführt werden. Dahinter biegen sie nach oben ab, damit man ein Aluprofil fixieren kann. Unsere Dachhaken waren in Höhe und Position verstellbar. Das ist deswegen nützlich, weil die Haken nicht auf den unteren Ziegel drücken dürfen. Durch eine punktuelle Belastung könnte der Ziegel in späteren Jahren brechen.

### **Nutfräserei**

Damit die Ziegel trotz Haken korrekt aufliegen, muss eine Nut Platz schaffen. Routinierte Profis schlagen die Nut mit einem Zimmermannshammer. Weil die Ziegel dabei aber auch unsichtbare Schäden davontragen können, greift man als Laie besser zum Winkelschleifer: Wir frästen die Nuten mit einer Diamantscheibe in die Ziegeln. Das staubt gewaltig, aber das Tragen von Staubschutzmasken ist man ja nun gewohnt.

Mit dem ersten Profil auf dem Dach hatten wir uns einen Befestigungspunkt

für einen Sicherungsgurt gebaut. Damit war der Weg aufs Dach frei: Stück für Stück setzten wir auf schrägen Ziegeln kniend Haken für Haken und Profil für Profil, bis wir den First erreicht hatten. Auf diese Konstruktion konnten wir das

erste Modul hieven und mit End- und Mittelklemmen fixieren. Für Klemmen, Profile und Haken gibt es mehrere Systeme, die sich alle wie ein Baukasten zusammensetzen lassen. Am Ende des zweiten Tages hatten wir schon das erste Modul auf dem Dach.

### **Wechselrichterturm**

Mit dem Anschrauben des ersten Mikrowechselrichters auf dem mittleren Profil ging es am nächsten Tag flott weiter. Jedes Modul hatte bei unserer Installation zwei Stecker am Wechselrichter, die Distanz überbrückten selbstkonfektionierte Verlängerungskabel mit 4 Quadratmillimetern Querschnittsfläche. Auf deren Anschluss waren wir mit der richtigen Crimpzange gut vorbereitet, denn die MC4-Stecker muss man unbedingt crimpeln und darf sie nicht weichlöten. Drückt ein Stecker auf ein verzinktes Kabel, weicht das Lötzinn über die Jahre aus und die Verbindung wird instabil oder kann sogar brandgefährlich heiß werden. Zudem liefern normale Lötkolben ohnehin nicht genug Wärme, um so dicke Kabel sauber zu verlöten.

Beim dreiphasigen Wechselstromanschluss hatten wir dann aber ein Problem. Wir hatten ein wasserdichtes T-Stück für die Außeninstallation besorgt, um beide Wechselrichter zusammenzuschlie-



**Statt mit dem Zimmermannshammer Nuten zu schlagen, frästen wir Schlitze mit einer Diamantscheibe. Zwei Ziegeln brachen trotzdem, aber erst beim Zurechtrücken.**



1blu

# Homepage Yes

## 10 .de-Domains inklusive

- > Kostenlose SSL-Zertifikate für alle Domains
- > Viele 1-Klick-Apps inklusive
- > Webbaukasten
- > Webkonferenzlösung
- > 120 GB Webspace
- > 750 E-Mail-Adressen
- > 75 GB E-Mail-Speicher
- > 75 MySQL-Datenbanken

DAUERPREIS

2,49  
€/Monat\*



Angebot bis zum  
28.02.2023  
verlängert!

\* Preis/Monat inkl. 19% MwSt. Es fällt keine Einrichtungsgebühr an. Vertragslaufzeit 6 Monate, jederzeit kündbar mit einem Monat Frist zum Vertragsende.

030 - 20 18 10 00 | nur unter [www.1blu.de/yes](http://www.1blu.de/yes)



**Am dritten Tag lag schon die Hälfte der Module auf dem Dach.  
Insgesamt arbeiteten wir zu dritt vier Tage lang an der Solaranlage.**

ßen sowie ein dickes Kabel, um es unter den Ziegeln nach innen zu führen. In dem bestellten T-Stück war aber nicht genug Platz, um die Kabel vertrauenswürdig zu verschrauben. Nach einer Stunde vergeblichen Fummelns gaben wir auf.

Die Idee zur Lösung kam uns, als wir ratsuchend auf unsere halb fertige Dachkonstruktion schauten: Anstatt die drei Phasen an einer Stelle nach außen zu führen, könnten wir auch die Anschlusskabel beider Wechselrichter direkt unter dem darunterliegenden Ziegel nach innen führen. Innen würden typische Feuchtraumdosen und Wago-Klemmen für solide und sichere Verbindungen sorgen. In unserem Fall war das die elektrisch solideste Lösung, die wir auch ohne Probleme umsetzen konnten.

## **Elektrik**

Nach drei Tagen lagen die Module auf dem Dach, die Wechselrichter waren angeschlossen, alle Ziegel kuschelten sich wieder in Position und ein Test mit dem Gartenschlauch bewies, dass das Wasser schön von den Modulen abließ und die Regenrinne erreichte. Einen wichtigen Meilenstein hatten wir geschafft: Die Regenfestigkeit des Dachs hatte durch die Aussparungen nicht gelitten.

Also war es Zeit für unseren letzten Schritt: Die Spannungsversorgung der Ga-

rage läuft über ein  $5 \times 2,5\text{-mm}^2$ -Kabel, das zum Haus führt und dort auch abgesichert ist. Daran hängen Steckdosen für ein Elektrorad, das Garagentor und die Beleuchtung. Außerdem gibt es noch eine CEE-16-Dose. Verteilt wird der Strom mit simplen Feuchtraumdosen.

Hätten wir die Solaranlage – unzulässigerweise – direkt an diesem Stromkreis angeschlossen, hätten Verbraucher bei Sonnenschein mehr als 16 Ampere beziehen können, weil die Sicherung im Haus von dem zusätzlichen Sonnenstrom nichts mitbekommen hätte. Im Falle einer Überlastung könnte es dann zum Brand kommen.

Um für elektrische Sicherheit zu sorgen, installierten wir einen Verteilerkasten mit vier Leitungsschutzschaltern. Die beiden Mikrowechselrichter hängen an einem Sicherungsautomaten  $3 \times 16\text{A}$  B-Typ. Ein zweiter gleicher Bauart sichert die CEE-Dose ab. Das Licht hängt an einem eigenen einphasigen Automaten. Den Steckdosen spendierten wir einen einphasigen Automat mit integriertem Fehlerstrom-Schutzschalter (FI, RCD).

Und hier endete unser Spielraum, Eigenleistung einzubringen. Die Inbetriebnahme der Wechselrichter überließen wir der Elektrofachkraft des Solarbetriebs. Die kann die Anlage beim Termin

mit dem Netzbetreiber verbinden und einschalten.

Gefährlich ist nicht nur die netzseitige Wechselspannung, auch die Gleichspannung der Module kann kritisch sein. Plant man die Anlage nicht mit Mikrowechselrichtern, sondern mit einem großen Wechselrichter, werden die Module in Reihe zu sogenannten Strings verschaltet. In der Reihenschaltung addieren sich die Spannungen – 400 bis 600 Volt kommen auch bei mittelgroßen Anlagen schnell zusammen, wenn die Sonne scheint. Unter keinen Umständen darf man in einem solchen String die MC4-Stecker unter Last abziehen – der entstehende Lichtbogen ist lang und gefährlich. Lebensgefährlich ist es ebenfalls, beide Enden eines Strings gleichzeitig zu berühren. Bei einer solchen Anlage sollten Sie den letzten Schritt, das Verbinden von Wechselrichter mit den beiden Enden des Strings, dem Profi überlassen.

## **Formulkultur**

Es ist wieder Abend geworden auf der Baustelle. Statt Feierabend stand die vielleicht schmutzigste Arbeit des Projektes an: Bevor die Anlage ans Netz geht, möchte der Netzbetreiber mit ausgefülltem Papier versorgt werden. Und was die für den



**Elektrotechnische Laien dürfen durchaus Sicherungskästen setzen und Kabel vorbereiten. Nur den Anschluss ans Stromnetz muss man einem Profi überlassen.**



**Pina Merkert verbindet hier das kurze Verlängerungskabel für den Gleichstromanschluss, während Jan Mahn das letzte Modul bereithält.**

Wohnort von Pina Merkert zuständigen Stadtwerke Kaiserslautern da vorbereitet haben, treibt selbst den Behördenveteranen unserer Runde zur Verzweiflung. Zugeschickt hat uns der Netzbetreiber Formulare, die man nur handschriftlich ausfüllen kann.

Auch inhaltlich gibt es Herausforderungen. Der Vordruck ist so gestaltet, dass man darauf jede Form von Energieerzeugungsanlage vom Kohlekraftwerk bis zur Photovoltaikanlage anmelden kann. Welche Abschnitte sich auf welche Art von Energieerzeugung beziehen, muss der Antragsteller sich erarbeiten. Unklare Formulierungen wie „!!!Zertifikat angehängt“ geben uns den Rest. Nach zwei Stunden der behördendeutschen Begriffsklärung hatten wir endlich doch ein gutes Gefühl mit unseren Eintragungen und erstmals einen Eindruck, woran es bei der Energiewende in Deutschland klemmt. Dachhaken, Module, Elektrik – alles machbar für normale Menschen mit ein wenig Unterstützung vom Fachbetrieb. Aber bei den zur Anmeldung einer simplen Anlagenweiterleitung geforderten Formularen hätten wir beinahe unseren Meister gefunden.

### Anmeldetag

Als das Auto der Elektrofirma auf den Hof rollte, steigerte sich die Spannung

für uns Teilzeit-Solarteure: Wird der Fachmann mit den Augen rollen? Muss er womöglich teuer nacharbeiten? Kann die Anlage vielleicht doch nicht gleich in Betrieb gehen?

Drei Stunden lang musterten kritische Blicke unser Werk. Ein Modul wurde noch mal abgeschraubt, um drunter zu schauen. Messgeräte prüften alle von uns verlegten

Kabel. Doch dann kam die Bestätigung: Wir haben alles richtig aufgebaut. Die Messwerte sind gut, die Anlage konnte ans Netz gehen.

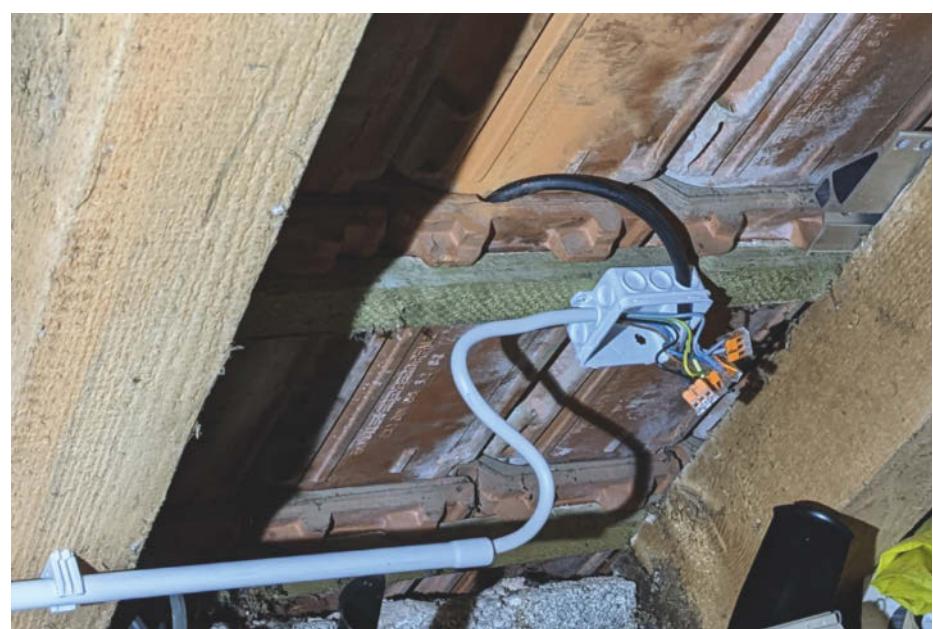
Nach einer Woche intensiver Handarbeit mit drei Personen und mehr als einem Tag in der Verwaltungshölle können wir ziemlich gut einschätzen, wie aufwendig Aufdach-Solaranlagen sind: Raketentechnik ist es nicht. Die technische Komplexität ist eher auf dem Niveau einer Waschmaschinenreparatur, nur eben auf einem Gerüst. Trotz unserer Sicherungsurteile würden wir uns auf dem Dach eines mehrstöckigen Hauses mulmig fühlen. Für die meisten Solaranlagen ist es sinnvoll, das Komplettangebot eines Solarteurs anzunehmen und auch ein paar Monate dafür zu warten. Wer sparen will oder ganz schnell eine Anlage braucht, kann aber versuchen, mit einem Solarteur etwas auszuhandeln. Und für kleine Anlagen auf Gartenhäusern, Vordächern oder Garagen kann sich der Selbstbau absolut lohnen. Bis 600 Watt geht das auch ohne den Papierkrieg, der für uns das größte Ärgernis war.

(pmk@ct.de) **ct**

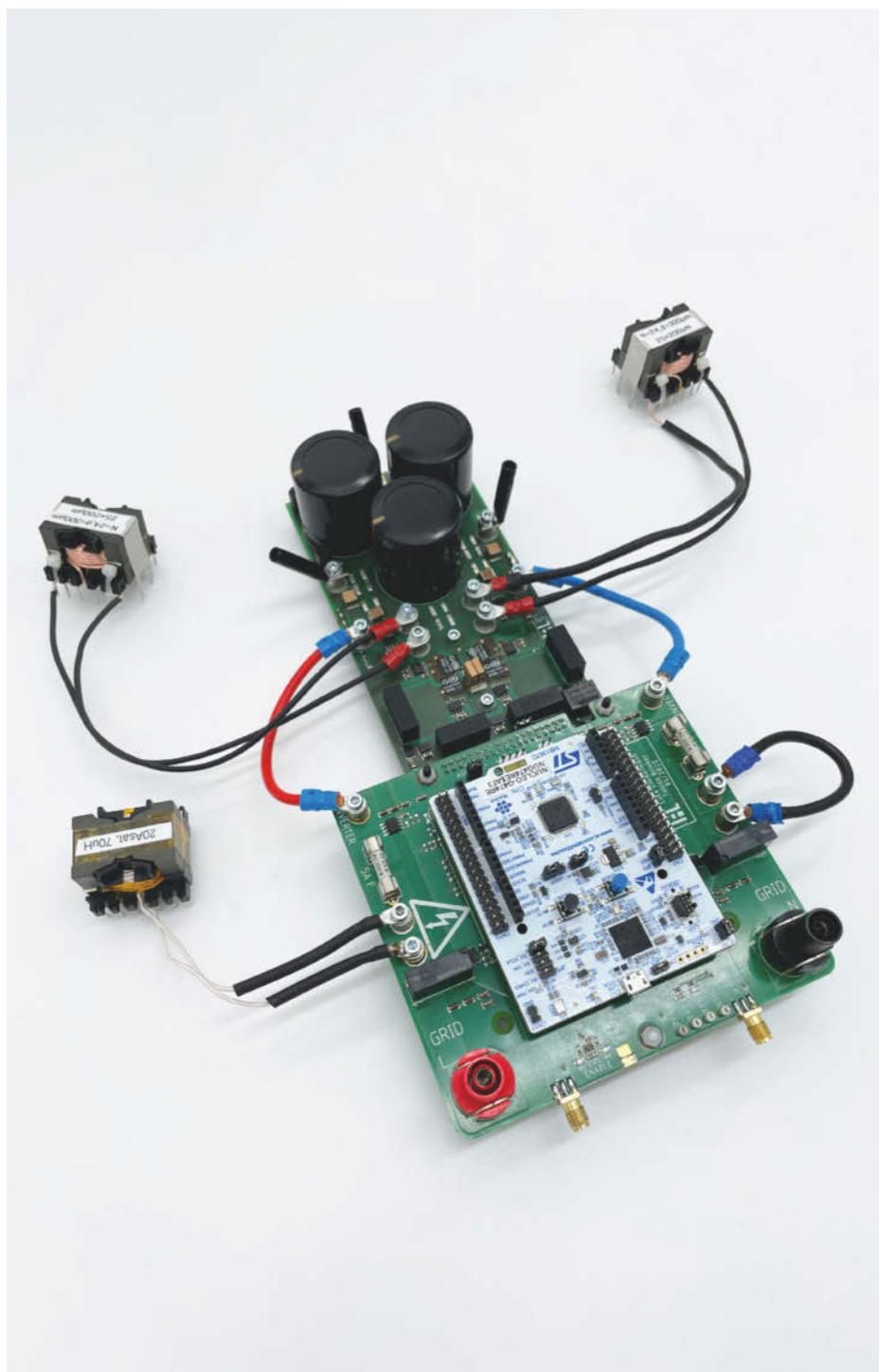
### Literatur

- [1] Jan Mahn und Andrijan Möcker, Heimkleinkraftwerk, Mit Balkonsolaranlagen die Stromrechnung senken, c't 15/2022, S. 20
- [2] Pina Merkert, Brower Aided Design, Einstieg in Onshape: 3D-Designs im Brower, c't 24/2020, S. 150

**CAD-Plan:** [ct.de/yemv](http://ct.de/yemv)



**Die kurzen Anschlusskabel der Mikrowechselrichter konnten wir einfach unter der Ziegel durchführen und innen die drei Phasen verkabeln.**



# Strömchen, wechsel dich!

Wie Solarwechselrichter arbeiten

Ohne Wechselrichter geht nichts an netzgebundenen Photovoltaikanlagen – ob nun am 600-Watt-Balkonkraftwerk oder auf riesigen Dachanlagen mit Dutzenden Kilowatt. Welche elektronische Magie drinsteckt, erklären wir in diesem Artikel.

Von Luca Zimmermann

**O**b klein oder groß: Basis des Sonnenkraftwerks ist meist ein Wechselrichter – also ein Gerät, das die von den Solarmodulen abgegebene Gleichspannung in Wechselspannung wandelt. Doch was passiert eigentlich im Detail in dem Kasten, den mir der Solateur im Keller an die Wand oder draußen aufs Profil schraubt? Und wie arbeitet das Maximum-Power-Point-Tracking (MPPT), von dem die Datenblätter sprechen?

Wer sich mit dem Thema Wechselrichter noch nie beschäftigt hat, ist ob der vielen Bezeichnungen schnell verwirrt. Deshalb lohnt sich ein kurzer Exkurs, der die Begriffe klärt, denn es gibt verschiedene Betriebsarten: Ein autarker Wechselrichter – auch **Inselwechselrichter** genannt – erzeugt seine Wechselspannung selbst und dient dort, wo keine Netzversorgung vorhanden ist – etwa in Wohnmobilien oder entlegenen Hütten – als Spannungsquelle. Manche Modelle haben auch Laderegler, um über angeschlossene Solarmodule Akkus zu laden.

Ein **Hybridwechselrichter** ist, einfach gesagt, ein Inselwechselrichter mit Netzan schluss. Er kann die Wechselspannung nicht nur selber erzeugen, sondern auch die Netzversorgung einfach durchreichen. Wobei die Netzversorgung auch ein herkömmlicher Generator mit Verbrennungsmotor sein kann – etwa als Notfallreserve, wenn die Photovoltaikanlage defekt ist oder im Winter den Leistungsbedarf nicht stillen kann. Die Ausstattung variiert von Modell zu Modell: Viele haben Solar-MPPT-Laderegler (siehe unten) integriert und manche können überschüssigen Solarstrom auf der Netzseite einspeisen, um ihn nicht zu vergeuden.

Ein **netzsynchroner Wechselrichter** benötigt eine vorhandene Wechselspannung, um zu funktionieren – beispielswei-

se die des europäischen Stromnetzes. Er synchronisiert sich mit ihr und speist dann ein, sodass er sich wie ein kleines Kraftwerk ins Stromnetz integriert.

Da in den meisten Photovoltaik-Neuinstallationen heute netzsynchrone Wechselrichter verbaut und diese insbesondere bei Balkonkraftwerken weit verbreitet sind, beschränken wir uns auf diesen Wechselrichtertyp. Damit auch Einsteiger am Ball bleiben, beschreiben wir das Grundprinzip anhand der Wechselrichterbauf orm, die der Autor für seine Informatik-Masterarbeit verwendet hat. Technisch gesehen führen viele Wege nach Rom beziehungsweise zum Stromfluss aus der Sonne. Der Wechselrichter in Ihrem Keller oder auf dem Dach arbeitet vermutlich nicht exakt gleich – sicher aber ähnlich.

Ein paar Grundlagen in Elektrotechnik und Photovoltaik helfen beim Verständnis; in [1, 2, 3] finden Sie einsteigerfreundliche Artikel.

## Leitstelle

Moderne netzsynchronen Wechselrichter besitzen immer eine digitale Steuereinheit. Meistens kommt dafür ein handelsüblicher Mikrocontroller zum Einsatz. Dieses Beispiel nutzt einen STM32-Mikrocontroller der Firma STMicroelectronics.

Die CPU ist ein mit 170 MHz getakteter ARM-Cortex M4 mit 512 KByte Programm speicher sowie 128 KByte Arbeitsspeicher. Speicherausstattung und Taktrate wirken erst einmal lächerlich gering. Doch auf der CPU läuft kein vollwertiges Betriebssystem, sondern eine Firmware, die genau für den Anwendungsfall gebaut ist und keine brachliegenden Zusatzfunktionen als Ballast mitschleppen muss. Zudem besitzt sie für einige der benötigten mathematischen Funktionen Hardwarebeschleuniger. Die einzelnen Bestandteile der Schaltung werden über 50 Ein- und Ausgänge abgefragt beziehungsweise angesteuert.

Oft verschweigen die Hersteller von Wechselrichtern CPU-Details. Bei den meisten dürften je nach Funktionsumfang ähnliche Mikrocontroller, FPGAs oder Mobilprozessoren (ARM, Xtensa etc.) – auch in Kombination – zum Einsatz kommen.

## Leistungspunktsuche

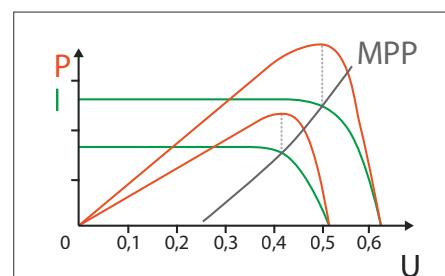
Die Leistungspunktsuche – im Solarjargon meist als Maximum-Power-Point-Tracking (MPPT) bezeichnet – ist eine Kern

funktion jedes Photovoltaikwechselrichters. Denn um Solarmodule optimal auszunutzen, kann man nicht einfach irgend eine Last anlegen.

Einzelne Solarzellen – nicht zu verwechseln mit Solarmodulen, die aus mehreren Zellen bestehen – erzeugen bei Bestrahlung eine Gleichspannung, je nach verwendetem Halbleitermaterial zwischen 0,5 und 0,7 Volt. In Reihe in einem Modul zusammengeschaltet ergeben sich die typischen 18 bis 50 Volt – je nach Modulgröße sowie Anzahl der Zellen und deren Ver schaltung. Während die Spannung im unbelasteten Zustand nahezu immer gleich bleibt, variiert die verfügbare

Leistung mit der Temperatur, Bestrahlung und Beschattung der Zellen. Belastet man das Modul mit einem Verbraucher, sinkt die Spannung zunächst etwas und bricht dann signifikant ein. Der Leistungspunkt (Maximum Power Point, MPP) ist also dort, wo das Produkt aus Strom und Spannung die größtmögliche Leistung ergibt.

Der Maximum-Power-Point-Tracking-Algorithmus versucht, diesen Leistungspunkt für das oder die angeschlossenen Solarmodule regelmäßig neu zu ermitteln. Die einfachste Methode dafür ist, die Solarmodule bei steigender Spannung zu belasten, bis die Leistung einbricht und dann die Belastung wieder zu reduzieren (Perturb & Observe, Bergsteigeralgorithmus). Da sich der Leistungspunkt bei steigender Temperatur in der Grafik nach links und sinkenden Temperaturen nach rechts bewegt, muss der Algorithmus nicht nur



**Der Leistungspunktsucher findet den Arbeitspunkt, an dem Strom und Spannung eines Photovoltaikmoduls die höchste Leistung liefern (MPP). Da sich die Bedingungen aufgrund von Verschattungen, Änderungen in der Sonneneinstrahlung und Verdreckung permanent ändern, muss der Leistungspunktsucher das Optimum ständig neu ermitteln.**

## ct kompakt

- Damit aus der Gleichspannung von PV-Modulen eine haushaltssüdliche Wechselspannung wird, braucht es Wechselrichter.
- Netzwechselrichter, wie sie auch Balkonkraftwerke nutzen, synchronisieren sich mit dem Stromnetz.
- Auch wenn die dafür nötigen Algorithmen komplex sind, kann man den Schaltungsaufbau leicht verstehen.

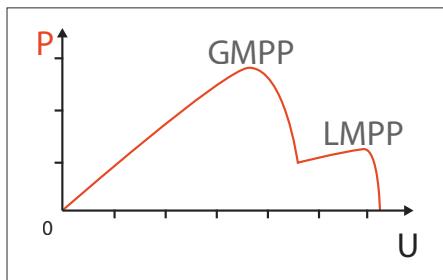
durch Erhöhen, sondern auch durch Absenken des Laststroms regelmäßig prüfen, ob der aktuelle Punkt noch dem Maximum entspricht. Dadurch oszilliert die Leistung immer leicht um den MPP. Das funktioniert problemlos bei nicht verschatteten Panels oder einzelnen Modulen.

## String- versus Mikrowechselrichter

Netzsynchronen Wechselrichter sind heute in zwei Bauformen verbreitet: Mikro- beziehungsweise Modulwechselrichter, die pro Solarmodul einen Eingang und oft sogar individuelle MPP-Tracker haben, und String-Wechselrichter, für die alle Solarmodule in Reihe geschaltet werden.

Die Leistungspunktsuche bei String-Wechselrichtern ist etwas komplizierter als im Beispiel zuvor: Während der Mikrowechselrichter jedes Panel oder zwei nebeneinanderliegende Panels gezielt optimieren kann, muss der String-Wechselrichter das für den ganzen Strang (engl. „String“) erledigen – also für alle Solarmodule gemeinsam. Wenn nun Wolken, Bäume, Antennen oder Schornsteine die Photovoltaikanlage teilweise verschatten, entsteht außer dem globalen Leistungsmaximum (GMPP) auch ein lokales (LMPP), an dem der MPP-Tracker hängenbleiben kann. Moderne String-Wechselrichter prüfen deshalb den gesamten Lastwiderstandsbereich nicht nur regelmäßig auf den optimalen Leistungspunkt, sondern auch dann, wenn sich die Leistungsabgabe der Anlage stark geändert hat.

Die gängige Behauptung, dass ein verschattetes Solarmodul die gesamte Anlage herunterzieht, stimmt bei aktuellen Solarmodulen nicht mehr, denn diese haben eine oder mehrere Bypass-Dioden, über die der



**Fällt Schatten auf einen Teil einer großen Photovoltaikreihenschaltung, dann können zusätzlich zum globalen Leistungsmaximum lokale Leistungsmaxima (LMPP) entstehen. Moderne String-Wechselrichter nutzen Algorithmen zur Leistungspunktsuche, die den gesamten Bereich regelmäßig „abfahren“, um das globale Maximum (GMPP) zu finden.**

Solarstrom an verschatteten und damit unzureichend beladenen Solarzellen vorbeifließen kann. Größere Teilverschattungen bewirken aber möglicherweise, dass die Spannung des Strings unter den Spannungspunkt fällt, ab dem der MPP-Tracker funktioniert, oder sogar so weit absinkt, dass der Wechselrichter seinen Dienst ganz einstellt. Aus diesem Grund setzen wir bei unserem Eigenbau Projekt ab Seite 22 zwei Mikrowechselrichter statt einen String-Wechselrichter ein.

Elektrisch wird die Leistungspunktsuche oft durch eine Spannungs- und Strom-regelbare DC-DC-Stufe umgesetzt – also durch einen Aufwärtswandler, den der Mikrocontroller steuern kann. Die DC-DC-Stufe stellt für die nachfolgenden Stufen eine geregelte Gleichspannung zur weiteren Wandlung bereit – die Zwischenkreisspannung. Durch Verändern des Stroms in den Zwischenkreis und damit indirekt auch ins Netz, regelt sie, wie stark die Solarmodule belastet werden. Die Spannung am PV-Eingang sowie der Strom werden dabei stetig überwacht.

Im Fall unserer Wechselrichterbauweise lädt das MPPT über den regelbaren Aufwärtswandler drei Kondensatoren mit 400 Volt auf, aus denen sich der Wechselrichter bedient.

### Gleich- werd' Wechselspannung

Um ins Stromnetz einspeisen zu können, muss der Wechselrichter die in den Kondensatoren gespeicherte Ladung in eine Sinusspannung mit 50 Hertz wandeln. Das erledigen moderne Wechselrichter digital.

Aufs Nötigste heruntergebrochen kann man einen Wechselrichter mit vier Feldefekttransistoren als elektronische Schalter

bauen. Zwei Transistoren werden mit dem positiven Potential der Gleichspannung verbunden – im Schaltplan  $Q_1$  und  $Q_3$  – und die anderen zwei mit dem negativen Potential beziehungsweise Masse ( $Q_2$ ,  $Q_4$ ). Das erlaubt, die positive Gleichspannung auf L – also Phase – und Masse auf N zu schalten und umgekehrt. Macht man das kontinuierlich, erhält man eine Rechteck-Wechselspannung: Schaltet man  $Q_1$  und  $Q_4$  gleichzeitig ein, so wird der obere Strang positiv und der untere negativ,  $V_{AC}$  ist in dem Fall ein Gleichstrom in Pfeilrichtung. Wenn hingegen  $Q_2$  und  $Q_3$  eingeschaltet sind, fließt der Strom genau entgegengesetzt.

Um nun eine möglichst saubere Sinusspannung zu erzeugen, verwendet der Mikrocontroller Pulsweltenmodulation (PWM) mit hoher Frequenz (140 Kiloherz). Dazu besitzt er Ausgänge, die zusätzliche Schaltkreise auf dem Chip haben, über die die hohe Schaltfrequenz ohne großes Zutun der CPU zustande kommt: die CPU konfiguriert den Ausgang, der zusätzliche Schaltkreis übernimmt den Rest. Ohne diese Unterstützung müsste die CPU sehr viel Rechenleistung für das schnelle Schalten der Ausgänge aufwenden (Software-PWM) – dann würde ein CPU-Kern mit nur 170 MHz Taktfrequenz möglicherweise nicht mehr genügen. Die PWM-Ausgänge sind mit den Steuereingängen der Transistoren ( $Q$ ) verbunden.

Da auch bei elektrischer Spannung Trägheit herrscht, kann man mittels PWM beliebige Spannungen unterhalb der Eingangsspannung erzeugen. Schaltet ein PWM-Ausgang die Transistoren mit hoher Frequenz (in diesem Fall mit 140 Kiloherz) nur während der Hälfte der Zeit ein, entspricht die Ausgangsspannung der Hälfte der Eingangsspannung – man spricht dann von 50 Prozent Tastgrad.

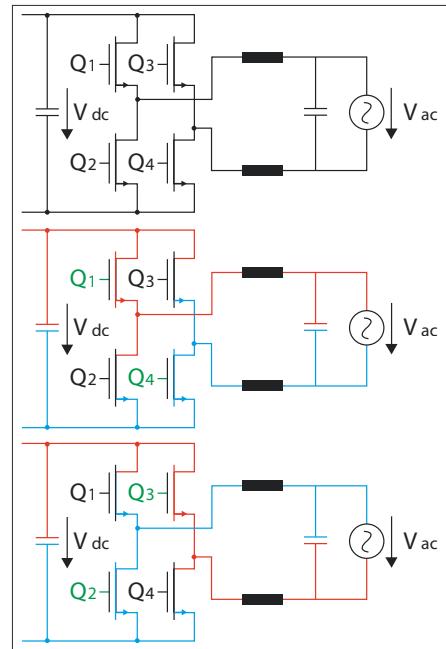
Erzeugt man nun eine linear steigende und fallende Serie an Tastgraden, entsteht eine Rechteckspannung. Weil man für das Wechselspannungsnetz jedoch einen sinusförmigen Verlauf benötigt, wird statt einer linearen Folge dementsprechend auch die Sinusfunktion für den Tastgrad zugrunde gelegt. Der Wechselrichter misst zusätzlich die Zwischenkreis-also Eingangsspannung ( $U_{DC}$ ). Sitzen Kondensatoren im Stromkreis, fließt die Energie der hochfrequenten Rechteckspannung zunächst in die Kondensatoren, sodass die Spannung hinter dem Kondensator nur langsam ansteigt. Beim Ausschalten entlädt der Kondensator ebenso langsam, was die Spannung so glättet, dass von der hohen PWM-Frequenz

nichts mehr zu sehen ist. Ein weiterer Kondensator am Wechselrichtereingang verhindert bei Belastung größere Einbrüche der Gleichspannung.

### Synchronisation & Einspeisung

Damit der Wechselrichter Leistung einspeisen kann, muss nicht nur die Höhe und Frequenz seiner Ausgangsspannung stimmen, auch deren Phase muss im Einklang mit der des Stromnetzes sein. Im einfachsten Fall werden dazu zwei analoge Eingänge des Mikrocontrollers über je eine Spannungsteilerschaltung – zwei Widerstände, über die die Spannung abfällt – mit Nullleiter und Phase verbunden. Der Mikrocontroller ermittelt daraus Spannung und Phasenlage des Netzes. Über eine Phasenregelschleife wird die erzeugte Wechselspannung mit der Netzspannung synchronisiert und kontinuierlich überwacht. Je nach Wechselrichter kann es einige Minuten dauern, bis er synchron ist. Im Optimalfall dauert es wenige Netzperioden.

Anschließend kann er seine Ausgangsspannung leicht erhöhen, sodass Strom ins Netz fließt. Den Ausgangsstrom steuert die Wechselrichterelektronik so, dass die abgegebene Leistung dem MPPT-Maximum entspricht.



Je nach Ansteuerung der Transistoren wird entweder N oder L mit dem positiven respektive negativen Potential der Zwischenkreisspannung verbunden. Macht man das mit hoher Frequenz und wechselnder Einschaltzeit, kann man eine Sinusspannung modulieren.

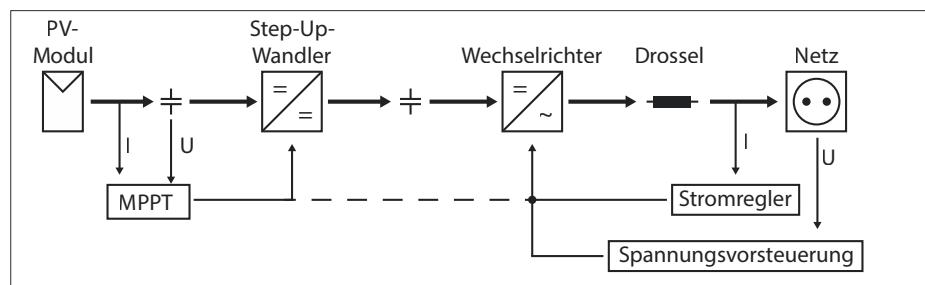
## Schutzabschaltung

Wechselrichter müssen beim Weg- oder Abfallen der Netzspannung oder Defekten im Gerät sofort abschalten. Dieser Netz- und Anlagenschutz ist nicht nur wichtig, weil der „kleine“ 5-Kilowatt-Wechselrichter mit dem Versorgen des gesamten Straßenzugs völlig überfordert wäre: Schalten Wechselrichter nicht unverzüglich ab, könnte es beim Ausstecken von Balkonkraftwerken oder Arbeiten am Leitungsnetz Verletzte oder gar Tote geben.

Der Mikrocontroller überwacht dazu ständig die Netzparameter: Spannung, Frequenz, Netzimpedanz. Befindet sich die Spannung in einem Bereich außerhalb der zulässigen Bereiche oder ist die Phasenlage des Wechselrichters nicht mehr synchron, so trennt der Controller die Verbindung zum Stromnetz über einen Trennschalter. Da auch dieser Schaden nehmen kann, etwa weil sich die Kontakte am Relais durch Stromspitzen zusammenschweißen, ist der Trennschalter mit zwei Relais redundant ausgelegt. PV-seitige Spannungseinbrüche oder Fehler in der Messelektronik muss der Wechselrichter ebenso erkennen. Sinkt die Spannung durch Verschattung so weit ab, dass der Wechselrichter nicht mehr zuverlässig einspeisen kann, so trennt er auch dafür temporär die Verbindung. Sobald wieder ausreichend Spannung anliegt, nimmt er den Betrieb wieder auf.

Spannungseinbrüche im Netz sind erkennbar, auch wenn der Wechselrichter selbst eine Spannung erzeugt. Durch die gleichzeitige Regelung und Messung des Stroms wird die Netzimpedanz mit überwacht, also etwa der Widerstand zum nächsten größeren Anschlusspunkt (Mittelpunktsstrafot). Fällt die Spannung im Netz ab und der Wechselrichter würde weiterhin versuchen, 230 Volt zu generieren, sind deutlich größere Ströme notwendig, um den gesamten Netzabschnitt auf die Spannung zu heben. In der Regel ist die Spannung des Wechselrichters selbst bei maximaler Leistung höchstens wenige Volt höher als die des Netzes. Sinkt die Spannung also rapide, schaltet der Wechselrichter ab. Gleicher gilt für starke Anstiege – etwa beim Ausstecken des Balkonkraftwerks.

Eine Ausnahme bildet dabei der so genannte Fault-Ride-Through. Tritt im Netz ein kurzzeitiger Abfall der Spannung auf, etwa durch einen Kurzschluss an anderer Stelle, so würde das sofortige Abschalten aller Erzeugungsanlagen zu einem Blackout führen. Daher gibt es Vorgaben nach DIN EN 50160, wie lange ein



**Der Netzwechselrichter als vereinfachtes Blockschaltbild vom Solarmodul links über den Wechselrichter zur Einspeisung ins Netz. Dabei werden diverse Parameter gemessen und kombiniert zur Regelung des Wechselrichters genutzt.**

bestimmter Spannungseinbruch toleriert werden muss: Die Spannung darf beispielsweise für 20 Millisekunden um 55 Prozent der Nominalspannung einbrechen oder für fast eine Sekunde um etwa 30 Prozent, ohne dass sich die Erzeugungsanlagen abschalten.

Moderne Netzwechselrichter reagieren auch auf einen Anstieg der Netzfrequenz, also auf ein netzseitiges Überangebot von Strom. Ab 50,2 Hertz bis 51,5 Hertz regeln sie ihre Leistungsabgabe linear herab, bis die Netzfrequenz sich wieder normalisiert. Alte Geräte schalten zum Teil bei 50,2 Hertz einfach ab. Heutige Geräte dürfen das nicht mehr, denn aufgrund der großen Verbreitung von Photovoltaikanlagen würde der schlagartige Wegfall der Produktionsleistung zu einem mehr oder minder starken Einbruch der Netzfrequenz führen. Die Gefahr eines Blackouts bestünde.

## Ensemble

Um die gesamte Funktionsweise besser zu verstehen, lohnt es sich, den Prozess noch einmal von der Gleich- bis zur Wechselspannung zu betrachten. Dazu finden Sie auf dieser Seite ein Blockschaltbild: Sobald die PV-Module bestrahlt werden und eine Spannung erzeugen, kann der Aufwärtswandler den Zwischenkreiskondensator laden. Dabei wird der Ladestrom langsam erhöht, bis die Spannung und damit auch die Leistung am Solarmodul einbricht. Das so gemessene Leistungsangebot zieht der Wechselrichter für seine Stromvorgabe heran.

Für die Erzeugung der Wechselspannung überwacht der Wechselrichter zunächst die Netzspannung und leitet daraus die Parameter wie Spitzenspannung und Phasenlage ab. Mithilfe dieser Werte generiert der Wechselrichter eine synchrone Wechselspannung. Über den vom MPPT ermittelten Leistungspunkt bestimmt der Wechselrichter die ans Netz abzugebende

Leistung. Dann erhöht er die Spannung, sodass Strom fließt: Die Sonnenenergie kann im Netz genutzt werden.

Schutzeinrichtungen verhindern, dass der Wechselrichter bei abnormalen Netzsituationen weiter produziert beziehungsweise das Überangebot vergrößert.

## Raffinierte Technik

Moderne Schaltungs- und Regelungstechnik mit digitalen Steuerungen treiben die Energiewende an. Ohne diese Technik könnte grüner Strom heute nicht so unkompliziert und kostengünstig im eigenen Haus produziert werden. Der hier beschriebene Aufbau steht zwar nur exemplarisch für einen bestimmten einphasigen Wechselrichter und das Verfahren wird sich von Hersteller zu Hersteller in Details unterscheiden. Doch er zeigt das Grundprinzip, das für jeden Wechselrichter ähnlich ist.

Wenn Sie jetzt selbst Lust bekommen haben, grünen Strom zu produzieren, lesen Sie ab Seite 22 unsere Reportage zum Eigenbau einer Photovoltaikanlage. Wollen Sie es lieber eine Nummer kleiner angehen, beginnen Sie mit unserem Artikel zu Balkonkraftwerken [1, 2]. Wer richtig tief einsteigen möchte, kann über ct.de/yfj9 die Masterarbeit des Autors abrufen, für die er einen Netzwechselrichter mitentwickelt und programmiert hat.  
(amo@ct.de) ct

## Literatur

- [1] Jan Mahn, Andrijan Möcker, Heimkleinkraftwerk, Mit Balkonsolaranlagen die Stromrechnung senken, ct' 15/2022, S. 20
- [2] Jan Mahn, Andrijan Möcker, Sonnenwandler, Mikrowechselrichter für Balkonkraftwerke: Grundlagenwissen und Marktübersicht, ct' 17/2022, S. 104
- [3] Jan Mahn, Stromschnellen, Was Sie über elektrischen Strom wissen müssen, ct' 24/2022, S. 122

**Masterarbeit zu Netzwechselrichtern:**  
[ct.de/yfj9](http://ct.de/yfj9)

# Mega-Meta-Strafe

## EU-Datenschützer zwingen irische Aufsicht zu schärferem Vorgehen gegen Meta

**Haben die Meta-Töchter Facebook und Instagram über Jahre Daten ihrer Nutzer ohne Rechtsgrundlage für personalisierte Werbung genutzt? Europas Datenschützer sehen das so. Der Rechtsstreit könnte gravierende Konsequenzen haben.**

Von Falk Steiner

Unmittelbar bevor die EU-Datenschutzgrundverordnung (DSGVO) im Mai 2018 wirksam wurde, hatte Facebook seine Nutzer vor die Wahl gestellt: Entweder sie akzeptieren die aktualisierten Geschäftsbedingungen und stimmen damit auch zu, dass Meta Daten über das Verhalten der Nutzer für seine Werbung nutzt, oder sie verlassen die Plattform. Das war unzulässig, befand im Dezember 2022 der Europäische Datenschutzausschuss (EDSA).

Mit der Entscheidung hat sich der EDSA über die eigentlich federführende Instanz im Verfahren gestellt, nämlich die irische Datenschutzaufsichtsbehörde (Data Protection Commission, DPC). Unter Datenschützern gilt die DPC als besonders unternehmensfreundlich: Weil Irland – ursprünglich wegen seiner niedrigen Steuersätze – ein besonders beliebter

Standort für die EU-Zentralen internationaler Konzerne ist, beaufsichtigt die DPC Aktivitäten vieler US-Tech-Giganten in Europa, darunter Microsoft, Alphabet (Google) und eben Meta. Den Rechtsstreit um die Friss-oder-Geh-Zustimmung bei Facebook und Instagram hatte die zivilgesellschaftliche Organisation „noyb“ des österreichischen Datenschutzaktivisten Max Schrems ins Rollen gebracht. 2018 reichte die Organisation Beschwerde bei der DPC ein, die sich damit seitdem augenscheinlich eher widerwillig beschäftigt.

Die EU-DSGVO gestattet einige Ausnahmen für die ansonsten verbotene Verarbeitung personenbezogener Daten. Außer auf eine Einwilligung kann sich ein Unternehmen auch darauf berufen, seine vertraglichen Verpflichtungen nur mit der Verarbeitung erfüllen zu können. Genau so hatte Facebook argumentiert: Die personalisierte Werbung sei Teil des Produkts, damit sei die Zustimmung in die Vertragsklausel ausreichend. Die irische DPC sah es ähnlich und wollte Facebook 2022 lediglich wegen mangelnder Transparenz eine vergleichsweise geringe Strafe zwischen 28 und 37 Millionen Euro auferlegen.

Daraufhin meldeten andere Aufsichtsbehörden Bedenken an: Die Rechtsauslegung der DPC sei nicht haltbar. Im Dezember überstimmten sie – versammelt im Europäischen Datenschutzausschuss (EDSA) – die DPC und zwangen diese damit zur Korrektur. Anfang Januar 2023

übersandte die irische Behörde nun den Bescheid an Meta. Für den Facebook-Verstoß werden 210 Millionen Euro fällig, für Instagram weitere 180 Millionen Euro – deutliche höhere, aber immer noch überschaubare Strafen.

### Aktive Einwilligung nötig?

Meta kündigte an, den Bescheid zu prüfen und voraussichtlich dagegen in Irland zu klagen. Bis zu einer endgültigen Entscheidung könnten folglich noch Jahre vergehen. Solange könnte der Konzern weitermachen wie bisher. Dennoch evaluiert er nach eigener Aussage, ob und wie er alternative Rechtsgrundlagen in der EU verwenden könnte. Für Meta geht es um viel: Sollte der Beschluss vor Gericht Bestand haben, könnte das bedeuten, dass ohne gültige Rechtsgrundlage erhobene Daten aus den Systemen gelöscht, mindestens aber nicht mehr für die Werbepersonalisierung genutzt werden dürfen. Ob die Nutzer aktiv in die Verwendung der Daten einwilligen würden, ist fraglich. Zumal man vor der ersten Verarbeitung unter anderem darüber informiert werden müsste, dass man seine Einwilligung gemäß Artikel 6 DSGVO jederzeit widerrufen kann – wie man es von den leidigen Cookie-Bannern kennt.

Für die Staatssekretärin im Bundesministerium für Umwelt und Verbraucherschutz (BMUV) Christiane Rohleder ist der Beschluss ein Meilenstein. Sie fordert: „Nutzerinnen und Nutzer müssen mit einer Ja/Nein-Einwilligungsoption wählen können, ob sie der Datensammlung für personalisierte Werbung zustimmen.“ Kritisch beurteilt Thomas Duhr, Vizepräsident des Bundesverbands digitale Wirtschaft (BVDW) den Beschluss. Er zeige insbesondere, „dass mit der DSGVO zwar eine EU-weit einheitliche Gesetzgebung vorliegen mag, die nicht einheitliche Auslegung eben dieser Gesetze das Ideal des Single Markets aber reine Illusion bleiben lässt.“

Die unzufriedene irische Datenschutzaufsicht will derweil selbst vor Gericht gehen – gegen den Europäischen Datenschutzausschuss. Der EDSA hatte mit seinem Beschluss nämlich die DPC Ireland nebenbei dazu verdonnert, im Meta-Reich genauer hinzuschauen und ein Audit bei Facebook durchzuführen. Dies sei eine Kompetenzüberschreitung durch die EU-Kollegen, moniert die irische Behörde. Beide Aspekte dürften daher auch in Brüssel und den Mitgliedstaaten mit viel Interesse verfolgt werden. (hob@ct.de) **ct**



**Beschwerdeführer und Datenschutzaktivist Max Schrems erklärt in einem Video, wie Meta Einwilligungen umgeht, indem der Konzern Informationen zur Datenverarbeitung in den AGB versteckt.**

# EU-Finanzminister gegen anonymen digitalen Euro

**Eine digitale Zentralbankwährung soll nach dem Willen der Euro-Gruppe weder die maximal mögliche Privatsphäre bieten noch programmierbar sein.**

Die Finanzminister der Euro-Gruppe stellen sich in einer Erklärung gegen Vorschläge, Verbrauchern maximale Anonymität zu gewähren, wenn sie mit dem geplanten digitalen Euro zahlen. Zwar messen sie dem Schutz der Privatsphäre „eine zentrale Rolle“ zu, den Begriff „anonym“ vermieden die Minister jedoch. Damit wollen sie Geldwäsche, illegale Finanzierung, Steuerhinterziehung und Sanktionsbruch verhindern. Um diese politischen Ziele zu erreichen, könnte lediglich „ein risikobasierter An-



Bild: Daniel Karmann / dpa

**Die EU-Finanzminister wollen verhindern, dass Bürger mit einem digitalen Euro ähnlich anonym bezahlen können wie mit Bargeld.**

satz verfolgt werden“, bei dem risikoarme Geldflüsse „mehr Privatsphäre“ genießen. Die Minister stellen sich damit gegen Verbraucher- und Datenschützer. Diese fordern, Zahlungen mit dem digitalen Euro so anonym wie mit Bargeld abzuwickeln. Eine potenzielle Nachverfolgung von Transaktionen sollte sich aber zumindest auf klar definierte Zwecke beschränken.

Zugleich betonte die Ministerrunde, dass Menschen auch offline mit dem digitalen Euro zahlen können müssten. Dafür gibt es aus ihrer Sicht zahlreiche Alltagsszenarien. Eine einfache und bequeme Nutzung trage außerdem zur finanziellen Inklusion bei.

Den digitalen Euro programmierbar zu machen, lehnen die Finanzminister indes ab. Damit widersprechen sie einer zentralen Forderung aus der Wirtschaft. Mit programmierbarem Geld könnten Maschinen wie E-Autos und Ladensäulen beispielsweise auf Basis von Smart Contracts selbstständig Preise aushandeln und die Zahlung anschließend in Echtzeit abwickeln. Zwar will die Ministerrunde Möglichkeiten schaffen, Zahlungen automatisch auszulösen, wenn bestimmte „vordefinierte Bedingungen erfüllt sind“ (programmierbare Zahlung). Bürger müssten den digitalen Euro aber jederzeit gleichwertig in Bargeld und Geschäftsbankengeld tauschen können. Die Minister wollen eine mögliche digitale Zentralbankwährung damit deutlich von Kryptoanlagen wie Bitcoin oder Ethereum abgrenzen. (mon@ct.de)

## Handy und Uhr am schnellsten an der Kasse

Mit dem Smartphone oder der Smartwatch zahlen Kunden an der Ladenkasse am zügigsten. Das geht laut Bundesbank aus einer aktuellen Erhebung hervor, in der sie die **Dauer von Zahlvorgängen** mit verschiedenen Zahlungsmitteln untersucht hat. Die beiden smarten Geräte brauchten im Schnitt nur 14 Sekunden. Dahinter landeten kontaktlose Kartenzahlungen ohne PIN-Eingabe mit durchschnittlich 15,2 Sekunden und Barzahlungen mit 18,7 Sekunden. Kontaktlose Kartenzahlungen mit PIN-Eingabe dauerten mit 23,3 Sekunden hingegen fast so lange wie gesteckte Kartenzahlungen (25,7 Sekunden).

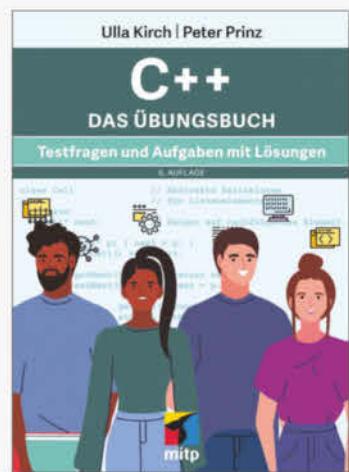
Die tatsächliche Geschwindigkeit hängt demnach insbesondere von der Höhe des Betrags ab. Für Bargeldzahlungen bis 10 Euro

bräuchten Kunden nur um die 15 Sekunden, bei größeren Summen müssten Kassierer hingegen länger zählen und häufiger wechseln. Zudem prüften sie große Banknoten öfter auf Echtheit. Kartenzahlungen ab 50 Euro verzögern sich aufgrund der PIN-Eingabe um weitere Sekunden. Auch die Branche spielt laut Bundesbank eine Rolle; in Supermärkten gehe es generell flotter als in Möbelhäusern oder Drogerien.

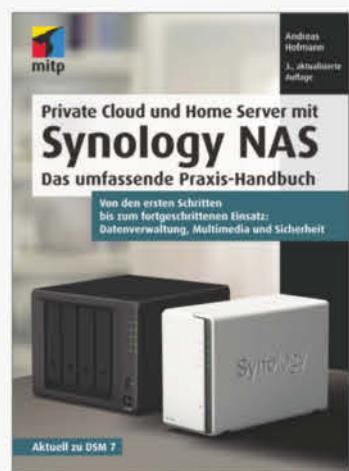
Die Erhebung ist Teil einer noch nicht veröffentlichten, umfassenderen Studie zu den Kosten des Bezahlen im deutschen Einzelhandel. Ihr liegen Zeitmessungen von 10.000 Zahlvorgängen in verschiedenen Branchen zugrunde. Die letzte Erhebung dieser Art fand 2017/18 statt. (mon@ct.de)



Auch als E-Book oder Bundle in unserem Shop erhältlich: [www.mitp.de/0479](http://www.mitp.de/0479)



Auch als E-Book oder Bundle in unserem Shop erhältlich: [www.mitp.de/0637](http://www.mitp.de/0637)



Auch als E-Book oder Bundle in unserem Shop erhältlich: [www.mitp.de/0607](http://www.mitp.de/0607)



**Georges Welz:** Die Definition, was souverän ist, liegt in der Hand des Souveräns, nicht in der Hand der Industrie. Wir übersetzen den Begriff aber gerne mit Wahlfreiheit. Wir wollen moderne Hyperscaler-Cloud-Technik für die Verwaltung nutzbar machen, ohne dass diese sich dabei in eine Abhängigkeit begibt. Man muss zum Beispiel ausschließen, dass jemand einen Dienst wie E-Mail oder Videokonferenz einfach abdrehen kann.

**c't:** Falls Microsoft aus irgendeinem Grund, zum Beispiel wegen eines Handelskonfliktes, keine Updates mehr an Sie ausliefert, wäre Ihre Cloud allerdings nicht mehr sicher nutzbar. Kann da von Souveränität die Rede sein?

**Welz:** Da die Cloud unter unserer Kontrolle ist, kann niemand unmittelbar den Betrieb einschränken. Und falls es keine Updates mehr geben sollte, könnten wir über Monate weiterarbeiten, weil die Cloud auch autark funktioniert. Insofern bieten wir durchaus Souveränität, nämlich einen Handlungszeitraum, um zu reagieren. Man könnte sich über Monate überlegen, wie man die Daten zu einer anderen Plattform bewegt. Deswegen verfolgen Bund und Länder auch eine Multi-Cloud-Strategie. Hier können wir uns im Vergleich zu heute nur verbessern. Wenn man heute keine Updates für Microsoft-Software im eigenen Rechenzentrum bekommt, hat man auch ein Problem.

**c't:** Manche Sicherheitslücken muss man binnen Tagen oder Stunden schließen. Riskieren Sie nicht eine hohe Verwundbarkeit, wenn Sie ohne Updates über Monate weiterarbeiten?

**Welz:** Im Grundsatz ist das richtig. Aber unsere Plattform hat keine unkontrollierte Verbindung mit dem Internet. Man kann das gesamte Umfeld, die Plattform und die angeschlossenen Behördennetze als eine Zone mit höherer Sicherheit betrachten als zum Beispiel einen öffentlichen Exchange-Server.

**c't:** Welche Verbindungen wird es zwischen Ihrer Plattform und Microsoft-Servern geben?

**Welz:** Es gibt Verbindungen, aber keine unkontrollierten. Einwärts gibt es eine Schnittstelle, an der wir und die Behörden die Updates von Microsoft überprüfen können.

# „Die Cloud ist unter unserer Kontrolle“

**Interview: Wie „souverän“ ist die Delos-Cloud für die Verwaltung wirklich?**

**Die SAP-Tochterfirma Delos Cloud GmbH verspricht Bund und Ländern eine „souveräne Cloud“, die vertrauliche Daten von Behörden schützen soll. Doch unter der Haube läuft proprietäre Software von Microsoft. Wir haben Delos-Chef Georges Welz gefragt, wie das zusammenpasst.**

**Von Christian Wölbert**

Auch deutsche Behörden wollen Clouddienste wie Microsoft 365 nutzen, doch bislang verhindern Datenschutzregeln das in vielen Fällen. Dieses Problem soll die SAP-Tochterfirma Delos lösen: Sie baut auf Basis von Microsoft

Azure und Microsoft 365 eine Cloudplattform für die Verwaltung auf.

Da Delos und SAP deutschem und europäischem Recht unterliegen, sollen US-Behörden juristisch keine Möglichkeit haben, auf Daten zuzugreifen. Auch mit technischen Mitteln will Delos Spionage verhindern. Sogar die Anforderungen an die Verarbeitung geheimer Verschlusssachen könnte man erfüllen, verspricht das Unternehmen. Aktuell läuft der Aufbau der ersten Rechenzentren, die Standorte verrät Delos aus Sicherheitsgründen nicht. 2024 soll der Betrieb starten – vorausgesetzt, das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt grünes Licht. Im Interview erklärt Delos-Chef Georges Welz, wie er die BSI-Anforderungen erfüllen will.

**c't:** Herr Welz, Sie versprechen eine souveräne Cloud für die Verwaltung. Was verstehen Sie unter Souveränität?

nen. Und wir müssen auch Informationen aus der Plattform herausbekommen, zum Beispiel Abrechnungsinformationen. Aber auch das ist eine Schnittstelle mit definierten Formaten. Es gibt keinen unkontrollierten Traffic. Zum Beispiel kann keine Applikation auf einen Lizenzserver oder ein Laufwerk in den USA zugreifen.

**c't: Wie läuft die Abrechnung zwischen der Verwaltung, Ihnen und Microsoft?**

**Welz:** Wir werden so nah wie möglich am klassischen System der Public Cloud bleiben. Das heißt, wir rechnen gemäß Nutzerzahl und Nutzung mit der Verwaltung ab und zahlen eine Lizenzgebühr an Microsoft, die wiederum von der Nutzerzahl und der Nutzung abhängt. Deshalb müssen wir Nutzungsinformationen an Microsoft weitergeben, aber diese werden sehr abstrakt sein und zum Beispiel keine Namen von Nutzern enthalten. Die Daten sind auch wichtig für die Kapazitätsplanung, also für die Frage, wann wir neue Hardware installieren müssen.

**c't: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert in seinen sogenannten roten Linien auch, dass kein Dritter, also auch nicht Microsoft, in der Lage sein darf, Daten aus der Cloud zu schmuggeln. Wie wollen Sie das sicherstellen, wenn die Software und Updates von Microsoft kommen?**

**Welz:** Man muss die Updates in Testumgebungen einspielen und schauen, was dort passiert. Microsoft ist auch bereit, eine gewisse Transparenz zu erzeugen. Quellcode-Inspektion funktioniert aber nicht mehr händisch. Es bringt nichts, sich in einen Raum zu setzen und zehn Millionen Zeilen Quelltext zu lesen. Da muss man mit Tools arbeiten. Und alles, was mit Kryptoschlüsseln zu tun hat, werden wir mit der deutschen Sicherheitsindustrie machen. Wir werden dafür keine Standardtools aus den USA verwenden.

**c't: Das heißt, Microsoft wird Ihnen oder den Behörden den Quellcode der Updates bereitstellen?**

**Welz:** Ja. Und das BSI erarbeitet zurzeit, wie man damit umgeht. Bei Verdachtsmomenten könnte man im Quellcode gezielt nachforschen. Aber wir müssen uns dabei auch auf Tools verlassen. Jeder Cloudanbieter macht ein paar Hundert Updates in

**Der ehemalige Microsoft-Manager Georges Welz baut nun als CEO der Delos Cloud GmbH ein spezielles Cloudangebot für die deutsche Verwaltung auf.**



Bild: Delos

Beispiel Dataports quelloffenes Phoenix-Office auf der Plattform laufen lassen. Wir werden nur die Verfehlungen und die wirtschaftliche Entwicklung der letzten 20 Jahre nicht mit einem Fingerschnippen umkehren.

**c't: Die Bundesregierung hat in den vergangenen Jahren immer mehr Geld für Microsoft-Lizenzen ausgegeben. Wird es mit dem Umstieg auf Ihre Cloud günstiger oder noch teurer?**

**Welz:** Das ist pauschal nicht zu beantworten. Im Vergleich wird die normale, öffentliche Microsoft-Cloud günstiger sein, weil die Anforderungen der Verwaltung einen erheblichen Zusatzaufwand bedeuten. Aber es gibt auch große Einsparpotenziale. Die öffentliche Hand betreibt wahrscheinlich über 150 Rechenzentren. Wenn in 100 davon Exchange läuft, und man konsolidiert das auf einer Plattform, dann spart man bei Energie, Fläche, Personal und so weiter automatisch viel ein.

**c't: Allerdings werden Sie mit Ihrer Delos-Cloud quasi ein Einhorn sein. Was schützt den Staat davor, dass Sie Monopolgewinne abschöpfen?**

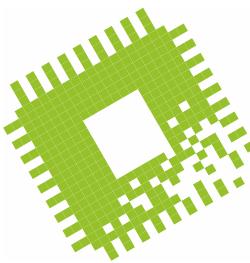
**Welz:** Ich glaube nicht, dass wir die einzige Anbieter sein werden. Wir haben dieses Projekt und die Entwicklung der roten Linien durch das BSI vor viereinhalb Jahren angestoßen. Aber andere können das auf Basis anderer Plattformen umsetzen. Und wir verstehen uns als Partner der öffentlichen Hand. Wir werden uns Mühe geben, dass wir in den Verhandlungen ein belastbares und gesundes Modell finden, das langfristig funktioniert.

**c't: Warum braucht der Bund Sie als private Betreibergesellschaft? Die staatlichen IT-Dienstleister der Behörden könnten die Plattform doch günstiger und genauso gut selbst betreiben.**

**Welz:** Ein staatlicher Betreiber würde dem Haushaltsgesetz unterliegen, das ist heute genau das Problem. Da muss man erst einmal sagen, was man braucht, dann verhandelt der Bundestag über den Haushalt, und erst dann kann man die Hardware nachrüsten. Das widerspricht komplett der Art und Weise, wie Cloud funktioniert. Dort bringen erst die Anbieter die Innovation ein, und die Kunden können sie dann je nach Bedarf nutzen. (cwo@ct.de) **ct**

# Bit-Rauschen

## Intel spart, (Un-)Vernunftprozessoren, UEFI-Löcher



**Die Intel-Führungsriege baut ihre Firma weiter um. AMD und Intel bringen deutlich effizientere PC-Prozessoren auf den Markt, letztere aber auch einen 6-GHz-Hitzkopf. Und wieder tauchen neue UEFI-Sicherheitslücken auf.**

Von Christof Windeck

Der bisher glücklose Intel-Chef Pat Gelsinger hatte im Oktober angekündigt, im Jahr 2023 mindestens 3 Milliarden US-Dollar Kosten einzusparen. Dazu wolle man auch die „Anzahl der Mitarbeiter optimieren“, sprich: Leute rausschmeißen. Doch mehr wurde zunächst nicht bekannt, Gelsinger blieb vage.

Wenn diese c't-Ausgabe am Kiosk liegt, hat Intel jedoch schon die Zahlen für das Jahr 2022 veröffentlicht und vermutlich konkrete Sparmaßnahmen verkündet. Manches geriet schon zuvor an die Öffentlichkeit: In Kalifornien, Irland und Israel bot Intel insgesamt mehreren Tausend Mitarbeitern bis zu drei Monate unbezahlten Urlaub an. Nach Zeitungsberichten sind noch längere Urlaubsphasen mit reduziertem Gehalt möglich und Intel zahlt Abfindungen, wenn man aus der Firma ausscheidet.

Intel spart beispielsweise in der Softwareabteilung: Anfang Januar wurden bei GitHub über 150 Open-Source-Projekte auf „archiviert“ gesetzt, Intel pflegt sie nicht weiter. Und die mit viel Tamtam ins Leben gerufene Grafikchipsparte wurde umstrukturiert. Zwar sollen die für 2024 und 2025 geplanten GPU-Generationen Battlemage und Celestial weiterhin kommen, aber die „Accelerated Computing Systems and Graphics Group“ (AXG) ist Geschichte. Ihre Aufgaben wurden anderen Sparten zugeschlagen und deren 2017

von AMD zu Intel gewechselter Manager Raja Koduri muss einen Karriereknick hinnehmen. Vielleicht wechselt er erst einmal (wieder) in den unbezahlten Urlaub.

Gelsinger hatte im Oktober klargestellt, dass das Zukunftsprojekt „IDM 2.0“ – also der Umbau von Intel zu einem Chip-Auftragsfertiger mit eigener Prozessorabteilung – trotz Sparzwang Priorität hat. Doch um die Finanzierung der neuen Fab in Magdeburg wird geschachert. Intel droht damit, den Bau hinauszuzögern, wenn die Fördermittel nicht kräftig und verlässlich sprudeln. So zäh hatte man sich in Sachsen-Anhalt die Intel-Ansiedlung wohl nicht vorgestellt.

### (Un-)Vernunftprozessoren

AMD stellte auf der CES drei 65-Watt-Versionen des Ryzen 7000 vor, die wesentlich effizienter rechnen als ihre stromdurstigen „X“-Geschwister, siehe Seite 84. An gesichts explodierender Strompreise fragt man sich, warum nicht gleich so? Bald sollen auch die Varianten mit vergrößertem L3-Cache folgen, der wie beim Ryzen 7 5800 X3D in Form eines zusätzlichen Siliziumchips aufgestapelt ist. Bei den Zwölf- und Sechzehnkernern mit je zwei Core Complex Dies (CCDs) – darin sitzen



Den 6-Gigahertz-Prozessor Core i9-13900KS liefert Intel in einer Plastikdose, die außen an einen Silizium-Wafer erinnern soll.

die CPU-Kerne – trägt aber nur je eines davon zusätzlichen L3-Cache. Dadurch haben einige Kerne direkten Zugriff auf besonders viel Cache, aber andere erreichen höhere Turbo-Taktraten. Bleibt zu hoffen, dass es der Scheduler von Windows schafft, bei einem solchen Mix von Eigenschaften die Software-Threads optimal auf die CPU-Kerne zu verteilen.

Auch Intel will bald 65-Watt-Versionen des Core i13000 „Raptor Lake“ liefern. Doch vorher schickt man den extra teuren Unvernunftprozessor Core i9-13900KS ins Rennen, der serienmäßig bis zu 6 GHz erreicht. Für diesen Rekordwert lässt er jedoch in der Spitze 320 Watt durch seine Transistoren rauschen.

### UEFI-Lecks

AMD und Qualcomm bauen in ihre aktuellen PC-Prozessoren jeweils den Microsoft-Sicherheitscontroller Pluto ein. Der funktioniert anfangs genau wie ein eingebettetes Trusted Platform Module (fTPM 2.0), soll in Zukunft laut Microsoft aber für viel höhere Sicherheit sorgen. Peinlich nur, dass Experten der Firma Binarly nun ausgerechnet im UEFI-BIOS-Referenzcode für den Qualcomm Snapdragon Sicherheitslöcher fanden. Die stecken zwar nicht im Pluto-Controller, aber er hilft auch nicht dagegen. Die Lücken ermöglichen es einem Angreifer, die Schutzfunktion Secure Boot auszuhebeln.

Wunsch und Wirklichkeit klaffen aber nicht nur bei Snapdragon-Sicherheitsfunktionen auseinander, sondern auch bei manchen PC-Mainboards. Während nämlich bei komplett mit Windows 11 verkauften Computern UEFI Secure Boot fast immer aktiviert ist, sieht das bei vielen im Einzelhandel verkauften Mainboards anders aus. Denn in den Voreinstellungen des BIOS („BIOS Setup Defaults“) ist Secure Boot häufig deaktiviert. Es lassen sich also beliebige Betriebssysteme installieren, auch welche ohne Microsoft-Signaturen – vermutlich halten sich die Board-Hersteller damit Supportanfragen vom Hals.

Bei vielen MSI-Boards funktioniert Secure Boot aber selbst dann nicht wie erwartet, wenn man es manuell einschaltet. Denn die BIOS-Setup-Option „Image Execution Policy“ erlaubt standardmäßig trotzdem das Ausführen nicht signierter Bootloader. Man staunt immer wieder, mit welchen kuriosen Einfällen manche Firmen Sicherheitsfunktionen aushebeln.

(ciw@ct.de)

Podcast Bit-Rauschen: [ct.de/yfp4](http://ct.de/yfp4)

# EuGH stärkt Auskunftsanspruch

**In einem datenschutzrechtlichen Verfahren gegen die Österreichische Post entschied der EuGH, dass das Unternehmen auf Nachfrage konkret beantworten muss, an wen es personenbezogene Daten etwa zu Marketingzwecken weitergibt.**

Der Europäische Gerichtshof (EuGH) hat die Rechte von Betroffenen bei datenschutzrechtlichen Auskunftsansprüchen gestärkt. Mit einem Urteil vom 12. Januar (Az. C-154/21) bestätigte die erste Kammer des höchsten EU-Gerichts, dass jeder das Recht hat zu erfahren, an wen seine personenbezogenen Daten weitergegeben werden. Unternehmen etwa haben demnach auf Anfrage die konkreten Identitäten aller Empfänger der Daten mitzuteilen. Eine Ausnahme gelte nur, wenn es gar nicht möglich sei, die Empfänger zu identifizieren, oder die Auskunftsanfrage der betroffenen Per-

son „offenkundig unbegründet oder exzessiv“ sei.

Im konkreten Fall ging es um einen österreichischen Bürger, der die Post gemäß Artikel 15 der Datenschutzgrundverordnung (DSGVO) bat, ihm mitzuteilen, an wen sie die zu ihm gespeicherten personenbezogenen Daten weitergegeben hat. In seiner Antwort hatte das Unternehmen lediglich erklärt, es verwende die Daten rechtlich zulässig im Rahmen seiner Tätigkeit als Herausgeber von Telefonbüchern und biete diese Daten Geschäftskunden für Marketingzwecke an. Daraufhin klagte der Bürger, weil er konkretere Auskünfte erwartet hatte.

Der Fall landete schließlich vor dem österreichischen Obersten Gerichtshof (OGH), der wiederum den EuGH um eine verbindliche Auslegung der DSGVO ersuchte. Der EuGH argumentierte, dass viele Betroffenenrechte erst dann prak-



Bild: Rati Labs/Österreichische Post AG

**Die Österreichische Post gibt sich mit einer Filiale im Metaverse und „Crypto-stamps“ IT-affin, hielt sich aber laut EuGH nicht an die EU-Datenschutzstandards.**

tisch wirksam sein können, wenn der Bürger weiß, wer seine Daten erhalten hat. Als Beispiele für derlei Rechte, die aus der DSGVO hervorgehen, nannte er im Urteil unter anderem die Rechte auf Berichtigung und auf Löschung („Recht auf Vergessen werden“). (hob@ct.de)



www.ratiodata.de/karriere/  
Bewirb dich jetzt unter

Wir sind Ratiodata.  
Effiziente und sichere IT-Lösungen.



**SWITCH  
IT UP ...**

RATIO DATA

Die Ratiodata SE zahlt zu den größten Systemhäusern und  
Technologiepartnern in Deutschland. Wir bieten zahlreiche  
Benefits wie mobiles Arbeiten, flexible Arbeitszeiten und  
Weiterbildungsmöglichkeiten. Mach es wie Dennis  
und überzeuge dich selbst.

Wir bewerten und implementieren neue  
Technologien für Finanzdienstleister und  
andere Branchen, dank Experten wie dir.

AND MAKE IT COUNT.

# High-End-Prozessoren mit 3D-Cache sowie bis zu 6 GHz Takt

**AMD und Intel bringen neue CPUs für Gaming-PCs. Die Ryzen 7000X3D erhalten einen größeren Cache. Intel dreht beim Core i9-13900KS hingegen an der Takschraube.**

Nach den Ryzen 7000X und den Ryzen 7000 mit 65 Watt schickt AMD als dritte Unterfamilie ab Februar die Ryzen 7000X3D mit zusätzlichem, aufgestapelten Level-3-Cache ins Rennen. Das soll vor allem bei 3D-Spielen ein deutliches Performanceplus bringen. Im Vergleich zum Vorgänger Ryzen 7 5800X3D verspricht der CPU-Hersteller bis zu 30 Prozent höhere Bildraten. Ryzen 7 7800X3D mit acht, Ryzen 9 7900X3D mit 12 und Ryzen 9 7950X3D mit 16 Kernen erhalten jeweils 64 MByte mehr L3-Cache.

Wegen der schlechteren Wärmeleitung durch den aufgestapelten Zwischen-Speicher begrenzt AMD die Thermal Design Power auf 120 statt 170 Watt und taktet die Prozessorkerne niedriger als die der Schwestermodelle. Der Achtkerner Ryzen 7 5800X erreicht maximal 5,0 GHz

statt 5,4 GHz beim Ryzen 7700X. Bei den zwei Ryzen-9-Cpus sitzt der zusätzliche L3-Cache nur auf einem der zwei CPU Core Dies (CCD). Das hat zur Folge, dass es ein CCD mit 32 MByte L3-Cache und hohem Turbotakt von bis zu 5,7 GHz und eines mit 96 MByte L3-Cache gibt, das jedoch langsamer taktet. AMD will einen aktualisierten Chipsatztreiber veröffentlichen, der dem Scheduler von Windows 11 hilft, Spiele und Anwendungen auf das jeweils optimale CCD zu packen.

Intel setzt beim Core i9-13900KS Special Edition hingegen auf hohe Taktfrequenz. Im Vergleich zum sonst identischen Core i9-13900K mit ebenfalls 8



Bild: AMD

**Den zusätzlichen Level-3-Cache packt AMD nur auf ein CPU Core Die (hier links) der Ryzen 7000X3D. Dummychips gleichen die Höhen-differenz zu den anderen Dies aus.**

Performance- und 16 Effizienz-Kernen erreicht die KS-Variante statt 5,8 bis zu 6 GHz. Allerdings gilt das nur bei Last auf wenigen, ausgewählten Kernen und bei ausreichender Kühlung. (chh@ct.de)

## High-End-Prozessoren von AMD und Intel für Desktop-PCs

Prozessor	Kerne / Threads	Takt / Turbo	L3-Cache	TDP / MTP	Preis
Core i9-13900KS	8 P + 16 E / 32	3,2 / 6,0 GHz	36 MByte	150 / 253 W	780 €
Ryzen 9 7950X3D	16 / 32	4,2 / 5,7 GHz	128 MByte	120 / 162 W	k. A.
Ryzen 9 7900X3D	12 / 24	4,4 / 5,6 GHz	128 MByte	120 / 162 W	k. A.
Ryzen 7 7800X3D	8 / 16	4,0 / 5,0 GHz	96 MByte	120 / 162 W	k. A.

TDP: Thermal Design Power, MTP: Maximum Turbo Power, P: Performancekerne, E: Effizienzkerne

## Sparsame Mobil-CPUs

Für billige Notebooks und Mini-PCs hat Intel **Alder-Lake-N-Prozessoren** vorgestellt. Die N-Serie löst die bisherigen Celeron J/N und Pentium Silver ab. Günstige Modelle heißen nun schlicht Intel Prozessor, während Intel die schnellste Variante als Core i3-N305 bezeichnet. Anders als es der Name vermuten lässt, handelt es sich jedoch bei der Architektur nicht um Core-Prozessoren. Denn die N-Cpus bestehen ausschließlich aus vier bis acht Gracemont-Kernen, die als Effizienzkerne in Core-i-Prozessoren der 12. und 13. Core-i-Generation zum Einsatz kommen. Leistungsfähige Performancekerne fehlen bei Alder Lake-N.

Der Core i3-N305 tritt mit acht Kernen und bis zu 15 Watt an und erreicht bis zu 3,8 GHz. Das 7-Watt-Modell Core i3-N300 unterscheidet sich nur beim thermischen Budget von maximal sieben Watt. Im unteren Segment gibt es zwei Vierkerne N100 und N200 mit je 6 Watt, die mit bis zu 3,7 beziehungsweise 3,4 GHz takten.

Alle CPUs können DDR4-, DDR5- oder LPDDR5-RAM sowie drei Displayausgänge ansteuern. Die Fähigkeiten der integrierten GPU mit 32 Execution Units (N100: 24 EU) und AV1-Videodekoder entspricht der UHD-770-Grafik der Core-i-Desktop-Prozessoren. (chh@ct.de)

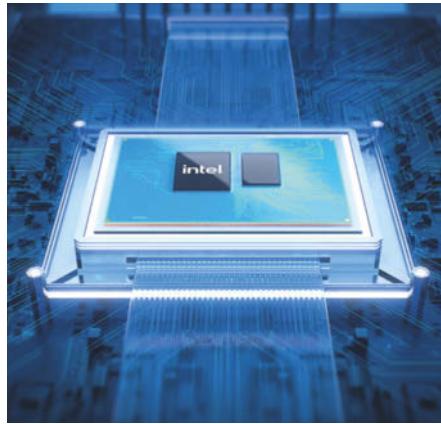


Bild: Intel

**Die Serie-N-Cpus sollen in günstige Laptops und Mini-PCs einziehen.**

## Kurz & knapp

Die RAM-Hersteller überbieten sich momentan mit immer höheren Geschwindigkeiten. Die DIMMs Trident Z5 RGB gibt es nun auch als **DDR5-8000-RAM** mit CL38-48-48-Latenzen. Das Kit aus zwei 16-GByte-Modulen kostet allerdings 550 Euro, rund das Vierfache von gebräuchlichen DDR5-4800-DIMMs.

Anfang Dezember hatte Nvidia mehrere **Sicherheitslücken in Grafiktreibern** für Windows und Linux bekannt gegeben. Deshalb hat der CPU-Hersteller für die rund 10 Jahre alten Grafikkarten der Serien GeForce 600 und 700 zwei Treiberupdates auf Version 474.14 (Windows 10 und 11) beziehungsweise 474.11 (Windows 7 und 8) veröffentlicht, die diese Lücken schließen.

**Download GeForce-Treiber:**  
[ct.de/y3cz](http://ct.de/y3cz)



# Einfach. Professionell. Verbunden.

Zuverlässige und flexible Telekommunikation für jedes Unternehmen.

**easybell**

SIP Trunks | Cloud Telefonanlage | VDSL für Geschäftskunden | Microsoft Teams-Anbindung  
ohne Mindestvertragslaufzeit

## Raspi-Kameras mit Autofokus

**Die Firma Raspberry Pi verkauft vier Varianten des neuen Raspi-Kamera-Moduls mit 12 Megapixel Auflösung und Autofokus.**

Das Raspberry Pi Camera Module 3 hat ein Autofokusobjektiv und den 12-Megapixel-Sensor Sony IMX708 (4608 × 2592 Pixel). Wie ihre weiter erhältlichen Vorgänger wird auch die neue Kamera über ein 20 Zentimeter langes Folienkabel mit dem Camera Serial Interface (MIPI CSI-2) mit einem Raspi verbunden und ist über die Softwarebibliothek libcamera sowie mit Picamera (beta) nutzbar.

Zusätzlich zu der ab rund 28 Euro erhältlichen Version mit Standardobjektiv gibt es eine 10 Euro teurere Weitwinkelvariante und von beiden sind „NoIR“-Ausführungen ohne Infrarotfilter etwa für Nachtaufnahmen lieferbar. Der Sony-Sensor liefert auch HDR-Aufnahmen mit höheren Kontrasten, aber nur 3 Megapixeln.

Von der 2020 eingeführten High-Quality-Kamera mit ebenfalls 12 Megapixeln (Sensor: Sony IMX477, 4056 × 3040 Pixel) kommt eine neue, zusätzliche

Version mit einem Anschluss für M12-Objektive. Der bisherige Typ hat einen Anschluss für C- und CS-Mount-Objektive.

(ciw@ct.de)



Bild: Raspberry Pi Ltd.

**Das neue Raspberry Pi Camera Module 3 ist in vier Versionen erhältlich: jeweils mit Standard- oder Weitwinkelobjektiv sowie mit oder ohne Infrarotfilter (NoIR).**

## Schalschrank-PC mit AMD Ryzen Embedded V3000

Die Firma SolidRun aus Israel hat den **modularen und lüfterlos gekühlten „Bedrock PC“** zum Einbau in Schalschränke und Fahrzeuge entwickelt. Als Prozessor ist ein AMD Ryzen Embedded V3000 eingebaut; die stärkste Version Ryzen Embedded V3C48 hat acht Zen-3-Kerne und 45 Watt TDP. Es gibt aber auch sparsamere Versionen wie den ebenfalls achtkernigen V3C18I, der mit 15 Watt auskommt, aber niedriger taktet.

Der Bedrock PC hat besonders viele Netzwerkports, nämlich bis zu viermal 2,5-Gigabit/s-Ethernet und zwei SFP+-Cages für 10-Gbit/s-Ethernet. Ein WLAN-Modul sowie ein LTE- oder 5G-Mobilfunkadapter sind optional erhältlich. Außerdem gibt es schnelle USB-3.2-Gen-2-Buchsen. Intern lassen sich bis zu 64 GByte DDR4-RAM sowie drei NVMe-SSDs mit PCIe 4.0 x4 einbauen. Preise und Liefertermine nennt SolidRun bisher nicht. (ciw@ct.de)



Bild: SolidRun

**Der SolidRun Bedrock PC ist für den Einbau in Schalschränke gedacht und mit einem AMD Ryzen Embedded V3000 bestückt.**

## Tools und Preise für Arduino-SPS

Das Schalschrank-Steuerungsmodul Arduino Pro Opta ist noch immer nicht lieferbar, aber **mittlerweile sind die Verkaufspreise bekannt und es gibt zusätzliche Software**. Die „Lite“-Version der speicherprogrammierbaren Steuerung (SPS alias PLC für Programmable Logic Controller) mit SMT32H7-Mikrocontroller und vier 230-Volt-Schaltrelais kostet 122 Euro. Für 134 Euro verkauft Arduino Pro die Opta RS485 mit serieller RS-485-Schnittstelle und für 161 Euro die Opta WiFi mit WLAN und Bluetooth.

Die Opta lässt sich mit Arduino-Sketches programmieren, aber – wie es sich für eine SPS gehört – etwa auch mit den nach IEC 61131-3 standardisierten Steuerungssprachen wie Funktionsplan (Function Block Diagram, FBD) oder Kontaktplan (Ladder Diagram, LD). Für FBD und LD sind kostenpflichtige Lizenzschlüssel nötig, der „PLC Key“ kostet 16 Euro. Die zunächst nur für Windows bereitgestellte Programmierumgebung Arduino PLC IDE 1.0 ist hingegen kostenlos und erzeugt auch Code für das Steuermodul Arduino Pro Portenta Machine Control.

(ciw@ct.de)

## Ryzen-7000-Boards für Server

**Asrock Rack kündigt Mainboards für den AMD Ryzen 7000 an, die Serverfunktionen wie ECC-RAM und Fernwartung bieten.**

Für Server verkauft AMD entweder Epyc-Prozessoren, die aufwendige und teure Mainboards verlangen, oder Embedded-Prozessoren wie den Ryzen Embedded V3000 für OEM-Hersteller. Den Einsatz der starken Ryzen-7000-CPU in Servern sieht AMD nicht vor. Diese Lücke schließt die Firma Asrock Rack mit Serverboards für den Ryzen 7000, also mit der Fassung

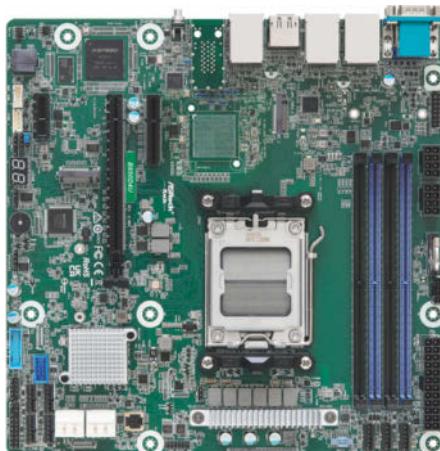


Bild: Asrock Rack

Das Asrock Rack B650D4U für einen AMD Ryzen 7000 hat klassische Serverfunktionen wie ECC-RAM und einen Fernwartungsschip.

AM5 und Steckplätzen für DDR5-Speicher. Darauf steuert der Ryzen 7000 auch RAM mit Zusatzchips für die Fehlerkorrektur per Error Correction Code (ECC) an und es gibt einen Fernwartungsschip (Baseboard Management Controller/BMC) mit separater Netzwerkbuchse.

Die Basisversion des AM5-Serverboards heißt Asrock Rack B650D4U und hat eine Platine mit MicroATX-Format. Darauf sitzen vier DIMM-Fassungen für insgesamt bis zu 128 GByte (ECC-)RAM, zwei PCIe-5.0-Steckplätze (PCIe 5.0 x16 und x4) und eine M.2-Fassung mit PCIe 5.0. Die zweite M.2-Fassung ist per PCIe 4.0 angebunden. Intel-Chips vom Typ I210-AT stellen zwei Gigabit-Ethernet-Ports bereit.

Als BMC kommt der Aspeed AST2600 zum Einsatz; dabei erwähnt Asrock Rack aber nur IPMI und nicht auch das moderne Redfish. Der AST2600 steuert auch einen VGA-Ausgang an; weil die Ryzen 7000 GPUs enthalten, hat das N650D4U aber auch je eine HDMI- und DP-Buchse.

Die teurere Version B650D4U-2T/BCM beherbergt den 10-Gbit/s-Ethernetchip Broadcom BCM57416 anstatt die beiden Intel-Chips. Der Broadcom-Adapter bindet zwei 10GBase-T-Buchsen an. Preise und Liefertermine für die B650D4U-Varianten hat Asrock Rack noch nicht verraten. Der AM4-Vorgänger X470D4U kostet rund 350 Euro.

(ciw@ct.de)

## Mehr PCIe-5.0-SSDs am Horizont

Adata und MSI haben erste lauffähige Muster ihrer PCIe-5.0-SSDs gezeigt. Adata nutzt bei seinem schlicht PCIe Gen5 SSD genannten Modell den SSD-Controller SM2508 von Silicon Motion. Damit soll die SSD lesend bis zu 14 GByte/s erreichen, beim Schreiben sind es rund 12 GByte. Weitere Kenndaten: Bei Zugriffen auf zufällige Adressen verspricht Adata bis zu 2 Millionen IOPS, ein Kühlkörper mit integriertem Lüfter soll die SSD dabei kühl halten.

MSI setzt bei seiner neuen SSD wie bei der bereits bekannten, aber immer noch nicht erhältlichen Spatium M570 auf den E26-Controller von Phison, nutzt aber bei der Spatium M570 Pro nun schnellere Flash-Speicher. 12 GByte/s soll diese beim sequenziellen Lesen erreichen, rund 2 GByte/s mehr als die einfache M570. Beim Schreiben aber schafft auch das Pro-Modell lediglich 10 GByte/s.

Der Hauptgrund für die Verzögerungen bei PCIe-5.0-SSDs ist der Mangel an schnellem Speicher. Der E26-Controller und wahrscheinlich auch der SM2508 nutzen zur Verbindung mit dem Speicher ONFI 5.0, die Schnittstellengeschwindigkeit beträgt 2400 MT/s. Der aktuell einzige Hersteller von passendem Flash ist Micron, doch das Unternehmen kann derzeit anscheinend noch nicht ausreichend Speicher produzieren.

(ll@ct.de)

Wann wurden Sie  
das letzte Mal  
gehackt?

[www.cyber-akademie.de](http://www.cyber-akademie.de)

**CAk**  
Cyber Akademie

Seminare und Workshops zu IT-Sicherheit  
in Behörden und Unternehmen finden Sie hier:



# Abkürzung mit Tücken

## Wie und warum die EU den Google-DNS-Resolven das Wasser abgraben will

**Die EU bewertet die Sicherheit und Vertrauenswürdigkeit der Internet-Namensauflösung in der EU als unzureichend und schiebt mit DNS4EU ein eigenes Projekt an. Das verwundert auf den ersten Blick, aber es gibt andere gute Gründe dafür.**

Von Monika Ermert und Dušan Živadinović

Die EU-Kommission hat neben vielen anderen Infrastrukturen auch die Namensauflösung im Internet untersucht und als kritisch eingestuft. Das ist nachvollziehbar, denn ohne die Übersetzung von Domainnamen zu IP-Adressen (DNS-Anfragen) funktioniert heute so gut wie kein Internetdienst mehr. Diese Arbeit erledigen DNS-Resolver im Hintergrund; eine Kurzbeschreibung finden Sie im Kasten „Resolver-Arbeit“.

Zugleich befand die EU, dass das Sicherheits- und Vertraulichkeitsniveau dieses essenziellen Dienstes in der EU unzureichend sei und initiierte deshalb das Projekt DNS4EU. Das verwundert, denn große Internet-Provider wie die Telekom, Telefónica, Vodafone oder 1&1 verstehen ihr Handwerk, einschließlich des Resolver-Betriebs. Diesen Widerspruch löst die EU zwar nicht auf, aber näher besehen gibt es offensichtliche Gründe für eine europaweit koordinierte Infrastruktur.

Die wichtigsten sind Monitoring und Gefahrenabwehr, Eindämmung des Datenabflusses zu Resolver-Anbietern außerhalb der EU, die Einhaltung der Datenschutzgrundverordnung und die auf die

EU beschränkte Erfassung und Bearbeitung der DNS-Anfragen. Nebenbei will die EU so die Unabhängigkeit von Resolven großer US-Provider wie Google oder Cloudflare fördern.

### EU-weite Gefahrenabwehr

Der vermutlich wichtigste Punkt ist das Monitoring. Dafür wertet man anonymisierte und aggregierte DNS-Anfragen möglichst vieler Nutzer aus und kann so Malware-Kampagnen oder auch Command-and-Conquer-Servers von Angreifern früh identifizieren. Zwar bieten große Resolver-Betreiber wie Google, Cloudflare oder OpenDNS solche Frühwarndienste seit Langem an, aber die Verfechter des EU-Projekts monieren, dass diese eher global orientierten Betreiber lokale Attacken nicht im gleichen Maße berücksichtigen. Eine EU-weite Koordination fehlt bisher, jeder Resolver-Betreiber erledigt das für sich und seine Kunden auf eigene Art.

**Robert Šefr, CTO des tschechischen Security-Spezialisten Whalebone, glaubt, dass das von seiner Firma aufgebaute Projekt DNS4EU bei der Gefahrenabwehr in der EU schneller und genauer sein wird als etablierte Anbieter wie Google und Cloudflare.**

Die Sache hat jedoch einen Haken: Generell funktioniert die Frühwarnung umso besser, je größer der Datenbestand ist. Doch der Anteil der DNS-Daten, den Provider der EU erhalten, schrumpft seit einigen Jahren. Dieses Phänomen haben Provider von autoritären Staaten und Überwachungsbehörden ausgelöst, indem sie DNS-Anfragen zensiert und zur Profilerstellung von Internetnutzern verwertet haben. Denn herkömmliche DNS-Anfragen sind unverschlüsselt, Resolver-Betreiber können sie wie Surf-Tagebücher lesen. Daraufhin hat unter anderem die Internet Engineering Task Force Methoden zur Verschlüsselung entwickelt, beispielsweise DNS-over-HTTPS (DoH). Browser wie Firefox und Chrome nutzen DoH, um ihre Anfragen geschützt an unzensierte Resolver von Google, Cloudflare oder anderen Anbietern zu schicken.

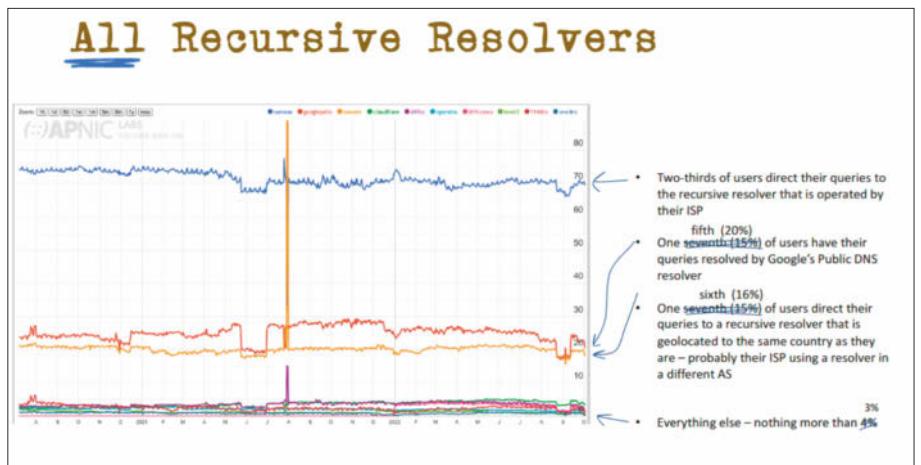
Leidtragende sind seriöse Provider, für die diese DNS-Anfragen unsichtbar sind. Das schmälert die Datenbasis für die Gefahrenabwehr und verhindert den Zugriff auf netzinterne Dienste, die Provider exklusiv für ihre Nutzer anbieten. Auch deshalb fördert die EU eigene Resolver.

### 13 Millionen für 13 Partner

Den Zuschlag für den Aufbau erhielt Ende Dezember 2022 die tschechische Firma Whalebone zusammen mit 12 Partnern (siehe ct.de/y6fy). Das mit 13 Millionen Euro geförderte Projekt hat Whalebone Mitte Januar vorgestellt. Beim Aufbau wollen die 13 Partner auf Infrastrukturen von Internetprovider zurückgreifen. Die großflächige Verteilung und Unabhängigkeit



Bild: Robert Šefr



Laut Messungen der DNS-Spezialisten Geoff Huston und Joao Damas stellen immer mehr Nutzer ihre Internetgeräte um und verschmähen die Resolver ihrer Provider zugunsten von Google und Cloudflare.

keit soll gegen DDoS-Attacken schützen. Am Ende sollen es „viel, viel mehr als einer pro Mitgliedsstaat“ werden, erklärte Robert Šepr, CTO von Whalebone, im Gespräch mit c’t.

DNS4EU wird nicht von der EU unterhalten; die 13 Millionen Euro sind nur als Anschubfinanzierung gedacht. Das Konsortium hat daher ein Konzept entwickelt, um den Betrieb über kommerzielle Angebote zu finanzieren. An erster Stelle stehen jedoch kostenlose öffentliche Cloud-Resolver für jedermann, dazu leicht zu bedienende Apps, mit denen Anwender ihre Geräte für die Nutzung von DNS4EU konfigurieren sollen. Das erinnert an Smartphone-Apps von Cloudflare und anderen Betreibern. DNS4EU könnte aber laut Šepr auch mit Jugendschutzfiltern oder Werbeblockern locken.

Für Internetprovider sind Cloud-Resolver und fertige, für deren Netze ausgelagerte Resolver vorgesehen. Unter anderem sollen die DNS4EU-Resolver Sicherheitsprotokolle von DNSSEC bis zum verschlüsselten DNS-over-QUIC beherrschen und so Providern die Pflege solcher Dienste ersparen. Auch die Cyberthreat-Plattform, über die Informationen über laufende Angriffe gebündelt und ausgetauscht werden, soll es als kostenlose Basis- und kostenpflichtige Premiumvariante geben.

Dabei werde man mit lokalen Sicherheitsteams zusammenarbeiten, aber auch mit Finanzdienstleistern und Regierungen, um lokale Attacken auszufiltern. Grundlage werde ein hierarchisches Meldesystem sein, über das lokale Teams laufend Phishing- und Malware-Kampagnen melden. Die lokale Analyse und Abwehr sowie

Schnelligkeit sieht Whalebone als die größten Vorteile des europäischen Resolvers.

Hier wolle man schneller und besser sein als die Konkurrenz, betont Šepr, und setzt auf ein Netz von Partnern. Dazu gehören die technische Universität Prag, Sicherheitsteams von Italien, Polen, Portugal und Ungarn, F-Secure und die Berliner DNS-Spezialisten von deSEC. Laut Šepr können die Ergebnisse der Analysen an Interessenten verkauft werden. Anfragen von Strafverfolgern zur Herausgabe von Nutzerdaten werde man aber nicht beantworten können, weil man derartige Daten nicht speichere. Funktionsumfang und genaue Preise stehen noch nicht fest.

### Zensurrichtlinien

Ob Nutzer auf DNS4EU in Massen umsteigen werden, hängt auch an der Frage der Zensur und da stehen die Mitbewerber besser da. Denn die EU hat in ihrer Ausschreibung auch das Ausfiltern von Inhalten zur Pflicht gemacht, um EU-Recht und die Vorschriften der 27 Mitgliedsstaaten zu erfüllen. Somit werden die Betreiber von DNS4EU auch Gerichtsentscheidungen zum Sperren von Webseiten umsetzen müssen, die als illegal eingestuft sind. Man werde aber nichts tun, versicherte Šepr, was nicht „100 Prozent rechtlich vorgeschrieben ist“. Google & Co. versprechen aber, überhaupt nicht zu filtern und das ist bisher der Hauptgrund für Anwender, auf solche Resolver auszuweichen.

Šepr hält dagegen, dass die aktuellen Blocklisten der Mitgliedsländer kurz seien. Aus der tschechischen Republik kenne man etwa die Sperren gegen im Land nicht zugelassene Glücksspielbetreiber. Whalebone sei aber noch nicht sicher, ob nur die DNS4EU-Resolver der Provider die lokalen Sperrlisten umsetzen müssten oder auch die offenen Cloud-Instanzen. „Wir holen dazu noch rechtlichen Rat ein“, sagte er.

ber. Whalebone sei aber noch nicht sicher, ob nur die DNS4EU-Resolver der Provider die lokalen Sperrlisten umsetzen müssten oder auch die offenen Cloud-Instanzen. „Wir holen dazu noch rechtlichen Rat ein“, sagte er.

### Mit Großen mithalten

So richtig attraktiv oder dringend erforderlich erscheint DNS4EU bisher nicht. Es gibt viele schnelle Resolver, die auch die Privatsphäre durch Verschlüsselung schützen. Und seriöse Resolver-Anbieter sichern in ihren AGB zu, keine DNS-Anfragen zu protokollieren. Mit kurzen Antwortzeiten glänzen beispielsweise Google, Cloudflare, OpenDNS und Quad9 schon seit Jahren und es wird spannend zu beobachten sein, ob DNS4EU da mithalten wird.

(dz@ct.de) ct

**Ausschreibung für DNS4EU: [ct.de/y6fy](http://ct.de/y6fy)**

## Resolver-Arbeit

Mit der Namensauflösung im Internet ist die Übersetzung von Domainnamen zu IP-Adressen gemeint. Zum Beispiel ist der Webserver von c’t mittelbar über den Domainnamen ct.de erreichbar; tatsächlich benötigt ein Browser zum Öffnen der c’t-Webseite entweder die IPv6- oder die IPv4-Adresse des Web-servers (zurzeit 2a02:2e0:3fe:1001:302:: und 193.99.144.80).

Die Auflösung der Domain zur IP-Adresse ist für fast jede Internetverbindung zwingend erforderlich und die Übersetzungsaufgabe erledigen die Resolver des Domain Name System (weltweite, hierarchisch organisierte Datenbank von Domainnamen, IP-Adressen und vielen anderen Informationen). Deshalb kann man Resolver als technische Plattform sehen, die in den Logs die Surf-Ziele der Anwender prinzipiell mitschreiben kann.

In Europa sind die meisten Router so konfiguriert, dass sie für diese Namensauflösung die Resolver des vom Kunden gewählten Internetproviders verwenden. Laut einer Studie der ICANN nutzen etwa 12 Prozent der Teilnehmer in der EU derzeit einen nicht-europäischen DNS-Anbieter wie Google oder OpenDNS. Die Nutzung von Googles öffentlichen Resolvern nimmt stetig zu.

## 5G-Router mit Wi-Fi-6E und flottem Ethernet

**5G-Mobilfunk liefert Daten im Gigabitbereich. Damit die ebenso schnell bei den Clients ankommen, bietet Netgears neuer Mobilrouter modernes WLAN und 2,5 Gbit/s am Kupferport. Dafür will der Hersteller aber auch gut Geld sehen.**

Nighthawk M6 Pro heißt Netgears neuester Mobilrouter – Modellnummer MR6450. Das 256 Gramm schwere Gerät gehört zur Klasse der akkubetriebenen Router. Sie verbinden über ein integriertes Mobilfunkmodem – etwa aus dem Rucksack heraus – andere Geräte mit dem Internet; wahlweise über USB, WLAN oder Ethernet.

Der MR6450 protzt mit einer stattlichen 5G-Datenrate: **Bis zu 6 Gbit pro Sekunde holt das integrierte Mobilfunkmodem SDX65 von Qualcomm heran.** Dazu bucht es sich in allen in Europa gebräuchlichen 5G-Frequenzbändern unterhalb von 6 GHz ein; bis zu drei davon können für eine höhere Datenrate gebündelt werden. Im

LTE-Modus (Kategorie 20) fasst der Router bis zu fünf Träger zusammen. Selbst das inzwischen von manchen Netzbetreibern rückgebaute UMTS ist noch an Bord.

WLAN-seitig versorgt der Router bis zu 32 Geräte mit Wi-Fi 6 auf 2,4, 5 und sogar 6 GHz (Wi-Fi-6E). Für Tri-Band-Betrieb eignet sich der Router indes nicht, Nutzer müssen sich entweder für 5 oder 6 GHz entscheiden. Netgear gibt fürs 2,4-GHz-Band rund 700 Mbit/s brutto als Spitzendatenrate an sowie rund 2900 Mbit/s für 5/6 GHz.

Für kabelgebundene Geräte hält der MR6450 einen **NBase-T-Port** bis 2,5 Gbit/s bereit. Außerdem reicht er die Netzwerkverbindung über einen Typ-C-USB-Port durch. Netgear spricht von 5 Gbit/s brutto, also USB- und Protokoll-Overhead mitgezählt.

Die mobile Stromversorgung läuft über einen herausnehmbaren 5-Ampere-stunden-Akku, mit dem der Router im Optimalfall 13 Stunden funkeln soll. Grundlegendes kann man über einen



Bild: Netgear

**Internet per 5G-Mobilfunk mit bis zu 6 Gbit/s, schnelles WLAN und 2,5-Gbit/s-Ethernet: Der MR6450 ist top ausgestattet.**

2,8-Zoll-Touchscreen einstellen, Details per Browser.

Der Netgear Nighthawk M6 Pro dürfte der derzeit am besten ausgestattete Mobilrouter auf dem Markt sein, aber auch der teuerste: Das Gerät ist ab sofort für 1000 Euro (UVP) erhältlich. (amo@ct.de)

## Kompakter Netzwerkspeicher mit Ryzen-Prozessor

Synology bringt mit seinem neuen 2-Bay-NAS DS723+ **mehr Wumms ins LAN**: Zwar stecken im von AMD schon 2019 vorgestellten Embedded-Prozessor R1600 zwei SMT-fähige Ryzen-Kerne der ersten Ge-

neration. Aber diese dürften dank ihres höheren Boost-Taktes von 3,1 GHz etwas mehr Single-Thread-Performance schaffen als die in dieser Klasse bisher üblichen Intel-Celerons. Mit 2 GByte DDR4-RAM ist die Werksausstattung nach heutigen Maßstäben zwar mager, schützt aber per ECC (Error Correction Code) vor Einzelbit-Fehlern; maximal fasst das NAS 32 GByte.

Die beiden Gigabit-Ethernet-Ports liefern maximal je 115 MByte/s ins Netzwerk. Mit dem optionalen NBase-T-Ethernetmodul E10G22-T1-Mini für 2,5, 5 und 10 Gbit/s LAN-Datenrate soll das NAS aber rund 470 MByte/s hergeben. Ein optionaler M.2-SSD-Cache könnte den Durchsatz noch steigern. Bei wachsendem Speicherplatzbedarf kann man das NAS über ein Erweiterungsgehäuse mit bis zu sieben zusätzlichen Laufwerken bestücken. Das DS723+ ist ab 510 Euro zu haben, das NBase-T-Modul kostet rund 150 Euro. (ea@ct.de)



Bild: Synology

**Das Ryzen-NAS Synology DS723+ schützt Daten mit ECC-RAM vor Verfälschung und soll mit einem optionalen NBase-T-Modul knapp 500 MByte/s ins LAN liefern.**

### Kurz & knapp

Die in Tschechien entwickelten Turris-Router bekommen mit **Turris OS 6.1.0** ein nützliches Upgrade: Die WAN-Schnittstelle soll nun VLAN-fähig sein, was bei Internetzugängen einiger Provider nötig ist. Ferner speichert der OpenVPN-Client nun Zugangsdaten mehrerer VPN-Anbieter, was den spontanen Wechsel erleichtern soll.

Sparklan vertreibt einen Synaptics-Baustein als **Wi-Fi-6E-Modul AP5881 für Embedded-Systeme**. Der quadratische WLBGA-Chip (Wafer Level Ball Grid Array) hat 8,5 Millimeter Kantenlänge bei 1 mm Dicke. Er nimmt per PCI-Express 3.0 Gen. 2, SDIO V3.0/2.0 oder USB 2.0 Verbindung zum Systemcontroller auf und funkelt über eine externe Antenne in einem der drei WLAN-Bänder 2,4, 5 oder 6 GHz mit maximal 600 Mbit/s brutto. Eine Bluetooth-5.2-LE-Schnittstelle steckt auch drin.

## Handschuh liest Blindenschrift

**Mit LED und Kamera ausgestattet erkennt eine neuartige Lesehilfe namens BrailleWear Buchstaben in Blindenschrift und gibt sie akustisch aus.**

Forscher des Start-ups ORama AI, einer Ausgründung der Cornell University in Ithaca im US-Staat New York, haben einen Handschuh entwickelt, der Sehbehinderten hilft, die international verbreitete Brailleschrift zu erlernen. Das System mit der Bezeichnung BrailleWear umfasst ein Elektronikmodul zwischen Daumen und Zeigefinger. Dieses leuchtet mit einer LED das Papier vor dem Zeigefinger schräg an, sodass eine kleine Kamera die Schatten der erhaben geprägten Braillepunkte aufnehmen kann. Ein einfacher Machine-Learning-Algorithmus erkennt die Buchstaben und eine Sprachausgabe liest sie laut vor. Zudem kann das Gerät auch ganze Wörter erkennen, wobei sich allerdings Erkennungsfehler summieren.



Bild: ORama AI

**BrailleWear** leuchtet die Blindenschrift auf dem Papier seitlich an und kann dann die Buchstaben erkennen. Der Leser hat zur Kontrolle die Fingerkuppen frei.

Die Fingerkuppen des Anwenders sind nicht vom Stoff des Handschuhs bedeckt. So kann er das Zeichen ertasten und prüfen, ob seine Einschätzung mit den in Echtzeit vorgelesenen Buchstaben übereinstimmt. „Viele Sehbehinderte haben Schwierigkeiten, die Brailleschrift zu erlernen, weil man dafür in der Regel einen Tutor benötigt“, sagt Orama-AI-Mitgründer Kushagra Jain. Der Handschuh soll es ihnen ermöglichen, sich die Blindenschrift im Selbststudium zu erarbeiten.

Die Entwickler haben ihren Prototyp zusammen mit der Perkins School of the Blind in Watertown, Massachusetts, entworfen und im Januar auf der Elektronikmesse CES in Las Vegas vorgestellt. Derzeit erreicht der Handschuh laut seinen Entwicklern eine Trefferquote von 90 Prozent. Bis Dezember 2023 plant das Start-up, eine serienreife Version zu bauen und mit Industriepartnern zu vertreiben.

(agr@ct.de)

## Tool entlarvt Propaganda

Mit einem eigens entwickelten Beobachtungs-Tool für Social Media spürt ein Forscherteam um Ulrich Schade am Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) Mechanismen der Meinungsmanipulation auf Twitter auf. Die Forscher untersuchten deutschsprachige Tweets zum Ukraine-Krieg. Ihr Tool **NewsHawk unterstützt Suchen mittels KI-Textanalyse**, indem es Tweets zunächst sammelt und dann inhaltlich kategorisiert und clustert.

Manipulative Anomalien offenbarten sich weniger in den Tweet-Inhalten selbst, sondern vor allem in Metadaten und Interaktionsmustern. Während Teilnehmer einen Tweet in nicht gesteuerter Diskussion über eine gewisse Zeitspanne retteten, kommentieren und zitieren, lassen sich auch andere Muster beobachten. Aufällig ist zum Beispiel eine besonders hohe Zahl an Retweets – das verzerrt die öffentliche Wahrnehmung eines Standpunkts. Eine starke Reaktion vieler Teilnehmer innerhalb eines sehr kurzen Zeitraums lässt vermuten, dass Bots am Werk sind. Diesem Verdacht kann der Anwender dann nachgehen.

NewsHawk visualisiert seine Suchergebnisse und unterstützt interaktive Analysen. Den Prototyp wollen die Entwickler an individuelle Einsatzszenarios anpassen. So könnten Anwender damit beispielsweise beobachten, ob Angreifer zu einem Thema oder einer Institution aktuell Desinformationen verbreiten.

(agr@ct.de)

**Sichern Sie Ihr gesamtes Bürogebäude mit nur EINEM System**  
IoT-basiert ■ Zutrittskontrolle ■ Einbruchalarmierung ■ Videoüberwachung

**Sicherheitstechnik wird einfach und digital.**

Jedes Unternehmen hat einen Bedarf an physischer Sicherheit. Darauf hat Kentix eine revolutionär einfache Antwort entwickelt.

**Lernen Sie diese jetzt kennen – [kentix.com](http://kentix.com)**



**KENTIX**

# Eiliger Beutelschneider

## Preiserhöhung für den Akkuwechsel von iPhones

**Apple hebt die Preise für den Akkuwechsel seiner Smartphones deutlich an. Die Höhe, die versteckte Art der Ankündigung und der Zeitpunkt der Preiserhöhung irritieren.**

Von Dušan Živadinović

Für die meisten iPhone-Nutzer dürfte der Akkuwechsel ein Reizthema sein, für Apple anscheinend auch: Der Konzern hat Anfang Januar eine saftige Preiserhöhung angekündigt, aber nur verschämt als Randnotiz auf einer Serviceseite, versteckt zwischen Beschreibungen des Reparaturvorgangs (siehe [ct.de/yxet](http://ct.de/yxet)).

Ab März verlangt die Firma 24 Euro mehr für den Akkuwechsel bei iPhones bis einschließlich Modell 13. So erhöhen sich die Servicekosten für Geräte ohne Home-Button – iPhone X, XR, XS, 11, 12 und 13 – von 75 Euro auf 99 Euro. Bei Modellen mit Home-Button, etwa iPhone SE, 6s oder 7 sind ab März bei Apple und Vertragswerkstätten nicht wie zuvor 55 Euro zu zahlen, sondern 79 Euro. Für die Geräte der aktuellen 14er-Reihe bleibt es bei 119 Euro.

Unterm Strich muss man bei Apple für den Akkutausch ab März also 80 bis 120 Euro veranschlagen; für den Postweg berechnet Apple zusätzlich 12 Euro. Aber für rund 120 Euro bekommt man aktuell schon ein brauchbares neues Android-Smartphone mitsamt neuem Akku ähnlicher Kapazität, darunter etwa das Samsung Galaxy A04 mit 32 GByte Speicher oder ein Motorola E40 mit 64 GByte Speicher. Ein technischer Grund für den teuren Akkuersatz ist nicht ersichtlich; Android- und Apple-Smartphones setzen auf dieselbe Li-Ion-Technologie.

Auch wirkt der Zeitpunkt der Preiserhöhung ungeschickt bis befremdlich, denn erst Mitte Dezember legte die EU fest, dass Akkus für Elektroautos, Laptops,

Smartphones und andere Geräte künftig leicht und „durch Endnutzer“ wechselbar sein müssen ([ct.de/yxet](http://ct.de/yxet)). Auch dürfen zur Demontage keine „speziellen Werkzeuge, Wärmeenergie oder Lösungsmittel verwendet werden“. Da die Verordnung eine Übergangsfrist von dreieinhalb Jahren gewährt, erscheint Apples Preiserhöhung wie der Versuch, bis zum Ende der Duldung noch möglichst viel aus diesem Ersatzteilgeschäft herauszuschlagen.

### Das exkommunizierte iPhone

Alternativen gibt es zwar, aber sie haben Tücken: Bei freien Werkstätten ist zu beachten, dass Apple ein iPhone von jeglicher weiterer Reparatur exkommuniziert, wenn der neue Akku nicht aus Apples Lieferkette, sondern vom freien Markt stammt. Für iPhones der Reihen 12 und 13 bietet Apple passende Ersatzteilsets ab 50 Euro, aber die Reparatur auf eigene Faust erfordert Feingefühl und ist auch wegen unerwarteter Hürden wie elektronischer und telefonischer Autorisierung sehr aufwendig. Mehr dazu finden Sie in der kommenden Mac-&-i-Ausgabe 1/23.

Noch weniger dürfte für viele Nutzer ein Wechsel auf ein anderes Smartphone-



Wie die allermeisten anderen Smartphones bezieht auch das iPhone seinen Strom aus einem Lithium-Ionen-Akku (im Bild rechts unten). Apple verlangt ab März je nach Modell bis zu 120 Euro für den Austausch dieses Verschleißteils.

betriebssystem infrage kommen, weil sich der Vorgang je nach Umfang der gespeicherten Daten Tage hinziehen kann und viel Erfahrung erfordert, beispielsweise für den Umzug von eSIMs, Banking-Apps und Apple-Pay-Kreditkarten.

So könnten sich am Ende viele Nutzer gezwungen sehen, ihren verschlissenen iPhone-Akku von Apple oder einer Vertragswerkstatt tauschen zu lassen, obwohl es Alternativen gibt.

### Lebensdauer verlängern

Zur Unzufriedenheit trägt Apple auch mit seinem halbherzigen Akkumanagement bei. Wer die Lebensdauer verlängern möchte, kann bestenfalls eine pseudo-intelligente Aufladung mit abgeflachter Ladekurve verwenden. Dann wird der Akku nachts langsam bis 80 Prozent und in den Morgenstunden schnell noch auf 100 Prozent geladen, bevor es der Nutzer üblicherweise wieder in die Hand nimmt. Diese Zwei-Schritt-Methode soll den Akku schonen. Die Rechnung geht aber nur dann auf, wenn man jeden Tag konstant um die gleiche Zeit beginnt.

Elektroautos und viele Notebooks, die wie Smartphones Li-Ionen-Akkus nutzen, kann man hingegen seit Jahren auf eine Obergrenze festnageln. Das schont den Akku nachhaltiger, weil es die Aufladung oberhalb von zum Beispiel 80 Prozent grundsätzlich verhindert. Manche Android-Smartphones können das inzwischen auch, darunter das Samsung Galaxy A51 und A52.

iPhone-User, die dieselbe Funktion wollen, sind auf zusätzliche Hardware angewiesen. Das Start-up Chargei hat einen Stecker entwickelt, den man per USB zwischen Netzteil und Smartphone einkoppelt (35 Euro). Eine gleichnamige Smartphone-App überwacht den Ladevorgang und steuert den USB-Stecker. Wer will, kann so automatisch unterbinden, dass der Akku jemals über 80 Prozent geladen wird.

(dz@ct.de) **ct**

**Akku-Infos:** [ct.de/yxet](http://ct.de/yxet)

## Umsatzbeteiligung bei Kurzvideos

**YouTube beteiligt Produzenten von Shorts künftig an Werbeeinnahmen. Dafür überarbeitete das Videoportal die Bedingungen für die Mitgliedschaft im YouTube-Partnerprogramm.**

Bisher beteiligte Google nur YouTuber an den Werbeeinnahmen, wenn sie mindestens 4000 Wiedergabestunden in den letzten zwölf Monaten vorweisen konnten – für teilweise nur wenige Sekunden lange Kurzvideos (Shorts) eine sehr hohe Hürde. Fortan zahlt Google den Produzenten auch dann Geld, wenn sie 10 Millionen Aufrufe in den letzten 90 Tagen vorweisen können und obendrein 1000 Zuschauer ihren Kanal abonniert haben.

Seit Mitte Januar dürfen Videoproduzenten, die in den zurückliegenden 90 Tagen die formalen Kriterien erfüllten, eine Mitgliedschaft für das YouTube-Partnerprogramm (YPP) beantragen. Erfüllt der Kanal auch die inhaltlichen Anforderungen, erhalten die YPP-Mitglieder 45 Prozent des Werbeumsatzes – frühestens ab 1. Februar. Den Fonds, aus dem das Videoportal bisher kurze Videoformate nach Gutedanken entlohnte, gibt es dann nicht mehr.

YouTube führte im September 2020 unter dem Titel „Shorts“ eine neue Videokategorie ein, um die junge Generation nicht an den Konkurrenten TikTok zu verlieren. (imj@ct.de)

## Kontroverse Fluchregeln

Videoproduzenten kritisieren, dass YouTube Werbeeinnahmen teils willkürlich und nach undurchsichtigen Kriterien entzieht. In den im November 2022 überarbeiteten „Richtlinien für werbefreundliche Inhalte“ setzt die Plattform neue Regeln für Kraftausdrücke: Bitte im Videotitel nur zensiert, keine Flüche in den ersten sieben sowie nur milde in den ersten fünfzehn Sekunden. Nach der ersten Viertelminute sind derbere Ausdrücke erlaubt, sofern sie „nur in einem kleinen Teil des Videos verwendet“ werden.

Darüber seien YouTube-Partner nicht rechtzeitig und eindeutig genug informiert worden, so die Kritik. Obendrein setze YouTube die Demonetarisierung bei längst veröffentlichten Videos durch und zöge teilweise die Werbeignung bei jahrealten Videos zurück. Außerdem kritisierten Videoproduzenten die Einseitigkeit der Regulation, denn der Konzern gewähre YouTube-Partnern kein Mitspracherecht bei der Werbeauswahl. Sie müssten hinnehmen, dass ihre Beiträge etwa durch Werbung für Glücksspiel-Apps oder für offensichtlichen Betrug unterbrochen würden. (imj@ct.de)



**YouTubes neue Regeln für Werbeignung lösen heftige Reaktionen aus, etwa bei dem kanadischen YouTuber Linus Sebastian.**

## Meisterhaft Ziele erreichen

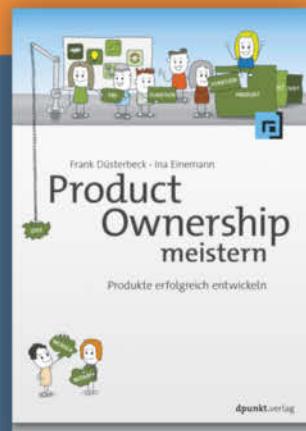


James Shore  
**Die Kunst der agilen Entwicklung**

Grundlagen, Methoden und Praktiken  
• 100 kleine Geschichten von Martin Fowler  
• Aus dem Englischen von Wolf-Günter Böhm und Tim Stöver  
• Übersetzung der 2. Auflage, aktualisierte deutsche Ausgabe

Der US-Bestseller  
in 2. Auflage

dpunkt.verlag



Frank Dürstbeck · Ina Einemann  
**Product Ownership meistern**

Produkte erfolgreich entwickeln

236 Seiten · in Farbe · 34,90 €

ISBN 978-3-86490-901-6

## mit agilen Methoden



Aina Vunge Corry  
**Antipatterns in Retrospektiven**

• 100 neue Antipattern und Lösungen für die Praxis der Retrospektiven

AUS ERFAHRUNG LERNEN

dpunkt.verlag



Robert Weichmann · Sven Röpstorff  
**Scrum in der Praxis**

Erfahrungen, Problemfelder und Erfolgsfaktoren

• 100 neue Lösungen und Fall-Vision

388 Seiten · 37,90 €

ISBN 978-3-86490-880-4

## und klarer Kommunikation



Uwe Vigorschow · Björn Schneider · Ines Meyrose  
**Soft Skills für Softwareentwickler**

Fragetechniken, Konfliktmanagement, Kommunikationsarten und -modelle

dpunkt.verlag



Veronika Jungwirth · Ralph Marka  
**Agile Teams lösungsfokussiert coachen**

• 100 neue Lösungen und Fall-Vision

4. Auflage · 300 Seiten · 34,90 €

ISBN 978-3-86490-896-5

# Microsoft 365: Neues Einsteiger-Abo

**Ab Februar führt Microsoft ein neues Abo mit 100 GByte Cloudspeicher, aber ohne lokal installierbare Office-Programme ein. Im Wesentlichen ist das ein neues Label für ein bestehendes OneDrive-Angebot.**

Microsoft kündigt für Anfang Februar eine neue Abstufe für Microsoft 365 (vormals Office 365) an. Sie soll die Lücke zwischen kostenlosen Accounts und dem günstigsten Angebot „Microsoft 365 Single“ schließen. Das neue Abo heißt „Microsoft 365 Basic“, kostet 2 Euro pro Monat oder 20 Euro pro Jahr und gewährt 100 GByte Cloudspeicher auf OneDrive. Zudem wird die Werbung aus Outlook.com entfernt und Abonnenten erhalten Support für Microsoft 365 und Windows 11. Für die Zukunft sind weitere Funktionen wie Ransomware-Schutz und kennwortgeschützte Freigabelinks angekündigt.

Microsoft 365 Basic **enthält nicht die lokal installierbaren Office-Programme**, sondern beschränkt sich auf die Browserversionen von Word, Excel und PowerPoint, die auch Nutzern eines kostenlosen Microsoft-Accounts mit nur 5 GByte OneDrive-Speicher zur Verfügung stehen. Im Wesentlichen handelt es sich bei Microsoft 365 Basic also um ein Cloudspeicher-Abo. Preislich liegt es gleichauf mit Google Drive; die Abos beim Konkurrenten Dropbox beginnen erst bei 2 TByte für zehn Euro pro Monat.

Tatsächlich ist Microsoft 365 Basic gar nicht so neu: Schon seit einiger Zeit bietet Microsoft ein OneDrive-Abo („OneDrive Standalone“) mit 100 Gbyte zum selben Preis an – jedoch ohne werbefreies Out-

look.com und die angekündigten Schutzfunktionen. Besitzer dieses Abos sollen automatisch auf Microsoft 365 Basic umgestellt werden.

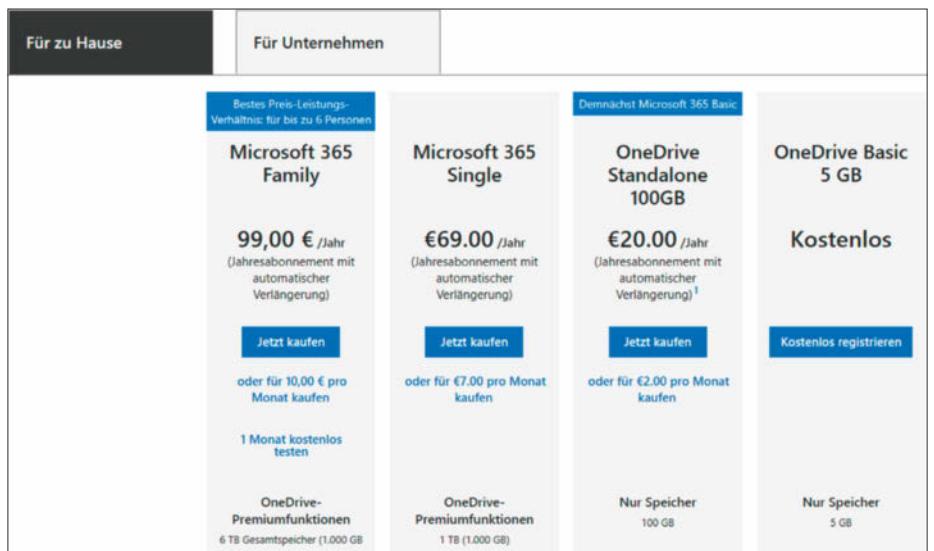
Microsoft 365 Basic ist nicht zu wechseln mit dem schon länger existierenden Plan „Microsoft 365 Business Basic“. Das ist ein Abo für kleinere Unternehmen und wird pro Benutzer bezahlt. Es enthält zwar ebenfalls nicht die lokal installierbaren Office-Programme, jedoch 1 TByte Cloudspeicher und E-Mailkonten mit Firmendomain. Zudem erlaubt es Teams-Konferenzen mit bis zu 300 Teilnehmern.

Unlängst wurde Abonnenten von Microsoft 365 Personal und Microsoft 365

Family angekündigt, dass ab Februar 2023 alle Mailanhänge in ihrem Outlook.com-Postfach vom OneDrive-Kontingent (üblicherweise 1 TByte) abgezogen würden. Allerdings stockt Microsoft dieses für eine Übergangsfrist von einem Jahr um 50 GByte auf.

Kostenlose Microsoft-Konten scheinen davon bislang nicht betroffen. Noch gibt es zu den 5 GByte Cloudspeicher zusätzlich 15 GByte für das Outlook.com-Mailpostfach inklusive Anhängen. Ob das so bleibt oder Microsoft eine ähnliche Änderung wie bei den MS-365-Konten plant, um zum Abschluss eines MS-365-Basic-Abos zu animieren, ist noch unbekannt.

(swi@ct.de)



The screenshot shows the Microsoft 365 pricing page. It is divided into two main sections: 'Für zu Hause' (For Home) and 'Für Unternehmen' (For Business). Under 'Für zu Hause', there are four options: Microsoft 365 Family (99,00 €/Jahr), Microsoft 365 Single (69,00 €/Jahr), OneDrive Standalone 100GB (20,00 €/Jahr), and OneDrive Basic 5 GB (Free). The OneDrive Standalone 100GB plan is labeled as 'Demnächst Microsoft 365 Basic'. Under 'Für Unternehmen', there are four options: Microsoft 365 Business Basic (99,00 €/Jahr), Microsoft 365 Business Standard (119,00 €/Jahr), Microsoft 365 Business Premium (139,00 €/Jahr), and Microsoft 365 E3 (159,00 €/Jahr). The OneDrive Standalone 100GB plan is also labeled as 'Demnächst Microsoft 365 Basic'. The Microsoft 365 Family and Single plans are highlighted with a blue box and the text 'Bestes Preis-Leistungs-Verhältnis für bis zu 6 Personen'.

**Das von Microsoft bislang als „OneDrive Standalone“ angebotene Cloudspeicher-Abo heißt in Zukunft „Microsoft 365 Basic“, erhält aber ansonsten wenig Zusatzfunktionen, zumindest zum Start.**

Bild: Microsoft

## MS Teams Premium startet

Auf der Ignite 2022 hatte Microsoft ein  **kostenpflichtiges Zusatzpaket für Microsoft Teams** angekündigt. Für voraussichtlich 10 Euro pro Monat und Nutzer erhalten Teams-Kunden nun einige neue Funktionen. Dazu gehören Corporate-Design-Gestaltungsmöglichkeiten für Lobbies, Meetings und den Together-Mode, Green-Rooms, in denen sich Moderatoren auf Meetings vorbereiten können und Erinnerungsmails an angemeldete Webinar-Teilnehmer. Microsoft hebt neue Sicherheitsfunktionen hervor, etwa die Möglichkeit, Aufzeichnungen

mit Wasserzeichen zu versehen, und eine Ende-zu-Ende-Verschlüsselung von Meetings mit bis zu 50 Teilnehmern. Sie wird wie auch einige andere Funktionen – zum Beispiel die automatische Kapitelaufteilung aufgezeichnete Konferenzen – erst später hinzukommen.

Eine vollständige Liste der Premiumfunktionen finden Sie unter <https://heise.de/s/5VdA>. Der Webseite lässt sich zudem entnehmen, dass einige bisher im regulären Teams verfügbare Funktionen hinter die Premium-Paywall rutschen. Dazu ge-

hören mehrsprachige Live-Untertitel, Zeitstrahlmarker in aufgezeichneten Meetings für später hinzukommende und vorzeitig gehende Teilnehmer sowie die individuelle Anpassung von „Together“-Szenen.

Derzeit gibt es einen Preview-Zugang, den Administratoren zentral aktivieren können. Sie erhalten dann auf 30 Tage begrenzte Lizenzen für maximal 25 Nutzer. Nach dem Testzeitraum verlieren Anwender die zusätzlichen Funktionen, wenn sie keine Lizenzen kaufen. (swi@ct.de)

# NVK-Entwickler demonstrieren 3D-Beschleunigung

**Der neue quelloffene Vulkan-Treiber für Nvidia-Grafikkarten NVK rendert erstmals 3D-Spiele.**

Der NVK-Entwickler und Red-Hat-Mitarbeiter Karol Herbst teilte über Mastodon einen Screenshot, der zeigt, dass der neue quelloffene NVK-Treiber das Spiel „The Talos Principle“ rendert. Bei NVK handelt es sich um einen freien Vulkan-Treiber für Nvidia-Grafikkarten in der Grafikbibliothek Mesa. Herbst, der ebenfalls am Nouveau-Projekt beteiligt ist, kommentiert, dass die Performance noch stark zu wünschen übrig lässt. Das eingebundene Performance-Overlay besagt, dass eine Nvidia GeForce GTX 1650 das Spiel bei einer Auflösung von  $1024 \times 576$  mit 5 Bildern pro Sekunde (fps) berechnet. Das Ergebnis soll sich aber verbessern, sobald der Nouveau-Treiber im Kernel den GPU System Prozessor (GSP) ansprechen kann.

Die Nouveau-Entwickler haben bereits eine Reihe von Codeänderungen für Linux 6.2 eingereicht, die den GSP-Support vorbereiten. Sobald der GSP mit Nouveau funktioniert, kann der Treiber dieselbe Firmware wie der herstellereigene Nvidia-Treiber nutzen und die Taktraten kompatibler Grafikkarten anheben, die zurzeit lediglich mit einem niedrigen Ba-

**Der Screenshot von „The Talos Principle“ demonstriert, dass der NVK-Treiber schon jetzt 3D-Spiele rendert kann. Bis der Treiber alltagstauglich ist, dürfte noch viel Zeit vergehen.**



Bild: Screenshot @karolherbst@chaos.social

sistakt laufen. Das Nouveau-Projekt profitiert dabei von Nvidias Veröffentlichung des Quellcodes der Kernel-Module des Grafiktreibers, wie der Nouveau-Entwickler David Airlie auf der Linux-Plumbers-Konferenz in einem Vortrag erklärte, den wir unter [ct.de/y7nw](http://ct.de/y7nw) verlinkt haben.

Der NVK-Entwickler und Collabora-Mitarbeiter Jason Ekstrand hatte den NVK-Treiber in einem Blogpost im Oktober vergangenen Jahres vorgestellt (siehe [ct.de/y7nw](http://ct.de/y7nw)). Sein Ziel sei es, dass NVK zukünftig über den gleichen Funktionsumfang wie RADV, der etablierte Vulkan-Treiber in der

Grafikbibliothek Mesa für Radeon-GPUs, verfügt. NVK wird derzeit noch in einem eigenen Zweig abseits von Mesa entwickelt. Bis der noch junge Treiber alltagstauglich ist und 3D-Spiele flüssig rechnet, haben die Entwickler noch viel Arbeit vor sich. Man kann aber schon mit dem Treiber experimentieren und den Quellcode in einem GitLab-Repository des Nouveau-Projekts einsehen, das wir unter [ct.de/y7nw](http://ct.de/y7nw) verlinkt haben. (ndi@ct.de)

**Vortrag über Neuerungen bei Nouveau und GitLab-Repository: [ct.de/y7nw](http://ct.de/y7nw)**

## Alles zu Hacking in einem Heft

Das neue c't Sonderheft Hacking-Praxis bringt Ihnen die typische Vorgehensweise und Werkzeuge von Hackern näher. Mit Beispielen aus der echten Welt sammeln Sie erste Erfahrungen und lernen hautnah, wie ein Hacker tickt.

In drei Kapiteln verteilt auf 84 Seiten lernen Sie Tools kennen, um in einer abgeschotteten Umgebung sicher Webserver zu hacken. OSINT-Techniken helfen Ihnen, Daten aus öffentlichen Quellen zu sammeln und auszuwerten. Außerdem analysieren Sie Malware und werfen einen Blick in deren Innenleben. Zusätzlich gibt es einen Videokurs, der Ihnen unter die Arme greift, Grundlagen erklärt und unterschiedliche Sicherheitslücken aufschlüsselt. Das Sonderheft bekommen Sie in der c't-App und im heise Shop digital für 12,99 Euro. Die gedruckte



Ausgabe kostet 14,90 Euro (zuzüglich Versand) und zusammen mit der PDF-Datei 19,90 Euro. (wid@ct.de)

## Open Source in Dortmund

Der Rat der Stadt Dortmund hat Ende Dezember beschlossen, eine **Koordinierungsstelle Digitale Souveränität und Open Source** einzurichten. Die soll darauf hinarbeiten, Open Source in der Verwaltung zu verankern, um die Stadt unabhängiger von proprietärer Software zu machen. Die Koordinierungsstelle im „Chief Information/Innovation Office“ soll zwischen der Verwaltung, dem stadteigenen IT-Dienstleister dosys, der Politik sowie zu bürger-schaftlichen Initiativen vermitteln.

Gemeinsam mit dem Fachverband „Kommunale Gemeinschaftsstelle für Verwaltungsmanagement“ (KGSt) ist laut Christian Nähle von der Initiative Do-FOSS geplant, eine ganzheitliche Open-Source-Strategie zu entwickeln. Dortmund steht außerdem mit Berlin und München im Austausch über Open Source. (ktn@ct.de)

## Sennheiser Conversation Clear Plus: Getarnte Hörhilfe

**Die neuen In-Ears von Sennheiser schlagen die Brücke zum Hörgerät. Außerdem hat die deutsche Traditionsmarke ein günstiges Kabel-Headset für Musikhörer vorgestellt.**

Die Sennheiser Conversation Clear Plus sind In-Ear-Kopfhörer, die primär als Hörhilfe gedacht sind. Sie richten sich an Menschen, die zum Beispiel in lauten Umge-

bungen Probleme haben, Gespräche zu folgen, aber nicht dauerhaft auf ein Hörgerät angewiesen sind.

Sennheiser greift für die In-Ears auf die Chips des Hörgeräteherstellers und Mutterkonzerns Sonova zurück, verkauft die Conversation Clear Plus aber ausdrücklich nicht als medizinisches Gerät. Anders als bisherige Sennheiser-Kopfhörer für besseres Hören sind die Conversation Clear Plus nicht primär fürs Fernsehschauen gedacht.

Vielmehr sollen sie helfen, Gespräche in lauten Umgebungen besser zu verstehen – auch beim Telefonieren. Dafür analysieren die Kopfhörer 166-mal pro Sekunde die Umgebungsgeräusche und leiten diese moduliert ans Ohr: Stimmen werden verstärkt, störende Geräusch reduziert. Der Conversation Clear Plus hat auch einen ANC-Modus, dieser dämpft Umgebungsgeräusche – genau wie es herkömmliche Kopfhörer mit aktiver Geräuschunterdrückung tun. Sennheiser ruft für die Conversation Clear Plus 849 Euro auf.



Bild: Sennheiser

Bild: Sennheiser

**Die Sennheiser Conversation Clear Plus sehen aus wie herkömmliche In-Ears, doch hauptsächlich sollen sie als Hörhilfe zum Einsatz kommen.**



**Kein ANC, kein Bluetooth, kein Schnickschnack: Sennheisers IE 200 sollen ähnlich gut klingen wie das Schwestermodell IE 600, kosten aber weniger als ein Viertel.**

Neu im Programm sind die kabelgebundenen In-Ears IE 200, deren Kabel sich austauschen lassen. Die 150-Euro-Kopfhörer weisen laut Hersteller eine ähnliche Klangsignatur auf wie das 700 Euro teure Geschwistermodell IE 600, das im c't-Test überzeugt hat (Test in c't 9/2022, S. 78).  
(rbr@ct.de)

## Headset mit neuen Bluetooth-Codecs

Die Audeze Maxwell mit langer Laufzeit und niedriger Latenz sollen laut Hersteller für Gamer sowie Leute gut sein, die an vielen Videokonferenzen teilnehmen. Der Mikrofonarm ist abnehmbar, ein beiliegender Funkdongle soll den Ton mit einer niedrigen Latenz von 18 ms übertragen. Zum

Verbinden kann man aber auch Bluetooth 5.3 oder ein USB-C-Kabel nutzen. Es ist eines der ersten, das das neue Bluetooth-Übertragungsverfahren LE Audio versteht. Im Zentrum von LE Audio steht der neue Codec namens LC3, der besseren Klang ermöglichen soll. Zudem sind SBC, AAC und LDAC an Bord. Beim kabellosen Betrieb verspricht Audeze eine Laufzeit bis zu 80 Stunden. Beim ersten Ausprobieren bei der CES-Messe in Las Vegas überzeugten uns der druckvolle Sound der planar-magnetischen 90-Millimeter-Treiber und die Räumlichkeit.

Audeze vertreibt eine Dolby-Atmos-zertifizierte Version für die Xbox und eine Playstation-Version mit Tempest 3D Audio. Derzeit sucht man noch einen auf Gaming spezialisierten Vertriebspartner für Deutschland, sagte Firmenchef Sankar Thiagasamudram gegenüber c't. Online-versender Thomann verkauft das Headset bereits, die Xbox-Version für 439 Euro, die Playstation-Version für 399 Euro.

(rbr@ct.de)



Bild: Audeze

**Vielseitige Kopfhörer mit kräftigem Sound: Die Audeze Maxwell sind mit Bluetooth 5.3 ausgestattet.**

## Ohrringhörer

Die Nova H1 verstecken **kleine Lautsprecher und Mikrofone in Ohrringen**. Per Bluetooth kann man darüber telefonieren und Musik hören. Das Unternehmen hat nach eigenen Angaben zwei Mikrofone pro Stecker eingebaut. Ein Akku im Perlenohrring soll bis zu zweieinhalb Stunden telefonieren ermöglichen. Im beiliegenden Case lädt der eingebaute Akku die 7,7 Gramm leichten Ohrringe dreimal auf. Der Akku lässt sich nach Herstellerangaben austauschen. Die Kickstarter-Kampagne für die Hörringe hatte der Hersteller bereits 2021 gestartet, jetzt startet der offizielle Verkauf. Die H1 gibt es als Stecker und als Clip ab 595 Euro.  
(rbr@ct.de)



Bild: Nova-Audio

**Die Nova H1 sind nicht als Ohrhörer zu erkennen. Es gibt sie als Clip und als Stecker.**



## B1 Consulting Managed Service & Support

individuell – umfassend – kundenorientiert

Neue oder bestehende Systemlandschaften stellen hohe Anforderungen an Ihr IT-Personal. Mit einem individuellen Support- und Betriebsvertrag von B1 Systems ergänzen Sie Ihr Team um die Erfahrung und das Wissen unserer über 150 festangestellten Linux- und Open-Source-Experten.

Unsere Kernthemen:

**Linux Server & Desktop · Private Cloud (OpenStack & Ceph) · Public Cloud (AWS, Azure, OTC & GCP) · Container (Docker, Kubernetes, Red Hat OpenShift & Rancher) · Monitoring (Icinga, Nagios & ELK) · Patch Management · Automatisierung (Ansible, Salt, Puppet & Chef) · Videokonferenzen**

Unser in Deutschland ansässiges Support- und Betriebsteam ist immer für Sie da – mit qualifizierten Reaktionszeiten ab 10 Minuten und Supportzeiten von 8x5 bis 24x7!



**B1 Systems GmbH - Ihr Linux-Partner**  
Linux/Open Source Consulting, Training, Managed Service & Support

ROCKOLDING · KÖLN · BERLIN · DRESDEN · JENA

[www.b1-systems.de](http://www.b1-systems.de) · [info@b1-systems.de](mailto:info@b1-systems.de)

## Mülltonnen-Ampel als Gedächtnisstütze

**In Heft 1/2023 riefen wir dazu auf, uns Projektideen zu schicken, um per API die Abfuhrdaten für verschiedene Müllsorten abzurufen. Zwei Sets aus 3D-gedruckter Mülltonnen-Ampel und passenden RGB-LEDs warten auf Gewinner.**

Unsere beiden Gewinner sandten zwei recht unterschiedliche Ideen ein. Steffen Zimmermann entwickelt als Open-Source-Projekt eine Home-Assistant-Integration via Python, in der er versucht, die Daten für möglichst viele Landkreise respektive Entsorger einzubinden (siehe [ct.de/ytbp](http://ct.de/ytbp)). Sein Projekt besteht aus einem generischen und einem speziellen Teil. Der generische Teil integriert die Daten in Home Assistant und kann auch bestimmte Müllsorten „ausblenden“. Der andere Teil des Codes besorgt die Abfuhrtermine von den jeweiligen Quellen, von denen Zimmermann nach eigenen Angaben bereits mehr als 40 aus deutschen Ortschaften und mehr als 130 weltweit abfragt. Man kann auch einfach neue Datenquellen, also Städte, Gemeinden oder Entsorgungsunternehmen einbinden. Mit diesem Projekt und einem Controller etwa auf Basis von ESPHome kann man prinzipiell eine Mülltonnen-Ampel basteln ohne zu programmieren.

Zimmermann weist darauf hin, dass es je nach Gemeinde schwierig sein kann, an die Abfuhrdaten zu kommen. Die Hindernisse reichen von einem erforderlichen Kundenkonto über Cookies und die Bindung an eine HTTP-Session bis hin dazu, dass man die nötigen Termin nur mit Data Scraping von HTML-Seiten beziehen kann. An Captcha-Kontrollen für Seitenaufrufe sei er hingegen bislang gescheitert. Um die Server der Entsorger nicht zu überlasten, lässt er die Abfuhrtermine nachts mit einem zufälligen Zeitversatz von bis zu 60 Minuten abrufen, sodass nicht alle Nutzer seines Projekts zugleich auf die Server zugreifen.

Der Lösungsvorschlag unseres Lesers Martin Brodeck ruft mangels API-Angebot des Entsorgungsunternehmens in seinem Landkreis eine CSV-Datei ab und extrahiert die Abfuhrdaten daraus. Mit ein wenig Nachforschung, so vermutet er, ließen sich dahinter aber wohl doch API-Calls identifizieren. Die Ampelsteuerung erledigt bei ihm ein Raspberry Pi Pico W, der sich kurzzeitig per WLAN mit dem Internet verbindet, sich via NTP die Uhrzeit besorgt und die bei ihm auf einer privaten lokalen Webseite zwischengelagerte CSV-Datei abruft. Damit die nötige Elektronik nicht auf dem Tisch herumfliegt, hat Brodeck sich zur Mülltonne noch einen Sockel gedruckt, in dem die Kabellage verschwin-



Die 3D-gedruckte halbtransparente Mülltonne erstrahlt mittels RGB-LED am Abend vor dem Abholtermin in der Farbe der jeweiligen Tonne und wirkt so als Erinnermich.

det. Die Projektdateien und Informationen stellt er auf seiner Gitea-Instanz (siehe [ct.de/ytbp](http://ct.de/ytbp)) zur Verfügung. (csp@ct.de)

**Mülltonnenampel-Projekte:** [ct.de/ytbp](http://ct.de/ytbp)

## Leser helfen Lesern: Ihre Ideen und Projekte

In der Rubrik „Leser helfen Lesern“ veröffentlichen wir **Projekte und Ideen, die unsere Leser umgesetzt haben**. Dabei spielt es keine Rolle, ob es sich um eine Hardwarebastelei, einen Life-Hack, ein Skript oder einfach nur eine clevere Konstruktion handelt. Das Onlineforum zu bisherigen Vorschlägen finden Sie unter [ct.de/lhl](http://ct.de/lhl).

Zögern Sie nicht, uns auch Probleme zu schildern, für die Sie auf eine Lösung aus der Community hoffen. Selbstverständlich können Sie selbst entscheiden, ob wir Ihren Namen nennen sollen oder ihn vertraulich behandeln. Schicken Sie uns Ihre Vorschläge bitte per E-Mail an

folgende Adresse: [leserhelfenlesern@ct.de](mailto:leserhelfenlesern@ct.de) oder in Kurzform [lhl@ct.de](mailto:lhl@ct.de).

Im Forum sind derweil noch einige offene Fragen zu finden. Vielleicht wissen Sie ja zu einer davon die Antwort oder können zur Lösung etwas beitragen.

So sucht Tino Fäustel eine Zertifizierungsstelle, die ihm ein MIME-Zertifikat für seinen E-Mail-Verkehr ausstellt. Das Problem: Er hat keine Firma, sondern ist Freiberufler. Einen Firmennachweis kann er so also nicht wie üblich via Handelsregisterauszug erbringen. Alternativ wäre auch ein öffentlich abrufbares, amtliches Register für Freiberufler möglich. Kennen Sie eine Lösung?

Der Heise-Forumsnutzer „sehrseit-sam“ sucht überdies eine Scanner-App oder Vergleichbares, das den Umstieg auf ein papierloses Office erlaubt. Die Lösung soll ähnlich den Apps für Smartphones mit nur wenigen Handgriffen zum Ziel führen, also möglichst schlank sein. Konkrete Anforderungen: Ein Dokument aus einem Bild – am besten mit Texterkennung und Konvertierung – erstellen, zuschneiden, als PDF abspeichern. Ein Android-Emulator kommt für sehrseit-sam dabei leider nicht infrage. Melden Sie sich doch in der Diskussion zu Wort, falls Sie hier weiterhelfen können.

# NEUE WEGE STATT AUS- GETRETERNER PFADE.

Cordaware **bestzero**: Mit Sicherheit einfach besser.



Remote Zugriff auf lokale Ressourcen **schnell** und **einfach** bereitstellen.

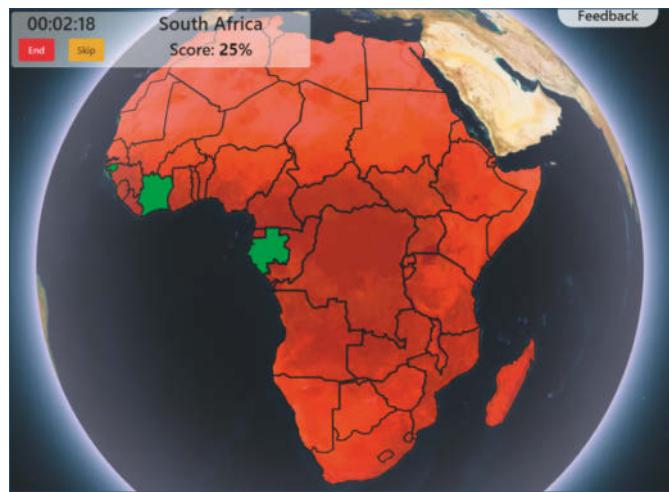
Keine offenen eingehenden Ports erforderlich => **Zero-Firewall-Config.**



Verfügbar für Windows, macOS, Linux und Android

Cordaware GmbH Informationslogistik +++ Fon +49 8441 8593200 +++ info@cordaware.com +++ www.cordaware.com





## Wo liegt eigentlich ...?

[geography-game.com](http://geography-game.com)

[geoguessr.com](http://geoguessr.com)

Kennen Sie sich gut in Geografie aus? Also, wenn Sie einen Globus präsentiert bekommen, auf dem nur die Umrisse der Länder, Meere und Gebirge dargestellt sind: Können Sie dann sagen, wo Moldawien, der Atlantische Ozean oder die Guinea Highlands liegen? Mit dem **Geography Game** von Art Perkitny finden Sie das heraus. Bei dem kostenlosen englischsprachigen Spiel wählen Sie zu Beginn eine Region aus, also zum Beispiel einen Kontinent, „50 US States“ oder die Berge eines Kontinents.

Dann werden Sie abgefragt. Klicken Sie dreimal in die falsche Region der Karte, zeigt das Spiel Ihnen, wo das gesuchte Land, der Berg oder das Meer liegen. Wenn Sie sich nicht sicher sind, können Sie eine Runde aussetzen. Knifflig ist es aber allemal. Am Ende zeigt Ihnen die Website eine Statistik mit dem Prozentsatz der richtig bestimmten Gegenden und der benötigten Zeit an, die Sie in sozialen Medien posten können.

Schauen Sie beim Geography Game sozusagen von oben auf die Weltkugel, werden Sie beim ebenfalls englischsprachigen **GeoGuessr** irgendwo auf der Welt ausgesetzt. Das Spiel zeigt Ihnen eine Streetview-Ansicht. Ihre Aufgabe ist es, anhand von visuellen Hinweisen herauszufinden, wo genau Sie sich befinden. Dazu können Sie auch in der Streetview-Karte herumlaufen. Fünf Minuten pro Viertelstunde können Sie mit einem kostenlosen Account rätseln – für eine schnelle Runde in der Mittagspause reicht das. Möchten Sie länger spielen, müssen Sie sich einen kostenpflichtigen Pro-Account zulegen (3,49 Euro pro Monat oder 23,88 Euro pro Jahr). Damit stehen Ihnen auch zusätzliche Spielmodi offen, etwa der Party-Modus. (jo@ct.de)

## Energ(et)ische Mischung

[app.electricitymaps.com/map](http://app.electricitymaps.com/map)

Nicht nur mancher politische Akteur wäre gut beraten, seine Aussagen zum deutschen Energiemix im Voraus zu prüfen.

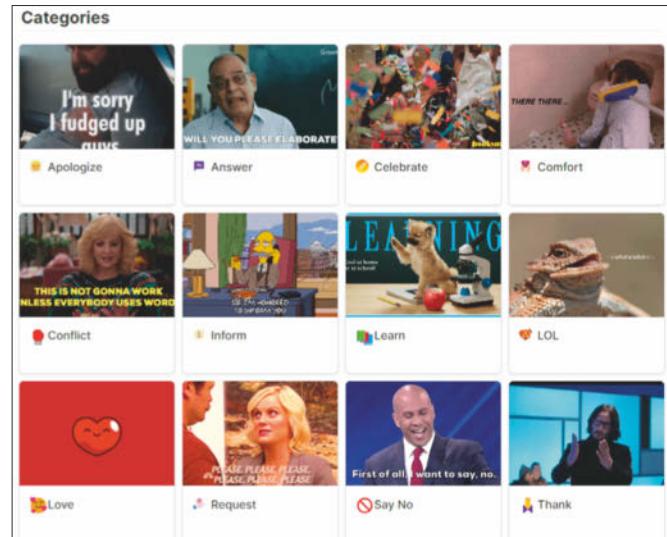
Auch in privaten Diskussionen kann es beruhigend auf energische Gemüter wirken, wenn man Behauptungen darüber auch belegen kann. **ElectricityMaps** sammelt nationale Daten zu Stromerzeugung, -verbrauch und -export für über 50 Länder, in Europa sind dies vorwiegend Daten des Verbands Europäischer Übertragungsnetzbetreiber (ENTSO-E).

Die Grafiken zeigen in Echtzeit oder für vergangene Zeiträume die Zusammensetzung des Energiemixes einer Region oder eines Landes. So sieht man schnell, ob in Deutschland die Windenergie gerade den größten Beitrag leistet oder überwiegend klimaschädliche Kohle verstromt wird. Die Seite färbt einzelne Länder plakativ nach der CO<sub>2</sub>-Intensität ein – Frankreich etwa ist deshalb grün koloriert, weil die Kernenergie dort den größten Beitrag zum Mix leistet. (Tobias Engler/jo@ct.de)

## Souffleur für schwierige Gespräche

[talkingpointsforlife.com](http://talkingpointsforlife.com)

Kommunikation ist knifflig, konstatieren die Betreiber der Website **Talking Points for Life**. Das gilt insbesondere in schwierigen Gesprächssituationen – wenn es etwa darum geht, Grenzen zu setzen, sich zu entschuldigen oder auf neugierige oder unan-



gemessene Fragen zu reagieren. Sie haben daher eine Sammlung mit gebrauchsfertigen Botschaften und Argumentationshilfen für schwierige soziale Situationen zusammengestellt.

Dass die Website in englischer Sprache verfasst ist, stört dank Übersetzern wie DeepL kaum. Bei Konversationen per Mail oder Chat kann man so in aller Ruhe unter den vorgeschlagenen Antworten eine passende heraussuchen. Aber auch vor kniffligen direkten Gesprächen – wenn etwa die übergriffige Schwiegermutter zu Besuch kommt – können Sie sich vorher verbal wappnen. (jo@ct.de)

Diese Seite mit klickbaren Links: [ct.de/yzzk](http://ct.de/yzzk)



**COMPUTEX**  
TAIPEI

**Together we create**

# **COMPUTEX TAIPEI**

**MAY 30 - JUNE 2, 2023**

**Taipei Nangang Exhibition Center,  
Hall 1 & 2 (TaiNEX 1 & 2)**

[www.ComputexTaipei.com.tw](http://www.ComputexTaipei.com.tw)

[www.InnoVEX.com.tw](http://www.InnoVEX.com.tw)

Organizers



**TCA**

# Falschspieler

## MediaMarkt weist Reklamation zu Unrecht ab



**Auch wenn man einen Sachmangel erst Wochen nach dem Kauf bemerkt, hat man Anspruch auf sachmangelfreie Ware. Bei MediaMarkt ist das offenbar nicht jedem Mitarbeiter bewusst.**

Von Tim Gerber

**D**er achtjährige Sohn von Daniel L. ist Fan der Pokémon. Zu seinem nächsten Geburtstag am 5. Oktober wollten seine Eltern ihm deshalb ein Pokémon-Kartenspiel schenken. Das bestellte Vater Daniel L. bereits am 18. August im Onlineshop von MediaMarkt. Zwei Tage später kam das Kartenspiel gut verpackt und äußerlich unbeschädigt bei Daniel L. an. Die Eltern packten das eingeschweißte Kartenspiel in Geschenkpapier und legten es gut versteckt für den großen Tag des kleinen Sohnes erst einmal beiseite.

An seinem Geburtstag freute sich der Junge über das Spiel, hatte aber an diesem Tag noch keine Gelegenheit, es gemeinsam mit den Eltern auszuprobieren. Die

kam erst am folgenden Tag, doch schon beim Verteilen der Karten wichen die anfängliche Freude einer gründlichen Enttäuschung: Das Spiel war nicht vollständig, eine Spielkarte fehlte. Ohne diese war das Spiel nicht zu spielen.

Vater Daniel L. reklamierte noch am selben Abend das unvollständige Spiel mit einer E-Mail an den MediaMarkt-Support und bat um Nachlieferung der fehlenden Karte. Der Kundenservice erkundigte sich am folgenden Tag aber erst einmal, warum der Kunde sich erst jetzt meldet. Das beantwortete Daniel L. sofort und plausibel, indem er auf den erst eben gewesenen achten Geburtstag seines Sohnes hinwies.

Am 10. Oktober teilte ihm der Kundenservice mit, dass man leider keinen Ersatz liefern könne. Stattdessen verwies man über einen Weblink an den Hersteller. Als Verkäufer verfüge man über keine Ersatzteile. Auch darauf reagierte Daniel L. sofort und bat MediaMarkt – da man ihm die fehlende Karte nicht nachliefern könne – um einen Rücksendeschein und anschließende Erstattung des Kaufpreises.

## Rabatt-Poker

Drei Tage später reagierte der Kundenservice abschlägig: Er befindet sich nicht mehr in der Widerrufsfrist, teilte man dem Kunden lapidar mit. Er möge sich an den Hersteller wenden. Auch darauf reagierte der Kunde postwendend, wies den Händler auf die bestehende Gewährleistung hin und fragte nach, warum man ihm denn nicht einfach ein vollständiges Spiel lieferne, da es im Onlineshop des Elektronikriesen ja noch verfügbar war.

Darauf teilte der Kundenservice per E-Mail vom 14. Oktober mit, dass der Artikel nicht im Bestand sei, bot dem Kunden aber einen Preisnachlass in Höhe von 5 Euro an. Dies lehnte Daniel L. indessen ab. Denn das Kartenspiel war mit der fehlenden Karte wertlos, sodass ihn auch der Nachlass nichts brachte. Deshalb bestand er weiterhin auf einer Nachlieferung oder Kaufpreiserstattung.

Das hatte man beim Kundenservice offenbar noch immer nicht verstanden. Jedenfalls bot man Daniel L. mit E-Mail vom 17. Oktober ein weiteres Mal einen Preisnachlass von 5 Euro an, was dieser freilich erneut ablehnte. Immerhin kam nun etwas Bewegung in die Sache, indem MediaMarkt dem Kunden am 19. Oktober ein Retourenlabel für die Rücksendung zusandte. In der Hoffnung, wenigstens den Kaufpreis für das unvollständige Spiel zurückzuerhalten, sandte Daniel L. damit das Spiel an MediaMarkt zurück.

Doch anstatt des erwarteten Geldes kam Anfang November lediglich das Päckchen mit dem unvollständigen Spiel wieder beim Kunden an. Der Bearbeiter hatte auf dem Retourenschein lediglich das Auftrags- und Rücksendedatum markiert und ein großes Fragezeichen darunter gesetzt. Am 10. November fragte Daniel L. deshalb ein weiteres Mal per E-Mail nach, was er denn für eine erfolgreiche Retoure des unvollständig gelieferten Spieles noch unternehmen solle. Darauf erhielt er umgehend per E-Mail ein zweites Retourenlabel und

sandte das Spiel ein weiteres Mal an den Händler zurück.

Doch schon nach einer Woche war das Spiel wieder beim Kunden. Diesmal fiel der Text etwas ausführlicher aus: „Sehr geehrter Herr L.“, war handschriftlich zu lesen, „Sie haben 14 Tage Umtauschrechung auf originalverpackte Ware. Daher schicken wir Ihnen das Spiel zurück“.

Daniel L. glaubte noch immer an ein Missverständnis und fragte am 17. November erneut, was er tun solle. Nun wollte der Kundenservice von ihm wissen, ob bei dem Spiel die Originalverpackung fehle. Er habe das Spiel stets in der Originalverpackung zurückgesandt, beteuerte der Kunde und erhielt noch am selben Tage das dritte Rücksendelabel.

Diesmal legte Daniel L. dem Päckchen einen freundlichen Brief bei, in welchem er schilderte, dass er das Spiel deshalb zurücksende, weil es von Anfang an unvollständig gewesen sei. Man möge es ihm kein drittes Mal zurücksenden, bat er.

## Eigene Regeln

Doch sein Flehen war vergeblich: Mitte Dezember lag das Päckchen wieder beim Kunden. Auf den freundlich bittenden Brief war handschriftlich für den „lieben Herrn L.“ vermerkt: „In so einem Fall hätten Sie den Mangel innerhalb von 7 Tagen nach Erhalt der Ware melden müssen.“ Das Thema sei mit der Serviceleitung des Marktes besprochen, eine Rücknahme sei leider nicht möglich.

Kurz darauf, am 13. Dezember, erhielt Daniel L. überraschend eine Nachricht vom Kundenservice, der sich seltsamerweise nach dem Verbleib des Päckchens erkundigte und verschiedene Fragen dazu hatte: Ob er es in einer Filiale abgegeben hätte, an welche Adresse es gesendet wurde und dergleichen mehr. Nun fühlte Daniel L. sich doch etwas auf den Arm genommen und antwortete dies am 16. Dezember auch genau so an den Kundenservice. Der forderte daraufhin noch einen Einlieferungsbeleg für das Päckchen, das er selbst ja längst zum dritten Mal an den Kunden hatte zurückgehen lassen.

Kurz vor Weihnachten rief Daniel L. noch ein letztes Mal bei MediaMarkt an, schilderte einem aufmerksamen Mitarbeiter den ganzen Kummer mit dem Kartenspiel für seinen Sohn und erhielt das Versprechen, dass die Sache weitergege-

ben werde und sich jemand bei ihm melden würde. Doch bis Jahresbeginn tat sich nichts mehr und so wandte sich Daniel L. am 3. Januar an c't.

## Merkwürdige Joker

Bei der Durchsicht der Korrespondenz fiel klar ins Auge, dass man beim MediaMarkt-Kundenservice offenbar das im Onlinehandel geltende Widerrufsrecht mit den beim Verkauf an Endkunden immer geltenden Gewährleistungsrecht verwechselt

hatte. Während das erste nur 14 Tage besteht, ist das Recht des Käufers aus seinem Vertrag ein mangelfreies, also vollständiges Produkt geliefert zu bekommen, praktisch nur durch die gesetzliche Verjährung gehemmt.

Wie der Kundenservice auf eine Pflicht zur Meldung von Sachmängeln innerhalb von 7 Tagen kam, ist völlig schleierhaft. So etwas mag unter Kaufleuten vertraglich vereinbart werden, im Geschäft mit Endkunden existieren solche Pflichten nicht. Zudem hatte Daniel L. den Grund für die späte Meldung ja plausibel und im Zweifel nachweisbar mit dem Geburtstag seines Sohnes begründet.

Auch der anfängliche Verweis an den Hersteller schien uns auf einem Missverständnis zu beruhen: Bei Elektronik besteht oftmals neben der gesetzlichen Gewährleistung eine Herstellergarantie, sodass Händler ihrer Gewährleistungspflicht nachkommen können, indem die Garantieleistungen des Herstellers in Anspruch genommen werden – sofern der Kunde dadurch nicht schlechter steht. Bei dem Kartenspiel des Kunden besteht aber eine solche Garantie nicht.

Wir fragten am 5. Januar bei der Unternehmenskommunikation des MediaMarkt-Saturn-Konzerns an und konfrontierten sie mit dem Fall sowie unserer Einschätzung. „Sie haben Recht“, war die unumwundene Antwort, die uns eine Konzernsprecherin am 11. Januar zuteilwerden ließ. Aufgrund des bestehenden Gewährleistungsanspruches „müssen wir den Kunden entweder dabei unterstützen, die fehlenden Karten zu erhalten, ein neues Kartenspiel zusenden oder den Kaufbetrag zurückerstatteten.“ Die Rückerstattung an den Kunden sei bereits in die Wege geleitet und werde zeitnah erfolgen. Immerhin eine erfreuliche Zusage, die kurz vor Redaktionsschluss sogar erfüllt wurde. (tig@ct.de) **ct**



# Sicher gespeichert

Daten durch Verschlüsselung komfortabel schützen



<b>Datenverschlüsselung: Wissen und Praxistipps</b>	..... Seite 62
<b>Windows BitLocker und VeraCrypt einrichten</b>	..... Seite 70
<b>Test: USB-Speicher mit Verschlüsselung</b>	..... Seite 74
<b>Verschlüsselte USB-Speicher hacken</b>	..... Seite 78

## Behalten Sie die Hoheit über Ihre Daten: Verschlüsselung verhindert fremde Zugriffe. Unser Praxisleitfaden liefert konkrete Tipps für pragmatischen Datenschutz, den Sie sofort aktivieren können.

Von Christof Windeck

**D**atenschutz ist eine heikle Sache, weil kleine Fehler große Folgen haben können. Sobald Daten in falsche Hände geraten, kann man sie nicht mehr zurückholen. Denn rasch sind sie kopiert und womöglich verkauft. In der Praxis schützen deswegen nur zwei Methoden zuverlässig: Entweder Sie schotten Computer und Datenträger von unbefugtem Zugriff ab oder Sie verschlüsseln die Daten. Meistens ist Verschlüsselung die wesentlich leichter umsetzbare, billigere und komfortablere Methode. Und bei Mobilgeräten und Wechseldatenträgern wie USB-Sticks, die man nicht sicher wegsperren kann, führt am Verschlüsseln sowieso kein Weg vorbei.

Alle aktuellen Betriebssysteme stellen Funktionen zur Verschlüsselung von Datenspeichern bereit, mehr dazu ab Seite 70. Außerdem gibt es kostenlose Tools, die unter mehreren Betriebssystemen laufen. Trotzdem zögern viele Menschen, Daten zu verschlüsseln, weil sie zusätzliche Probleme befürchten oder bereits darauf gestoßen sind. Daher liefern wir auch Tipps, wie man solche Hürden überwindet. Auf Seite 70 zeigen wir die konkrete Einrichtung von BitLocker. Ab Seite 74 stellen wir einige USB-Speicher mit eingebauter Verschlüsselung vor, die ein Experte untersucht hat. Wie er dabei vorgeht, erklärt er ab Seite 78.

### Sicher ruhen

Schon seit 2007 bringen die Pro- und Enterprise-Versionen von Microsoft Windows die Funktion BitLocker zur Vollverschlüsselung von Datenträgern mit. Man spricht von Full Disk Encryption (FDE) im Unterschied zur Verschlüsselung von einzelnen Dateien oder Ordnern. Für letztere hat Windows das Encrypted File System

(EFS) für NTFS-Datenträger an Bord. Seit Windows 10 gibt es für Windows Home eine beschnittene BitLocker-Version namens Geräteverschlüsselung (Device Encryption), die unter bestimmten Voraussetzungen automatisch aktiv ist.

Bei Apple macOS heißt die FDE-Funktion FileVault beziehungsweise FileVault 2. Bei Linux ist Linux Unified Key Setup (LUKS) das verbreitetste Verfahren zur Verschlüsselung von Festplatten, SSDs sowie von logischen Volumes. Für Linux gibt es aber auch dm-crypt und das Dateisystem zfs mit integrierter Verschlüsselungsfunktion.

In den Smartphonebetriebssystemen Android und iOS/iPad OS sind Verschlüsselungsfunktionen für den internen Flash-Speicher sowie eventuell eingesteckte MicroSD-Karten eingebaut. Android verwendet seit Version 7.0 File-Based Encryption (FBE). Sie schützt die einzelnen Dateien mit unterschiedlichen Schlüsseln, die sich aus einem Master Key ableiten. In iOS heißt die Funktion „Datensicherheit“ (Data Protection). Seit mehreren Jahren sind die Flash-Verschlüsselungen von An-

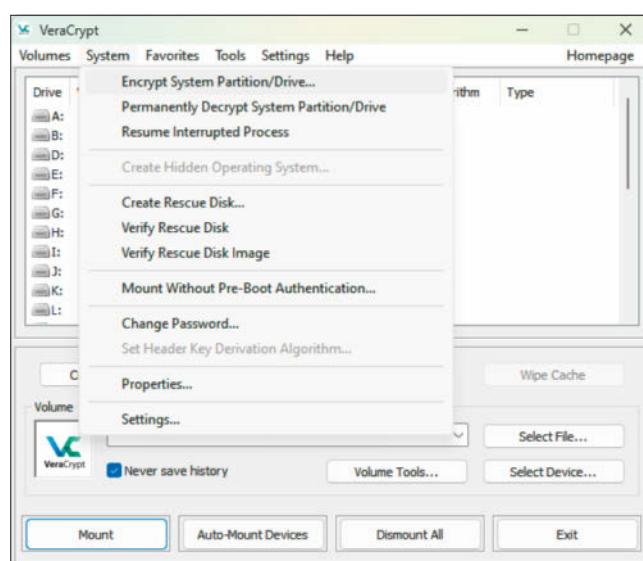
droid und iOS automatisch aktiv und lassen sich bei den meisten Smartphones auch nicht mehr abschalten.

Bei all den oben erwähnten Funktionen spricht man von „Data-at-Rest-Encryption“, weil die Daten dabei verschlüsselt auf Datenträgern „ruhen“. Im Unterschied dazu gibt es zahlreiche Verfahren, um Daten beim Transport zu schützen, etwa per https oder ssl auf dem Weg durch Netzwerke oder per RAM-Verschlüsselung in virtuellen Maschinen von (Cloud-)Servern.

Die genannten Data-at-Rest-Verschlüsselungsfunktionen verwenden alleamt den Advanced Encryption Standard (AES) mit 128 oder 256 Bit langen Schlüsseln. AES-128 gilt bislang als sehr sicher. Weil selbst Smartphone-CPUs integrierte AES-Beschleuniger enthalten, bremst die Verschlüsselung Dateizugriffe nicht und frisst auch nicht nennenswert Akkustrom.

### Unmerklicher Schutz

Viele Menschen wissen gar nicht, dass sie bereits Data-at-Rest-Verschlüsselung nutzen, weil sie im Hintergrund automatisch läuft und im Alltag kaum auffällt. Daher ist es auch nicht so leicht zu verstehen, worin der wesentliche Vorteil liegt: nämlich in der Verknüpfung der Verschlüsselung mit einem passwortgeschützten Benutzerkonto. Wie die Hersteller ihre mitunter relativ komplizierte Verknüpfung im Detail umsetzen, ist nicht so wichtig. Der Punkt ist letztlich: Dank FDE haben Unbefugte ohne Passwort keinen Zugriff auf Daten, wenn das jeweilige Gerät abgeschaltet ist, im Sperr- oder Schlafmodus ruht oder entsorgt wurde.



**Wer proprietären Verschlüsselungsfunktionen von Windows und macOS misstraut oder mehrere Betriebssysteme nutzt, kann Daten mit VeraCrypt verschlüsseln.**

**BitLocker-Laufwerkverschlüsselung**

Das Schützen der Laufwerke mit BitLocker trägt dazu bei, Dateien und Ordner vor nicht autorisiertem Zugriff zu schützen.

**1 Zu Ihrer Sicherheit werden einige Einstellungen vom Systemadministrator verwaltet.**

**Betriebssystemlaufwerk**

**Windows (C): BitLocker aktiviert**

**Festplattenlaufwerke**

**Wechseldatenträger - BitLocker To Go**

**ESD-USB (D): BitLocker deaktiviert**

**BitLocker aktivieren**

Damit das klappt, muss der Anwender jedoch sämtliche Benutzerkonten des jeweiligen Gerätes mit sicheren Passwörtern, einer PIN oder mit biometrischem Zugriffsschutz (Fingerabdrucksensor, Apple Face ID, Windows Hello et cetera) schützen. Er darf kein Konto ohne Passwort einrichten und das Gerät sollte möglichst rasch in den Sperrmodus wechseln, wenn man es nicht benutzt. Auch wenn die eigentlichen FDE-Funktionen als sicher gelten, entbindet die Technik Benutzer und Administratoren also nicht vom Mitdenken. Sonst reißen sie leicht Lücken auf.

Wer seine Daten per automatischem Backup auf Cloudserver spiegelt oder Tools wie OneDrive, iCloud, Dropbox und Microsoft 365 nutzt, muss dem dort vorhandenen Datenschutz vertrauen. Und bombensichere SSD-Verschlüsselung kann nicht helfen, wenn unverschlüsselte (Sicherheits-)Kopien auf einer USB-SSD im selben gestohlenen Aktenkoffer liegen. Datenschutz durch Verschlüsselung muss folglich auch Cloudserver, NAS, externe Festplatten, USB-Sticks oder die MicroSD-Karte im Android-Smartphone einbeziehen, dazu unten mehr.

## Sicherheitsfragen

Die Frage aller Fragen bei Verschlüsselung lautet: Ist das wirklich sicher? Und die Antwort lautet: ziemlich. Das BSI bestätigt etwa, dass sich penibel konfigurierte iPhones und iPads für amtliche Verschlusssachen der Sicherheitsstufe „Nur für den Dienstgebrauch“ (VS-NfD) eignen.

Absolute Sicherheit gibt es jedoch nicht. Für guten Schutz ist es das Wichtigste, dass ausgereifte, von zahlreichen Ex-

**In Windows ab der Pro-Version ist BitLocker eingebaut; BitLocker To Go verschlüsselt USB-Speichermedien.**

es unerlässlich, dass der jeweilige Hersteller die Software oder das Gerät unterstützt, auf Berichte über Sicherheitslücken professionell reagiert (etwa durch ein Product Security Incident Response Team, PSIRT), seine Kunden rasch benachrichtigt und Updates oder Handlungsanweisungen liefert. Nicht jede Sicherheitslücke schließt sich per Update. Im Extremfall kann es nötig werden, die Daten auf ein anderes Medium zu kopieren oder mit einer anderen Software zu verschlüsseln und unsichere Datenträger sicher zu löschen und zu entsorgen. Jedenfalls ist es widersinnig, Datenverschlüsselung ohne Support zu nutzen. Der läuft bei Hardware typischerweise nach drei bis fünf Jahren aus.

Oft hört man den Rat, Daten besser mit Open-Source-Tools wie VeraCrypt, LUKS oder 7-Zip zu verschlüsseln als mit proprietären Systemen wie BitLocker und FileVault. Manche unterstellen den Verschlüsselungssystemen von US-Konzernen eingebaute Hintertüren (Backdoors) für die von Geheimdiensten wie der NSA angeordneten Zugriffe. Bei Open-Source-Software ist es im Prinzip möglich, den Quellcode zu untersuchen, ihn zu kompilieren und mit der verwendeten Binärversion zu vergleichen, um Manipulationen zu enttarnen. Das muss nur auch tatsächlich geschehen, obendrein durch vertrau-

perten unabhängig geprüfte Algorithmen wie AES, sichere Schlüssel (RSA-2048 oder besser) und starke Passwörter zum Einsatz kommen. Trotzdem schaffen es Sicherheitsforscher und Hacker immer wieder, bestimmte Verschlüsselungstools zu knacken, siehe auch Seite 78. Meistens liegen die Fehler aber nicht bei den Basisalgorithmen, sondern bei falscher Konfiguration der jeweils verwendeten Software oder Firmware.

In jeder konkreten Umsetzung können Schwachstellen auftreten. Daher ist

 BitLocker-Laufwerkverschlüsselung (C:)

### Wie soll der Wiederherstellungsschlüssel gesichert werden?

**1 Einige Einstellungen werden vom Systemadministrator verwaltet.**

Ein Wiederherstellungsschlüssel kann für den Zugriff auf Dateien und Ordner verwendet werden, falls Sie Ihren PC nicht entsperren können. Es wird empfohlen, mehrere Wiederherstellungsschlüssel getrennt vom PC aufzubewahren.

→ [In Microsoft-Konto speichern](#)

→ [In Datei speichern](#)

→ [Wiederherstellungsschlüssel drucken](#)

[Wie finde ich später meinen Wiederherstellungsschlüssel?](#)

[Abbrechen](#)

Den Wiederherstellungsschlüssel für die jeweilige Verschlüsselung sollte man unbedingt auf mehrere Zettel aufschreiben und an verschiedenen sicheren Orten lagern.



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



[ct.de/angebot](http://ct.de/angebot)

Jetzt gleich bestellen:

 [ct.de/angebot](http://ct.de/angebot)

 +49 541/80 009 120

 [leserservice@heise.de](mailto:leserservice@heise.de)

**ICH KAUF MIR DIE c't NICHT. ICH ABBONNIER SIE.**

Ich möchte c't 3 Monate lang mit über 30 % Neukunden-Rabatt testen.  
Ich lese 6 Ausgaben als Heft oder digital in der App, als PDF oder direkt im Browser.

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



enswürdige Personen oder Institutionen. Für VeraCrypt wurden solche Audits beispielsweise erfolgreich durchgeführt. Nutzer müssen aber auch bei Open-Source-Software darauf vertrauen, dass Sicherheitslücken rasch durch Updates geschlossen werden. Und sie müssen sicherstellen, dass sie tatsächlich eine nicht manipulierte Version der Software installieren. Bei den integrierten Lösungen der Betriebssysteme und bei Linux-Distributionen schützt die kryptografische Signaturkette der jeweiligen Anbieter vor der Ausführung unsignierter Programme.

Doch trotz aller Bemühungen und Professionalität: Nicht immer werden Sicherheitslücken von den Richtigen entdeckt, sondern von böswilligen Hackern, die sie missbrauchen, statt sie dem Hersteller zu melden. Das nennt man Zero-Day-Attacken, weil die jeweilige Lücke seit „Null Tagen bekannt“ ist, also eben der Öffentlichkeit unbekannt.

Ein anderes Problem betrifft den langfristigen Schutz von Daten. Denn was heute als sicher gilt, ist das in zwei Wochen oder fünf Jahren vielleicht nicht mehr. Beispielsweise könnten in einigen Jahren superschnelle Computer Verfahren wie AES-128 knacken, die Experten derzeit als verlässlich einstufen. Manche erwarten beispielsweise, dass künftige Generationen von Quantencomputern RSA-1024-Schlüssel brechen könnten und raten schon heute zu RSA-2048 als Minimum. Man spricht auch von Post-Quan-

tum Cryptography (PQC, [1]). Wer Daten schützen will oder durch gesetzliche Vorgaben dazu verpflichtet ist (Stichwort DSGVO), muss letztlich in voraussichtlichen Abständen prüfen, ob er dafür Updates oder neue Konzepte benötigt.

### Schutzniveau

Klar ist aber auch: Verschlüsselte Daten sind viel besser gegen unbefugten Zugriff geschützt als unverschlüsselte. Daher empfehlen wir uneingeschränkt, vorhandene Verschlüsselungen immer zu nutzen, konkret: Schalten Sie Funktionen wie BitLocker, Gerätverschlüsselung und FileVault stets ein, insbesondere bei Mobilgeräten wie Notebooks.

Selbst wenn sie proprietären Code nutzen oder Sicherheitslücken enthalten sollten, halten Verschlüsselungsmethoden immerhin technische Laien davon ab, unbefugt Daten auszulesen. Denn nur wenige davon sind in der Lage, Sicherheitslücken als Einfallstor zum Brechen der Verschlüsselung zu missbrauchen. Viele dürften schon mit der Bedienung von Knacksoftware wie Jack the Ripper oder Hashcat [2, 3, 4] überfordert sein.

Ganz anders sieht es aus, wenn Experten unbeschränkten Zugriff auf eine verschlüsselte Datei haben. Dann hängt der Schutz davon ab, ob die Implementierung frei von kritischen Sicherheitslücken war und ob ausreichend komplexes und zufälliges Schlüsselmaterial verwendet wurde.

Letztlich müssen Sie für Ihre Daten einschätzen, gegen welche Bedrohungen Sie sie schützen wollen. Dabei hilft ein Vergleich mit der analogen Welt: Nehmen wir an, Sie wollen ein vertrauliches Dokument oder Bargeld sicher aufbewahren. So etwas würden Sie nicht offen auf dem Schreibtisch herumliegen lassen, sondern in eine Schublade oder einen Schrank packen, die Sie abschließen können – und den Schlüssel nicht im Schloss stecken lassen. Das bedeutet in der digitalen Welt: BitLocker und Co. schützen vor Gelegenheitsdieben und neugierigen Kollegen, sofern Sie sichere Passwörter verwenden und die nicht auf einem Zettel auf der Unterseite der Tastatur oder einem Klebeetikett am Monitor notieren. Zudem müssen Sie bei jedem Verlassen des Büros auch den PC sperren (per Windows+L wie „Lock“). So erfüllen Sie Basisanforderungen zum Schutz sensibler Daten von Kunden und Mitarbeitern.

Wenn Sie allerdings wichtige Geschäftsgeheimnisse schützen müssen oder



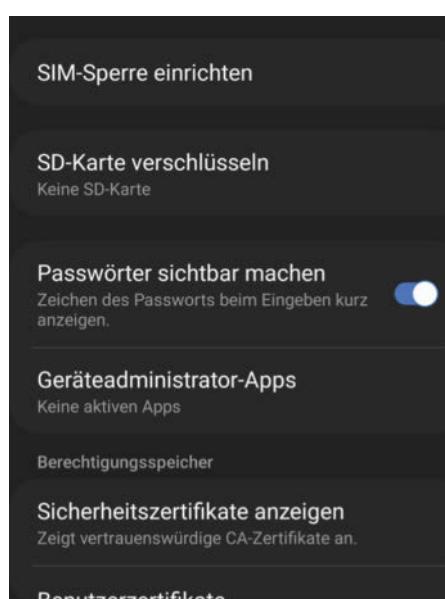
Bei USB-Sticks mit Hardware-Verschlüsselungsfunktionen muss man darauf vertrauen, dass der jeweilige Hersteller sie korrekt umgesetzt hat.

als Whistleblower ihre berufliche Existenz aufs Spiel setzen, brauchen Sie stärkeren Schutz. Denn Experten mit größeren finanziellen und technischen Ressourcen rücken verschlüsselten Datenträgern mit großem Besteck zu Leibe. Für Datenforensiker gibt es spezielle Knacksoftware und dank Cloudrechenzentren ist extreme Rechenleistung für Brute-Force-Attacken leicht verfügbar.

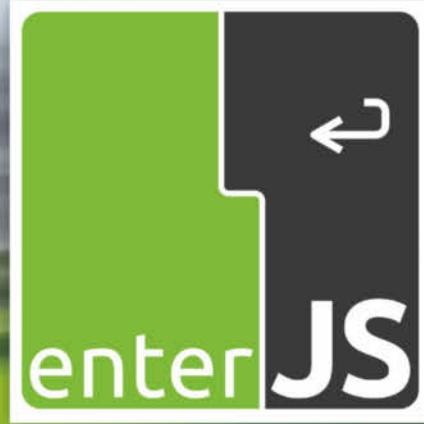
Um auch solche Gegner abzuwehren, ist Expertenwissen nötig, das den Rahmen dieses Artikels weit übersteigt. Denn schon der kleinste Fehler macht den Schutz zunichte. Und selbst die stärkste Verschlüsselung versagt vor kriminellen Organisationen oder Geheimdiensten von Diktaturen, die körperliche Gewalt oder Erpressung anwenden.

### Hardware-Knackschutz

Das Brechen einer Verschlüsselung benötigt außer Rechenleistung auch Zeit. Haben Fachleute unbeschränkten Zugriff auf eine verschlüsselte Datei oder ein Festplatten-Image, dann können sie beliebig lange versuchen, sie zu knacken. Ist der Algorithmus frei von Sicherheitslücken, dann hängt die zum Knacken nötige Rechenzeit vor allem davon ab, wie lang und wie zufällig das Schlüsselgeheimnis ist. Eine typische Empfehlung für ein ausrei-



Manche Android-Smartphones verschlüsseln auf Wunsch auch eingesteckte MicroSD-Speicherkarten.



# Web-Performance Day

Tipps, Tricks und Tools für  
schnellere Webanwendungen

15. Februar 2023  
Online



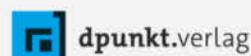
[enterjs.de/web-performance.php](http://enterjs.de/web-performance.php)

Plus 2-Tages-Highspeed-Workshops: JavaScript (6./7.2.2023), Angular (13./14.2.2023)

Veranstalter



heise Developer



chend schwieriges Passwort lautet: Es sollte mindestens 12 Stellen lang sein, aus Ziffern, Zeichen und Sonderzeichen bestehen und nicht auch für andere Zwecke benutzt werden. Denn nichts liegt näher, als bereits erbeutete Passwörter mit weiteren Konten desselben Benutzers auszutesten.

Lange Passwörter sind im Alltag jedoch unpraktisch. Deshalb schützen die erwähnten FDE-Funktionen BitLocker, FileVault & Co das eigentliche Schlüsselmaterial mit Hardwarefunktionen und geben den Zugriff darauf durch komfortablere Methoden frei: PIN und Passwort mit Zeitsperre oder biometrische Authentifizierung wie Windows Hello oder Fingerabdruckleser, meistens verknüpft mit einem Benutzerkonto. Denn auch eine relativ kurze PIN gilt als sicher, wenn ein Angreifer nicht beliebig viele durchprobieren kann, weil nach mehreren falschen Eingaben eine anwachsende Zeitverzögerung dies verhindert. PIN- und Passwort-Schutzfunktionen lassen sich oft so einstellen, dass sie nach einer gewissen Anzahl falscher Eingaben das FDE-Schlüsselmaterial löschen: Dann sind alle Daten futsch, also auch für Angreifer verloren.

Hardware-Schutzfunktionen erschweren das Brechen einer Verschlüsselung, werden aber meistens proprietär umgesetzt und können daher unerkannte Sicherheitslücken oder gar Hintertüren enthalten. Bei BitLocker, FileVault und der iOS/Android-Verschlüsselung schützen Sicherheitschips das Schlüsselmaterial, beispielsweise ein Trusted Platform Module (TPM) auf dem Mainboard. Meistens ist es als Firmware-TPM (fTPM 2.0) in den Prozessor oder den Chipsatz integriert.

## Verschlüsselungsfunktionen und -Tools

Betriebssystem	eingebaute Funktionen
Windows	Pro/Enterprise: BitLocker, Home: Device Encryption
Linux	Linux (LUKS), dm-crypt
macOS	FileVault 2
iOS/iPad OS	Data Protection
Android	File Based Encryption (FBE)

Apple verwendete früher den T2-Chip, dessen Funktionen mittlerweile in die hauseigenen ARM-SoCs wie M1, M2, A13 und A14 eingebaut sind. Android-Smartphones verwenden die TrustZone-Technik von ARM plus Firmware (etwa von Trustonic) oder separate Chips von Samsung oder Google (Titan). Man spricht auch von einem „Secure Element“ (SE). Solche Bauenteile sind oft zertifiziert (siehe Textkasten „Zertifizierung“ auf S. 69), aber selten offengelegt. Nutzer müssen also dem jeweiligen Hersteller vertrauen.

Alternativen bieten LUKS und VeraCrypt: Dabei können Sie das eigentliche Schlüsselgeheimnis auf einem Hardware-Sicherheitsschlüssel speichern, etwa auf einem Nitrokey (siehe ct.de/ys5a). Den wiederum schließen Sie per USB an den geschützten Rechner an, müssen dann jedoch dem Hersteller des Sicherheitsschlüssels vertrauen.

### Krypto-Sockenschuss

Ist der Zugriff auf die verschlüsselten Daten mit einem Sicherheitschip verknüpft, drohen Pannen. Ist der Chip nämlich defekt oder geht verloren, kommen Sie nur noch an Ihre Daten heran, wenn Sie einen sogenannten Wiederherstell-

lungsschlüssel (Recovery Key) haben. Das ist genau das Ziel dieser Funktionen.

Im Umkehrschluss bedeutet das jedoch: Egal wie Sie Daten verschlüsseln müssen Sie vorher klären, wie Sie im Notfall wieder Zugriff erhalten. Die beste Absicherung, die auch beim Verlust des kompletten Gerätes oder Datenträgers greift, ist ein Backup. Und zwar nicht nur eine einzige Sicherheitskopie, sondern mindestens zwei, die an verschiedenen Orten lagern. Das ist ohnehin und für alle Daten wichtig, egal ob verschlüsselt oder nicht.

Bei BitLocker und FileVault können (und sollten) Sie schon bei der Einrichtung einen Wiederherstellungsschlüssel anzeigen lassen und diesen auf einem anderen Datenträger abspeichern. Achtung: So praktisch USB-Sticks auch sind, die darin eingebauten Flash-Speicherchips erhalten Daten nicht für die Ewigkeit. Nehmen Sie zumindest einen nagelneuen Stick dafür, gebrauchte vergessen ihre Daten schneller. Wir raten dringend dazu, Wiederherstellungsschlüssel zusätzlich auszudrucken oder noch besser abzuschreiben, und zwar auf mindestens zwei Blätter Papier, und diese an getrennten Orten sicher zu verwahren. Damit können Sie oder ein Datenrettungsunternehmen den verschlüsselten Datenträger notfalls auch an einem anderen System entschlüsseln.

So manches Windows-Notebook sowie die meisten Apple-Geräte und Smartphones haben keinen entnehmbaren Massenspeicher mehr, sondern fest aufgelöste Flash-Speicherchips. Hier gestaltet sich die Datenrettung aufwendig und sehr teuer. Daher abermals der Hinweis: kein Backup, kein Mitleid!

Android- und iOS-Geräte sind ohne ein Benutzerkonto bei Google beziehungsweise ohne Apple ID kaum sinnvoll nutzbar. Daher liegt es nahe, auch die jeweiligen Wiederherstellungsschlüssel in diesem Konto zu speichern – und genau so geschieht es auch. Die Sicherheit Ihrer Smartphonedenaten hängt folglich auch am sicheren Schutz dieses Kontos, also an einem sicheren Passwort plus möglichst einem zweiten Faktor (Zwei-Faktor-Authentifizierung, 2FA). Seit iOS 15 kann man auch einen Wiederherstellungsschlüssel einrichten, für Android gibt es diese Möglichkeit nach unserer Kenntnis nicht.

Auch bei Windows und macOS lässt sich der Wiederherstellungsschlüssel in einem (Online-)Benutzerkonto speichern: im Active Directory (AD) auf dem Firmen- server, im Microsoft-Konto, in iCloud oder



Die VeraCrypt-Verschlüsselung lässt sich an externe Sicherheitschips koppeln, etwa an den Nitrokey Pro.

im Mobile Device Management (MDM). Solche Funktionen sind für Admins wichtig, die vergessene Passwörter zurücksetzen oder gestohlene Notebooks schützen müssen. Man braucht sie aber auch, um aus dem Unternehmen ausgeschiedenen Mitarbeitern den Zugriff auf Firmendaten zu entziehen, etwa um Compliance-Regeln technisch umzusetzen.

Die BitLocker-Variante „Geräteverschlüsselung“ (Device Encryption) für Rechner mit Windows Home speichert den Wiederherstellungsschlüssel nur im Microsoft-Konto. Nutzt man ein aktuelles Windows-11-Gerät mit fTPM und einem Microsoft-Konto, ist die Geräteverschlüsselung meistens automatisch aktiviert. Es ist daher eine gute Idee, vorsorglich den Wiederherstellungsschlüssel im Microsoft-Konto abzurufen und zu notieren.

## Krypto-Hürden

Verschlüsselung verzeiht keine Fehler und wirkt nur, wenn man sie jederzeit einsetzt. Deshalb sind BitLocker, FileVault und Co. vorteilhaft: Sie sind relativ komfortabel und millionenfach erprobt. Schalten Sie sie ein! Nun folgt eine etwas größere Hürde: die Verschlüsselung von externen Datenträgern, NAS und Cloudspeichern. Dafür gibt es bisher leider keine allgemein empfehlenswerte Lösung, die alle Wünsche und individuellen Konstellationen abdeckt.

Bei den Pro-Versionen für Windows können Sie BitLocker auch für USB-Sticks einrichten, aber die lassen sich dann nur am selben Rechner komfortabel entsperren oder an zentral verwalteten Firmencomputern (via Active Directory). Einen BitLocker-verschlüsselten Stick kann man nicht problemlos an anderen Rechnern oder mit anderen Betriebssystemen verwenden.

Eine pragmatische Lösung für das letztgenannte Problem ist es, Daten auf USB-Sticks mit der freien Software 7-zip zu schützen, die es für Windows, macOS und Linux gibt. Sie erstellt bei richtiger Konfiguration auch per AES sicher verschlüsselte ZIP-Archive (siehe Seite 70); zum Entschlüsseln unter Windows packt man die portable Version von 7-zip mit auf den Stick. Das Entschlüsselungspasswort gibt man über einen zweiten Kanal an den Empfänger weiter, etwa per Telefon, per verschlüsselter E-Mail oder über sichere Messenger wie Signal. Verschlüsselte ZIP-Dateien widerstehen Knacksoftware aber nur dann, wenn ein ausreichend langes Passwort verwendet wurde. VeraCrypt kann ebenfalls externe Speicher verschlüsseln und kommt auch in einer „Portable“-Version, die man nicht installieren muss.

Bei den meisten aktuellen NAS lässt sich Datenverschlüsselung leicht aktivieren. Für Clouddienste gibt es Verschlüsselungssoftware wie Cryptomator [5].

Schwierig wird es, wenn man externe Datenspeicher (auch) an Geräte anschließen möchte, auf denen man keine Software zur Entschlüsselung installieren oder ausführen kann. Das gilt beispielsweise für Drucker, Fernsehgeräte, Messgeräte mit USB-Anschluss oder auch Auto-Entertainment sowie für fernverwaltete Firmencomputer, die nur vorinstallierte Software ausführen. Um Daten trotzdem zu schützen, gibt es externe (USB-)Speichermedien mit eingebauter Verschlüsselung sowie mit eigenen Tasten oder Fingerabdrucksensoren zum Entsperren. Deren Eigenschaften und Tücken stellen wir ab Seite 74 vor. (ciw@ct.de) ct

## Literatur

- [1] Wilhelm Drehling, Ding, ding, Fight!, Post-Quantum-Kryptografie: Wie es mit dem NIST-Auswahlverfahren weitergeht, c't 22/2022, S. 132
- [2] Karola Marky, Hacker-Angriff gegen mich selbst, Festplattenverschlüsselung mit Brute-Force knacken, c't 13/2020, S. 162
- [3] Uli Ries, Die Passwortknacker, Ein Blick hinter die Kulissen der Cracker, c't 3/2013, S. 80
- [4] Jürgen Schmidt, Knack mich, wenn du kannst, Die Tools und Techniken der Passwortknacker, c't 3/2013, S. 84
- [5] Stefan Wischner, Schloss in den Wolken, MS-Office-Dateien auf OneDrive mit Cryptomator verschlüsseln, c't 25/2022, S. 142
- [6] Christof Windeck, Unter Chip-Knackern, Sicherheits-Chips im Härtetest: Die „guten Hacker“ von TÜViT, c't 5/2018, S. 20

Software-Tools: [ct.de/ys5a](http://ct.de/ys5a)

## Zertifizierungen: FIPS und CC

Einige Anbieter lassen ihre Geräte mit Verschlüsselungsfunktionen von Prüfinstituten nach Standards wie FIPS 140-3 und CC zertifizieren. FIPS ist die Abkürzung für die Federal Information Processing Standards und stammt von der US-Behörde National Institute of Standards and Technology (NIST). CC steht für Common Criteria for Information Technology Security Evaluation, die die internationale Norm ISO/IEC 15408 festlegt. Derartige Zertifizierungen führt hierzulande etwa TÜViT durch [6].

Eine FIPS- oder CC-Zertifizierung kann jedoch keinen absoluten Schutz gegen Sicherheitslücken und gut versteckte Hintertüren garantieren. Immerhin weist sie nach, dass außer dem Entwickler des Produktes noch eine unabhängige Instanz „draufgeschaut“ hat. Damit verringert sich zumindest die Wahr-

scheinlichkeit, dass bekannte Schwächen oder gar hanebüchene Fehler eingebaut wurden. Das kommt bei ungeprüften Produkten immer wieder vor.

Kritiker bemängeln, dass auch proprietäre Verfahren zertifizierbar sind, während Open-Source-Produkte von einer viel größeren Anzahl von Experten auf Schwachstellen abgeklopft werden können. Die theoretische Möglichkeit garantiert allerdings nicht, dass dies in der Praxis auch geschieht. Selbst in jahrelang und millionenfach genutzten Open-Source-Tools wie OpenSSL tauchen noch neue Schwachstellen auf.

Einige Hersteller tricksen in der Produktbeschreibung und werben mit FIPS- oder CC-Zertifikaten, obwohl das jeweilige Gerät gar nicht geprüft wurde. Dann ist oft gemeint, dass ein zertifizierter Chip

im Inneren rechnet. Doch viele Sicherheitslücken stecken nicht in den Chips selbst, sondern in der Firmware. So haben etwa auch die meisten PC-Mainboards ein zertifiziertes Trusted Platform Module (TPM/fTPM) und Verschlüsselungsverfahren wie Apple FileVault 2 und Microsoft BitLocker sind ebenfalls zertifiziert. Damit der potenziell starke Schutz aber tatsächlich wie vorgesehen wirkt, muss der gesamte PC richtig konfiguriert sein.

FIPS- und CC-Zertifizierungen sind vor allem für gewerbliche Nutzer wichtig, weil sie belegen, dass Sorgfaltspflichten erfüllt wurden. Für manche Einsatzbereiche schreibt der Gesetzgeber bestimmte Zertifizierungen vor. Private Leute signalisieren Zertifikate immerhin, dass der jeweilige Hersteller anerkannte Verfahren umgesetzt hat.



# Schloss dranhängen

**Tragbare Laufwerke verschlüsseln – schnell, flexibel oder komfortabel**

**Kennen Sie auch dieses Unbehagen, wenn Sie einen USB-Stick dabeihaben – unverschlüsselt, aber mit sensiblen Dateien darauf? Hier zeigen wir Ihnen drei Wege zum guten Gewissen beim Herumtragen von Daten.**

Von Jan Schüßler

**D**ie meisten externen Medien wie USB-Sticks und SSDs speichern Daten von sich aus nur unverschlüsselt. Manche kommen zwar mit vorinstallierter Krypto-Software, doch die ist oft mit Vorsicht zu genießen: Wer weiß, wie sicher die Tools sind und auf Dauer auch bleiben. Viele gibt es außerdem nur für Windows, weshalb sich Linux- und macOS-Nutzer selbst nach geeigneter Software umsehen müssen.

Eine bessere Idee ist es, eine erprobte und verbreitete Software für die Verschlüsselung zu nutzen. Da drängen sich vor allem zwei Tools auf: erstens der universelle Laufwerksverschlüssler VeraCrypt und zweitens das Microsoft-eigene BitLocker. Letzteres ist die komfortablere

Variante, beglückt aber nur Besitzer von Windows-Rechnern – und die brauchen zumindest die Pro-Version, um BitLocker überhaupt einrichten zu können. Hinzu kommt hin und wieder ein diffuses Gefühl des Misstrauens gegenüber der Firma Microsoft. Aber: BitLocker verwendet wie die meisten anderen Verschlüsselungsprogramme den AES-Algorithmus, der bis dato als unmöglich (oder besser gesagt: nur mit astronomischem Zeitaufwand) zu knacken gilt. Daten auf ruhenden Laufwerken sind also auch damit sicher.

Doch bevor wir näher auf VeraCrypt und BitLocker eingehen, stellen wir erst mal eine dritte Möglichkeit vor, nämlich das größtenteils quelloffene und kostenlose 7-Zip: Damit kann wirklich jeder seine

Dateien schnell und unkompliziert so verschlüsseln, dass es nicht mal schadet, wenn er sie bedenkenlos auf einen USB-Stick wirft und diesen irgendwo in den Öffis verbaselt.

### Die schnelle Methode: Zip-Container

Falls Sie 7-Zip noch nicht installiert haben: Den Download finden Sie via [ct.de/ynyw](http://ct.de/ynyw). Kopieren Sie die zu verschlüsselnden Dateien zunächst auf Ihrem PC in einen eigens dafür erstellten Ordner, klicken Sie ihn mit der rechten Maustaste an und wählen Sie „7-Zip/Zu einem Archiv hinzufügen“. Nun wählen Sie zip als Archivformat, vergeben im Bereich Verschlüsselung ein sicheres Kennwort, stellen das Verfahren auf AES-256 um und bestätigen das Ganze mit OK. Erst wenn die verschlüsselte Datei erstellt ist, schieben Sie sie auf Ihr USB-Medium.

Wer das Archiv entpacken will, braucht ebenfalls ein Zip-Programm. Das muss nicht zwingend 7-Zip sein, auch ähnliche Tools wie WinZip und WinRAR kommen mit den AES-verschlüsselten Archiven klar. Zwar könnte Windows Dateien, die Sie mit dem älteren ZipCrypto-Verfahren verschlüsselt haben, auch ohne Installation zusätzlicher Software entsperren, aber lassen Sie bitte trotzdem die Finger davon. ZipCrypto gilt seit geraumer Zeit als leicht zu knacken.

Ein Haken bleibt allerdings: Zwar kann man die im verschlüsselten Zip-Archiv enthaltenen Dateien ohne Kennwort nicht entpacken, durchaus aber deren Namen im Klartext lesen. Ergo: Ein verschlüsseltes Zip ist schnell erstellt, aber nicht die verschwiegenste aller Möglichkeiten.

### Die komfortable Methode: BitLocker

Die Microsoftsche Laufwerksverschlüsselung BitLocker ist in Windows in Pro und höheren Editionen sinnvoll nutzbar. Für USB-Medien nennt Microsoft sie hier und dort auch „BitLocker To Go“. Stecken Sie das USB-Laufwerk an, klicken Sie in der Ansicht „Dieser PC“ des Datei-Explorers mit der rechten Maustaste darauf und wählen Sie „BitLocker aktivieren“ (in Windows 11 finden Sie den Menüpunkt unter „Weitere Optionen anzeigen“).

Zunächst wählen Sie die Entsperrmethode. Setzen Sie ein Häkchen vor „Kennwort ...“ und geben Sie ein hinreichend starkes Kennwort ein. Im nächsten Schritt fordert der Einrichtungsassistent Sie auf, den sogenannten Wiederherstellungs-

## ct kompakt

- Packer wie 7-Zip sind klasse, um Dateien und Ordner mal eben zu verschlüsseln.
- Für reine Windows-Umgebungen lohnt sich ein Blick auf Microsofts BitLocker – wenn die Edition es hergibt.
- VeraCrypt ist eine Universallösung: quelloffen, flexibel und systemübergreifend.

schlüssel zu sichern. Ohne das getan zu haben, geht es nicht voran. Die naheliegende Option ist, den Schlüssel auszudrucken – entweder auf Papier oder über den Standard-PDF-Drucker von Windows. Über diesen 48-stelligen Schlüssel bekommen Sie auch dann noch Zugriff aufs Laufwerk, wenn Sie das Kennwort vergessen haben.

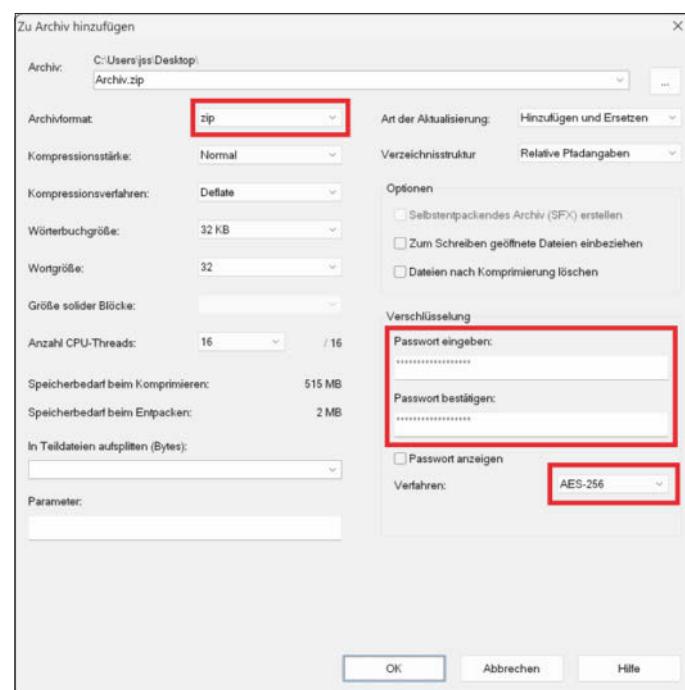
Danach entscheiden Sie, ob BitLocker den kompletten Datenträger oder nur dessen benutzte Bereiche verschlüsseln soll. Die Idee dahinter: Waren sensible, aber inzwischen gelöschte Daten darauf gespeichert, ließen sich Teile davon möglicherweise mit Datenrettungssoftware rekonstruieren, sofern die betroffenen Speicherbereiche nicht zwischenzeitlich neu beschrieben wurden. Mit der Option

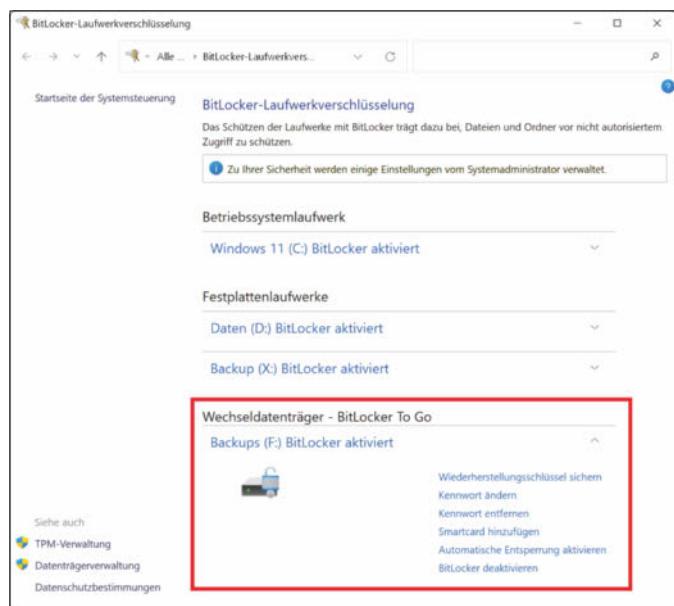
„Gesamtes Laufwerk verschlüsseln“ schließen Sie dieses Risiko aus, denn eventuelle Rückstände alter Dateien werden einfach mitverschlüsselt. Bisweilen kostet die zusätzliche Sicherheit allerdings (zu) viel Zeit: Schnelle externe SSDs können auch bei vollständiger Verschlüsselung nach ein paar Minuten fertig sein, lahme USB-Sticks brauchen jedoch durchaus mehrere Stunden. Also: Ist das Medium fabrikneu oder war noch nie etwas Sensibles in unverschlüsselter Form darauf gespeichert, nehmen Sie die schnellere Variante.

Im nächsten Schritt wählen Sie noch den Verschlüsselungsmodus aus. Der „neue Modus“ verwendet den AES-Algorithmus im moderneren XTS-Verfahren, das verschlüsselte Daten etwas besser vor unerkannten Manipulationen schützt. Der Nachteil: Nur Systeme ab Windows 10 Version 1511 können damit etwas anfangen. Soll der Stick auch an Rechnern mit älterem Windows andocken, wählen Sie sicherheitshalber den „kompatiblen Modus“. Nun klicken Sie noch auf „Verschlüsselung starten“.

Mobile Datenträger mit BitLocker sind denkbar einfach zu benutzen: anstecken, den Hinweis auf die Verschlüsselung anklicken, Kennwort eingeben, fertig. Wer im Kennwort-Pop-up auf „Weitere Optionen“ klickt, kann mit einem Häkchen festlegen, dass der Stick künftig ohne Kennworteingabe entsperrt wird – und zwar nur auf dem jeweiligen PC, nicht auf anderen. So können Sie den Stick beispielsweise zu

**Mit 7-Zip verpacken Sie Dateien im Handumdrehen in einem verschlüsselten Archiv – perfekt für schnell-mal-eben.**





**Nostalgisch: Auch in Windows 11 finden Sie die BitLocker-Verwaltung noch in der klassischen Systemsteuerung.**

wort – VeraCrypt selbst empfiehlt mindestens 20 Zeichen. Danach fragt der Assistent, ob Sie Dateien speichern möchten, die größer als 4 GByte sind. Abhängig von Ihrer Antwort wählt das Programm als Dateisystem den uralten Klassiker FAT oder das deutlich modernere exFAT aus. Im Folgedialog können Sie die Einstellung bei Bedarf auch in NTFS oder ReFS ändern.

Nun bewegen Sie den Mauszeiger möglichst wirr auf dem Fenster des VeraCrypt-Assistenten hin und her, bis sich der Fortschrittsbalken für die gesammelte Entropie grün färbt. Die Idee dahinter ist, den AES-Schlüssel nicht ausschließlich auf einer vom Rechner erzeugten Zufallszahl aufzubauen, sondern zusätzlich unvorhersehbare menschliche Bewegungen einfließen zu lassen.

Falls Sie einen fabrikneuen Datenträger verwenden oder bislang keinerlei unverschlüsselte, sensible Daten darauf gespeichert wurden, können Sie getrost ein Häkchen vor „Schnell-Formatierung“ setzen. VeraCrypt verzichtet dann darauf, den Datenträger von Kopf bis Fuß mit Zufallsdaten zu beschreiben, was den Zeitaufwand von einigen Minuten oder gar Stunden auf wenige Sekunden verkürzt. Nach einem abschließenden Klick auf Formatieren bestätigen Sie die Hinweise und drücken die Beenden-Schaltfläche.

Die Handhabung eines Datenträgers mit VeraCrypt-Verschlüsselung ist nicht ganz so komfortabel wie bei BitLocker, denn er lässt sich nicht über den Laufwerksbuchstaben ansprechen, den Windows ihm zunächst zuweist. Zugriff bekommen Sie, indem Sie im VeraCrypt-Hauptfenster einen freien Buchstaben auswählen (zum Beispiel V:), dann auf Datenträger klicken und wie zuvor bei der Einrichtung die Partition auf dem Laufwerk auswählen (nicht

Hause sehr komfortabel und flexibel einsetzen, doch wenn Sie ihn einmal verlieren, kann ein Finder ihn mangels Ihres Rechners nicht entsperren.

Um die automatische Entsperrung wieder abzuschalten, öffnen Sie die BitLocker-Verwaltung (Windows-Taste, **bitlocker**, Eingabetaste) und klicken Sie beim betreffenden Laufwerk auf „Automatische Entsperrung deaktivieren“. In diesem Menü ändern Sie auch das Kennwort, drucken den Wiederherstellungsschlüssel erneut aus oder schalten die Verschlüsselung ganz ab. Mit Windows-Home-Editionen können Sie BitLocker zwar nicht einrichten oder verwalten, aber bereits verschlüsselte Medien trotzdem verwenden – Kennwortänderung & Co. sind aber nicht drin.

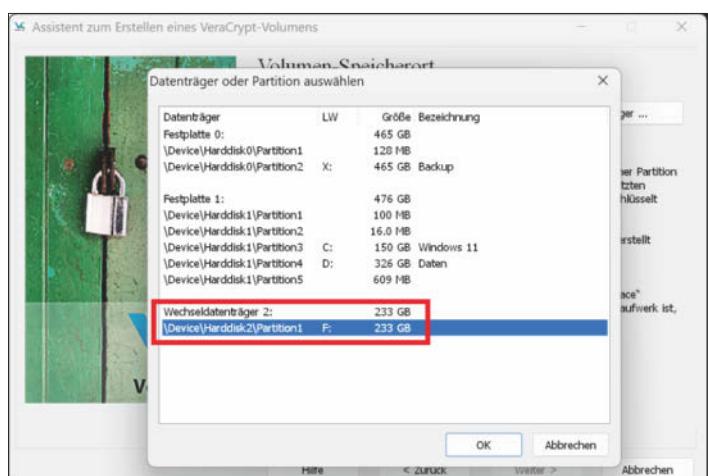
Einige BitLocker-Funktionen sind vor allem in Firmennetzen interessant. Admins können per Gruppenrichtlinie zum Beispiel erzwingen, dass Domänenbenutzer ihre Dateien ausschließlich auf BitLocker-verschlüsselte USB-Medien schreiben und zum Entsperren die passende SmartCard verwenden oder dass Wiederherstellungsschlüssel automatisch zentral im Active Directory hinterlegt werden.

## Die vielseitige Methode: VeraCrypt

VeraCrypt ist der Nachfolger des erfolgreichen, aber vor ein paar Jahren urplötzlich eingestellten TrueCrypt-Projekts. Es läuft nicht nur auf Windows (einschließlich Home), sondern ist auch für Linux, macOS, Raspi-Systeme und FreeBSD zu haben. In diesem Artikel zeigen wir die Verwendung der Windows-Version.

Nach Installation und Start der Software klemmen Sie einen USB-Datenträger an und klicken auf „Volume erstellen“, um den Assistenten für VeraCrypt-Volumes zu starten. Zunächst wählen Sie die mittlere Option „Eine Partition/ein Laufwerk verschlüsseln“ und danach das „Standard-VeraCrypt-Volume“. Für den Volume-Speicherort klicken Sie als Nächstes auf „Datenträger ...“ und wählen die Partition aus, die VeraCrypt verschlüsseln soll. Achtung: Wählen Sie nicht den Eintrag „Wechseldatenträger“ aus, sondern die darunter gelistete Partition mit einem Namen wie „\Device\Harddisk2\Partition1“.

Im nächsten Schritt wählen Sie „Verschlüsseltes Volumen erstellen und formatieren“; dann übernehmen Sie die vorgeschlagenen Algorithmen (die Vorgaben AES und SHA-512 sind völlig ausreichend). Bestätigen Sie die Größe der Partition und vergeben Sie ein möglichst starkes Pass-



**Nicht das Laufwerk auswählen, sondern die Partition darauf – VeraCrypt mag nicht wahnsinnig komfortabel sein, ist aber plattformunabhängig, flexibel und quelloffen.**

das Laufwerk selbst). Klicken Sie dann auf „Einhängen“ und tippen Sie Ihr Passwort ein – nach ein paar Sekunden sehen Sie das VeraCrypt-Laufwerk im Datei-Explorer als virtuellen Datenträger.

Um den Komfort zu verbessern, empfehlen wir zwei Handgriffe. Erstens: Entfernen Sie den Laufwerksbuchstaben des physischen Laufwerks. Der ist unnötig und nervt nur, denn per VeraCrypt können Sie ausschließlich über das virtuelle Laufwerk auf den Datenträger zugreifen. Dazu öffnen Sie die Datenträgerverwaltung, etwa per Windows+X, klicken mit der rechten Maustaste auf das RAW-Laufwerk des Wechselseitigen und dann auf „Laufwerksbuchstaben und -pfade ändern...“. Dort markieren Sie den Buchstaben, klicken auf Entfernen und bestätigen die Dialoge.

Zweitens können Sie VeraCrypt mitteilen, dass es beim Anstecken des Mediums automatisch nach dem Kennwort fragen soll – so müssen Sie das Programm nicht jedes Mal extra öffnen. Dafür klicken Sie in der Buchstabenliste von VeraCrypt

mit der rechten Maustaste auf „Zu Favoriten hinzufügen...“; setzen ein Häkchen vor „Ausgewähltes Volumen einhängen, wenn sein Host-Gerät angeschlossen wird“ und bestätigen mit OK. Von nun an sollte VeraCrypt eine Kennwortabfrage anzeigen, sobald Sie das Laufwerk anklammern.

Ähnlich wie normale USB-Sticks & Co. sollten Sie auch VeraCrypt-Medien aushängen, bevor Sie sie vom PC abstöpseln. Am einfachsten geht das über das VeraCrypt-Icon im Infobereich der Taskleiste: Rechtsklick darauf und „Trennen...“ anklicken.

VeraCrypt kann deutlich mehr, als wir hier zeigen – zum Beispiel das Systemlaufwerk verschlüsseln und verschlüsselte Containerdateien erstellen. Auch versteckte Volumes sind möglich, also ein im ungenutzten Bereich eines normalen VeraCrypt-Volumes platziertes Geheimlaufwerk, dessen Existenz von außen nicht erkennbar ist. Zudem können Sie reichlich Details einstellen, zum Beispiel den Verschlüsselungsalgorithmus konfigurieren

oder dem Passwort eine Schlüsseldatei hinzufügen, die als eine Art zweiter Faktor zum Entsperren nötig ist.

## Fazit

Zip-Archive sind klasse, um Dateien im Handumdrehen zu verschlüsseln, bevor man sie auf den Stick oder die externe Platte schiebt. Doch wer ständig mit verschlüsselten Daten hantiert, braucht eine praktischere Lösung. Wer ausschließlich Windows 10 oder 11 nutzt und auf dem eigenen PC mindestens die Pro-Edition betreibt, hat mit BitLocker bereits eine richtig komfortable Verschlüsselung an Bord. Auf Seite 180 finden Sie eine FAQ zum Thema BitLocker – mit Antworten auf Fragen, die Sie uns häufiger stellen. Und VeraCrypt ist die Universallösung: sehr flexibel einstellbar, quelloffen und vor allem für alle gängigen Plattformen zu haben.

(jss@ct.de) 

**Download 7-Zip und VeraCrypt:  
[ct.de/nyw](http://ct.de/nyw)**

# Wir schreiben Zukunft.

**2 Ausgaben MIT Technology Review  
als Heft oder digital  
inklusive Prämie nach Wahl**



[mit-tr.de/testen](http://mit-tr.de/testen)



[mit-tr.de/testen](http://mit-tr.de/testen)



+49 541/80 009 120



[leserservice@heise.de](mailto:leserservice@heise.de)



# Sichere Datenträger für unterwegs

## USB-Speicher mit Hardwareverschlüsselung

**Persönliche Daten sollten nicht in fremde Hände geraten, geschäftliche Daten dürfen es schon gar nicht. Zum geschützten Transport eignen sich selbst verschlüsselnde USB-Datenträger – etwa die aus diesem Test.**

Von Lutz Labs

Windows aktiviert bei modernen Büro-PCs und Notebooks heutzutage automatisch die Bitlocker-Verschlüsselung für SSDs und Festplatten, bei MacBooks lässt sich FileVault 2 einschalten. Bei einem Diebstahl oder einem Defekt kommt dann niemand an die Daten auf den internen Massenspeichern heran. Doch für Backups oder zum Transport setzt man häufig externe USB-Speicher ein, je nach Datenmenge Sticks, SSDs oder auch Festplatten. Gehen diese verloren oder werden sie gestohlen, können sensible Daten in falsche Hände geraten. Daher sollte man Daten auf externen Speichermedien stets verschlüsseln.

Komfortabler ist es oft, wenn die Datenträger selbst für Verschlüsselung sor-

gen. Dann ist man als Anwender zwar gezwungen, eine PIN einzugeben oder das Speichermedium auf eine andere Art freizuschalten; um die Sicherheit aber muss man sich keine Gedanken mehr machen: Selbst wenn der Speicher verloren geht, sind die Daten vor fremden Augen geschützt. Das gilt zumindest, wenn die Hersteller der Speichermedien beim Verschlüsseln alles richtig machen und ohne Sicherheitslücken umsetzen.

Wir haben uns drei solcher Speicher besorgt. Wir testeten die USB-SSD Samsung SSD T7 Touch mit Entsperrung durch einen Fingerabdruckscanner und zwei eher für gewerbliche Nutzer ausgelegte Speicher: die USB-Festplatte Apricorn Aegis Padlock und den USB-Stick Sentry



## Apricorn Aegis Padlock

Die einzige Festplatte im Test bietet den meisten Speicherplatz pro Euro. In der Apricorn Aegis Padlock steckt eine Seagate Barracuda Compute, eine 2-TByte-Festplatte mit SMR-Aufzeichnung. Auf den Innenringen sinkt die Geschwindigkeit auf knapp 70 MByte/s.

Direkt nach dem Einstecken läuft die Platte an, das Freischalten macht etwas Angst: Da das USB-Kabel nur 10 cm lang ist, muss man die Platte mit einer Hand halten, während die andere die PIN eintippt. Apricorn bestückt die Gehäuse auch mit SSDs, die sich für eine solche Behandlung weit besser eignen, aber auch deutlich teurer sind.

- ⬆️ günstig
- ⬆️ FIPS-Zertifizierung
- ⬇️ komplizierte Bedienung

Preis: circa 308 Euro (USB-Festplatte, 2 TByte)



## Datalocker Sentry K350

Den USB-Stick Sentry K350 von Datalocker gibt es mit bis zu 512 GByte Speicherplatz. Die Bedienung ist durch das kleine Display komfortabler als bei der Aegis Padlock, zudem sorgt ein kleiner Akku im Gerät dafür, dass der Stick dabei nicht im USB-Port stecken muss.

An einem USB-2.0-Port wollte der Sentry K350 nicht starten, auch mit einer USB-Verlängerung kam das Gerät nicht zurecht. Beim Lesen und beim Schreiben erreichten wir mehr als 200 MByte/s, beim Schreiben allerdings nur für kurze Zeit: Der kleine Cache des Sticks ist ratzfatz gefüllt.

- ⬆️ FIPS-Zertifizierung
- ⬇️ sehr teuer
- ⬇️ komplizierte Einrichtung

Preis: circa 290 Euro (USB-Stick, 64 GByte)



## Samsung SSD T7 Touch

Schnell, günstig und komfortabel: Die Samsung-SSD T7 Touch ist eigentlich ideal für den Transport schützenswerter Daten. Sie ist etwa scheckkartengroß, aber etwas dicker, und passt so in jede Hemdtasche. Im Test haben wir beim Lesen und Schreiben fast 1000 beziehungsweise 900 MByte/s gemessen.

Die T7 Touch kennt keinen Administratormodus; wenn man das Passwort vergisst, kann man sie nur noch zurücksetzen. Der Fingerabdrucksensor entsperrt die Platte zwar komfortabel, er ist aber auch ein Angriffspunkt für Datendiebe.

- ⬆️ einfache Bedienung
- ⬆️ flott und günstig
- ⬇️ keine FIPS-Zertifizierung

Preis: circa 93 Euro (USB-SSD, 500 GByte)

K350 von Datalocker. Die Kapazität der Geräte ist sehr unterschiedlich: Während der USB-Stick mit 64 GByte Speicherplatz nur wenige Daten fasst, sind die USB-SSD mit 500 GByte und die USB-Festplatte mit 2 TByte für größere Datentransporte geeignet.

Den Unterschied zwischen den beiden Profi-Lösungen und der Samsung-SSD sieht man auch am Preis: Während die Apricorn-Festplatte und der Datalocker-Stick rund 300 Euro kosten, ist die Samsung-SSD mit Fingerabdruckscanner für rund 90 Euro zu haben – zumindest unser 500-GByte-Modell. Es ist damit kaum teurer als das Modell ohne biometrische Entsperrung.

### Offene Verschlüsselung

Manche Anwender vertrauen nur offengelegten Verschlüsselungsmethoden, deren Quellcode einsehbar ist – Open Source hält. Das bieten viele Softwarelös-

sungen wie Microsoft Bitlocker nicht, erst recht nicht selbstverschlüsselnde Geräte. Man muss sich daher blind auf die Fähigkeiten und die Sorgfalt der jeweiligen Hersteller verlassen, was nicht immer gut geht. Zu oft schon gab es Meldungen über geknackte Hardwareverschlüsselungen, zuletzt Mitte 2022 [1]: Da kamen einige USB-Speicher von Verbatim in Verruf, weil ihre Verschlüsselung sehr einfach zu umgehen war.

Wir haben für diesen Schwerpunkt deshalb den Entdecker der Verbatim-Sicherheitslücke, den Sicherheitsspezialisten Matthias Deeg, um Mitarbeit gebeten. Er hat die drei Geräte aus diesem Test exemplarisch und tiefergehend auf mögliche Sicherheitsprobleme hin untersucht und dabei keine offensichtlichen Probleme gefunden. Details zu seinen Angriffen auf die Verschlüsselung und vor allem seine Vorgehensweise lesen Sie im Artikel auf Seite 78.

### Speicher für Consumer und Profis

Bei selbstverschlüsselnden USB-Speichern gibt es zwei Konzepte: Geräte, die das Speichern unverschlüsselter Daten zulassen und solche, die genau das nicht tun. Während Samsung den Kunden bei der T7 Touch die Wahl lässt, lassen Apricorn und Datalocker dies nicht zu. Beide verlangen vor der ersten Datenspeicherung zwingend das Einrichten mit einem Passwort.

Für Privatleute ist Komfort oft wichtiger als maximale Sicherheit – bestes Beispiel dafür ist das Entsperren moderner Mobiltelefone durch Fingerabdruck. Das Knacken ist zwar möglich, aber dazu ist ein gewisser Aufwand und etwas Fachwissen nötig, was die Hürde gegen Datendiebstahl von Laien im Vorbeigehen erhöht.

Beim gewerblichen Einsatz geht die Sicherheit vor, etwa um Datenschutzvor-

## USB-Speicher mit Verschlüsselung: Benchmarks

	sequenzielle Transferraten <sup>1</sup> Schreiben / Lesen [MByte/s]	IOPS <sup>1</sup> Schreiben / Lesen	Leistungsaufnahme idle / Lesen / Schreiben [W]	Data Drive Benchmark <sup>2</sup> [Punkte]
Apricorn Aegis Padlock	besser ►	besser ►	► besser	besser ►
Datalocker Sentry K350	135/137	211/117	1,6/3,9/4,2	397
Samsung SSD T7 Touch	96/223	6416/4817	0,6/1,2/1,2	440
	886/976	33924/51115	0,7/3,3/3,3	871

<sup>1</sup> gemessen mit Iometer <sup>2</sup> gemessen mit PCMark 10

gaben einzuhalten. Die USB-Speicher sollten dazu eine Zertifizierung einer unabhängigen Prüforganisation haben; internationaler Standard ist die FIPS-Zertifizierung, welche sowohl die Aegis Padlock als auch der Sentry K350 haben. Ein stärkerer Datenschutz bedeutet jedoch auch weniger Komfort, der Umgang mit den beiden Speichern verlangt eine gewisse Einarbeitung.

Ebenfalls nur bei den Profigeräten findet man eine zweistufige Verwaltung: Administratoren haben mehr Rechte als Anwender; sie können etwa Passwörter der Nutzer zurücksetzen oder Parameter einstellen, die den Anwendern verwehrt sind. Zudem lassen sich die Profigeräte per Software administrieren – das aber kostet bei Apricorn und Datalocker einen zusätzlichen Obolus [2]. In diesem Artikel konzentrieren wir uns auf die Hardware. Interessenten können bei den Herstellern nach einer Remote-Demonstration der Softwarefähigkeiten fragen, Datalocker bietet dazu Webinare an.

### Aus- und einschalten

Zieht man die getesteten Speicher vom USB-Port ab, dann sind sie beim nächsten Anstecken gesperrt. Bei den beiden Profilösungen sind die Daten auch nach einem Neustart des Rechners oder dem erneuten Hochfahren aus dem Ruhezustand geschützt. Die Samsung-SSD zeigt ihre Inhalte im Test selbst nach einem Neustart hingegen weiterhin an – solange die SSD Strom bekommt, sperrt sie sich nicht. Da nach dem Wiederhochfahren eine Benutzeranmeldung fällig wird, kann man das zumindest in einer Einzelplatzlösung oder an einem privaten PC verschmerzen.

Apricorn hat in seiner Firmware eine Funktion namens Lock-Override eingebaut, die dem Administrator erlaubt, das gleiche Verhalten einzustellen. Eine blau blinkende LED weist Anwender auf die veränderte Einstellung hin.

### Sicher löschen

Manchmal reicht das einfache Löschen von Dateien nicht aus, etwa wenn man den

Speicher verkaufen oder verschenken will. Dann sollte man das Gerät zurücksetzen, was nicht nur die Daten, sondern die gesamte Konfiguration löscht. Apricorn und Datalocker haben dazu Funktionen vorgesehen, doch bei Samsung wird es kompliziert – zumindest auf den ersten Blick.

Laut Anleitung muss man sich dazu an den Samsung-Kundendienst wenden, der dann die T7 Touch auf die Werkseinstellungen zurücksetzt. Das haben wir ausprobiert. Zunächst verlangte der Dienstleister von uns die Rechnung der SSD und ein unterschriebenes Formular, das ihn von Regressansprüchen beim Zurücksetzen der SSD freispricht. Dann schickte er eine Anleitung und einen Link – zum Magician, dem SSD-Verwaltungsprogramm von Samsung. Dies ist nämlich in der Lage, die T7-Serie zurückzusetzen, man muss dazulediglich die an der Seite aufgedruckte PSID-Nummer eingeben. Den Aufwand mit dem Dienstleister kann man sich also sparen.

Die Geräte von Apricorn und Datalocker kennen zudem einen sogenannten Self-Destruct-Modus: Wird man etwa bei

der Einreise in ein fremdes Land aufgefordert, die Inhalte der Medien freizulegen, kann man stattdessen „versehentlich“ auch eine andere PIN eingeben und damit sämtliche Daten löschen.

### Fazit

Unternehmen müssen bei der Auswahl abwägen, denn sowohl Apricorn als auch Datalocker haben weitere verschlüsselnde USB-Speicher im Programm. Die Sicherheitsbeauftragten müssen sich zunächst entscheiden, wie viel Speicher sie benötigen und wie schnell dieser sein muss. Festplatten fassen mehr Daten, SSDs sind schneller, Sticks kleiner und leichter. Vor allem aber sollten sich Interessenten die Verwaltungssoftware anschauen, denn bei steigender Zahl von zu verwaltenden USB-Speichern verliert man ohne diese schnell die Übersicht.

Für Privatanwender ist die Wahl hingegen einfach: Die Samsung SSD T7 Touch ist günstig und komfortabel und mit ausreichend Speicherplatz erhältlich.

(ll@ct.de) ct

### Literatur

[1] Christof Windeck, Verschlüsselte Verschlüsselung, Schwere Sicherheitslücken in verschlüsselnden USB-Speichern, c't 15/2022, S. 108

[2] Lutz Labs, Doppelt sicher, USB-Sticks mit Hardwareverschlüsselung und Management, c't 14/2018, S. 120

Download der Testprogramme:  
[ct.de/yjq7](http://ct.de/yjq7)

## USB-Speicher mit Verschlüsselung: technische Daten

Modell	Aegis Padlock	Sentry K350	SSD T7 Touch
Hersteller, URL	Apricorn, <a href="http://apricorn.com">apricorn.com</a>	Datalocker, <a href="http://datalocker.com">datalocker.com</a>	Samsung, <a href="http://samsung.de">samsung.de</a>
Typ	USB-Festplatte	USB-Stick	USB-SSD
Bezeichnung	A25-3PL256-2000	SK350-064-FE	MU-PC500K/WW
Kapazität laut Hersteller <sup>1</sup>	2 TByte	64 GByte	500 GByte
von Windows erkannte Kapazität	1863 GByte	59 GByte	466 GByte
Entsperrung	Zehnertastatur	Zehnertastatur	Fingerabdrucksensor, Software
Verschlüsselung <sup>2</sup>	AES-XTS 256 Bit	AES-XTS 256 Bit	AES 256 Bit
Zertifikate <sup>2</sup>	FIPS 140-2 Level 3	FIPS 140-2 Level 3, IP67, MIL-STD-810G	–
Maße, Gewicht	12 mm × 85 mm × 19 mm, 204 g	101 mm × 21 mm × 14 mm, 34 g	85 mm × 57 mm × 8 mm, 63 g
Geräteanschluss	USB-A	USB-A	USB-C
mitgelieferte Kabel	– (fest angebaut, 10 cm)	–	USB-A, USB-C (40 cm)
Formatierung bei Auslieferung	NTFS	exFAT	exFAT
Garantie	3 Jahre	3 Jahre	3 Jahre
Straßenpreis	308 €	290 €	93 €
Preis pro Gigabyte	15,4 ct	453,1 ct	18,6 ct
weitere erhältliche Kapazitäten	500 GByte (188 €), 1 TByte (240 €)	128 GByte (428 €), 256 GByte (475 €), 512 GByte (655 €)	1 TByte (130 €), 2 TByte (245 €)

<sup>1</sup> Die Hersteller rechnen mit 1 GByte = 1.000.000 000 Byte. Für Windows dagegen ist 1 GByte = 1.073.741.824 Byte, die angezeigte Kapazität ist daher kleiner.  
<sup>2</sup> Herstellerangaben



21. - 23. MÄRZ 2023

im Phantasialand bei Köln

## Die Konferenz der Java-Community

[www.javaland.eu](http://www.javaland.eu)

Mehr Infos zum Event findet Ihr hier:



### The Zen of Programming

In seiner Keynote schildert Sander Hoogendoorn seine persönliche Reise durch Plattformen, Sprachen, Prinzipien, Zweifel und Kämpfe, die vielen Entwickler:innen im Laufe ihrer Karriere begegnen.



### Community-Keynote

Sexismus, Mobbing und Bossing, unkontrollierter Narzissmus und fehlende Eskalationswege im Job haben in den letzten Jahren auch vor der Java-Community keinen Halt gemacht. Wir lüften den dunklen "Tabu-Vorhang".

Teilt eure Story mit uns: [kummerkasten@ijug.eu](mailto:kummerkasten@ijug.eu)



2.000+ JAVA-FANS



160+ SESSIONS



50+ AUSSTELLER



100 % AUSTAUSCH



54 JAVA USERGROUPS



100 % SPASS



Präsentiert von:

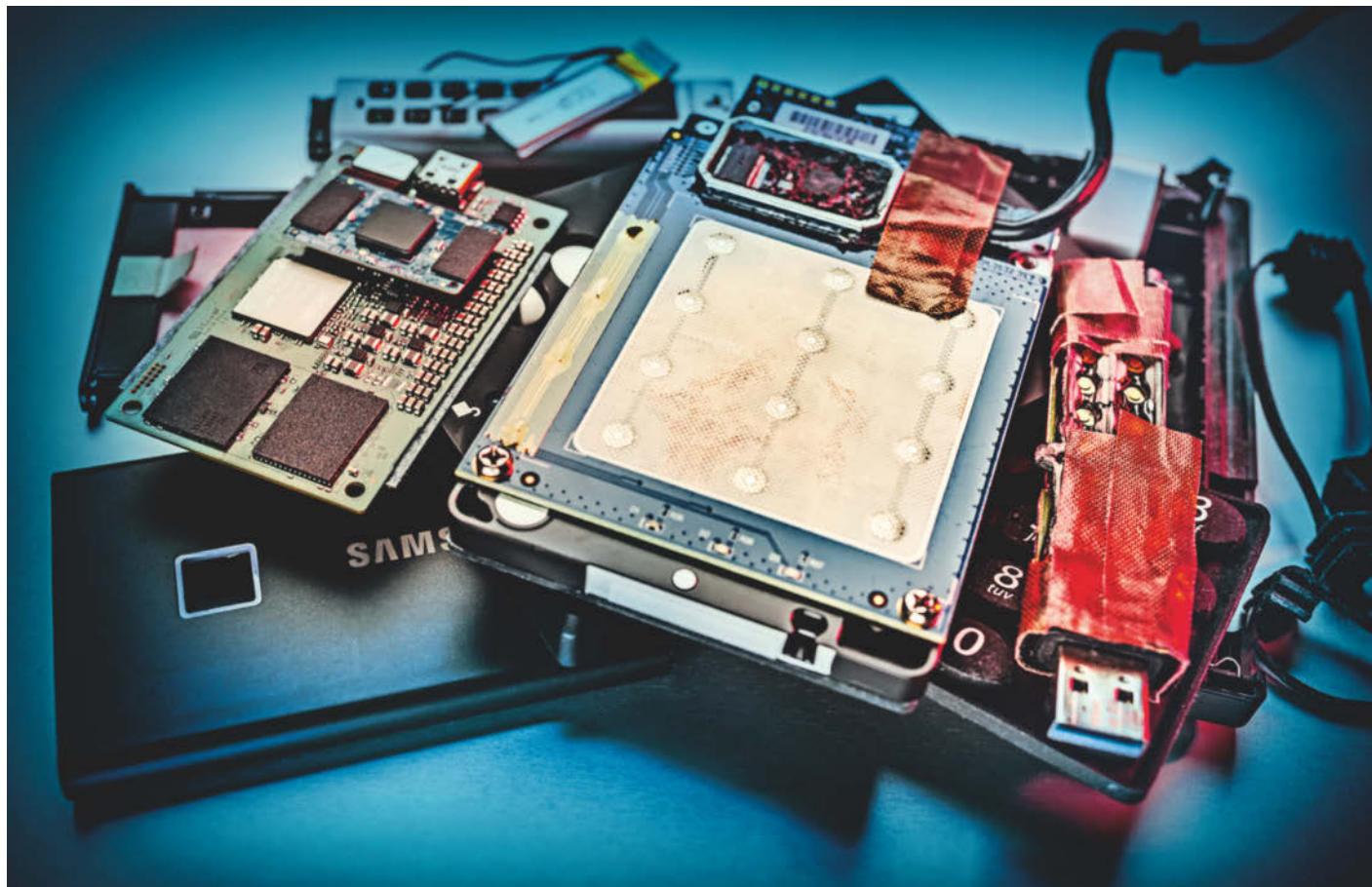


Heise Medien

DOAG

Veranstalter:





# Ein Blick in die Eingeweide

## IT-Sicherheitsanalysen bei verschlüsselten mobilen Datenträgern

**Wer seine Daten auf verschlüsselten USB-Medien speichert, erwartet, dass diese die Daten nur nach Eingabe des richtigen Passworts herausrücken. Wir testen, ob das auch stimmt.**

Von Matthias Deeg

**D**er Sicherheitsforscher Matthias Deeg hat bereits einige Schwachstellen in USB-Speichern entdeckt, unter anderem bei Sticks von Verbatim. Er beschreibt hier aus der Ich-Perspektive, wie er ein Produkt typischerweise analysiert, und zwar am Beispiel der verschlüsselten USB-Medien aus dem vorangegangenen Test ab Seite 74. Los gehts.

Ende Oktober 2022 erhielt ich ein Paket mit drei mobilen Datenträgern, die laut den Herstellern eine sichere und verschlüsselte Datenspeicherung gewährleisten und dazu nur berechtigten Personen Zugriff auf die geschützten Daten im Klartext ermöglichen: die USB-Festplatte Apricorn Aegis Padlock, die USB-SSD Sam-

sung Portable SSD T7 Touch und den USB-Stick DataLocker Sentry K350.

Zur Verschlüsselung nutzen alle drei Geräte den Verschlüsselungsstandard Advanced Encryption Standard (AES) mit einer Schlüssellänge von 256 Bit, welcher, richtig angewandt, als sicher gilt. Für die Benutzerauthentifizierung verwenden Apricorn Aegis Padlock sowie DataLocker Sentry K350 PINs beziehungsweise Passwörter, welche die Benutzer jeweils über die Zehnertastatur des Geräts eintippen. Die Portable SSD T7 Touch von Samsung hat einen Fingerabdrucksensor für eine biometrische Authentifizierung, sie lässt sich jedoch auch mithilfe einer Software für Android, macOS und Windows und einem Passwort entsperren.

Für eine Sicherheitsanalyse dieser drei verschlüsselten mobilen Datenträger hatte ich zwei Wochen Zeit. Das war etwas knapp bemessen, reicht aber zum Erkennen grundlegender Sicherheitsprobleme aus.

## Angriffsszenarien

Die Angriffsszenarien sind bei dieser Gerätekategorie überschaubar. Die spannendste Frage ist, ob Schwachstellen existieren, die einen unautorisierten Zugriff auf die geschützten Daten ermöglichen. Voraussetzung für einen Angreifer ist ein physischer Zugriff auf das Gerät.

Ein Angriff kann je nach Angriffsszenario vor oder nach der ersten Verwendung des Geräts durch ein potenzielles Opfer passieren. Der Angreifer kann dazu unterschiedlich viel Zeit haben, vielleicht nur wenige Minuten, aber vielleicht kann er auch dauerhaft auf den Speicher zugreifen. Ich beschränke mich auf das wahrscheinlich wichtigste Szenario, bei dem ein Angreifer im Besitz eines bereits mit Daten bespielten Gerätes ist.

Eine gewisse Relevanz besitzen sogenannte Supply-Chain-Attacken, bei denen Schwachstellen von Hardware ausgenutzt werden, bevor diese überhaupt ihre potenziellen Opfer erreicht. Die prüfte ich in diesem Fall aber nicht, auch ein Angriff auf den Fingerabdrucksensor der Samsung-SSD fand aus Zeitgründen nicht statt.

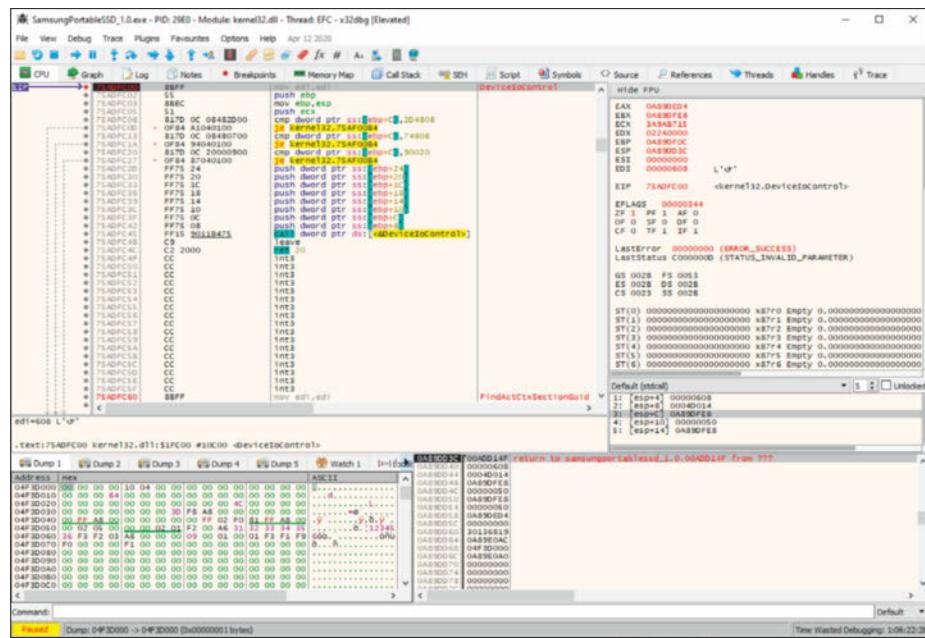
## Angriffsfläche

Als Angriffsfläche bezeichnen Sicherheitsspezialisten die Summe aller möglichen Wege, auf denen ein Angreifer in ein Gerät oder Netzwerk eindringen und an Daten gelangen kann. Sie ist von den eingesetzten Technologien, den verwendeten Komponenten und dem jeweiligen Funktionsumfang der Geräte abhängig. Bei verschlüsselten Datenträgern besteht die Angriffsfläche aus drei Elementen:

- Hardwarekomponenten und entsprechende Schnittstellen, beispielsweise für die Kommunikation oder zu Analyse- und Debug-Zwecken
- Firmwarekomponenten, die das Verhalten der Hardware definieren und vom Gerät ausgelesen oder über das Internet heruntergeladen werden können
- Softwarekomponenten, die zusammen mit der Hardware genutzt werden

## Testmethodik

Ich versuchte zunächst, die Gehäuse der Datenträger zu öffnen. So kann ich ein-



Über den Debugger x64dbg lässt sich die USB-Gerätekommunikation analysieren, hier am Beispiel der Übertragung des Passworts 123456 an die SSD.

gebaute Chips wie Mikrocontroller und Speicherbausteine identifizieren und im Web nach Datenblättern und technischer Dokumentation forschen. Weiter suche ich auf den Chips nach Testpunkten und Debug-Schnittstellen, die mir vielleicht eine einfachere Analyse der Kommunikation zwischen den Komponenten ermöglichen oder gar Zugriff auf die Firmware oder Konfigurationsdaten geben.

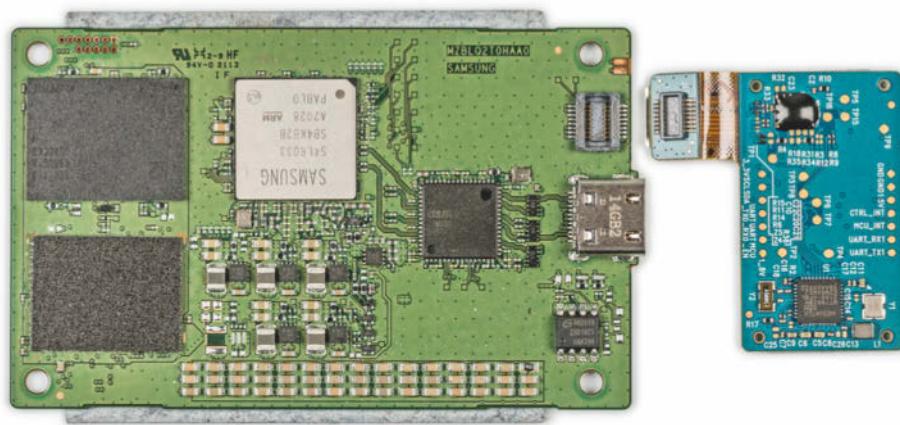
Wenn ich durch Downloads oder das Auslesen von Speicherbausteinen Zugriff auf die Geräte-Firmware erhalte, suche ich im nächsten Schritt nach Informationen über die Firmware und wie sie funktioniert. So kann ich den Code mit Software-

Tools wie Disassembler und Dekompilier besser verstehen.

Sofern die Hersteller Software-Tools zur Verwaltung der USB-Speicher mitliefern oder im Web bereitstellen, kann ich sie mit Reverse-Code-Engineering-Methoden wie der statischen und dynamischen Codeanalyse untersuchen. Bei der statischen Codeanalyse kann man beispielsweise benutzte verdächtige Programmblibliotheken entdecken, bei der dynamischen die Datenübertragung mitschneiden.

## Sicherheitsanalyse

Zu Beginn meiner Sicherheitsanalyse konfigurierte ich alle drei Testgeräte gemäß



Die Hardwareanalyse hilft, sich einen grundlegenden Überblick der Komponenten zu verschaffen: Samsungs SSD T7 Touch besteht aus zwei Flash-Chips, einem SSD-Controller und einem USB-PCIe-Wandler. Dazu gesellt sich über eine Zusatzplatine der Fingerabdruckscanner.



**Beim Freilegen der Chips des Datalocker-Sticks habe ich diese beschädigt, sodass weitere Analysen nicht mehr möglich waren.**

Anleitung. Die danach auf dem Gerät gespeicherten Daten waren damit nur Benutzern zugänglich, die das Passwort oder die PIN kennen beziehungsweise den registrierten Fingerabdruck im Lesegerät reproduzieren können. Nach dem Einrichten der Geräte prüfte ich, ob die Benutzerauthentifizierung wie von den Herstellern beschrieben funktioniert.

Anschließend testete ich manuell, ob sich die Geräte bei fehlgeschlagenen Authentifizierungsversuchen gemäß ihrer Spezifikation und Konfiguration verhalten. Beispielsweise sind der DataLocker-Stick und die Apricorn-Festplatte so einstellbar, dass sie nach einer festgelegten Zahl fehlgeschlagener Anmeldeversuche die Daten löschen und zusätzlich ihre gesamte Konfiguration.

Die Samsung Portable SSD T7 Touch lässt sich dieses Verhalten anders als bei den beiden anderen Geräte nicht anwiesen. Ein gewisser Schutz gegen automatisiertes Passwort-Raten – aka Brute Force – besteht in der Geschwindigkeit, mit der die SSD Benutzerauthentifizierungen entgegennimmt: Nach fünf Fehlversuchen ist nur noch etwa ein Versuch pro Sekunde möglich. Nach Ab- und Anstecken der SSD vom USB-Port lässt die Firmware erneut maximal fünf schnelle Anmeldeversuche zu; anschließend greift wieder der ausbremsende Brute-Force-Schutz.

## **Identifikation der Hardware**

Durch das eingangs beschriebene Öffnen der Geräte konnte ich mehr über ihre Komponenten herausfinden. Die interessanten Chips des Apricorn Aegis Padlock sowie des DataLocker Sentry K350 sind in Epoxidharz vergossen und damit nicht zu-

gänglich. Bei der Samsung Portable SSD T7 Touch hingegen sind mit Ausnahme eines Chips auf der Platine des Fingerabdrucksensors alle Hardwarekomponenten erreichbar und über ihre Beschriftungen beziehungsweise Gravuren identifizierbar. Der Kunstharzschutz sicherheitsrelevanter Komponenten ist bei Geräten mit Sicherheitszertifizierungen die Regel, der DataLocker Sentry K350 ist beispielsweise nach dem amerikanisch-kanadischen Prüfstandard FIPS 140-2 Level 3 zertifiziert (siehe S. 62).

Mit etwas Chemie in Form von Aceton und etwas Physik in Form von Wärme versuchte ich nun, die in Kunststoff vergossenen Chips freizulegen. Beim DataLocker Sentry K350 scheiterte dies, der USB-Stick funktionierte danach nicht mehr. Das Eingießen bietet also einen gewissen Schutz. Mit dem Apricorn Aegis Padlock hingegen hatte ich mehr Erfolg; ich konnte die zwei interessanten Chips so freilegen, dass dieses Gerät immer noch funktioniert und weitere Analysen möglich sind.

Ich fand jedoch keine Informationen zu den Chips und ein Mitlesen der Kommunikation zwischen den beiden unbekannten Mikrocontrollern, beispielsweise während der Benutzerauthentifizierung, lieferte auch keine Erkenntnisse.

Der DataLocker Sentry K350 nutzt einen Mikrocontroller der STM32L4-Serie von STMicroelectronics, laut Hersteller mit der Programmabibliothek X-Cube-Cryptolib. Ich fand zwar Datenblätter und Programmierhandbücher zur STM32L4-Serie, aber im Testzeitraum konnte ich nicht auf den internen Speicher zugreifen, etwa auf die Firmware oder auf

Daten wie dem kryptografischen Schlüsselmaterial.

Die Portable SSD T7 Touch von Samsung nutzt den USB-Controller ASM2362 von ASMedia, eine USB-PCIe-Bridge. Danach folgen der SSD-Controller S4LR033, auch als Samsung Pablo bekannt, und zwei Flash-Speicherchips – den Controller verwendet Samsung auch in der PCIe-SSD 980, im Prinzip steckt also eine PCIe-SSD in der USB-SSD.

Mit Hilfe des Universal-Programmers XGecu T56 las ich die Firmware des USB-Controllers aus dem SPI-Flash-Memory-Chip (GigaDevice 25D10CTIG) aus. Ohne Datenblatt und weiteren Informationen beispielsweise über den Instruktionssatz des ASM2362 ist eine Firmwareanalyse ein hoffnungsloses Unterfangen.

So blieb die Analyse der Kommunikation mit einem Logikanalysator. Dabei kam jedoch nichts Spannendes raus, denn die via UART, SPI oder I2C ausgetauschten Daten lieferten ohne weitere Informationen zu den vermutlich proprietären Nachrichtenprotokollen keinen Mehrwert.

## **Softwarehilfe**

Samsung stellt für seine Portable SSD T7 Touch zwei Anwendungen bereit: Die Verwaltungssoftware Samsung Portable SSD und Samsung Magician, ein Tool, das auch das sichere Löschen der SSD erlaubt. Eine Analyse mit dem Softwaredebugger x64dbg sowie der Reverse-Engineering-Suite Ghidra lieferte Hinweise darauf, dass die SSD Merkmale der Opal-Storage-Security-Subsystem-Class-Spezifikation der Trusted Computing Group (TCG) implementiert. Ich legte meinen Fokus auf die passwortgestützte Authentifizierung, mit der sich die geschützte Partition entsperren lässt.

Zur Kommunikation zwischen SSD und Windows-Rechner nutzt Samsung SCSI-Befehle, die ich durch einen Haltepunkt auf die Windows-API-Funktion DeviceIoControl im Debugger beobachten konnte. Die Anzahl der ausgetauschten Nachrichten ist recht hoch; für die weitere Protokollanalyse musste ich den Datenverkehr aufzeichnen. Daher schrieb ich ein kleines Skript für das Binary-Instrumentation-Framework Frida. Das Skript speichert automatisiert die interessanten Daten der bidirektionalen USB-Kommunikation.

So konnte ich Aktionen der Software mit den entsprechenden Datenpaketen in Zusammenhang bringen, beispielsweise denen zur Passwortprüfung. Die nächste

Frage ist nun, ob sich durch eigene Nachrichten oder durch das Abspielen von vorher aufgezeichneten Nachrichten (Replay-Angriff) Sicherheitsprobleme ergeben. Ich erweiterte mein Frida-Skript also um die Funktion, aus mitgeschnittenen Nachrichten der USB-Kommunikation C-Code für meine eigene Clientsoftware zu erstellen.

Damit konnte ich selbst via USB mit der Portable SSD T7 Touch kommunizieren und wesentlich angenehmer als in einem Debugger analysieren, wie die Gerätefirmware auf Nachrichten in unerwarteter Reihenfolge oder nicht wohlgeformte Nachrichten reagiert. Bei diesen Tests stellte ich fest, dass die Samsung-SSD Abweichungen nur selten toleriert und schnell nicht mehr antwortet. Danach half nur noch ein Abstöpseln und Neustart. Automatisches Fuzzing des USB-Kommunikationsprotokolls geht somit nur mit einem Testaufbau, der Geräteneustarts unterstützt.

Die Tests zeigten immerhin, dass automatisierte Passwortrateangriffe



Beim Freilegen der Chips der Apricorn-Festplatte kamen unter dem Epoxidharz interessante Chips zum Vorschein.

gegen die Portable SSD T7 Touch möglich sind. Die Gerätefirmware verhindert aber, dass man das effizient tun könnte, weil sie die Benutzerauthentifizierung nach fünf fehlgeschlagenen Anmeldeversuchen verlangsamt.

## Fazit

Die – zugegeben – nicht in allerletzter Konsequenz ausgeführte Sicherheitsanalyse der drei Testgeräte entblößte keine kritischen Schwachstellen. Ein unautorisierte Zugriff auf die geschützten, verschlüsselt gespeicherten Daten im Klartext war bei keinem der Produkte möglich. Allerdings führt dies vor Augen, dass sich viele spannende Fragen zur Sicherheit proprietärer Hardware mangels recherchierbarer Dokumentation nicht beantworten lassen.

Mit mehr Zeit finden sich eventuell mehr Informationen über die Komponenten und mit aufwendigeren Analysen wie einer Hardware-Fault-Injection oder IC-Reversing offenbaren sich vielleicht doch noch Sicherheitsprobleme. Für die allermeisten Angreifer aber dürften die Verschlüsselung und die Schutzfunktionen dieser drei USB-Speicher eine zu hohe Hürde sein.

(ll@ct.de) **ct**

Erwähnte Tools: [ct.de/yygk](http://ct.de/yygk)

 **heise Academy**

# DIE LERNPLATTFORM FÜR IT-PROFESSIONALS

Wir machen IT-Weiterbildung digital



**JETZT  
KOSTENLOS  
TESTEN**

### Das erwartet dich:

- Über 100 Online-Trainings und 80 Online-Kurse
- Die wichtigsten IT-Themen für heute und morgen
- Erfahrene IT-Experten
- Individuelle Lernumgebung
- Übungsaufgaben und Wissenstests

Hier geht's zu deiner Weiterbildung: **heise-academy.de**



# Es gibt was auf die Ohren

**40 Jahre c't: Wir verlosen zum Auftakt eine Teufel Power HiFi**



**c't feiert, und Sie können dabei sein und etwas gewinnen. Einfach so gibts unseren Preis aber nicht, denn wer in die Verlosung will, muss vorher unser Bildrätsel lösen.**

**Von Georg Schnurer**

Das Thema Raumfahrt interessiert viele c't-Leserinnen und -Leser. Deshalb haben wir uns für das erste Gewinnspiel im Rahmen unserer Aktionen zum 40-jährigen Jubiläum ein kniffliges Bildrätsel mit Space-Shuttle-Motiv ausgedacht: Die beiden Bilder rechts unterscheiden sich nur in winzigen Details. Wir haben mal auf dem oberen Bild etwas weggelassen oder hinzugefügt, mal weist das untere Details auf, die es auf dem anderen Bild nicht gibt. Ihre Aufgabe ist es nun herauszufinden, wie viele Unterschiede es zwischen den beiden Bildern gibt.

Jeder Unterschied zwischen den beiden Bildern zählt nur einmal. Schauen Sie

mal auf die Logos im Bild unten. Da ist auf dem linken Flügel des Shuttles die amerikanische Flagge, auf dem rechten das NASA-Logo. Auf dem oberen Bild ist es aber genau andersherum. Das zählt dann als ein Unterschied, nämlich, dass die Logos vertauscht sind – ups, jetzt haben wir doch tatsächlich schon etwas verraten ...

Dass die Logos in der Spiegelung des Shuttles im Wasser im unteren Bild nicht stimmen, ist zwar eine physikalische Unmöglichkeit, aber eben kein Unterschied zwischen den beiden Bildern.

So, genug Tipps fürs Erste – oder vielleicht doch noch einer: Wir haben mehr als 5 und weniger als 50 Unterschiede in den beiden Bildern versteckt. Wenn Sie glauben, alle Unterschiede entdeckt zu haben (inklusive des bereits verratenen) und an dem Gewinnspiel teilnehmen wollen, schreiben Sie uns bitte bis spätestens 5. Februar 2023 eine E-Mail an [40.Geburtstag@ct.de](mailto:40.Geburtstag@ct.de). Im Betreff muss „Rätsel c't 04/2023 – Anzahl der Unterschiede“ stehen, also etwa „Rätsel c't 04/2023-6“, wenn Sie sechs Unterschiede entdeckt haben. An die E-Mail hängen Sie bitte noch eine Bilddatei (JPG), in der Sie die gefundenen Unterschiede gut sichtbar markiert haben. Alle rechtzeitig eingegangenen Einsendungen mit der richtigen Lösung nehmen an der Verlosung teil, der Rechtsweg ist ausgeschlossen, Mitarbeiter von Heise dürfen nicht am Gewinnspiel teilnehmen. Des Rätsels Lösung verraten wir in c't 6/2023, der Gewinner wird per E-Mail benachrichtigt.

Die beiden Bilder stellen wir auch in hoher Auflösung zum Download ([ct.de/y37b](http://ct.de/y37b)) bereit, so können Sie ganz genau hinsehen und wirklich alle relevanten Unterschiede ausmachen. Wer mag, kann noch eine Zusatzfrage beantworten: Von welcher NASA-Mission stammt das Bild, das wir für diese Aktion verfälscht haben?

## Der Preis

Zu gewinnen gibt es ein Exemplar des modularen Lautsprechersystems „Power HiFi“, zur Verfügung gestellt von Teufel. Die Power HiFi besteht aus drei aufeinander gestapelten Komponenten: Das Fundament bildet das über 35 Kilogramm schwere Bassmodul mit zwei 12-Zoll-(305 mm-)Basstreibern. Die zueinander angewinkelte Anordnung der beiden Lautsprecher spart nicht nur Platz, sondern soll laut Hersteller auch die Leistung der Basseinheit verbessern. Für warme, natürliche Mitten und gute Sprachverständlichkeit ist das Mitteltonmodul mit seinem 200-Millimeter-Treiber verantwortlich.

Über allem thront die Hochtöneinheit mit ihrem Horn. Im gleichen Gehäuse finden auch die drei Class-D-Verstärker mit einer Gesamtleistung von 380 Watt ihr Zuhause. Die Bedienelemente sind seitlich ins Gehäuse eingelassen und ermöglichen die Steuerung direkt am Gerät: Eingangswahl, Bluetooth-Pairing, 3-Band-Equalizer und Lautstärke. Eine Fernbedienung erlaubt die Steuerung aus der Distanz.

Alle drei Module sind aus Holz gefertigt und machen nicht nur im Wohnzimmer von Soundenthusiasten kräftig Druck, sondern heizen auch im Probenkeller oder auf der Bühne ordentlich ein. Power HiFi lässt sich per Bluetooth mit verschiedenen Geräten koppeln, weitere Zuspieler finden per Stereo-Cinch, optischem Digitalkabel oder XLR-Anschluss. Bei Bedarf lassen sich mehrere Power-HiFi-Systeme via XLR koppeln. [gs@ct.de\) ct](mailto:(gs@ct.de) ct)

Datenschutzrechtlich verantwortlich sowie Veranstalter des Gewinnspiels ist die Heise Medien GmbH & Co. KG. Außer der Übermittlung der E-Mail-Adresse zur Teilnahme am Gewinnspiel ist zunächst keine weitere Übermittlung personenbezogener Daten erforderlich. Im Gewinnfall werden wir zusätzlich nach Namen und Postanschrift zum Zwecke des kostenfreien Gewinnversands fragen. Rechtsgrundlage für die Datenerarbeitung ist Art. 6 Abs. 1 lit. b) DSGVO. Weitere Informationen zum Thema Betroffenenrechte sowie Kontaktmöglichkeiten unter [www.heise.de/privacy](http://www.heise.de/privacy).

**Bilder zum Download: [ct.de/y37b](http://ct.de/y37b)**



**Der Gewinner unseres ersten Preisrätsels bekommt eine Power HiFi von Teufel.**

**Teufel**





# Warum nicht gleich so?

## Effiziente Ryzen-7000-Prozessoren mit sechs, acht und zwölf Kernen

**AMD bietet seit Anfang Januar Zen-4-CPUs mit moderaten 65 Watt Thermal Design Power an, die sich leichter kühlen lassen als die kräftigeren Ryzen 7000X. Die Performanceunterschiede fielen im Test geringer aus als vermutet.**

Von Christian Hirsch

Die Ende September 2022 vorgestellten Ryzen-7000X-Prozessoren brachten die neue AM5-Plattform mit DDR5-RAM und PCI Express 5.0. Zudem liefern die

Desktop-CPUs deutlich mehr Performance als die Vorgänger, verheizen dabei aber auch wesentlich mehr Energie. Zum Jahresanfang hat AMD das Angebot an AM5-Prozessoren um preiswerte und sparsamere Varianten mit 65 Watt Thermal Design Power (TDP) erweitert. Dazu gehören der Ryzen 5 7600 mit sechs, der Ryzen 7 7700 mit acht und der Ryzen 9 7000 mit zwölf Kernen.

Die Ryzen 7000 ohne X kosten 260, 370 beziehungsweise 480 Euro und sind damit jeweils rund 20 Euro günstiger als die bereits erhältlichen X-Varianten mit 105 beziehungsweise 170 Watt TDP. Im Unterschied zu den leistungsstarken Ryzen liefert AMD bei den 65-Watt-Prozessoren passende Kühler mit. Beim Ryzen 7 7700 und Ryzen 9 7900 packt der CPU-

Hersteller den Wraith Prism mit RGB-LED-Beleuchtung und beim Ryzen 5 7600 den einfacheren Wraith Stealth bei.

Wegen des geringeren thermischen Budgets von maximal 88 Watt takten die neuen Ryzen 7000 langsamer als die Ryzen 7000X, bei denen erst bei 142 (Ryzen 7) beziehungsweise 230 Watt (Ryzen 9) Schluss ist. Der garantierter Nominaltakt liegt abhängig von der CPU bei 3,7 beziehungsweise 3,8 GHz um 700 bis 1000 MHz tiefer. Den maximalen Turbo-takt hat AMD jedoch lediglich um 100 beziehungsweise 200 MHz abgesenkt. Der Ryzen 9 7900 darf beispielsweise mit bis zu 5,4 GHz laufen.

### Schnelle Zen-4-Kerne

Die weiteren technischen Eigenschaften sind identisch mit denen der vier bisher vorgestellten Ryzen 7000X „Raphael“ [1]. Die CPUs bestehen aus mehreren Chiplets. In allen AM5-Prozessoren sitzt ein in 6-Nanometer-Technik gefertigtes I/O-Die, das unter anderem eine Radeon-GPU enthält. Mit lediglich 128 Shader-Kernen taugt die RDNA2-GPU jedoch lediglich für simple 3D-Aufgaben, denn sie erreicht gerade einmal 2150 Punkte im 3DMark Firestrike. Für Office-Anwendungen reicht das aber vollkommen aus. Die CPU-Kerne packt AMD jeweils zu acht in ein CPU Core Die (CCD) aus der 5-Nanometer-Fertigung.

Für die Tests haben wir das gleiche System wie für die bisherigen Ryzen 7000 verwendet: Die CPUs sitzen auf dem High-End-Board Gigabyte X690E Aorus Master mit X670E-Chipsatz. Ihnen stehen 32 GByte DDR5-5200-RAM zur Seite. AMD verspricht für die Zen-4-Architektur der Ryzen 7000 einen 13-prozentigen Zuwachs bei der Leistung pro Takt zu den Vorgängern. Hinzu kommen die höheren Taktfrequenzen. Bei Singlethreading-Anwendungen rechnet der Achtkerner Ryzen 7 7700 je nach Anwendung nach unseren Messungen zwischen 7 und 25 Prozent schneller als der Vorgänger Ryzen 75700X.

Bei Multithreading-Aufgaben wie dem Rendering mit Cinebench R23 oder dem Videokodieren mit Handbrake legen die 65-Watt-Varianten um über 40 Prozent und somit deutlich stärker zu. Dadurch kann sich der Ryzen 7 7700 vom gleich teuren Intel-Konkurrenten Core i7-12700 absetzen. Je nach Anwendung liegt der Vorsprung zwischen 3 und 16 Prozent, obwohl im Intel-Prozessor zusätzlich zu den acht Performance- noch vier Effizienzkerne rechnen.

Die eigentliche Konkurrenz finden die drei neuen Ryzen 7000 aber im eigenen Haus: Denn die drei Neuvorstellungen müssen sich den im Herbst präsentierten X-Varianten mit höherer TDP nur knapp geschlagen geben, verbraten dabei aber viel weniger Strom. Die Sechs- und Achtkerner Ryzen 5 7600 und Ryzen 7 7700 kommen bei der Performance im Schnitt bis auf fünf Prozent an die 105-Watt-Modelle Ryzen 5 7600X und Ryzen 7 7700X heran.

## Unter Last sparsam

Dabei arbeiten sie viel effizienter. Im Cinebench R23 schluckt das Gesamtsystem mit dem Ryzen 7 7700 beispielsweise 50 Watt weniger, was einem Rückgang von 36 Prozent entspricht. Noch größer ist der Unterschied beim Ryzen 9 7900 mit zwölf Kernen und 65 Watt TDP zur X-Variante mit 170 Watt TDP. Zwar fällt die Performanceeinbuße im Cinebench mit neun Prozent größer aus, dafür konsumiert das System aber auch 111 Watt weniger (-44 Prozent). Statt Wasserkühlung oder gigantischen Kühltürmen reicht nun ein handelsüblicher Tower-Luftkühler aus, um den Prozessor leise zu kühlen.

Die Effizienzwertung führt der Ryzen 9 7900 mit 187 Cinebench-Punkten pro Watt an, weil die vielen Kerne wegen des vergleichsweise niedrigen Power-Limits unter Volllast niedrig takten und mit geringer Spannung laufen. Die übrigen Ryzen 7000 liegen mit 99 bis 134 Cinebench-Punkten pro Watt dichter beisammen und können sich kaum von den Ryzen 5000 mit 65 Watt TDP absetzen. Zwar rechnen die aktuellen AMD-Prozessoren dank feinerem Fertigungsprozess effizienter, dafür verheizen die AM5-Boards bereits im Leerlauf signifikant mehr Energie [2].

Sensor	Current
Core Powers	5.553 W
Core 0 Power	5.481 W
Core 1 Power	5.693 W
Core 2 Power	5.750 W
Core 3 Power	5.396 W
Core 4 Power	5.689 W
Core 5 Power	5.720 W
Core 6 Power	5.624 W
Core 7 Power	5.672 W
Core 8 Power	5.560 W
Core 9 Power	5.342 W
Core 10 Power	5.179 W
Core 11 Power	5.529 W

**Unter Volllast benötigt jeder der zwölf CPU-Kerne des Ryzen 9 7900 gerade einmal fünfeinhalb Watt.**

In 3D-Spielen liegt die Bildrate mit den neuen 65-Watt-Typen ebenfalls nur wenige Prozent unter der leistungshungrigeren Ryzen-7000X-Varianten. Im Vergleich zu den Vorgängern liefern die überarbeiteten Zen-4-Rechenwerke klar mehr Wumms bei Spielen. Bei Shadow of the Tomb Raider klettert die durchschnittliche Zahl der Bilder pro Sekunde vom Ryzen 7 5700X zum Ryzen 7 7700 um 18 Prozent. Das 5-Prozent-Perzentil, das angibt, welche Bildrate zu 95 Prozent der Zeit mindestens erreicht wird und ein gutes Maß für die Ruckelfreiheit ist, steigt gar um 30 Prozent an.

Beim Preis-Leistungsverhältnis liegen die Ryzen 7000 mit und ohne X auf ähnlichem Niveau. Das liegt daran, dass

AMD die Ryzen 7000X im Weihnachtsgeschäft deutlich rabattiert hat und sie weiter vergünstigt anbietet. Die Core i-12000 haben zwar CPU-bezogen ein schlechteres Preis-Leistungsverhältnis. Allerdings muss man bei den Ryzen 7000 berücksichtigen, dass AM5-Mainboards mit Einstiegspreisen ab rund 200 Euro mehr kosten als vergleichbare LGA1700-Boards mit B660-Chipsatz für Intels 12. und 13. Core-i-Generation (ab 100 Euro). Zudem benötigen die Ryzen 7000 im Unterschied zu aktuellen Intel-CPU DDR5-RAM, der 50 Prozent teurer ist als DDR4-RAM gleicher Kapazität.

## Fazit

Die 65-Watt-Varianten zeigen endlich das volle Potenzial, das in den Ryzen 7000 steckt: Sie bieten hohe Rechenleistung bei überschaubarem Energiebedarf. So können Käufer nicht nur bei der CPU, sondern auch bei Netzteil und Kühler einige Euros sparen. Die bisherigen 105-Watt-CPU Ryzen 5 7600X mit sechs und Ryzen 7 7700X mit acht Kernen macht AMD durch den Ryzen 5 7600 und Ryzen 7 7700 quasi überflüssig, denn der Performanceunterschied ist vernachlässigbar.

In einer der kommenden c't-Ausgaben müssen sich die Ryzen-7000-Prozessoren im Test gegen die kürzlich vorgestellten 65-Watt-Typen der 13. Core-i-Generation von Intel beweisen. (chh@ct.de) **ct**

## Literatur

- [1] Carsten Spille, Fünf ist Trümpf, Ryzen 7000: Vier Desktop-Prozessoren für die Fassung AM5, c't 22/2022, S. 56
- [2] Christian Hirsch, Premiumaufschlag, AM5-Mainboards für Ryzen-7000-Prozessoren im Test, c't 24/2022, S. 90

## Sparsame Ryzen-7000-Prozessoren: Benchmarks und Leistungsaufnahme

Prozessor	Kerne / Threads	Takt / Turbo	Cinebench R23 1T [Punkte]	Cinebench R23 MT [Punkte]	Kcbench, Linux 5.19.5 [s]	Handbrake 1.5.1, Fast 1080p30 [fps]	Sysmark 25 [Punkte]	Shadow of the Tomb Raider <sup>1</sup> , 5%-Perzentil / Durchschnitt [fps]	Effizienz [Cinebench/W]	Preis/Leistung [Cinebench/€]	Leistungsaufnahme Leerlauf / Volllast [W]
Ryzen 9 7900	12 / 24	3,7 / 5,4 GHz	besser ▶ 1954	besser ▶ 26516	◀ besser 50	besser ▶ 104	besser ▶ 2065	besser ▶ 193/250	besser ▶ 187	besser ▶ 55	◀ besser 38/141
Ryzen 7 7700	8 / 16	3,8 / 5,3 GHz	1933	19202	74	87	2117	174/233	134	52	44/144
Ryzen 5 7600	6 / 12	3,8 / 5,1 GHz	1851	14519	84	73	1988	163/232	102	56	38/142
Ryzen 9 7900X	12 / 24	4,7 / 5,6 GHz	2042	29265	47	101	2119	204/237	116	59	41/297
Ryzen 7 7700X	8 / 16	4,5 / 5,4 GHz	2008	20212	64	86	2250	182/240	104	53	39/217
Ryzen 5 7600X	6 / 12	4,7 / 5,3 GHz	1959	15597	80	75	2149	162/224	99	56	40/193
Ryzen 7 5700X	8 / 16	3,4 / 4,6 GHz	1537	13609	97	61	1629	134/198	131	65	32/104
Ryzen 5 5600X	6 / 12	3,7 / 4,6 GHz	1536	10965	117	55	1578	126/194	110	59	31/102
Core i7-12700	8P+4E / 20	2,1 / 4,9 GHz	1882	16521	86	82	1843	141/195	103	46	28/206
Core i5-12600	6 / 12	3,3 / 4,8 GHz	1844	12500	112	67	1769	140/190	83	45	27/178

<sup>1</sup> 1080p, Höchste Qualität, DirectX12, SMAA, mit Radeon RX 6900 XT gemessen



## Leichte In-Ear-Kopfhörer

**Nothings neue In-Ears namens Ear (stick) unterdrücken zwar keine Umgebungsgeräusche, punkten aber mit langer Akkulaufzeit und hohem Tragekomfort – so sie denn passen.**

Der Name Nothing ist bei den Ear (stick) Programm: Die 4,4 Gramm schweren Kopfhörer sitzen federleicht im Ohr wie ein Hauch von Nichts. Nach einer gewissen Zeit vergisst man die Stöpsel fast, so bequem sind sie – zumindest dann, wenn sie zur Form des Ohres passen. Das ist bei In-Ears aus hartem Plastik Glückssache, eine Möglichkeit zur Anpassung durch Aufsätze aus Silikon gibt es nicht.

Dank der offenen Bauform dringen Außengeräusche durch, sodass man mitbekommt, was um einen herum geschieht. Der Gehörgang fühlt sich nicht so verstopft an. Die Konstruktion hat aber auch Nachteile: Weil der Ear (stick) Geräusche weder aktiv noch passiv unterdrückt, kommt der Sound in lauter Umgebung nicht so störungsfrei und klar an wie bei fest abschließenden In-Ears. Aktive Geräuschunterdrückung gibt es nicht, passive ebenfalls kaum.

Der teils transparente Kunststoff gibt den Blick auf das Innenleben frei, womit das Design der von den Nothing Ear (1) und dem Phone (1) bekannten Linie folgt. Mit einer Akkuladung könnten wir sechs bis sieben Stunden am Stück Musik hören, das ist angesichts des geringen Gewichts beachtlich. Die runde Ladehülle mit Drehmechanismus hält ungefähr vier weitere Ladungen vor. Sie sieht ebenfalls ungewöhnlich aus, verkratzt in der Tasche aber mit der Zeit. Sie ist relativ groß geraten

und stört in engen Hosentaschen. Geladen wird per USB-C-Kabel.

Das unbestechliche Messgerät und der subjektive Höreindruck sind sich einig: Die Ear (stick) bringen einen ausgewogenen Sound mit deutlichem Hang zu höheren Frequenzen. In den Tiefbassbereich dringen sie nicht vor.

Selbst voll aufgedreht bleiben sie zu leise, um laute Umgebungsgeräusche zu übertönen, was den Musikgenuss etwas trübte. Beim Telefonieren mit den Ear (stick) ist man klar und deutlich zu verstehen.

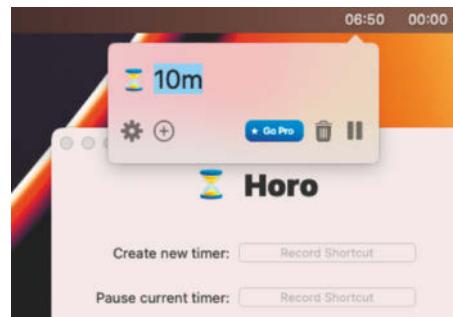
Die App für die Kopfhörer heißt Nothing X. Sie enthält einen Equalizer, Optionen für die Trageerkennung, einen Modus mit niedriger Latenz sowie Einstellungen für die Steuerung der Bedienelemente. Die Ear (stick) werden nicht per Touch bedient, sondern wollen mit zwei Fingern gedrückt werden und quittieren das mit einem hörbaren Klicken. Wer seine Kopfhörer verlegt hat, kann sie über die App piepsen lassen.

Mit den Ear (stick) stellt Hersteller Nothing seinen Ear (1) eine Alternative mit langer Akkulaufzeit und hohem Tragekomfort zur Seite; auf eine aktive Geräuschunterdrückung muss man dafür verzichten. Passen Ohr und Hörer zueinander, sind die In-Ears bequeme, unaufdringliche Begleiter für den ganzen Tag.

(sht@ct.de)

### Nothing Ear (stick)

In-Ear-Kopfhörer	
Hersteller, URL	Nothing, de.nothing.tech
Maße Kopfhörer (H × B × T) / Gewicht / Schutztart	30 × 19 × 18 mm / 4,4 g / IP54
Maße Case (H × B × T) / Gewicht	87 × 30 × 30 mm / 46 g
Systemanf.	Android ab 5.0, iOS ab 13.0
Preis	119 €



## Eieruhr für den Mac

**Wer arbeitet, soll auch Pausen machen. Doch in die Arbeit vertieft, braucht es einen Gehilfen, der an die Kaffeepause um 14 Uhr erinnert. Während die macOS-Uhr 10 Klicks für die Einrichtung eines Timers fordert, braucht Horo nur einen.**

Horo ist eine kleine Anwendung, die im Mac-App-Store kostenlos bereitsteht und sich in der Menüleiste einnistet: draufklicken, ⌘14 tippen, mit Enter bestätigen und schon läuft der Wecker für die Kaffeepause um 14 Uhr. Um zusätzlich einen 10-Minuten-Timer für die Pizza zu stellen, geben Sie 10m ein. Und mit dem Befehl stopwatch startet eine Stoppuhr. Dabei läuft die Zeit immer sichtbar oben in der Menüleiste mit.

Horo eignet sich auch, um nach der populären Pomodoro-Methode regelmäßig Pausen bei langwierigen Aufgaben einzulegen: 50 Minuten arbeiten, 10 Minuten Pause. Eigentlich nicht komplex und zwei einfache Timer (10m und 50m) reichen, trotzdem gibt es eine Menge aufgebläster Pomodoro-Apps im App-Store, die den Nutzer in starre Rhythmen zwängen oder Geld verlangen. Horo hingegen hält es wie die gute alte Eieruhr: wenige, sinnvolle Funktionen mit klarem Zweck.

Das reicht für die meisten Wünsche. Ganz Ambitionierte erwerben Horo Pro: Für einmalig 12 Euro können Sie dann den Alarmton ändern und einzelne Timer mit einer Markierung versehen.

(Manuel Ottlik/jam@ct.de)

### Horo

Timer für macOS	
Hersteller, URL	matthewpalmer.net/horo-free-timer-mac
Funktionen	Timer, Wecker, Stoppuhr
Systemanf.	macOS ab 10.13
Preis	kostenlos / Horo Pro: 12 €

## JSON visualisiert

**JSON verbindet Websites und Apps mit APIs und speichert Konfigurationsdaten. Für menschliche Augen sind große JSON-Strukturen aber nicht leicht zu erfassen. JSON Crack macht Entwicklern das Leben leichter, indem es die Daten visualisiert.**

JSON, die „JavaScript Object Notation“ ist schon lange mehr kein Phänomen des JavaScript-Universums allein. In der hierarchischen Struktur können allerlei Objekte und Listen ineinander verschachtelt werden. Ein Objekt kann also wiederum Unterobjekte enthalten oder eine Liste aus Objekten. Der Verschachtelung sind dabei technisch keine Grenzen gesetzt. Wenn Sie jedoch vor der Aufgabe stehen, die Verschachtelung in einem Dokument zu verstehen, hilft JSON Crack. Das Werkzeug verwandelt ein JSON-Dokument in eine Baumstruktur und steigert dadurch die Lesbarkeit. Am schnellsten gelingt das im Browser online unter [jsoncrack.com/editor](http://jsoncrack.com/editor).

Sie können den Baum von links nach rechts oder von oben nach unten aufspannen, einzelne Knoten auf- und zuklappen oder innerhalb des Baumes nach einem bestimmten Begriff suchen. Wenn sich noch andere für die Visualisierung interessieren, können Sie Ihren Kollegen direkt einen Link dazu schicken. Bis zu 15 Dokumente können Sie speichern und teilen, wenn Sie die kostenlose Variante des On-

line-Editors nutzen. Alternativ dürfen Sie den Graphen als Bild herunterladen und dann teilen. Um das Werkzeug auf der eigenen Website einzubinden, erzeugen Sie per [jsoncrack.com/embed](http://jsoncrack.com/embed) den passenden Code-Schnipsel. Für 5 US-Dollar im Monat gibt es einen Premium-Account. Damit darf man bis zu 200 JSON-Objekte speichern und per Link verschicken. Außerdem können Premium-Kunden JSON Crack per API bedienen und zum Beispiel in eigene Anwendungen integrieren.

Um mal schnell eine ohnehin öffentliche Datenstruktur zu untersuchen, ist der kostenlose Online-Editor ausreichend. Wenn Sie dagegen sensible Daten untersuchen wollen, die nicht auf fremden Websites landen sollen, betreiben Sie dieselbe Oberfläche einfach selbst lokal. Dafür stellt der Entwickler in seinem GitHub-Repository ein vorbereitetes Dockerfile bereit. Noch einfacher kommen Nutzer der IDE Visual Studio Code an JSON Crack. Sie installieren einfach die Erweiterung „JSON Crack“ und können das Werkzeug in einer geöffneten JSON-Datei mit dem Befehl `> Enable JSON Crack visualization` aufrufen.

(Manuel Ottlik/jam@ct.de).

## JSON Crack

### JSON-Visualisierung

Hersteller, URL	<a href="http://jsoncrack.com">JSON Crack, jsoncrack.com</a>
Erweiterung für VSC	JSON Crack
Preis	<b>kostenlos</b> (Open Source), Premium für 5 US-\$/Monat

## Bauen Sie Ihren Wunsch-PC

+ GRATIS Webinar im Wert von 99,- €

Neben den Bauvorschlägen für PCs unterstützt Sie dieses Sonderheft mit einer umfangreichen Kaufberatung zu gängigen PC-Komponenten.

Die Artikel helfen Ihnen nicht nur beim Bau eines neuen Rechners, sondern auch beim Aufrüsten bestehender Systeme. So beschaffen Sie Ihrem Rechner einen zweiten Frühling, tun der Umwelt etwas Gutes und sparen obendrein noch Geld!

- Selbstbau-Wunsch-PC
- Allround-PC: Sparsam, leise, trotzdem schnell
- Komponenten im Test
- Kaufberatung SSDs und Festplatten
- Ratgeber Hardware-Kauf
- inkl. GRATIS-Webinar:  
Sichere Konfiguration von Büro-PCs – Hardware und BIOS-Setup

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

 [shop.heise.de/ct-hardwareguide22](http://shop.heise.de/ct-hardwareguide22)

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



# Flottes Brett

## Schneller Flachbettscanner für Dokumente

**Der Flachbettscanner Avision FB25 produziert flotte 300-dpi-Scans – im Test brauchte er dafür weniger als vier Sekunden. Die Softwarebeigaben helfen beim Digitalisieren von Dokumenten und Zeitschriften.**

Von Rudolf Opitz

**B**raucht man nur hin und wieder eine digitale Kopie, reicht der Scanner eines Multifunktionsgerätes oder man zückt einfach das Smartphone. Wer häufig viele verschiedene Vorlagen wie Rechnungen, Belege und Akten scannen muss, ist mit einem Einzugscanner besser bedient. Weil diese aber nur Einzelblätter verarbeiten, eignen sie sich nicht für Gebundenes wie Zeitschriften und Bücher. Der beste Kompromiss ist ein schneller A4-Flachbettscanner wie der Avision FB25, der einen Scan in der für Dokumente optimalen Auflösung von 300 dpi in nur vier Sekunden erledigt. Das bewies der Scanner in unserem Labor.

Das sehr schlichte Gerät hat weder Tasten noch Schalter. Auf der Rückseite gibt es lediglich eine USB-Buchse für die Verbindung zum PC und eine Niedervolt-Buchse für den Rundstecker des mitgelie-

ferten 12-Volt-Steckernetzteils. Alles Weitere übernimmt die Software. Die Scharniere der Scannerklappe liegen an der oberen Schmalseite und haben kein Spiel, lassen sich zum Scannen von dicken Büchern aber leicht aus der Halterung ziehen.

Außer den Twain- und WIA-Treibern – sogar ein ISIS-Treiber ist verfügbar – liefert Avision die Programme Button Manager und AV Scan X sowie den Dokumentenmanager Nuance PaperPort SE 14 mit – allerdings nur für Windows. Button Manager eignet sich eher für Einzugscanner mit Profilauswahl, zum Arbeiten mit dem FB25 empfiehlt sich AV Scan X, das ähnlich dem beliebten ScanSnap von Fujitsu erst multimodal scannt, also gleichzeitig in Farbe, Graustufen und Schwarz-Weiß, und danach Optionen zum Weiterverarbeiten und Speichern der Scans anbietet. Über das Twain-Modul scannt der FB25 auch direkt in Anwendungen wie Acrobat, PaperPort oder in Programme für Bildbearbeitung.

Bei 300-dpi-Testscans landete das Ergebnis in knapp vier Sekunden auf dem Bildschirm. Textseiten waren kontrastreich und gut lesbar, aber von der Farbwiedergabe waren wir nicht begeistert: Magazinbilder zeigten überhöhte Kontraste, Grafiken zu helle Grauflächen und zu dunkle Farben. Durch Einstellungen im Twain-Treiber oder im Scanprogramm kann man die Scanergebnisse aber verbessern.

Gut gefiel die in den Scanprogrammen integrierte Texterkennung, die nur bei sehr großen Schriften patzte und bei kleinen Tabellenzeichen einige Fehler machte. Bei Zeitungsscans in geringer Auflösung (150 und 200 dpi) störten in Bildern Raster und Moirés. Der Hintergrundfilter (Einstellung: weich, Filter: Moiré) verschlimmerte das Ergebnis durch gelöschte Farbflächen. Wer nicht in arger Speichernot ist, scannt besser gleich mit 300 dpi, was die Moirébildung stark vermindert. Unerwünschte Hintergrundfarben filterte die Automatik von AV Scan X vorbildlich. Auch Buchscans gelangen, der Filter „Schatten entfernen“ leistete an der Bindungskante gute Arbeit.

Für Fotos taugt der Avision-Scanner weniger. Bei 600 dpi scannt er zwar detaillreich, dunkle Bildbereiche saufen aber im Schwarz ab – typisch für Dokumentenscanner. Als CIS-Scanner (Contact Image Sensor) hat der FB25 praktisch keine Tiefenschärfe: Schon bei wenigen Millimetern, etwa bei erhaben geprägten Buchstaben, werden die Scans unscharf.

### Fazit

Wer für unterschiedlichste Dokumente einen zuverlässigen und schnellen Scanner mit guter Softwareausstattung sucht, liegt mit dem Avision FB25 richtig. Zu Preisen ab 150 Euro ist er zwar nicht billig, Einzugsscanner kosten aber mehr als 200 Euro und taugen nicht für Bücher und gebundene Zeitschriften. Avision bietet unter dem Namen FB15 eine A5-Version des Scanners an, der sich besonders zum schnellen Digitalisieren etwa von Ausweisen eignet.

(rop@ct.de) **ct**

### Avision FB25

Schneller USB-Flachbettscanner für Dokumente	
Hersteller, URL	Avision, avision.de
Scanzeile, Beleuchtung	CIS, LED
Auflösung optisch	1200 dpi
Schnittstelle	USB 2.0
Abmessungen (B × T × H) / Gewicht	28 cm × 40 cm × 4,4 cm / 1,8 kg
Treiber	Windows ab 7: Twain, WIA, ISIS
Software	Button Manager, AV Scan X, PaperPort 14 SE
Lieferumfang	USB-Kabel, Steckernetzteil, 2 DVDs, Kurzanleitung
Scanzeiten	Vorschau: 3 s, 300 dpi: 4 s, 600 dpi: 17 s
Geräuschmessung	Scannen 300 dpi: 3,1 sone
Leistungsaufnahme	Aus: < 0,1 W, Sleep: 1,2 W, Bereit: 3,4 W, Scannen (300 dpi): 5,6 W
Garantie	2 Jahre
Preis	150 €

# Moderne Retrokamera

## Fujifilm X-T5 mit 40 Megapixeln

**Die T-Modelle von Fujifilms X-Familie umwerben Fotografien mit klassischem Bedienkonzept und Retrolook. Die X-T5 setzt auf hohe Auflösung statt Geschwindigkeit. Der Test zeigt, ob sie auch bei schlechtem Licht mit 26-Megapixel-Kameras mithalten kann.**

Von Peter Nonhoff-Arps

Die Systemkamera Fujifilm X-T5 vereint ein kompaktes Gehäuse mit hoher Auflösung: Der Sensor mit 40 Megapixeln ist einzigartig im APS-C-Segment. Der Bildstabilisator (IBIS) gleicht nicht nur Verwacklungen aus, er ermöglicht auch das sogenannte Pixel Shift, mit dem sich die Auflösung vervierfachen lässt. Im Test erzielten wir real 80 Megapixel. Für jedes Sensorpixel erhält man mit dieser Technik die volle RGB-Information. Die Interpolation der Farben entfällt.



Bild: Fujifilm

Die Fujifilm X-T5 bedient man fast wie analoge Kameras. Jeder Belichtungsparameter hat ein eigenes Einstellrad.

Feine Übergänge in Farbverläufen etwa an einem Blütenblatt erscheinen dadurch genauer und detailreicher.

### Handhabung

Gegenüber dem Vorgänger X-T4 ist das Gehäuse geschrumpft und um 50 Gramm leichter. Fotografen können einen Handgriff hinzukaufen, wenn ihnen der Griffwulst zu klein erscheint. Die X-T5 setzt auf analoges Feeling und manuelle Einstellungen: Jeder Belichtungsparameter hat ein eigenes Bedienrad. Auf diesen können Fotografen ablesen, was gerade eingestellt ist. Ein Schulterdisplay ist somit überflüssig. Das rückseitige Display ist lediglich neigbar, aber nicht neben die Kamera schwenkbar.

Das Autofokussystem der X-T5 erkennt und verfolgt Motive mit Deep-Learning-Algorithmen für Gesichter und Augen, aber auch für Tiere, Autos, Motorräder, Flugzeuge und Züge.

Trotz der hohen Sensorsauflösung schafft die X-T5 kein 8K-Video, im Gegensatz zur neuen X-H2 des gleichen Herstellers, aber immerhin sind 6K mit 30 Bildern pro Sekunde drin. Ohne Schacht für CF-express-Karten kann sie 8K-Videodaten nicht schnell genug speichern.

### Messwerte und Bildkritik

Die Messungen bescheinigen der Fujifilm X-T5 eine gute Bildqualität. Für den Test standen uns das lichtstarke Standardzoom XF 16-55mm 1:2.8 R LM WR und die Porträtbrennweite XF 56mm 1:1.2 R WR zur Verfügung. Bei niedrigen ISO-Werten bis ISO 400 erzielten wir mittig die volle Auflösung von 2576 Linienpaaren pro Bildhöhe (Lp/Bh). Zwischen ISO 800 und ISO 6400 rutscht die Auflösung etwas ab auf etwa 90 Prozent des Maximalwertes, um bei ISO 12.800 um weitere zehn Prozent auf 2100 Lp/Bh abzufallen.

Das visuelle Rauschen (VN) erhöhte sich von 0,9 bei ISO 125 bis ISO 6400 kontinuierlich bis auf VN 2,0. Der Wert kenn-

zeichnet das wahrnehmbare Rauschen. Werte bis 0,8 stehen für weitgehende Rauschfreiheit, Werte bis 2 für einen geringen, Werte bis 3 für einen mäßigen und Werte darüber für einen deutlich störenden Rauscheindruck. Bei ISO 12.800 war das Rauschen mit VN 3,2 deutlich sichtbarer als von vergleichbaren 26-MP-Kameras. Der Dynamikumfang pendelte um zehn Blendenstufen, das ist gute Hausmannskost.

Die X-T5 löst feine Linienmuster insgesamt gut auf. Bei hohen ISO-Werten rauschen die Raw-Bilder zwar stärker als die JPEGs, hingegen wirken flächige Strukturen weniger glattgerechnet.

### Fazit

Die X-T5 bietet hohe Auflösung und moderne Technik in einem kompakten Gehäuse. Der APS-C-Sensor nimmt bei niedrigen ISO-Stufen mehr Details auf als die Vorgänger. Auch mit einer Vollformatspiegellosen wie der Nikon Z 6 II, die in der gleichen Preisliga spielt, kann er mithalten. Bei höheren ISO-Werten werden feine Strukturen wie Holzmaserung glatt gerechnet. Klare Kanten löst die Kamera hingegen gut auf. (akr@ct.de) ct

Einen ausführlichen Test dieser Kamera lesen Sie in c't Fotografie 1/2023.

## Fujifilm X-T5

APS-C-Systemkamera	
Hersteller, URL	Fujifilm, fujifilm.com
Sensorformat	APS-C (23,5 mm × 15,6 mm)
Sensorsauflösung / Megapixel	7728 × 5152 / 40 Megapixel
Sensortyp / Cropfaktor	CMOS (X-Trans, BSI) / 1,5
Lichtempfindlichkeit	ISO 125 bis ISO 12.800
Autofokustyp / Messfelder	Hybrid-AF / 425
Bildstabilisierung	5-Achsen, IBIS und objektivseitig
kürzeste / längste Verschlusszeit	1/8000 s (1/180.000 s elektr.) / 30 s (Bulb)
Serienbildrate / Raw in Folge	15 B/s (20 B/s elektr.) / 400
Videoformat / max. Auflösung	MOV, MP4 / 7680 × 4320 (30 fps)
Videokomprimierung	ProRes 422, H.265 / H.264
Sucher / Vergrößerung	OLED / 0,8x (KB-äquiv.)
Sucherauflösung	1280 × 960 Pixel, 4:3
Displaytyp / Auflösung	7,5 cm LCD / 960 × 640 Pixel, 3:2
Display: bewegl. / touch	✓ / ✓
SpeicherTyp	2 × SD (UHS-II)
Akku / Aufnahmen	Lilon 2200 mAh / 770 (lt. Herst.)
Gehäusematerial / wasserfest	Magnesiumlegierung / ✓
Bajonet	Fujifilm X-Mount
Abmessungen / Gewicht	130 mm × 91 mm × 64 mm / 557 g
Anschlüsse	USB-C 3.2, Micro-USB, HDMI Typ A, Mikro-, Kopfh., Fernbed.
Wireless	WLAN, Bluetooth, NFC
Preis (UVP / Straße)	2000 € / 2000 €

## Der wertvolle Boost für Ihr Netzwerk!



**c't ADMIN**  
Verstehen · Vernetzen · Administrieren  
**PLUS**  
FritzOS 7.50 mit Win 10 & Win 11

**ONLINEKURS**  
Mit komplettem Active-Directory-  
ONLINEKURS

Active Directory beherrschen  
Nutzenkonten, Gruppen und Berechtigungen  
Windows-PCs mit Gruppenrichtlinien  
Domain Controller ausländischer Betreiber

FritzOS 7.50 ist da  
Was das große Gratis-Update bringt.  
Die letzte Fritzbox für Ihren Anschluss  
VPN optimal einsetzen

Schwachstellen im Netz finden  
SMB: Wie aus der Abhängigkeitshölle  
NPM-Unerwünscht: Wer schlimm es wirklich ist  
SIEM: Angriffe im Netzwerk erkennen

47 Lektionen: Active Directory mit Windows Server 2019 anschaulich erklärt  
• Profi: Sie sind Gelehrte in Wissenschaft  
• Praktisch: Lassen Experten über ihre Erfahrungen  
• Methodisch: Schritt für Schritt  
• Anwendungsorientiert: Praktische Beispiele

+ GRATIS Online-Kurs im Wert von 99,- €

Wie baut man in der Firma oder zu Hause leistungsfähige Netzwerke, welche Elemente müssen modernisiert werden, wie hält man sie in Gang? Diese Fragen beantwortet Ihnen das Sonderheft c't Admin 2022.

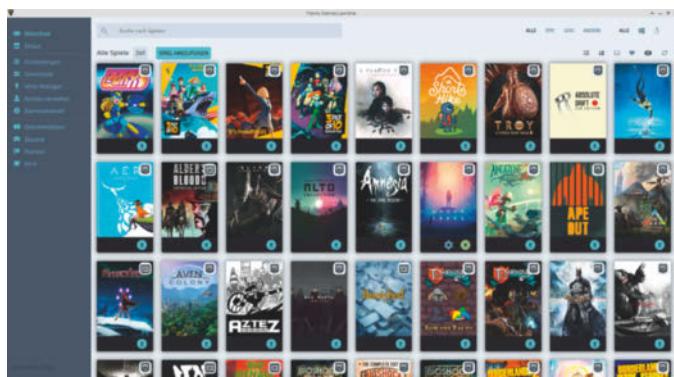
- Was das große Gratis-Update FritzOS 7.50 bringt
- Vernetzen mit Funk und Kabel
- Glasfaseranschluss richtig auswählen
- Schwachstellen im Netz finden
- Active Directory beherrschen
- inkl. GRATIS-Onlinekurs Active Directory mit 47 Lektionen

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

 [shop.heise.de/ct-admin22](http://shop.heise.de/ct-admin22)

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

 **heise Shop**



## Alternativer Spiele-Launcher

**Die schlanke Launcher-Alternative installiert und startet plattformübergreifend Spiele von Epic Games und GOG.com. Updates und Spiele-Downloads arbeitet Heroic jetzt automatisch in einer Warteschlange ab.**

Das Open-Source-Tool Heroic Games Launcher vereint die Spielebibliotheken von Epic Games und GOG.com unter einer Oberfläche. Nach der Anmeldung im jeweiligen Store kann man Spiele kaufen und sie anschließend in der Bibliothek herunterladen und installieren. Fehlt unter macOS, Linux oder auf dem Steam Deck die native Version eines Spiels, startet Heroic die Windows-Versionen mit Hilfe von Kompatibilitätsschichten wie Wine und Proton. Unter Linux füllt Heroic eine Lücke, da keiner der beiden Hersteller eigene Launcher dafür anbietet; unter macOS fehlt der Epic-Launcher. Weniger Tracker und ein schlankerer Unterbau machen das Tool auch unter Windows interessant.

Die Heroic-Version 2.5 „Yamato“ bringt erstmals einen Downloadmanager mit, der das Herunterladen vereinfacht. Beim Download oder Update mehrerer Titel muss man nicht warten, sondern kann alle in eine Warteschlange einreihen, die Heroic zuverlässig abarbeitet. Kleiner Schönheitsfehler: Die angezeigten Spiele-Cover waren meist die falschen.

Der Wine-Manager verwaltet installierte Wine/Proton-GE-Versionen und lädt neue herunter. Neben globalen Einstellungen für Wine & Co. nimmt Heroic spieldaten spezifische Einstellungen entgegen und nutzt bei Bedarf zusätzliche Tools wie DXVK, VKD3D, FSR oder den Systemmonitor MangoHud.

Neben Spielen von Epic und GOG lassen sich beliebige Anwendungen oder anderweitig installierte Spiele zur auch in

Deutsch verfügbaren Heroic-Oberfläche hinzufügen. Unter Linux und macOS gilt das auch für Skripte, AppImages oder Windows-Programme und -Spiele, die mit Wine, Proton oder Crossover laufen. Im Test ließen sich alle Spiele über Heroic starten. Nicht unterstützte Spiele, die über ein externes Hersteller-Tool wie Origin heruntergeladen werden müssen, kennzeichnet Heroic mit einem entsprechenden Icon. Bei Spielen wie Fortnite weist unter Linux ein großer roter Balken auf der Detailseite darauf hin, dass es aufgrund der verwendeten Anticheat-Software vermutlich nicht funktioniert.

Die in Heroic integrierten Informationen der Website HowLongToBeat verraten, wie lange es in etwa dauert, ein Spiel durchzuspielen. Eine Handvoll vorinstallierter CSS-Themes verändert die Optik der Heroic-Oberfläche; zwei neue sind hinzugekommen. Heroic lädt auf Wunsch auch eigene Themes und solche aus der Community.

Heroic Games Launcher funktioniert auch auf dem Steam Deck und erweitert dessen Spielefundus um die Epic- und GOG-Bibliothek. Installierte Spiele kann Heroic automatisch in den Steam-Client übertragen, sodass sie im Game Mode des Steam Deck erreichbar sind. Heroic kennzeichnet fehlende Spiele, etwa solche, die auf einer nicht eingelegten SD-Karte des Steam Decks installiert wurden.

Spielekauf, Downloads und Spielestarts klappten im Test reibungslos. Praktisch ist, dass Heroic nicht unterstützte Spiele jetzt kennzeichnet und so vergebliche Downloads erspart. (lmd@ct.de)

## Heroic Games Launcher 2.5.2

Game-Launcher	
Hersteller, URL	Flávio F. Lima, <a href="http://heroicgameslauncher.com">heroicgameslauncher.com</a>
Systemanf.	Linux (mind. Ubuntu 20.04, Fedora 33, Arch Linux, SteamOS), macOS ab 10.15 Windows 10/11
Preis	kostenlos (GPLv3)



## Synthesizer-Emulation

**Cherry Audio emuliert Yamahas legendäre Synthesizer GX-1 und CS-80, mit denen schon Vangelis den Soundtrack zu Blade Runner einspielte.**

Die epischen Klänge aus dem Science-Fiction-Film „Blade Runner“ von 1982 sind unvergessen. Als Geheimwaffe spielte der Komponist Vangelis den Yamaha CS-80, einen polyphonen Synthesizer mit 16 Stimmen. Das Original von 1976 kostete damals 7000 US-Dollar und war eine abgespeckte Version des GX-1, einer wuchtigen „Heimorgel“ für 50.000 Dollar. Diese kombinierte zwei CS-80 und erweiterte die Klangerzeugung um besondere Bandpassfilter. Der Spieler glitt mit den Händen über drei Klaviaturen und spielte mit den Füßen zusätzliche Basspedale.

Cherry Audio emuliert den GX-1 mit einer Software, die sich auch als Plug-in in Musikprogramme und Digital Audio Workstations einklinken lässt. Der Preis beträgt kaum mehr als ein Promille des Originals. Die orgelähnliche Bedienoberfläche mit Schiebestellern und Wipptastern wirkt zwar etwas altmodisch, ist aber übersichtlich zu bedienen. Spielen lässt sie sich über jede herkömmliche MIDI-Tastatur und verarbeitet sogar polyphonen Aftertouch, um jeden Ton eines Akkords einzeln zu beeinflussen.

Die Software erzeugt ihre Klänge in vier sogenannten Ranks: Pro Rank gibt es einen Oszillator (Sinus, Dreieck oder Puls-welle), gefolgt von einem Bandpass- sowie einem Hoch- und Tiefpass-Filter. Diese

Filter sind für den typischen Klang des GX-1 verantwortlich und lassen sich über separate Hüllkurven steuern. Für jedes Rank-Pärchen gibt es ferner einen Ringmodulator, der sich fein zwischen etwas Schmutz und den typisch unharmonischen Klängen dosieren lässt. Die übrigen Effekte setzen sich aus Chorus, Flanger, Delay und Hall zusammen.

Für den Sound eines CS-80 schaltet man die Klangerzeugung in den Singlemodus, sodass bei jedem Ton nur zwei Ranks erklingen. Im Dualmodus kommen die Ranks 3 und 4 hinzu, sodass sich der Sound noch komplexer gestalten lässt. Im Splitmodus spielt man mit jeweils zwei Ranks im oberen Teil des Keyboards andere Klänge als auf dem unteren Teil.

Der GX-80 gefällt durch den typisch fetten, oft spektakulären CS-Sound mit lebendigen Stereoflächen. Die Anforderungen an die Rechenleistung fallen moderat aus und liegen etwa 50 Prozent unter denen von Arturias Simulation des CS-80 – auch bei Nutzung aller vier Ranks. Cherry Audios Reinkarnation klingt zudem authentischer und, nicht zuletzt aufgrund der doppelten Rankzahl, deutlich wuchtiger als die der Mitbewerber. Der GX-80 setzt somit ein Glanzlicht im momentan eher langweiligen Segment der virtuellen Instrumente. (Kai Schwirzke/hag@ct.de)

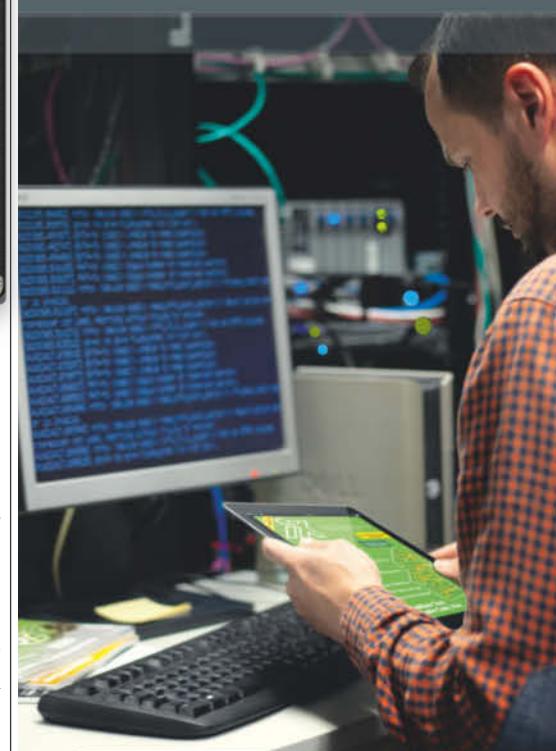
## Cherry Audio GX-80

### Software-Synthesizer

Hersteller, URL	Cherry Audio, <a href="http://cherryaudio.com">cherryaudio.com</a>
Formate	Standalone, VST2/3, AU, AAX
Systemanf.	Windows ab 7, macOS ab 10.13
Preis	59 US-\$

Es gibt **10** Arten von Menschen.

iX-Leser und die anderen.



**Jetzt Mini-Abo testen:**

3 digitale Ausgaben +  
Bluetooth-Tastatur  
nur **19,35 €**

[www.iX.de/digital-testen](http://www.iX.de/digital-testen)

**iX**  
MAGAZIN FÜR PROFESSIONELLE  
INFORMATIONSTECHNIK

[www.iX.de/digital-testen](http://www.iX.de/digital-testen)

[leserservice@heise.de](mailto:leserservice@heise.de)

49 (0)541 800 09 120

# 17 für 11

## Desktop-Virtualisierer VMware Workstation 17 im Test

**Versionssprünge bei VMwares Einzelplatz-Virtualisierern bringen meist nur kleine Veränderungen. Diesmal gibts allerdings eine Neuerung, die den Umgang mit Windows 11 deutlich erleichtert.**

Von Jan Schüßler

Unter den kommerziellen Desktop-Virtualisierern für Windows ist VMware Workstation seit langer Zeit äußerst beliebt. Die Version 17 enthält neben Detailverbesserungen vor allem einen praktischen Satz an Voreinstellungen für Windows-11-Gäste.

Die Software ist englischsprachig; es gibt sie in den Varianten Player und Pro. Dem Player fehlen einige für Power-User essenzielle Funktionen, darunter Snapshots, die verschiedene VM-Betriebs- und Konfigurationszustände so spei-

chern, dass man sie mit ein paar Klicks wiederherstellen kann, sowie der Editor für virtuelle Netzwerke, mit dem sich VMs und Host individuell vernetzen oder unterschiedlichen externen Verbindungen zuweisen lassen. Das schlägt sich im Preis nieder: Für die geschäftliche Nutzung kostet der Player etwas weniger als Pro; für den Privatgebrauch ist er sogar gratis.

Eine hilfreiche Neuerung steckt in dem Einrichtungsassistenten für VMs, der nun auch Windows 11 mit seinen harten Systemanforderungen kennt. Die Vorgängerversion 16 war zwar ebenfalls dafür freigegeben, bot aber keinen Satz an sinnvollen Voreinstellungen dafür an. Man musste die Laufwerksgröße und den zugewiesenen Arbeitsspeicher für jede neue VM von Hand anpassen und die VM komplett verschlüsseln, um danach noch ein virtuelles Trusted Platform Module (vTPM) hinzufügen zu können. Dass die VM für ein vTPM verschlüsselt sein muss, hat einen Grund: Sonst ließe sich das vTPM Host-seitig auslesen, ohne dafür irgendeine Schutzmaßnahme umgehen zu müssen.

### Mehr Komfort

Der 17er-Assistent bietet fix und fertige Einstellungen mit passenden Parametern: zwei CPU-Kerne, 64-GByte-Laufwerk, virtuelles TPM. Auch dafür muss die VM verschlüsselt werden, damit das vTPM geschützt ist. Es gibt in der neuen Version allerdings neben der bisherigen Vollverschlüsselung (alle Einstellungsdateien und virtuelle Festplatte) auch eine Art Light-Verschlüsselung. Bei der werden nur jene Dateien verschlüsselt, die zum sicheren Betrieb des vTPM erforderlich sind, nicht aber die virtuelle Festplatte. Das macht die VM schneller, das Tempo entspricht dann der von gänzlich unverschlüsselten VMs. Komfortabel ist das im Alltag vor allem beim Entfernen alter Snapshots und bei der Host-seitigen Laufwerksberei-

nigung. Auf unserem Testsystem (Ryzen 7 5700G, 32 GByte RAM, NVMe-SSD Samsung 970 Pro) dauern solche Vorgänge mit verschlüsselten Datenträgern rund zweimal länger.

Apropos Komfort: Um das Kennwort verschlüsselter VMs beim Öffnen nicht jedes Mal eintippen zu müssen, fragt der Assistent direkt, ob er das Kennwort im „Credential Manager“ ablegen soll. Das ist verwirrend, denn eine Funktion mit diesem Namen findet sich nirgends. Gemeint ist die Windows-Anmeldeinformationsverwaltung, die auch in Windows 11 noch Teil der klassischen Systemsteuerung ist.

### Fazit

Für ein Upgrade auf Version 17 Geld auszugeben, ist eine gute Idee, wenn Sie viel mit Windows-11-Gästen hantieren – und bislang vom Fehlen eines passenden Hardwareprofils oder von der lahmen Performance bei verschlüsselten Laufwerken generiert waren. Wenn Sie die Player-Variante gratis nutzen, kostet ein Update eh nichts.

Für unseren Geschmack punktet VMware Workstation in beiden Editionen mit einem guten Bedienkomfort. Kostenlosen Privatgebrauch erlaubt aber auch Oracle VirtualBox – und anders als das VMware-Gratisprodukt unterstützt es auch Snapshots. Wer Windows als Pro- oder höhere Edition nutzt, hat mit Hyper-V gleich einen Virtualisierer, der ohne Aufpreis kommerziell genutzt werden darf, muss aber mit der sperrigeren Bedienung klarkommen. Dazu noch ein Lesetipp: In c't 14/2022 lesen Sie einen detaillierten Vergleich der drei Programme [1].

(jss@ct.de) **ct**

### Literatur

- [1] Jan Schüßler, Spielwiesen, Drei Desktop-Virtualisierer für Windows-11-VMs im Test, c't 14/2022, S. 114

**VMware-Download:** [ct.de/yc6d](http://ct.de/yc6d)

### VMware Workstation 17

Desktop-Virtualisierer	
Hersteller, URL	VMware, <a href="http://vmware.com/de">vmware.com/de</a>
Systemanf.	Windows ab 8.1, Windows Server ab 2012, Linux, nur 64-Bit-Hosts möglich
Preise	Pro: 200 € (Vollversion) / 100 € (Upgrade) Player: 150 € (Vollversion) / 80 € (Upgrade) Player im Privatgebrauch <b>kostenlos</b>

In VMware Workstation 17 wird die Einrichtung von Windows-11-Gästen deutlich bequemer – dank vorgefertigtem Hardwareprofil.

# Natürliches Licht

## Raw-Entwickler: Capture One Pro 23

**Capture One Pro holt natürliche Farben und feine Details aus Raw-Dateien heraus; das brauchte bislang aber seine Zeit. Der Hersteller hat nun am Workflow gebastelt. Wir haben getestet, ob Version 23 schneller zum Ziel führt.**

Von André Kramer

Neutzen einer Vorversion fallen in Capture One Pro 23 sofort die großen beschrifteten Symbole für die Karteireiter auf. Vorher musste man auswendig wissen, was die winzigen Symbole bezeichnen; jetzt steht da „Bibliothek“, „Tether“, „Form“, „Stil“, „Anpassungen“ und so weiter. Die größeren Symbole brauchen aber mehr Platz, vier der zehn Reiter verstecken sich nun hinter einem Ausklappmenü. Die Palette für kostenpflichtige Stile oder Tethering kann man mit wenigen Klicks durch die Paletten für „Farbe“ oder „Exportieren“ ersetzen. Davon ab-

gesehen hat sich äußerlich wenig geändert.

### Schnelle Auswahl

Eine umfangreiche Bildverwaltung wie Lightroom CC bietet Capture One nicht. Die neue Version enthält aber einen durchdachten Workflow, um Fotos beim Import auszuwählen und zu bewerten. Auf Wunsch gruppieren dieser Dialog Fotos nach Ähnlichkeit. Die horizontalen Pfeiltasten wechseln durch Gruppen, die vertikalen durch Fotos innerhalb der Gruppen. Die Tasten S und A wählen für den Import an oder ab. Bewertungen vergibt man hier über Zifferntasten; Farbetiketten weist der Importdialog nicht zu. Die Fotos zeigt Capture One blitzschnell an. Den Bewertungsdialog ruft die Schaltfläche „Auswerten“ in der Kopfzeile auch nach dem Import auf.

Über „Bild/Aufnahmezeit ändern“ kann man nun das Exif-Datum und die Zeit ändern, sie beispielsweise verschieben, um die Zeitzone anzupassen – eine wichtige und überfällige Standardfunktion. Metadaten speichert das Programm bei Raw-Fotos in einer XMP-Begleitdatei, nicht im Original. Virtuelle Varianten

einer Raw-Datei kann man nun in verschiedenen Alben organisieren.

### Intelligente Anpassungen

Fotos entwickelt man im Anpassen-Feld mit seinem guten Dutzend Dialogen für Weißabgleich, Belichtung, Tonwerte, Gradientskurven, Farbbebalance oder Schwarz-Weiß. Neu ist das Feld „Intelligente Anpassungen“. Die Einstellungen jeweils für Weißabgleich und Belichtung eines Bilds kann man hier als Referenz festlegen. Ein Vorschaubild zeigt, welches Foto das Programm referenziert. Beide Eigenschaften weist das Programm auf Knopfdruck einem oder mehreren Bildern zu. Intelligent daran ist, dass Capture One die Einstellungen für Farbe und Helligkeit an jedes einzelne Foto anpasst, damit am Ende der Look übereinstimmt und nicht der Reglerwert. Das geht einfach von der Hand und erzielt gute Ergebnisse.

Über das Ebenenbedienfeld im Anpassen-Reiter lagert Capture One Sätze von Bildeinstellungen übereinander. Mit Verlaufs- und Pinselfiltern wendet man sie auf Bildregionen an. Zwar gibt es hier einen „Zauberpinsel“, er markiert Motive aber längst nicht so zuverlässig wie die KIAuswahl in Lightroom. Auch die erwähnten Bildstile, von denen Capture One eine Handvoll für Schwarz-Weiß und Farbverfremdung mitliefert, kann man nun auf Ebenen anwenden.

Der Reiter „Farbe“ ist redundant, denn er wiederholt, was in „Anpassen“ schon vorhanden ist. Sperrig, unbeschriftet und unnötig kompliziert kommt der Farbbebalance-Editor daher. Hier zeigt sich, dass die Oberfläche nicht konsequent modernisiert wurde.

### Fazit

Capture One entwickelt Fotos mit Sinn für feine Nuancen. Stück für Stück erleichtert der gleichnamige Hersteller auch die Bedienung. Noch wirkt das aber etwas halbherzig. Die neuen Funktionen für Bildauswahl und intelligente Anpassung zeigen aber, dass er Fotografen im Blick hat, die viele Bilder in kurzer Zeit bearbeiten müssen, ohne Kompromisse bei der Qualität machen zu wollen. (akr@ct.de) ct

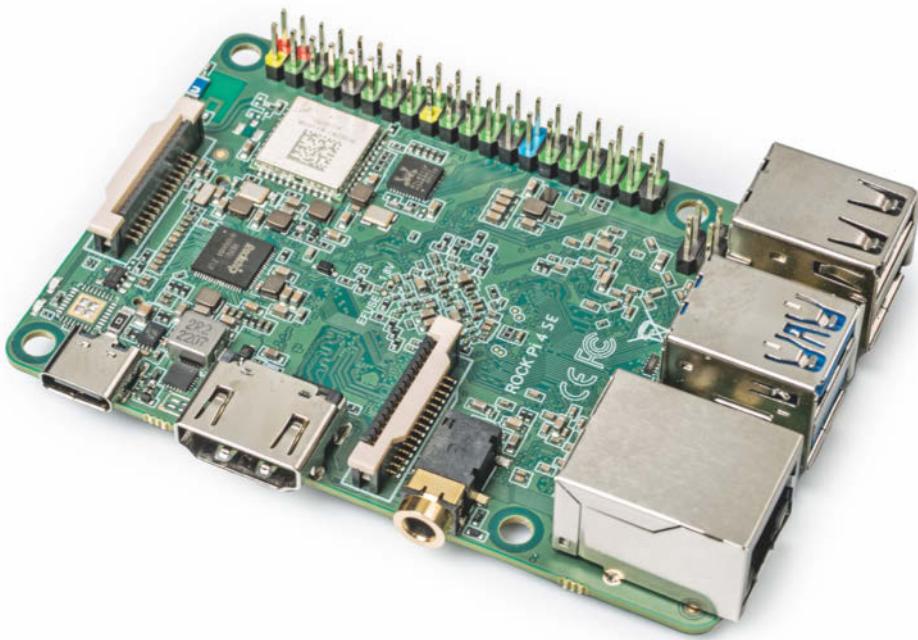
## Capture One 23 Pro (16.0)

### Raw-Entwickler

Hersteller, URL	Capture One, <a href="http://www.captureone.com/de">www.captureone.com/de</a>
Systemanf.	Windows ab 10, mac OS ab 11
Preis	349 € einmalig oder 29 € monatlich



Weniger auswendig lernen: Capture One Pro 23 bringt freundlich große und vor allem beschriftete Symbole auf den Schirm.



# WannaPi

## Der Einplatinencomputer OKdo/Radxa Rock 4 SE als Raspi-Alternative

**Der Rock 4 SE der britischen Firma OKdo soll eine Alternative zum Raspberry Pi 4 sein. Das schafft er aber nur in bestimmten Fällen, wie der Test zeigt.**

Von Christof Windeck

**S**chon seit Jahren kommt der ARM-Prozessor Rockchip RK3399 auf Einplatinencomputern wie Banana Pi, NanoPi, Orange Pi, Tinkerboard und Rock Pi zum Einsatz. Ende 2022 brachte die britische Firma OKdo in Kooperation mit dem chinesischen Hersteller Radxa den Rock 4 SE auf den europäischen Markt, ausdrücklich als Alternative zum derzeit schlecht lieferbaren Raspberry Pi 4. Der rund 90 Euro teure Rock 4 SE – das SE steht für Special Edition – ähnelt weitgehend dem seit 2019

verkauften Radxa Rock Pi 4 Model B mit 4 GByte RAM. Herzstück ist das ARM-SoC Rockchip RK3399-T, eine Variante des RK3399. Wir haben einen Rock 4 SE bei OKdo bestellt und getestet.

### Papiertiger

Der Rock 4 SE hat dieselben Abmessungen wie ein Raspi 4 und viele ähnliche Anschlüsse: 4 x USB-A (je zweimal USB 2.0 und 3.0), Gigabit-Ethernet, WLAN mit 2,4 und 5 GHz, Bluetooth, MicroSD-Kartenleser, 40-poliger GPIO-Pfostenstecker, Audio-Klinkenbuchse, USB-C zur Stromversorgung, MI-PI-DSI für ein Display und MIPI-CSI für eine Kamera. Statt zweier Micro-HDMI-Ausgänge gibt es beim Rock 4 SE nur eine einzige normal große HDMI-Buchse, die aber ebenfalls 4K-Displays mit 60 Hz ansteuern kann.

Dem Raspi voraus hat der Rock 4 SE eine M.2-Fassung für eine NVMe-SSD sowie eine Echtzeituhr (RTC), die sich optional per Lithiumzelle puffern lässt. Auch die GPIO-Leiste stellt einige Funktionen mehr bereit als beim Raspi. Außerdem kann man auf den Rock 4 SE als Bootmedium auch ein eMMC-Flashmodul in proprietärer Bauform aufstecken; das ist mechanisch robuster als eine MicroSD-Karte.

Der Rockchip RK3399-T hat sechs ARM-Kerne: Zwei starke Cortex-A72 mit bis zu 1,5 GHz sowie vier Cortex-A53-Effizienkerne mit nur 1 GHz. Zum Vergleich: Der Broadcom BCM2711 des Raspi 4 hat vier Cortex-A72 mit 1,8 GHz, in älteren Versionen mit 1,5 GHz. Im BCM2711 steckt eine VideoCore-VI-GPU (VC6) mit weitgehend quelloffenen Linux-Treibern. Der RK3399-T nutzt eine ARM Mali T860MP4, für den durch Reverse Engineering der Linux-Treiber Panfrost entwickelt wurde.

Der 40-polige GPIO-Pfostenstecker des Rock 4 SE ist genauso belegt wie beim Raspberry Pi und bietet ebenfalls 27 nutzbare GPIO-Kontakte. Davon kann man welche für Schnittstellen wie I2C, SPI, I2S, UART umschalten und zwei für PWM. Man steuert sie unter Linux per Libmraa an und konfiguriert die Funktionen der Pins in der Datei boot/hw\_intfc.conf. Allerdings gibt es Unterschiede, weshalb man für einen Raspi geschriebene GPIO-Programme anpassen muss. So liegen etwa die Hardware-PWM-Funktionen auf anderen Pins und vier GPIO-Pins sind beim Rock 4 SE nicht nutzbar, weil sie als SPI-Schnittstelle dienen, die auch mit dem aufgelösten SPI-Flash verbunden ist. Im Vergleich zum Raspi hat der Rock 4 SE aber auch zusätzliche GPIO-Fähigkeiten wie die Ausgabe von SPDIF-Signalen sowie einen Analog-Digital-Wandler (A/D-In), der bis zu 1,8 Volt verträgt.

### Leistungsvergleich

Zum Betrieb des Rock 4 SE empfiehlt Radxa ein USB-Power-Delivery-Netzteil mit 9 bis 12 Volt und mindestens 18 Watt Belastbarkeit. Wir haben ihn trotzdem mit dem USB-C-Netzteil des Raspi 4 betrieben, das nur 5 Volt liefert. Der Rock 4 SE arbeitete daran stabil, auch mit eingesteckter M.2-SSD. Dabei schluckt er ähnlich viel Strom wie ein Raspi 4.

Frisch aus  
**ct** Nerdistan

Verwendet man den Rock 4 SE wie einen Linux-PC, reagiert er spürbar träger als ein Raspi 4. Das liegt vermutlich vor allem daran, dass nur zwei statt vier Cortex-A72-Kerne bereitstehen und die A53-Kerne eher als Hilfsmotoren dienen. Den Browser-Benchmark Google Octane 2.0 absolviert der Rock 4 SE etwa 20 Prozent langsamer als der Raspi 4.

Auch beim Komprimieren und Dekomprimieren mit 7-zip war der Rock 4 SE langsamer als der aktuelle Raspi. Dieser Benchmark (7zr b) lief unter Armbian etwas schneller als unter dem von Radxa bereitgestellten Debian Bullseye.

Doch manches kann der Rock 4 SE auch deutlich schneller als der Raspi, etwa ver- und entschlüsseln: Anders als die Cortex-Kerne im Broadcom BCM2711 haben die des RK3399-T auch AES-Beschleuniger und erreichen damit mehr als den zehnfachen openSSL-Durchsatz.

Die Gigabit-Ethernet-Schnittstelle liefert volle Geschwindigkeit. Der wie beim Raspi per SDIO angebundene WLAN-Adapter arbeitet eher gemächlich, zum Websurfen reicht es.

Das Lesen von einer NVMe-SSD gelang mit mehr als 500 MByte/s. Von einem USB-3.0-Stick konnten wir mit mehr als 170 MByte/s lesen. Doch keine der USB-SSDs aus unserem Fundus wurde richtig erkannt; daher konnten wir damit keine Datentransferraten messen. Daran änderte auch ein USB-PD-Netzteil nichts, aus dem sich der Rock 4 SE mit 12 Volt versorgte.

## Linux-Distros

Auf dem Raspi 4 kann man außer Raspberry Pi OS noch zahlreiche andere Linux-Distributionen mit offizieller Unterstützung installieren, etwa Ubuntu Desktop 22.04.1 LTS und 22.10, Ubuntu Server, Fedora Core 37, Armbian und Projekte wie LibreElec. Das Linux-Angebot für den Rock 4 SE ist vermeintlich ebenfalls groß: Auf der Radxa-Website finden sich außer Radxa-Images mit Debian 11 Bullseye, Debian 10 Buster, Ubuntu 20 Server und Android 11 auch Verweise zu Armbian, LibreElec, DietPi, Manjaro und andere Distributionen.

Bei genauerem Hinsehen und nach stundenlangen Versuchen wird aber klar: Radxa pflegt im Wesentlichen Debian 11 Bullseye mit Linux-Kernel 4.4.194 aus dem Jahr 2019. Dessen Support durch die Kernel-Maintainer ist allerdings im Februar 2022 ausgelaufen und es sind bereits

einige Sicherheitslücken bekannt. Auch im Radxa-Image für Ubuntu 20 Server steckt Kernel 4.4. Von Debian 10 Buster gibt es eine Betaversion mit Kernel 5.15, die aber beispielsweise keine 4K-Auflösung liefern kann.

Wir haben alternativ zwei Varianten von Armbian 22.11.1 für den Rock 4 Model B ausprobiert: „Bullseye Current“ ohne grafischen Desktop, um die NAS-Software OpenMediaVault (OMV) zu testen, sowie „Jammy Current“ mit Gnome. Über den Armbian-Versionen für die Radxa-Boards schwiegt ein Damoklesschwert, weil die Distribution händeringend Maintainer sucht.

Gewerblichen Nutzern, die den Rock 4 SE als Entwicklungsbasis einsetzen, stellt Radxa via GitHub ein Board Support Package (BSP) bereit. Damit können Hersteller eigene Images auf Debian-Basis als Firmware für ihre Geräte bauen.

## Verwirrspiel

Auf der Radxa-Website finden sich zwar viele Informationen zum Rock 4 SE, aber die Anordnung ist unübersichtlich. Das macht den Einstieg schwieriger als nötig. Bei Armbian heißt der Rock 4 SE „Rockpi 4 Model SE“, was uns verwirrte. Das Radxa-Image für Debian Bullseye mit XFCE-Desktop schrieben wir gemäß Anleitung mit Balena Etcher auf eine MicroSD-Karte; davon bootete der Rechner problemlos. Statt jedoch nach dem ersten Start die Einrichtung eines neuen Nutzers vorzuschlagen sowie die Bedienungssprache und Zeitzone abzufragen, geht es mit englischer Lokalisierung, US-Zeitzone sowie dem Standardbenutzer „rock“ mit dem Passwort „rock“ los. Hier ist Fleißarbeit nötig, um alles anzupassen.

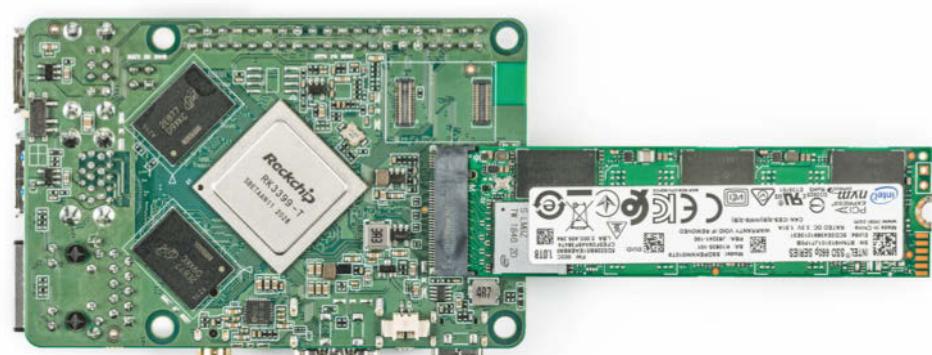
Auch die obere USB-3.0-Buchse funktioniert nicht, weil sie als Device- statt als Hostport konfiguriert ist für USB OTG. Die nächste Hürde: Das Update der Distribution mit `sudo apt-get update && apt-get upgrade` schlägt fehl. Zuvor muss man nämlich einen Schlüssel von einem Radxa-Server importieren. Der HDMI-Ausgang lieferte zwar 4K-Auflösung, aber keinen Ton.

Benutzerfreundlicher laufen die Armbian-Images: Sie fragen beim ersten Booten die gewünschte Lokalisierung von Tastatur und Oberfläche ab und erzwingen das Einrichten eines neuen Nutzers und eines Root-Passworts. Mit Armbian funktionierte zwar HDMI-Sound, aber es war höchstens Full-HD-Auflösung möglich. Auch DietPi [1] funktionierte in unseren Versuchen, zeigte aber ebenfalls maximal Full-HD-Auflösung.

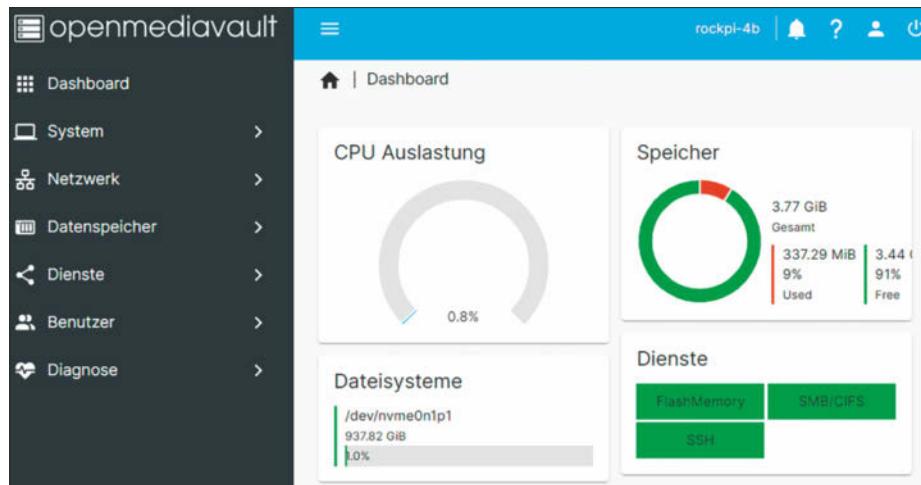
Außer von der MicroSD-Karte bootet der Rock 4 SE auch von eMMC-Flash oder einer M.2-SSD. Wir konnten zwar ein Image auf das eMMC-Modul schreiben und das System startete auch, doch dann traten Fehler bei Zugriffen auf den Flash-Speicher auf – Ursache unklar. Um von einer M.2-SSD zu booten, muss man die Firmware im SPI-Flash-Speicherchip mit einer anderen Version überschreiben und den Bootloader auf dem jeweiligen Speichermedium anpassen; das haben wir nicht probiert.

Radxa pflegt eine Kompatibilitätsliste mit M.2-SSDs, auf der unter anderem die Intel SSD 660p und die Kingston A2000 stehen; beide funktionierten in unseren Tests auch. Eine Samsung SSD 960 Pro wurde hingegen nicht erkannt und fehlt auch auf der Radxa-Liste.

Nachdem wir das erwähnte Armbian 22.11.1 „Bullseye Current“ auf einer Micro-



Beim Rock 4 SE sitzt der (Rockchip-)Prozessor auf der Unterseite. Anders als beim Raspi 4 gibt es eine M.2-Steckfassung für eine SSD, die aber weit über die Rock-Platine hinausragt.



Unter Armbian 22.11.1 ließ sich auf dem Rock 4 SE die NAS-Software Openmediavault (OMV) installieren.

SD-Karte geflasht hatten, konnten wir mit armbian-config reibungslos OMV installieren und die NVMe-SSD als Datenspeicher einbinden. Damit lieferte der Rock 4 SE die für Gigabit-Ethernet üblichen Datentransferraten von jeweils rund 110 MByte/s beim Schreiben und Lesen. Längere M.2-SSDs im Format 2280 stehen aber weit über die Kante der Rock-Platine heraus und es gibt keine Befestigungsmöglichkeit – das ist eine wackelige Konstruktion.

## Raspi-Vergleich

Es ist schwierig, den Rock 4 SE mit dem Raspberry Pi 4 zu vergleichen, weil sehr viele Einzelheiten zu berücksichtigen sind. Je nach Perspektive fällt die Gegenüberstellung unterschiedlich aus.

Unerfahrenen Bastlern muss man vom Rock 4 SE abraten: Die Linux-Unterstützung ist dermaßen lückenhaft, dass man rasch auf schwer lösbarer Probleme stößt, die den Spaß am Experimentieren verleiden. Dann dürfte der Rock 4 SE bald wieder in der Schublade verschwinden.

Wer solide Erfahrungen auf der Linux-Kommandozeile hat, umschifft hingegen viele Klippen. Dann könnte der Rock 4 SE im Prinzip einen passablen Netzwerkspeicher oder Miniserver abgeben. Dem steht allerdings entgegen, dass man eine M.2-SSD zwar einstecken, aber nicht sicher befestigen kann, und dass der Linux-Kernel mancher kompatiblen Distributionen veraltet und somit unsicher ist [2]. Zudem steckt im First-Stage-Bootloader Binär-Code der chinesischen Firma Rockchip und auch die Mali-GPU benötigt proprietäre Firmware.

Als Steuermodul ohne direkten Inter-

netzugang würde sich der Rock 4 SE eignen, falls die jeweils gewünschte Software läuft. Dafür ist er mit 90 Euro aber ziemlich teuer.

Für professionelle Entwickler, die ein Rockchip-Board als Embedded System in ihre Produkte integrieren wollen, ist der Rock 4 SE gut geeignet. Dank des Board Support Package können sie eigene Firmware-Images auf Linux-Basis backen.

## Fazit

Der Rock 4 SE kostet rund 50 Prozent mehr, als der Listenpreis des Raspi 4 mit 4 GByte beträgt. Auch wenn man letzteren derzeit nur zu Mondpreisen ergattern kann – falls überhaupt –, wirkt der Rock 4 SE ziemlich teuer. Obendrein bestätigt der Test die Vorbehalte vieler Linux-Freunde gegenüber Rockchip-Einplatinencomputern: Schöne Hardware, hässliche Software. Aussicht auf bessere Linux-Unterstützung besteht nicht, weil der RK3399 schon seit vier Jahren auf solchen Platinchen zum Einsatz kommt und die Probleme fortbestehen. Die Gründe erklärt [3]. Der Rock 4 SE eignet sich deshalb nur für Profis und erfahrene Bastler, die seine durchaus vorhandenen Vorteile durch geduldiges Tüfteln ausreizen können.

(ciw@ct.de)

## Literatur

- [1] Dennis Gerbig, Himbeer-Diät, DietPi: Alternativ-Distribution für Raspis, c't 6/2021, S. 86
- [2] Thorsten Leemhuis, Flickschusterei, Linux-Distributionen korrigieren manche Schwachstellen in ihren Kerneln nicht, c't 16/2021, S. 144
- [3] Thorsten Leemhuis, Für einander gemacht, Warum es mit Upgrades bei Android hakt, erläutert an Linux beim Raspberry Pi, c't 8/2020, S. 120

## OKdo (Radxa) Rock 4 SE

ARM-Einplatinencomputer mit Rockchip RK3399-T	
Hardware-Ausstattung	
CPU / Kerne / Takt	Rockchip RK3399-T / 2 × ARM Cortex-A72 + 4 × Cortex-A53 / 1,5/1,0 GHz
RAM	4 GByte LPDDR4-3200
Grafik(-speicher)	ARM Mali T860MP4 (vom Hauptspeicher)
SSD-Steckplatz	1 × M.2 (PCIe 1.0 x4) (PCIe 2.0 per Software einschaltbar)
Soundchip	Everest ES8316 (I2S)
Netzwerk-Interface (Chip, Anbindung)	1 Gbit/s (Realtek RT8211, PHY)
WLAN-Adapter	AzureWave CM-SM256SM (SDIO, 1 x 1,433 Mbit/s, Bluetooth 4.2)
Power Management IC (PMIC)	Rockchip RK808-D mit RTC
Abmessungen	8,7 cm × 2,1 cm × 6,0 cm (CPU auf der Unterseite)
Spannungsversorgung	USB-C, 5 bis 12 Volt, 15 W
Anschlussbuchsen	1 × HDMI, 2 × USB-A 5 Gbit/s, 2 × USB-A 2.0, 1 × LAN, 1 × Audio-Klinke, 1 × USB-C (Strom)
Anschlüsse onboard	40-pol GPIO, 1 × MIPI-CSI, 1 × MIPI-DSI, 1 × PoE-Header
Steckfassungen / Anschlüsse unten	1 × MicroSD, 1 × M.2, 1 × eMMC ( proprietär), 1 × RTC (2-pol)
Elektrische Leistungsaufnahme, Datentransfer-Messungen	
Soft-Off / Energie Sparen	0,2 W / –
Leerlauf mit 4K-Monitor an HDMI	3,4 W (ohne Display: 2,7 W; mit Display & Ethernet: 3,9 W)
Leerlauf mit M.2-SSD & LAN	5,9 W
Volllast: CPU / CPU und Grafik	7,3 / 9,0 W
M.2-SSD lesen (schreiben)	520 (258) MByte/s (Intel SSD 660p)
LAN RX (TX)	> 110 MByte/s
Systemleistung	
openSSL AES-128 ohne / mit AES-NI	79 / 1065 Mbit/s
7zr b komprimieren / dekomp.	3415 / 5580 MIPS
Preis / Garantie	89 € / k.A.
✓ funktioniert	– funktioniert nicht



# MIT Mac & i IMMER DER ZEIT VORAUS

+ Geschenk  
nach Wahl



z. B. 10 € Amazon.de-Gutschein oder Apple-Watch-Ständer

**2x Mac & i mit 35% Rabatt testen!**

**Mac & i – Das Magazin rund um Apple**

- Tipps & Praxiswissen
- Hard- und Softwaretests
- Reports und Hintergründe
- inkl. Club-Mitgliedschaft

Für nur **16,80 € statt 25,80 €**  
(Preis in Deutschland)

Genießen Sie mit  
der Mac & i Club-  
Mitgliedschaft  
exklusive Vorteile!



Jetzt bestellen:

[www.mac-and-i.de/minabo](http://www.mac-and-i.de/minabo)



# Forever young

## Gigaset GS5 Senior mit seniorengerechter Androidoberfläche

**Smartphones für Senioren sollen alles können, ohne zu überfordern. Gigaset versucht sich an diesem Spagat, spart allerdings deutlich an der Hardware.**

Von Steffen Herget

Ach nee, in meinem Alter komme ich mit so einem Smartphone nicht mehr zurecht – solche Argumente hören viele von ihrer betagten Verwandtschaft. Einfach abfinden muss man sich damit aber noch lange nicht, schließlich sind Smartphones für alle Altersklassen praktisch. Sicher, viele Modelle schrecken mit ihren rutschigen Glasgehäusen, viel zu kleiner Schrift und überladener Benutzeroberfläche ältere Menschen ab. Doch der deutsche Hersteller Gigaset hat mit dem knapp 300 Euro teuren GS5 Senior ein Android-Smartphone von Grund auf für die Bedürf-

nisse älterer Nutzer konzipiert, anstatt wie das Gros der Anbieter nur hier einige Bauteile oder da ein paar Software-Features anzupassen.

Das beginnt bereits beim Lieferumfang. Im Karton liegt nicht nur das Smartphone, sondern auch eine passende Lederhülle zum Aufklappen, ein Netzteil, ein USB-C-Kabel mit magnetischem Adapter zum leichteren Anstöpseln und das Gigaset-Trainingsbuch. Darin bekommen Smartphone-Neulinge die Bedienung und grundlegenden Funktionen genau erläutert. Die mit vielen Screenshots illustrierten, verständlich formulierten Anleitungen setzen kaum Grundwissen voraus. Der Akku für das GS5 liegt separat in der Kiste. Um ihn einzusetzen, muss man zunächst die hintere Abdeckung des Smartphones entfernen – aber auch das erklärt das Trainingsbuch.

Beim Einschalten des GS5 Senior grüßt eine übersichtliche Android-Oberfläche in Schwarz-Weiß-Optik mit großen Schriften und Symbolen. Die quadratischen Schalt-

flächen erinnern ein wenig an die Kacheln von Windows Phone. Alles was über die voreingestellten Grundfunktionen wie Telefon, SMS, Mail oder Kamera hinausgeht, wird komplett ausgeblendet und muss gesondert aktiviert werden. Das ist sinnvoll: Selbst absolute Späteinsteiger können damit direkt loslegen und die Komplexität allmählich erhöhen. Zu den zuschaltbaren Funktionen gehören unter anderem die normale statt der vereinfachten Bildschirmtastatur sowie die Spracherkennung, jedoch keine Kartenapp zur Orientierung – die muss man gesondert installieren.

Einen zweiten Bildschirm darf der Nutzer mit eigenen Apps bestücken. Das Starten anderer als der vorinstallierten Apps lässt sich komplett deaktivieren. Als Benachrichtigung zeigt das Gerät statt kleiner Punkte an App-Symbolen auffällige orange Balken an. Häufig kontaktierte Personen merkt sich die Kurzwahlliste. Außerdem gibt es die Möglichkeit, Notfallkontakte zu hinterlegen, mit einem Klick den Rettungsdienst zu rufen oder Notfall-SMS zu versenden.

### Weniger Funktionen, mehr Durchblick

Gigaset schiebt eine zusätzliche Sicherung zwischen die angepasste Oberfläche und die Systemeinstellungen. Die lassen sich erst aufrufen, nachdem man eine Warnung bestätigt hat, dass hier nur erfahrene Anwender ran sollen. Manche Apps wie der Chrome-Browser bekommen auf dem Homescreen ein eindeutiges Logo und starten dann ganz normal. Andere sind standardmäßig eingeschränkt, um die Bedienung zu vereinfachen. Die Kamera-App beispielsweise bietet nur die Modi Foto, Video und Selfie, schaltet aber nicht zwischen Hauptkamera und Ultraweitwinkel um. Wer mehr Optionen möchte, muss die als „Profi-Kamera“ bezeichnete normale App aktivieren. Auch die Fotogalerie-App hat Gigaset stark beschnitten, sie kann Bilder nur drehen und verschicken, aber nicht anderweitig bearbeiten.

Bei all den sinnvollen Anpassungen der Benutzeroberfläche und dem kompletten Verzicht auf Apps von Drittanbietern bleibt ein Problem: die Updates. Zum Redaktionsschluss hing das GS5 Senior noch auf dem Sicherheitsstand von September 2022 und Android 12 fest. Auf Nachfrage teilte der Hersteller mit, das Smartphone solle „bis 2025“ mit Updates versorgt werden. In welcher Frequenz die Patches auf dem GS5 Senior eintreffen sollen, bleibt dabei unklar.

Das Seniorensmartphone bringt außer dem üppigen Lieferumfang auch einige Ausstattung mit, die sogar nur noch wenige teure Handys besitzen, etwa eine Benachrichtigungs-LED, eine 3,5-Millimeter-Kopfhörerbuchse und eine abnehmbare Rückseite. Zwei echte SIM-Karten passen hinein, aber eine programmierbare eSIM unterstützt das GS5 Senior ebenso wenig wie das Einbuchen in 5G-Netze. Ein Fingerabdrucksensor an der Rückseite oder Gesichtserkennung via Frontkamera entsperren das Gerät, falls PIN, Passwort oder Muster nicht genügen. Unnötig: Hat man das GS5 erfolgreich entsperrt, landet man nicht etwa direkt auf dem Homescreen, sondern auf einem weiteren Sperrbildschirm, der zum langen Drücken auf ein Schlosssymbol auffordert, bevor er den Weg freigibt.

Technisch bewegt sich Gigaset in der Einsteigerklasse. Der MediaTek-Prozessor liefert eine lahme Performance ab, wozu auch der knappe Arbeitsspeicher von 4 GByte beiträgt. Für Videotelefonate über WhatsApp, Signal und andere reicht die Performance aber aus. Dass das Gigaset-Handy nicht für grafisch herausragende Spiele oder hochauflösende Videos gedacht ist, verwundert nicht und ist absolut nachvollziehbar. Umso erstaunlicher, dass es unser Testvideo in 4K-Auflösung mit 120 fps sogar abspielte, wenn auch extrem ruckelig. Für die anvisierte Zielgruppe dürfte die Performance zwar ausreichen. Ein so langsames Handy kann aber gerade Neulinge verunsichern, wenn etwa nach dem Tippen erst einmal nichts passiert, weil sich das Smartphone noch eine Denkpause gönnnt.

Ein wenig mehr als die 64 GByte interner Flash-Speicher hätten es ebenfalls sein dürfen, denn wenn die Familie häufig Fotos und Videos schickt, reicht der Platz nicht

lange. Immerhin: Mittels Speicherkarte lässt sich die Kapazität um bis zu 512 GByte aufstocken. Das hilft allerdings nur bedingt, denn nicht jede App lagert ihre Daten auf den zusätzlichen Speicher aus und für ein dediziertes Seniorengerät ist das ganze Procedere eigentlich zu kompliziert.

### Trübes Display ohne Extrahertz

Der Bildschirm des GS5 Senior hat ein LCD-Panel, das Farben ein wenig blasser darstellt als viele OLED-Displays. Das merkt man allerdings erst dann, wenn man den Schwarz-Weiß-Homescreen verlässt. Gigaset bietet keine Optionen, die Farbdarstellung an die eigenen Vorlieben anzupassen. Die gemessene Helligkeit von bis zu 260 cd/m<sup>2</sup> im Alltag ist viel zu gering, um das Display bei direkter Sonneninstrahlung gut zu erkennen. Die automatische Helligkeitsregelung reagiert stark verzögert, schnelles Wechseln von dunkler in helle Umgebung ignoriert sie viel zu lange. Die Bildwiederholrate des Displays beträgt fest eingestellte 60 Hz. Höhere Frequenzen, die flüssigere Animationen und sanfteres Scrollen ermöglichen, beherrscht das GS5 Senior nicht.

Im Akkutest entpuppte sich das GS5 Senior nicht gerade als Ausdauerwunder, in unseren Tests lief es kürzer, als wir aufgrund der nominellen Akkukapazität von 4500 mAh und des trüben Displays erwartet hätten. Besonders kurz hielt das Seniorensmartphone beim 4K-Video durch, nach nur gut fünf Stunden Wiedergabe war Schluss. Mit seinen mageren 10 Watt Leistung braucht das mitgelieferte Ladegerät rund drei Stunden, um den Akku komplett zu laden. Das Ladekabel mit dem Magnetadapter, der im Smartphone stecken bleiben kann, ist indes praktisch: Wird das Telefon versehentlich während des Ladens weggezogen, löst es sich sofort vom Kabel und die empfindlichen Steckerverbindungen bleiben intakt.

Mit der Hauptkamera schießt das GS5 Senior bei guten Lichtverhältnissen noch brauchbare Fotos, spätestens in der Dämmerung gerät es an seine Grenzen. Auffällig: Selbst unter hellen Laborbedingungen aufgenommene Bilder zeigen deutliches Bildrauschen, das sich in vielen Testfotos negativ auf die Detailwiedergabe auswirkt, vor allem in dunklen Bildbereichen und bei langen Belichtungszeiten. Insgesamt fehlt es den Bildern an Schärfe. Das Ultrawinkel ist qualitativ noch schlechter, damit sollte man wirklich nur im Notfall fotografieren.

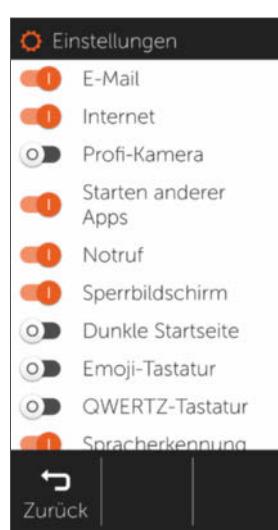
## Gigaset GS5 Senior

Android-Smartphone	
Hersteller, URL	Gigaset, <a href="http://gigaset.com">gigaset.com</a>
Betriebssystem / Patchlevel	Android 12 / September 2022
Android-Updates / Sicherheits-patches lt. Herst. bis min.	k.A. / 2025
Ausstattung	
Prozessor / Kerne × Takt / GPU	Mediatek Helio G85 / 2 × 2 GHz, 6 × 1,8 GHz / Mali-G52
Arbeitsspeicher / Flash-Speicher (frei) / Wechselspeicher	4 GByte / 64 GByte (49 GByte) / ✓
LTE / 5G / SAR-Wert <sup>1</sup>	✓ / – / 0,29 W/kg
WLAN (Antennen) / Bluetooth / NFC / Kompass / Standortbest.	Wi-Fi 6 (2) / 5.1 / ✓ / ✓ / GPS, Glonass, Beidou, Galileo
SIM / Dual / eSIM	Nano-SIM / ✓ / –
Fingerabdrucksensor / Kopfhörer-anchluss / USB-Anschluss / OTG	✓ (Display) / ✓ / USB-C 2.0 / ✓
Akku / drahtlos ladbar / wechselbar	4500 mAh / – / ✓
Abmessungen (H × B × T) / Gewicht / Schutztart	15,8 × 7,5 × 1,1 cm / 205 g / –
Kamera	
Hauptkamera Auflösung / Blende / OIS	48 MP (8000 × 6000) / f/1,8 / –
Ultrawinkel Auflösung / Blende / OIS	8 MP (3264 × 2448) / f/2,0 / –
Frontkamera Auflösung / Blende / OIS	8 MP (3264 × 2448) / f/2,0 / –
Display	
Diagonale / Technik / max. Bild-wiederholrate	6,3" / LCD / 60 Hz
Auflösung (Pixeldichte) / Helligkeitsregelbereich	2340 × 1080 Pixel (410 dpi) / 1,86 ... 953 cd/m <sup>2</sup>
Benchmarks, Lauf- und Ladezeiten	
Ladezeit 50 % / 100 %	1,1 h / 3 h
Laufzeiten <sup>2</sup> lokales Video 720p / lokales Video 4K, 120 fps/ 3D-Spiel Asphalt 8 / Stream	13,2 h / 5,3 h / 10,7 h / 13,6 h
Geekbench V4 Single, Multi / V5 Single, Multi	1694, 5025 / 346, 1259
3DMark Wild Life / Wild Life Extreme	745 / 189
GFXBench Car Chase / Manhattan 3.0 / Manhattan 3.1 (je On-, Offscreen)	7,5 fps, 9 fps / 23 fps, 24 fps / 14 fps, 15 fps
Preis / Garantie	300 € / 24 Monate

<sup>1</sup> Herstellerangabe <sup>2</sup> gemessen bei 200 cd/m<sup>2</sup>  
✓ vorhanden – nicht vorhanden

## Fazit

Das Gigaset GS5 Senior reißt in Sachen Performance keine Bäume aus und auch Akku, Display und Kamera haben mehr Schwächen als Stärken. Der mehr als komplette Lieferumfang und die vielen sinnvollen Softwareanpassungen machen das Smartphone aber für betagtere und technisch wenig versierte Menschen interessant, die die App-Fülle klassischer Smartphones überfordert. Es ist für den Alltag auf jeden Fall deutlich besser als all die halbherzig auf seniorengerecht getrimmten Feature-Phones und trotz der schwachen Hardware sein Geld wert. Mit etwas höherer technischer Qualität wäre den älteren Semestern dennoch etwas besser gedient. (sht@ct.de) 





# Broogle-Boxen

## Musiksystem LE von Braun im Test

**Die Marke Braun verbindet man heutzutage eher mit Bartpflegeprodukten für den wohl situierten Herren ab 40. Das Musiksystem LE hingegen knüpft an die Tradition von Musik- und Hi-Fi-Produkten im Bauhaus-Design an, mit denen das Unternehmen bis in die 80er-Jahre Designgeschichte geschrieben hat.**

Von Sven Hansen

**S**ein dem Verkauf der Braun AG an den Gillette-Konzern 1967 haben die Markenrechte rund um den ikonischen BRAUN-Schriftzug viele Wege genommen. Heute steht hinter „Braun Audio“ der britische Radio-Hersteller Pure, der unter dem Logo ein vernetztes Musiksystem bestehend aus den Smart Speakern LE01, LE02 und LE03 anbietet.

Schon die Produktbezeichnung „LE“ schlägt einen weiten Bogen aus den Anfängen der Hi-Fi-Ära. Brauns Passivlautsprecher LE1 arbeitete nach dem Prinzip des Elektrostaten. Dabei schwingt eine Spezialmembran mit ihrer gesamten Fläche, wodurch die störenden Einschwingvorgänge dynamischer Lautsprecher weg-

fallen. Nebeneffekt: Die Lautsprecher-technik kam ohne voluminöse Dauer-magnete und Spulen aus. Nur so konnte Design-Ikone Dieter Rams den LE1 für Braun als flaches Sound-Brett entwerfen – 1959 ein wahrlich revolutionäres Design. Restaurierte Versionen des LE1 gehen heute zum Preis von 7000 Euro über die Ladentheke.

Die LE-Serie von heute kommt mit herkömmlicher Lautsprechertechnik. Für die klassischen Treiber braucht es trotz Neodym-Magneten mehr Tiefe als 1959: War der LE1 noch 3,2 Zentimeter flach, kommen die LEs von heute mit fast 10 Zentimeter Tiefe deutlich dicker daher. Sitzt man davor, fällt das zum Glück

kaum auf. Doch gerade das Topmodell LEO1 ist, leicht von der Seite betrachtet, ein recht massives Brett.

Alle drei Vertreter zeigen Braun-typisch klare Kanten und Viertelkreise, frei nach Dieter Rams' Motto „Gutes Design ist unsichtbar“ halten sich die LE-Speaker vornehm zurück. Die Verarbeitung ist hochwertig, das Chassis ist in ein umlaufendes Aluband gefasst. Die LE-Serie ist in den Farben Schwarz und Weiß zu haben. Die kreisrunden Knöpfe und Tasten mit Signalfarben an der Oberseite nehmen das Braun-Design der 80er auf.

Die große Grundfläche sorgt dafür, dass die Speaker schon auf ihren Silikonfüßen sicher stehen. Bei den größeren LEO1 und LEO2 sind zusätzliche Metallbügel beigelegt – 1959 lässt grüßen. Optional erhältlich sind schicke Lautsprecherständer mit massiver Steinplatte, mit denen sich selbst die wuchtigen LEO1 fast schwebend im Raum platzieren lassen.

Auf der Oberseite liegen die Bedienelemente zur Lautstärkensteuerung, Bluetooth-Kopplung und – beim kleinen LEO3 – das integrierte Mikrofon-Cluster. Bei den größeren Brüdern sind die Mikrofone seitlich platziert. Der mechanische Mikrofon-Taster trennt die Mikros physisch und soll für mehr Privatheit sorgen. Hat der Spea-

**Die Bedienelemente der LE-Speaker erinnern an das Braun-Design der 80er.**



ker taube Ohren, leuchtet die Taste in Signalfarbe Orange und auch die vier Status-LEDs in der Front leuchten dauerhaft. Wer sich für die Assistenzfunktion nicht interessiert, muss mit dem Lichtspiel leben, weil man es nicht abschalten kann.

### Google Inside

Jede Braun-Box ist ein vollwertiger Smart Speaker, der via Google Assistant Sprachbefehle entgegennimmt. Andere Assistenten wie Alexa oder Bixby kann man nicht verknüpfen. Die Geräte unterstützen zudem Chromecast und AirPlay 2 als Streaming-Standard (nicht aber Spotify Connect und Tidal Connect) und lassen sich über Bluetooth (A2DP) mit Musik bespielen. Dabei ist man auf die Wiedergabe von Standardformaten maximal in CD-Qualität beschränkt. Es mangelt an der Unterstützung von HighRes- oder 3D-Formaten sowie an verbesserten Bluetooth-Codecs; Chromecast unterstützt weiterhin kein Gapless, zwischen zwei Songs pauisiert die Wiedergabe also eine Sekunde. Auch das Hands-Free-Protokoll unterstützen sie nicht, man kann sie daher trotz Mikrofonen nicht als Konferenzlautsprecher einsetzen. Schon der kleine LEO3 verfügt zusätzlich über einen Line-in-Eingang, um eine analoge Quelle zum Klingeln zu bringen.

Installiert man die Braun-Audio-App, wird man sofort an Google Home weitergereicht. Dort erscheint der Eintrag „Braun Audio LEOX einrichten“ immerhin automatisch beim Start. Man ordnet den Lautsprecher einem Zuhause zu und der Scanvorgang startet. Das Smartphone verbindet sich mit dem Speaker und man muss das gewünschte WLAN wählen – die Geräte funken mit 2,4 GHz und 5 GHz.



**Die größeren LEO1 und LEO2 stellt man auf Silikonfüße oder nutzt die mitgelieferten Metallbügel, um sie leicht anzuwinkeln.**

Positiv fällt auf, dass Google die Dialoge zum Datenschutz beim Einrichten von Lautsprechern generell erweitert hat. Neu ist zum Beispiel der Hinweis, dass man auch Gäste auf das Vorhandensein von Mikrofonen im Raum aufmerksam machen sollte.

Am Ende der Prozedur geht es zurück zur Braun-Audio-App. Mit ihrer Hilfe lassen sich Klangeinstellungen an den Speakern vornehmen. Die App fragt dazu Informationen zum Aufstellort der Lautsprecher ab und passt die Musikwiedergabe an. Die klanglichen Veränderungen sind eher subtil und im A/B-Vergleich kaum wahrnehmbar. Ebenfalls über Braun Audio lassen sich Bässe und Höhen justieren, eine Loudness-Option fehlt und ebenso die Möglichkeit, die LEDs auszuschalten.

Google Home ermöglicht das Anlegen von Gruppen oder kann zwei bauliche LEOX zu einem Stereosystem verknüpfen. Das Herumhantieren mit zwei Apps erwies sich im Test als nervig. Zwar zeigt Braun Audio an, welcher Song gerade gespielt wird, doch kontrollieren kann man die Wiedergabe nicht. Andersherum kommt man über Google Home nicht an die Klangeinstellungen heran, wenn der Bass doch mal übertrieben dröhnt.

### Klang

Die LE-Serie arbeitet mit Breitbandlautsprechern, die von einem eingebauten Subwoofer unterstützt werden. Der für Mono-Wiedergabe ausgelegte LEO3 kommt so mit zwei Schallwandlern, beim Top-Modell LEO1 sind es fünf (3 Breitband, 2 Subwoofer). Jedem Fullrange-Speaker ist auch ein Class-D-Verstärker zugeordnet, die Subwoofer allerdings

haben keinen eigenen Verstärker. Damit unterscheidet sich das System etwa von Sonos-Lautsprechern, bei denen jedem Schallwandler ein eigener Verstärker zugeordnet ist. Nur so lässt sich etwa Sonos' Einmessfunktion realisieren, bei der der Klang auf den jeweiligen Standort hin optimiert wird.

Im Hörtest spielt schon der kleine LEO3 recht ordentlich auf. Die Bässe wirken in der Neutraleinstellung ein wenig überzogen, lassen sich über die App jedoch einbremsen. Die Höhenabstrahlung des Breitbandlautsprechers ist stark gerichtet, so ergibt sich ein recht unterschiedlicher Höreindruck je nach Position im Raum. Ein Eindruck, der sich bei den großen Brüdern fortsetzt und schlussendlich auch dem klar nach vorne ausgerichteten Design geschuldet ist.

Der LEO2 legt eine Schippe drauf. Das liegt vor allem an der Stereowiedergabe, aber auch an den größer dimensionierten

**LEO1 und LEO2**  
haben auf der Rückseite den analogen Line-In und einen LAN-Anschluss. Letzterer fehlt dem kleinen LEO3.



Treibern. Differenzierte Höhen, eine breite Stereobühne – allerdings variiert besonders das räumliche Klangerlebnis durch die auch hier stark gerichteten Höhen je nach Position vor dem Speaker. Dabei geht es eher um Zentimeter als um Dezimeter, die man den Kopf in die ein oder andere Richtung bewegt. Solche Effekte kennt man sonst eher von Sound-Projektoren, die 3D-Klang gezielt auf eine Abhörposition hin abfeuern.

Das Topmodell LEO1 ist insgesamt deutlich lauter als der LEO2. Der kraftvolle Sound macht auch bei mittleren Lautstärken Spaß. Bei so viel Wumms fehlt einem ein wenig der Tiefbass, etwa wenn es beim Frequenzlauf in *Lana del Reys „Video Games“* mal ganz in den Keller geht. Dass man nun vor drei gerichteten Breitbandlautsprechern sitzt, macht die räumliche Wiedergabe nicht besser. Gefühlt hämmert der LEO1 die Höhen in Scheiben in den Raum, sodass der Stereoeffekt nur bei unveränderter Hörposition stabil bleibt.

Legt man besonderen Wert auf die räumliche Wiedergabe etwa bei Klassik oder Jazz, sollte man eher zwei Braun-Speaker als Stereopaar konfigurieren, mit zwei LEO1 quasi der Doppelwumms.

## Fazit

Braun Audio nimmt besondere Nachhaltigkeit für sich in Anspruch, das scheint mit Google als Plattformanbieter eher fraglich. Googles Weg ist mit eingestampften Services und nutzlos gewordener Hardware gepflastert. Sollte der Internetriese den Stecker ziehen, schaut es auch mit der LE-Serie mau aus. Immerhin: Der Line-in-Eingang würde dauerhaft funktionieren.

Die Bedienung mit zwei Apps ist wahrlich nicht aus einem Guss – das hätte den

Braun-Urvätern sicherlich nicht gefallen. Neben der Nachhaltigkeit ein weiterer Grund, warum man anstatt zu Googles Standard-Plattform vielleicht zu eigener Streaming-Technik hätte greifen sollen. Die hat Pure durchaus im Portfolio, einst hatte man mit den Jongos ein gut funktionierendes Mehrraumsystem im Angebot. Eine breitere Codec-Unterstützung wäre damit kein Problem gewesen. Musik in hoher Auflösung oder in innovativen 3D-Formaten stünde dem Braun-System gut zu Gesicht.

Klanglich schlagen sich die LEs wacker, wobei sie gerade im Vergleich zu Sonos bei doppeltem Preis längst nicht doppelt so guten Sound liefern. LEO3 und LEO2 sind deutlich teurer als Play:1 und Play:5 – da wird die Luft für Braun Audio dünn. Das Topmodell LEO1 sticht klanglich heraus, doch für 1200 Euro wird man schon bei High-End-Schmieden wie Bluesound fündig. So muss man am Ende entscheiden, ob die Freude am Design des britischen Braun-Remakes den Mehrpreis aufwiegt.

(sha@ct.de) 



Die Braun-Audio-App kann die Klangcharakteristik eines Lautsprechers an den Aufstellort anpassen. Die Profile sind fest hinterlegt, aktiv einmessen lassen sich die Speaker nicht.

## Braun Audio LE-Serie

Musikverteilsystem	
Hersteller, URL	Braun Audio, <a href="http://braun-audio.com">braun-audio.com</a>
Modell	LEO1 / LEO2 / LEO3
Anschlüsse	Line-in (3,5mm Klinke), Ethernet (nur LEO1/LEO2)
Bestückung	1,5" Fullrange, 3,5" Sub / 2 x 2,5" Fullrange, 1 x 5,25" Sub / 3 x 2,5" Fullrange, 2 x 5,25" Sub
Sprachassistentz	Google Assistant (4 / 4 / 2 Mikrofone)
Kommunikation	Wi-Fi 5 (2,4 GHz, 5 GHz), Bluetooth
Audio-Codecs	HE-AAC, LC-AAC, MP3, Vorbis, WAV (LPCM), FLAC, Opus
Streaming	Bluetooth (A2DP), Chromecast, AirPlay 2
Standby	2,1 W / 2,2 W / 2,1 W
Preis	1200 €, 800 €, 380 €

# Von Hackern lernen

**c't HACKING-PRAXIS**

Testumgebung aufsetzen · Recherche- & Analyse-Tools anwenden

**Der große Security-  
ONLINEKURS**

heise Academy

► VIDEOKURS

Max Engelhardt

Angriffsszenarien im Netzwerk

Der Kurs zur Absicherung von Netzwerken aus der Position des Angreifers

Angriffe verstehen und abwehren, anschaulich erklärt in 65 Lektionen, Laufzeit: 6:29 Stunden

► Prüfen Sie das Gelernte in Wissenstests

**PLUS**  
heise-Academy-  
Webinar im Wert  
von 129,- Euro

**Hacking ausprobieren**

Trainingsumgebung einrichten  
Server hacken Schritt für Schritt  
Profi-Tools vorgestellt

**Informationen gewinnen**

OSINT: Informationen aus öffentlichen Quellen sammeln  
Unternehmens-Hack: Pentester über die Schulter geschaut

**Malware-Tricks verstehen**

System für Malware-Analyse installieren  
VM mit Analyse-Tools aufrüsten  
Schadcode-Analyse für Einsteiger

**+ GRATIS Webinar im Wert von 129,- €**

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

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

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



[shop.heise.de/ct-hackingpraxis23](http://shop.heise.de/ct-hackingpraxis23)

# Kritzelboard

## Apple Freeform ausprobiert

**Auf Apples neuem Whiteboard toben sich Nutzer kreativ aus, allein oder im Team. Wir testen, was es kann und ob es sich von der Konkurrenz abhebt – immerhin kommt Apple damit ein bisschen spät zur Party.**

Von Anke Brandt

**A**uf Online-Whiteboards visualisiert man seine Ideen und kann zeit- und ortsunabhängig mit anderen darüber brainstormen. Apple hat mit Freeform seine eigene App veröffentlicht. Sie kommt automatisch mit den Updates auf iOS 16.2, iPad OS 16.2 und macOS Ventura 13.1 auf die Geräte. Ältere Systeme müssen darauf verzichten. Eine Web-App gibt es ebenfalls nicht, sodass Nicht-Apple-Nutzer Freeform nicht verwenden können.

Wir haben die iPad-Version unter die Lupe genommen. Das iPhone eignet sich aufgrund des kleinen Displays nur für kurze Notizen oder um etwas auf einem Whiteboard nachzuschauen, nicht aber um produktiv damit zu arbeiten. Die Mac-Variante ist der auf dem iPad recht ähnlich. Der größte Unterschied besteht darin, dass die Zeichenfunktionen auf dem Mac fehlen.

### Viele Optionen

Öffnet der Nutzer die App zum ersten Mal, landet er auf einem Whiteboard, einer zunächst leeren Leinwand, die sich bei Bedarf unendlich erweitert. Anders als in vielen anderen Whiteboard-Anwendungen gibt es nur eine einzige, sehr übersichtliche Menüleiste am oberen Rand und die Zoom-Einstellungen unten links. Hier kann der Nutzer nicht nur in sieben vorgegebenen Stufen die Darstellung vergrößern oder verkleinern, sondern auch den „Inhalt passend zoomen“. Dann wählt die App eine Zoomstufe, auf

der alles auf dem Board zu sehen ist. Falls es schon reichlich gefüllt sein sollte, ist jedoch nicht alles gut erkennbar. Hier hilft die Schaltfläche „Auswahl zoomen“ weiter, sodass zum Beispiel ein ausgewählter Klebezettel bildschirmfüllend erscheint.

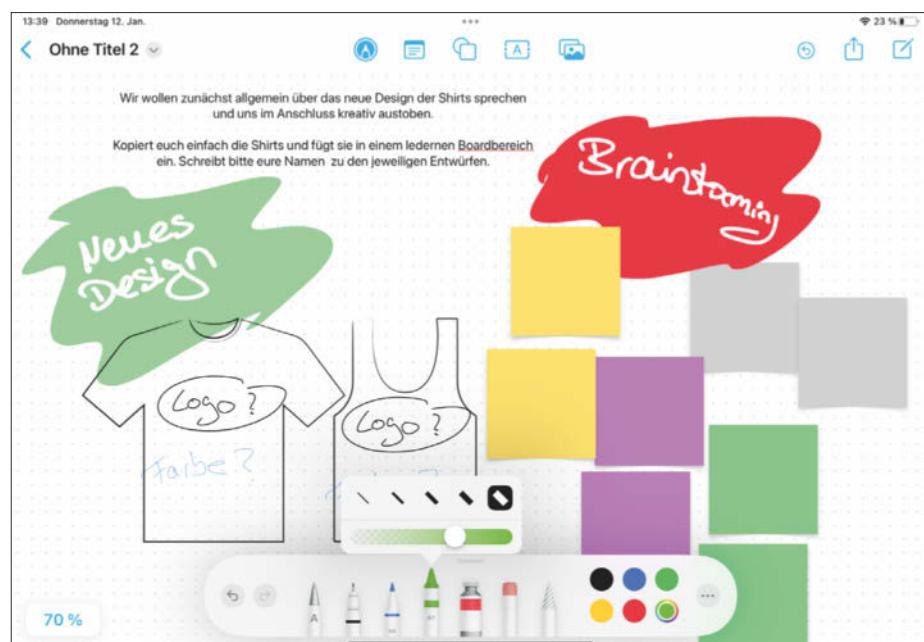
Durch Tippen auf die Klammer am oberen linken Rand ruft der Nutzer das Dashboard auf. Darauf listet Freeform alle Boards: zuletzt bearbeitete, geteilte und solche, die man zu seinen Favoriten hinzugefügt hat. Was zu Beginn übersichtlich erscheint, wurde im Test im Laufe der Zeit schnell zur großen Sucherei, als sich viele Boards im Dashboard tummelten. Es wäre schöner, wenn man eigene Unterkategorien hinzufügen könnte, beispielsweise private und geschäftliche Boards. Ein Tippen auf den Boardtitel öffnet ein Aufklappmenü, über das Nutzer das Fangraster für neue Objekte auf dem Board aus- und einblenden, das Whiteboard umbenennen, zu den Favoriten hinzufügen, es als PDF-Datei exportieren und drucken können.

Außerdem gibt es eine Findefunktion, die auf dem Board hinterlassene Notizen durchsucht. Oben rechts platziert Apple die Symbole, über die man eine neue Leinwand öffnet oder die aktuelle mit anderen teilt.

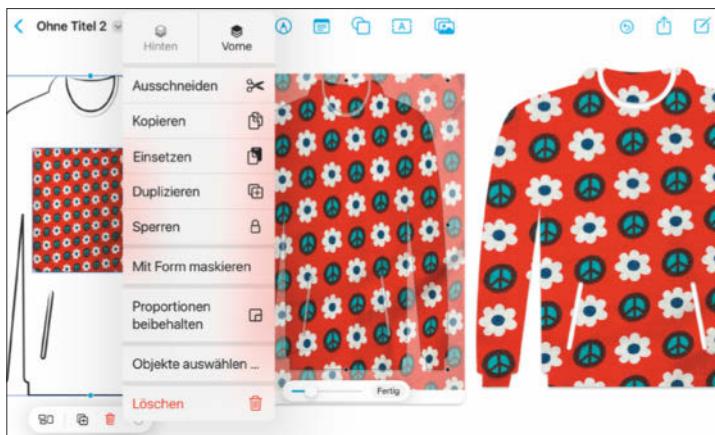
Über die Menüleiste oben in der Mitte fügt man dem Board Elemente hinzu. Die Werkzeugpalette (Stiftsymbol) enthält verschiedene – Überraschung! – Stifte, Radierer, eine Farbtube und ein Auswahlwerkzeug. Einen Textmarker gibt es nicht. Hier muss man sich bei Bedarf mit dem frei einstellbaren Transparenzgrad der Farbstifte beziehungsweise der Farbtube behelfen. Sie füllt freihändig gezeichnete Flächen. Sollen Dinge von der Leinwand verschwinden, wählt der Nutzer zwischen Pixel- und Objektradierer aus. Alle anderen Inhalte löscht man über ihr Kontextmenü. Schön wäre eine Option, um krakelige Linien automatisch zu begrenzen oder sie zu einer Form zu konvertieren, wie Apple es in der Notizen-App anbietet. Warum das Lineal aus ebendieser App in Freeform fehlt, erschließt sich ebenfalls nicht.

### Formen anpassen und sperren

Will man mehrere Elemente gemeinsam verschieben, wählt man sie aus und gruppieren sie über das Kontextmenü. Auf demselben Wege hebt man die Gruppierung wieder auf. Das klappt am einfachsten mit dem Finger. Das Auswahlwerkzeug des



**Apples Freeform verführt mit durchdachten Zeichenwerkzeugen und vielen vorgefertigten Formen zum Drauflosarbeiten.**



Objekte aus Freeforms Formenbibliothek versieht man auf Wunsch mit einem Foto als Hintergrund. Über den Zoom-Regler passt man die Größe des Fotos an.



Vektorgrafiken aus der Bibliothek kann Freeform in Einzelteile zerlegen – eine Funktion, die zum Spielen einlädt.

Stiftes fängt nur Formen ein, die auch mit dem Stift gezeichnet wurden. Besonders gefallen hat im Test, dass man ein Objekt an die Größe eines anderen anpassen kann, auch wenn das etwas Fingerspitzengefühl braucht: Größe von Objekt eins verändern, Finger auf dem iPad lassen, Objekt zwei antippen und beide loslassen.

Ausgewählte Elemente schiebt Freeform in den Vorder- oder Hintergrund, kennt dabei jedoch nur diese zwei Abstufungen. Andere Whiteboard-Anwendungen wie Canva stufen feiner ab und schicken auf Wunsch nur eine Ebene nach vorn oder hinten. Das ist hilfreich, wenn mehr als zwei Elemente übereinander liegen, beispielsweise bei einer Collage. In Freeform muss man dafür ein wenig puzzeln.

Als weitere nette Spielerei kann man die Vektorgrafiken der Formenbibliothek über das Kontextmenü in einzelne Bestandteile zerlegen, etwa um sie umzufärben oder neu zu arrangieren. Falls die mitgelieferten Grafiken nicht ausreichen, kann man seine eigenen zusammenbasteln, indem man zwei oder mehr Formen aus der Bibliothek übereinander schiebt, markiert und im Gruppieren-Menü „Formen zusammenfügen“ auswählt. Freeform bietet vier Varianten an, wie es die Objekte behandelt: verbinden, überschneiden, subtrahieren oder ausschließen.

Um einzelne Bereiche davor zu schützen, versehentlich verschoben zu werden, sperrt man sie über das Kontextmenü. Das ist nützlich, um ein Board zu strukturieren, bevor man mit anderen daran arbeitet.

Während sich die Mitstreiter zum Beispiel auf der linken Seite kreativ austoben dürfen, sollen sie rechts auf vorab eingefügten Klebezettelchen ihren Gedanken freien Lauf lassen.

### Teilen und exportieren

Seine eigenen Boards findet man automatisch auf allen Geräten mit identischer Apple-ID wieder. Damit das klappt, beziehungsweise um ein Board mit anderen Freeform-Nutzern teilen zu können, muss man zunächst iCloud für Freeform aktivieren. Im Menü legt man fest, ob „Jede:r mit diesem Link“ bearbeiten oder ansehen darf oder „Nur eingeladene Personen“. In unserem Test hatten wir wiederholt Probleme, Boards mit anderen Nutzern zu teilen, laut Fehlermeldung sei die Synchronisation noch nicht abgeschlossen. Nach dem Neustart der App funktionierte es jedoch jedes Mal tadellos.

Freeform exportiert Boards als PDF-Datei. Das klappt jedoch nur mit dem kompletten Inhalt. Will man beispielsweise nur die Klebezettel des Brainstormings zum neuen Produktdesign speichern, nicht jedoch die daraus folgenden Entwürfe, klappt das nicht.

### Lücken

Wer bereits mit anderen Web-Whiteboards gearbeitet hat, dürfte in Freeform einige Funktionen vermissen. Die App verzichtet auf Vorlagen, mit denen man beispielsweise das Raster für SWOT-Analysen zur Strategieentwicklung mit einem Klick einfügen kann. Stattdessen muss man es selbst zeichnen. Damit Gruppenarbeitsphasen sich nicht endlos hinziehen,

wäre ein Timer hilfreich, der die verbleibende Zeit anzeigt.

Eine Kommentarfunktion haben wir ebenfalls vermisst. Man könnte seine Meinung oder Rückfrage auf einem Klebezettelchen hinterlassen. Das birgt jedoch insbesondere bei vielen Boardinhalten das Risiko, dass der Kommentar untergeht, spätestens beim PDF-Export. Auf Boards anderer Anbieter kann man einzelne Inhalte ausblenden. Eine Versionierung bietet Apple ebenfalls nicht an. Auch eine Agenda mit anklickbaren Links, die zu bestimmten Board-Bereichen führen, fehlt.

### Fazit

Für Unternehmen taugt Freeform durch die Begrenzung auf Apple-Geräte ohnehin meist nicht. Außerdem fehlen allerlei Funktionen für die Zusammenarbeit, die man aus anderen Web-Whiteboards kennt. Dennoch macht die App vor allem auf einem iPad in Kombination mit einem Stift richtig Spaß: Allerlei Gedanken und Scribbles landen auf der Leinwand, um sie bei Bedarf mit anderen weiterzuspinnen. Wenn Apple an den beschriebenen Stellen noch nachlegt, könnte Freeform sich zur ausgewachsenen Whiteboard-App entwickeln und zur Konkurrenz für Canva, Figjam & Co. werden. (abr@ct.de) **ct**

## Apple Freeform

### Whiteboard-App

Hersteller, URL	Apple, apple.com
Systemanf.	iOS 16.2, iPadOS 16.2 und macOS Ventura 13.1
Preis	gratis



# Filmsammlungen im Griff

## Fünf Filmverwaltungen für Desktop und Smartphone im Test

**Sie haben den ganzen Schrank voller DVDs und Blu-rays, dazu noch Dutzende Filme auf iTunes oder Festplatten und verlieren den Überblick? Verwaltungsprogramme für Filme bringen Ordnung in Ihre heterogene Sammlung: Im Test beweisen fünf Programme, wie gut das klappt.**

Von Hartmut Gieselmann

**V**or 20 Jahren hatten es Filmsammler noch einfach und konzentrierten sich auf DVDs. Heutzutage müssen sie aber ein halbes Dutzend Medien und Anbieter im Blick behalten. Spätestens, wenn die

Sammlung vierstellig wird, kommt man um ein übergreifendes Verwaltungsprogramm kaum noch herum, will man den ein oder anderen Doppelkauf vermeiden. Selbst Serienjunkies, die von Netflix oder Disney+ streamen, können ihre bereits angeschauten Staffeln protokollieren. Und auch wer endlich Platz schaffen und seine angesammelten Discs verkaufen will, behält mit einer Software besser den Überblick.

Für den Test haben wir fünf plattformübergreifende Datenbanksysteme ausgewählt, die sowohl auf Desktoprechnern oder im Browser laufen als auch eine mobile App zum Überblick über den Filmbestand und zum Scannen neuer Titel anbieten. So müssen Sie die ganzen Informationen zu Filmen und Serien nicht von Hand eintippen, sondern können die Daten bequem von einem Server laden.

Filmotech von Pascal Pluchon ist die einzige Freeware-Filmverwaltung. Invelos verlangt für seinen unter Windows laufenden „DVD Profiler 4.0“ einmalig 15 Euro und für die zugehörige Mobil-App 3,50 Euro. Die dänischen Spezialisten von Binnerup Consult bieten die Grundversion von „My Movies 5“ kostenlos für Windows an, die Mac-Version namens „My Movies 2 Pro“ kostet 24 Euro, die Mobil-App „My Movies 4 Pro“ 19 Euro.

Der US-Anbieter Collectorz vertreibt die Mobil-Version „CLZ Movies“ und den Browserzugang „Movie Connect“ nur im Abo, für die 1,49 und 3 Euro/Monat fällig werden. iCollect Everything hat Verwaltungsprogramme wie „iCollect Movies“ und die „Movie Database“ für viele verschiedene Produktgruppen im Angebot. Die Film-Apps kosten einmalig 12 Euro für die Mobilversion und 25 US-Dollar für den

zugehörigen Desktopableger namens „Collectors“ von Sort it! Apps. Außen vor ließen wir „Readerware 4“, weil die Desktopversion bei einer Stichprobe keinerlei Filmübereinstimmungen fand und die Mobil-App keine Verbindung zum Desktopserver aufbauen konnte.

### Datenbankqualität

Wer schon mal einen Abspann im Kino gesehen hat, weiß, dass Filme unzählige Angaben umfassen: vom Studio und Erscheinungsjahr über Regisseure, Darsteller, Kameraleute, Komponisten und so weiter. Die will niemand von Hand abtippen. Hinzu kommen spezifische Formatangaben für eine Disc- oder Streamingversion: Sprachen, Tonformate, Untertitel, Auflösung, Seitenverhältnis, Farbtiefe, Lauflänge und Extras. Obendrein unterscheiden sich die Angaben von Land zu Land. Eine Disc hat in Deutschland womöglich nur Stereoton, die US-Version hat hingegen eventuell noch eine Dolby-Atmos-Spur und läuft im Extended Cut 20 Minuten länger.



**Mit dem Smartphonescanner bekommen Sie selbst große Sammlungen ruckzuck in Ihre Datenbank. Besonders schnell und fehlerfrei klappt das bei My Movies.**

Wer all diese Daten up to date halten will, muss sehr viel Arbeit in seine Film-datenbank investieren. Amazon unterhält die Internet Movie Database (IMDb), die wohl weltweit größte Filmdatenbank. Die IMDb weiß zwar über Filme, Serien, Schauspieler und Studios Bescheid, enthält jedoch keine Daten zu verschiedenen Disc- oder Streamingversionen in unterschiedlichen Ländern. Diese Zusatzangaben müssen sich die Hersteller der Verwaltungsprogramme selbst zusammen-suchen.

Collectorz nutzt beispielsweise die umfangreichen Filmangaben aus der IMDb und ergänzt sie mit eigenen Discangaben, die aber lückenhaft und zuweilen sogar falsch sind. Die Folge ist eine zuge-müllte Datenbank mit zusammengeklaubten Infos. Wenn Ihr Film keine eindeutige Kennzeichnung hat (UPC/EAN oder IMDb-Kennung), ist die Chance groß, dass Sie einen falschen Eintrag erwischen.

My Movies von Binnerup gleicht seine Filmdaten zwar auch mit der IMDb ab, geht bei Datenbankergänzungen zu Discformaten aber wesentlich rigider vor als Collectorz und hält fehlerhafte Angaben auf einem Minimum. Nutzer können ihre eigenen Ergänzungen und Berichtigungen zur Server-Datenbank hochladen und erhalten dafür Punkte, mit denen sie unter Windows weitere Programmefunktionen freischalten. Das System klappt ausge-sprochen gut und der Support ist überaus eifrig. Ein von uns gemeldeter fehlender Film wurde innerhalb von zwei Tagen ergänzt, ein Fehler nach drei Tagen korri-giert.

Das kostenlose Filmotech gleicht seine Datenbank mit dem Filmarchiv TMDb ab (The Movie Database). Die ist nicht ganz so umfangreich bestückt wie die IMDb. Der Entwickler iCollect betreibt eine eigene kleine Filmdatenbank, die jedoch sehr lückenhaft gefüllt ist und bereits bei einer Stichprobe mit 50 Filmen fast jeden dritten Titel nicht erkannte.

Invelos unterhält für den DVD Profiler eine eigene riesige Datenbank, die weltweit alle Discveröffentlichungen auf dem neusten Stand hält. Bei unseren Stichproben fanden wir keine Fehler, nur ganz we-nige Discausgaben fehlten. Allerdings gilt dies nur für die Windowsversion: Die mo-bile iOS-App greift offenbar auf einen an-deren Datenbestand zu, dem einige Ein-träge fehlten. Zudem kann der DVD Pro-filer nur Discs, aber keine digitalen Stream-ing-Versionen verwalten.

### Export von Apple TV

Apple ist einer der größten Anbieter von digitalen Streamingfilmen. Die Prä-sentation der eigenen Mediathek ist in der Apple-TV-App aber unübersicht-lich. Sie können eine Liste Ihrer iTunes-Filme jedoch auch in eine Tabelle und von dort als CSV-Datei exportieren, um sie in Movie Connect von Collectorz oder Filmotech zu importieren und von dort aus eventuell an My Movies weiter-zureichen.

Rufen Sie dazu Ihre Filmmediathek in der TV-App unter macOS auf. Wech-seln Sie über das Menü „Darstellung“ in die Listenansicht und klicken mit der rechten Maustaste auf die Spaltenbe-zeichnungen. Nun können Sie sich die gewünschten Spalten anzeigen lassen: Titel, Regisseur und so weiter. Die Liste zeigt ihnen sogar an, welche Filme Sie bereits gesehen haben, und welche noch nicht. Das Produktionsjahr wird jedoch häufig falsch angegeben. Die langen Beschreibungstexte lassen Sie aus. Anschließend markieren Sie die Liste mit cmd+A und fügen Sie per Copy & Paste in eine Tabellenkalkula-tion ein.

Die TV-App gibt die Laufzeiten im Format hh:mm an, diese müssen Sie für Filmotech und Collectorz in eine Minu-tenzahl umwandeln. Markieren Sie dazu in der Tabellenkalkulation Numbers die Laufzeitfelder, ändern deren Datenfor-mat in „Dauer“ und markieren Sie unter „eigene Einheiten“ nur das „min“ mit dem Stil „0“. Ändern Sie in der Spalte „Kaufdatum“ das Format in Datum dd:mm:yyyy ohne Zeitangabe. Schauen Sie bei den Regisseuren eventuell nach Einträgen „Unknown“ und korrigieren Sie diese. Wenn Sie die Titel, Genres und Jahresangaben geprüft haben, ex-portieren Sie die Tabelle als CSV.

Zu den digitalen Filmen, für die man bei Apple, Amazon und YouTube Dauer-lizenzen kaufen kann, hält bislang keines der Programme Informationen zu Bild- und Tonformaten bereit. Diese muss man manuell eintragen – und später korrigie-ren, wenn etwa Apple eine HD-Version mit Stereoton durch eine 4K-Fassung mit Dolby Atmos ersetzt.

Praktischer ist es, wenn man digitale Filme in einem Verzeichnis auf der Fest-

platte liegen hat. Sowohl My Movies als auch Filmotech scannen die Verzeichnisse automatisch, und nehmen alle erkannten Titel auf. Bei My Movies muss jeder Film in einem eigenen Unterordner stehen, dann klappt es auch mit DRM-geschützten Downloads von Apples TV-App. Downloads von Amazon Prime lassen sich allerdings nicht importieren.

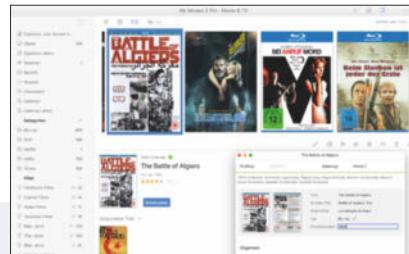
### Flinke Scanner

Zur eindeutigen Identifikation einer Film-disc verwenden alle Anbieter die EAN/UPC-Nummern, die auf der Verpackung unter dem Strichcode aufgedruckt sind. Wer die 13-stelligen Nummern nicht abtippen will, kann den Strichcode mit der Smartphone-App der Verwaltungsprogramme scannen. Diese übertragen die Daten entweder per WLAN direkt zum Desktopprogramm (DVD Profiler), oder synchronisieren sie über die Cloud zum eigenen Nutzerkonto (Collectorz, iCollect, My Movies).

Im Test klappte das Scannen aber nicht immer: Die magere Mobil-App von Filmotech zeigt auf dem Smartphone lediglich die Desktopdatenbank an, bietet aber keine Scan- oder Editierfunktionen. Beim DVD Profiler konnte die vier Jahre alte iOS-App die Kamera auf einem iPhone 14 Pro nicht scharf stellen und scannte nichts. Die Android-Version ist aus dem Google Play Store mittlerweile verschwunden. Die Movie Database von iCollect konnte zwar scannen, erkannte aber viele Filme nicht und hatte sie nicht in ihrer Datenbank.

Wesentlich besser klappte es mit CLZ Movies von Collectorz. Die App scannte die Filme sehr schnell und ordnete ihnen Einträge zu. Zwar stimmten die eingebundenen Angaben der IMDb, die Formatangaben zu den Discs fehlten jedoch größtenteils oder waren falsch zugeordnet.

Am komfortabelsten scannte My Movies 4. Kam eine Disc nicht aus dem voreingestellten Hauptland (Deutschland), fragte die App nach, welche der möglichen Discs aus anderen Ländern gemeint sind. Aus einer großen Testsammlung mit knapp 800 Discs erkannte die App bis auf einzelne Ausnahmen alle Filme und ordnete sie richtig zu. Einzig eine Ausgabe von Russ-Meyer-Filmen bereitete Probleme. My Movies weigerte sich, acht mit FSK 16 und FSK 18 eingestufte Titel aufzunehmen – weil die Nutzungsbedingungen der App-Stores angeblich erotische Inhalte verbieten würden. Eine andere Edition mit in-



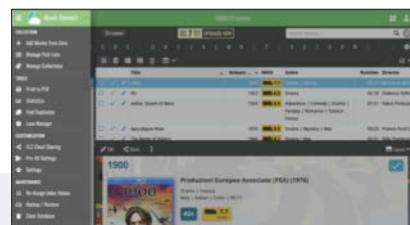
### Binnerup „My Movies“

Binnerup bietet My Movies für verschiedene Plattformen an. Die Windows-Version 5 ist kostenlos und lässt sich mit Punkten erweitern, die Sie entweder kaufen oder für Datenbankeinträge erhalten. Das ist allerdings nur notwendig, um mit My Movies Filme direkt abzuspielen, oder um eigene private Filme aufzunehmen. Die macOS-Version 2 kostet 24 Euro und kann Filme direkt per VLC-Player starten, mit Käufen von Apple TV klappt das nicht. Die Windows-Version kann darüber hinaus auch iTunes steuern, verlangt dazu aber die Login-Daten vom Anwender. Wir raten von der Weitergabe dringend ab, da Binnerup damit Zugriff auf Ihren kompletten Apple-Account erhält.

Die Apps können Dateiverzeichnisse nach Filmen durchsuchen und manuelle Einträge aufnehmen. Mit einer angeschlossenen Kamera lassen sich Strichcodes von Disc-Hüllen scannen. Das klappt mit der Mobil-App (Android, iOS) „My Movies 4 Pro“ für 19 Euro allerdings deutlich besser. Der Scanner war der beste im Test und erkannte bis auf wenige Ausnahmen selbst Raritäten akkurat und sicher. Alle drei Apps synchronisieren ihre Daten mit den Servern von Binnerup.

My Movies übernimmt Filmdaten von der IMDb. Fehlende Disc-Angaben ergänzen die Nutzer, Streaming-Formate können sie nur in der Mobil-App eintragen. Dank eines rigiden und ausgeklügelten Prüfsystems klappt das hervorragend, sodass die Datenbank zwar keinen vollständigen, aber sehr gut gepflegten Eindruck macht.

- ⬆️ toll gepflegter Datenbestand
  - ⬆️ gute Bedienung, flotter Scanner
  - ⬇️ eingeschränkte Datenübernahme
- Preise: kostenlos (Windows)  
bis 24 Euro (macOS)



### Collectorz „Movie Connect“ und „CLZ Movies“

Collectorz bietet für Smartphones die Mobil-App „CLZ Movies“ und für Desktoprechner die Browserversion „Movie Connect“ an. Beide lassen sich sieben Tage testen, danach werden Abgebühren fällig. Darüber hinaus bietet Collectorz eine Stand-alone-Version für Windows an, die jedoch vom Hersteller nicht weiter gepflegt wird.

App und Browser synchronisieren ihre Daten über den Online-Account. Beide Apps gleichen die Filminformationen mit der IMDb ab, Angaben zu Bild und Ton verschiedener Disc-Ausgaben ergänzt Collectorz aus seinen Datenbeständen. Im Test wurden zwar viele Filme erkannt, allerdings stellten wir auch zahlreiche Fehler oder Falszuordnungen fest. Oftmals fielen diese erst auf den zweiten Blick auf, weil die Fehleinträge die richtigen Cover anzeigen.

Die Mobil-App scannt Disc-Hüllen schnell ein und lässt sich auch sonst flott bedienen. Statistiken geben interessante Infos zur Filmsammlung. Im Browser lassen sich zudem Doublets schnell finden.

Bemerkenswert sind die umfangreichen Importfunktionen, die anders als bei My Movies keine leere Datenbank benötigen. Aufgrund des schlecht gepflegten Datenbestands muss man aber besonders beim automatisierten Import von CSV-Listen und Filmenamen ohne IMDb-Kennung aufpassen, dass Collectorz nicht den falschen Eintrag erwischt. Bei der Verlinkung sollten Sie keinesfalls die grüne Taste zur automatischen Übernahme klicken.

- ⬆️ umfangreiche Importfunktionen
  - ⬇️ zugemüllter Datenbestand
  - ⬇️ laufende Abo-Gebühren
- Preise: 1,49 Euro/Monat (mobil) und 3 Euro/Monat (Browser)



## Invelos „DVD Profiler“

Trotz seines Namens nimmt der DVD Profiler auch Blu-ray Discs und UHDs auf. Digitale Filme lassen sich mit der Software allerdings nicht verwalten.

Die Windows-Software für 15 Euro stammt aus dem Jahr 2017 und wurde seitdem nicht erneuert. Der Datenbestand ist allerdings up to date. Die Filme lassen sich am besten durch Eingabe der UPC-Nummer unter dem Strichcode hinzufügen. Der DVD Profiler erkannte bei unserer Stichprobe selbst seltene Discs und führte neben umfangreichen Filmangaben alle Bild- und Tonformate korrekt auf. Zahlreiche Diagramme verraten interessante Statistiken zur Discsammlung.

Das Bedienkonzept wirkt mit seinen verschiedenen Fenstern altbacken, moderne Listen-Ansichten mit konfigurierbaren Filtern wie bei „My Movies“ sind nicht vorgesehen. Neue Funktionen lassen sich durch Plug-ins hinzufügen, so etwa den Export für Access-Datenbanken. Ansonsten sind die Import- und Exportfunktionen sehr dürftig.

Die zugehörige englischsprachige Mobil-App für 3,50 Euro wurde ebenfalls seit fünf Jahren nicht mehr erneuert und ist nur noch für iOS erhältlich. Im Test konnte der Scanner auf einem iPhone 14 Pro die Kamera nicht scharf stellen und somit keine Strichcodes von Disc-Hüllen scannen. Die Datenbestände synchronisiert das Smartphone mit der Windows-App über eine direkte IP-Verbindung im LAN. Über eine optionale Onlineverbindung können Freunde die Sammlung im Browser ansehen.

- ⬆️ sehr gute Disc-Datenbank
  - ⬇️ veraltete Software ohne Digitalfilme
  - ⬇️ mobiler Scanner funktioniert nicht
- Preis: 15 Euro (Windows) und 3,50 Euro (iOS)



## iCollect Everything „iCollect Movies“, „Movie Database“ / Sort it! Apps „Collectors“

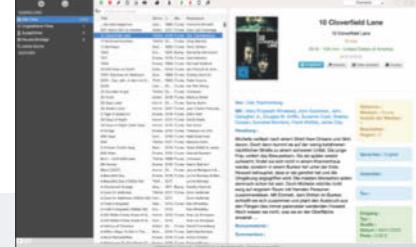
Der Vertrieb der Movie Database ist verworren: Zunächst lädt man die kostenlose mobile App für Android (iCollect Movies) oder iOS (Movie Database: Blu-ray 4K DVD) herunter. Die zugehörige Desktopversion von Sort it! Apps ist unter dem „Collectors-Reiter“ ganz unten für 25 US-Dollar zu finden. Nach dem Kauf schickt der Hersteller dem Kunden Download-Links zu den Desktop-Apps per Mail zu.

Sämtliche Filmtitel werden in der Onlinedatenbank des Herstellers gespeichert. Ein Import oder Export fremder Listen oder Datenbanken ist nicht möglich. iCollect Everything bietet über ein Dutzend verschiedene Sammelkategorien an.

Die Funktionen für Filmsammlungen fallen sehr dürftig aus und bleiben selbst hinter dem kostenlosen Filmotech zurück. Zwar konnten wir Strichcodes scannen, von knapp 50 Filmen erkannte die Mobil-App aber rund ein Drittel nicht, für ein weiteres Drittel waren die Einträge unvollständig oder falsch – insbesondere bei UHDs.

Der Hersteller konzentriert sich auf den US-amerikanischen Markt und berücksichtigt keine deutschen Beschreibungen oder Alterseinstufungen. Die Datenbank reagierte bei Abrufen zuweilen träge.

- ⬇️ lücken- & fehlerhafte Daten
  - ⬇️ kein Import oder Export
  - ⬇️ dürftiger Funktionsumfang
- Preise: 12 Euro (mobil) bis 25 US-Dollar (Windows/macOS)



## Pascal Pluchon „Filmotech“

Filmotech ist eine kostenlose Datenbank, insbesondere für Personen, die ihre Filme verleihen oder Handel mit ihnen treiben. Anhand des Filmtitels lassen sich lediglich generelle Angaben zum Film (Darsteller, Regisseur, Jahr, etc.) sowie ein Coverbild und ein Link zum Trailer aus der TMDb in verschiedenen Sprachen laden.

Spezielle Angaben zur Disc, etwa zu Sprachen, Untertiteln und Tonformaten, muss man von Hand eingeben, ebenso wie Kauf- und Verleihdaten sowie Preise. Zusatzinformationen wie Kamera, Schnitt, Produktion finden keinen Platz. Eigene neue Felder konnten wir nicht anlegen. Meist stehen mehrere Cover zur Wahl, die jedoch selten mit den Bildern der Disc-Hülle übereinstimmen.

Die Software hat diverse Import- und Exportfunktionen, darunter Tabelle in XML und CSV. Ebenso lassen sich Festplattenverzeichnisse anhand verschiedener Dateiendungen von Filmen durchsuchen.

Die begleitende mobile App kann lediglich die auf einem Desktoprechner angelegte Filmdatenbank laden und die Filmeinträge auflisten sowie filtern. Dazu startet man im Desktopprogramm einen Datenbankserver und tippt die dort angezeigte IP-Adresse und Portnummer in die App ein. Es lassen sich weder neue Einträge anlegen, vorhandene bearbeiten oder Strichcodes scannen. Wer die unauffälligen Werbeinblendungen ausblenden möchte, zahlt 5 Euro.

- ⬆️ flexible Import und Export
  - ⬇️ kein Strichcodescanner
  - ⬇️ TMDb-Daten ohne Disc-Formate
- Preis: kostenlos

haltsgleichen Russ-Meyer-Filmen zeigte die App jedoch klaglos an.

### Im- und Export

Einige der getesteten Apps wurden bereits seit mehreren Jahren nicht mehr mit Programmupdates versorgt – der DVD Profiler zuletzt 2017. Es besteht die Gefahr, dass die Hersteller die Weiterentwicklung irgendwann einstellen. Deshalb ist es unabdingbar, dass die Filmverwaltung Ihre Datensammlung in einem allgemeinen Format exportieren und möglichst von anderen Programmen importieren kann.

Bei iCollect sind weder Import noch Export möglich – ein Ausschlusskriterium. Der DVD Profiler kann lediglich Datenbanken von Vorgängerversionen übernehmen und seinen Datenbestand als XML- oder Access-Datenbank (per Plug-in) exportieren. My Movies ist beim automatisierten Import wählerisch: Es akzeptiert nur Datensätze mit einer eindeutigen EAN/UPC- oder IMDb-Nummer und importiert diese nur in eine frische neue Datenbank. Spätere Einträge – etwa von

iTunes-Filmen – muss man einzeln manuell vornehmen oder aber die Filme herunterladen und in einem Dateiordner scannen.

Bei Filmotech klappt der Im- und Export ohne solche Einschränkungen. In der Desktopsoftware kann man simple CSV-Listen (Comma Separated Values) importieren. Die richtige Reihenfolge der Spalten ist aber nicht offensichtlich. Man erkennt sie, wenn man aus Filmotech eine CSV-Datei exportiert und in einer Tabellekalkulation auf die Importdatei überträgt. Sind nur Listen mit Filmtiteln vorhanden, muss man jeden Film einzeln dem richtigen TMDb-Eintrag zuordnen. Einen Batch-Import erlaubt Filmotech nur, wenn die Filmdateien in einem Verzeichnis auf Festplatte liegen.

Die umfangreichsten Import- und Exportfunktionen bietet Movie Connect von Collectorz. Es erlaubt im Browser jederzeit den Import von CSV-Listen, ermöglicht eine freie Spaltenzuordnung und versucht sogar, die Einträge automatisch mit den passenden IMDb-Einträgen zu verlinken.

Das geht jedoch häufig schief, weil die Collectorz-Datenbank vor Fehleinträgen strotzt. Hier muss man jeden Treffer einzeln prüfen. Das geht mit ein paar Klicks aber immer noch schneller als bei Filmotech oder My Movies. Für 200 Titel sollte man rund eine Stunde rechnen.

### Filter und Statistiken

Hat man alle Filme in seiner Datenbank, kann man die Sammlung filtern und neu sortieren: Welche Filme habe ich aus den 60ern? Wo hat Robert de Niro mitgespielt? Welche Filme haben in der IMDb mindestens 8 Punkte? Derartige Fragen beantwortet My Movies in der macOS-App besonders komfortabel. Ebenso gibt der DVD Profiler umfangreiche Statistiken zu den gesammelten Discs an. Collectorz und Filmotech zeigen immerhin einige Grundinformationen wie Genres und Produktionsjahre an. Bei iCollect ist hingegen Fehlanzeige: Die Desktop- und Mobil-Apps verzichten auf Filter und statistische Überblicke.

Wer Freunden, Leih- oder Kaufinteressenten einen Überblick geben will,

## Warum eigentlich immer noch Discs?

Digitale Streamingangebote sind zwar auf dem Vormarsch, trotzdem wurden 2021 in Deutschland bei den Filmverkäufen noch immer 60 Prozent der Umsätze mit Discs (DVD, Blu-ray und UHD) erwirtschaftet und 40 Prozent mit Dauerlizenzen für Streamingfilme (Electronic-Sell-Through, EST).

Solche ESTs bieten in Deutschland Amazon, Apple und YouTube an; YouTube betreibt sein EST-Geschäft allerdings nur nebenbei und schreckt Interessierte mit deutlich höheren Preisen ab. Apple sticht mit der größten Auswahl an 4K-Filmen und Atmos-Tonspuren heraus. Zudem lassen sich die Filmkäufe auch als Liste exportieren und in die Programme von Filmotech und Collectorz laden. Amazon und YouTube bieten das nicht an, bei diesen Diensten muss man jeden Titel einzeln in eine Datenbank übertragen.

Wichtigster Unterschied zum Kauf einer Film-Disc: Bei den ESTs steht der „Kauf“ lediglich für eine dauerhafte Nutzungserlaubnis. Wenn ein Film später aufgrund sich ändernder Rechte aus dem Onlineshop verschwindet, können Käufer in der Regel zwar weiterhin auf die

Streams zugreifen. Es besteht jedoch die Gefahr, dass die Firmen irgendwann einmal komplett aus dem digitalen Filmvertrieb aussteigen und ihr Onlineangebot einstellen – wie zuletzt Sonys Playstation-Sparte. Seit September 2022 können dort ehemalige Käufer auf 300 Titel von Studio Canal nicht mehr zugreifen.



**Spezialanbieter wie Alive, Eureka, die Murnau-Stiftung oder Plaion bemühen sich um die Rechte vergessener Filme, restaurieren diese und veröffentlichen Sie in schmucken Sonderausgaben in kleiner Auflage auf Disc, die meistens deutlich besser aussehen als die digitalen Streamingversionen.**

Verglichen mit Filmen auf Blu-ray Disc oder UHD ist zudem die Bild- und Tonqualität bei vielen ESTs schlechter, weil die Streaminganbieter aus Kostengründen mit niedrigeren Datenraten arbeiten. Selbst wenn Sie einen digitalen Film in 4K mit Dolby Vision sehen, erreicht dieser nicht die Bildqualität einer UHD. Deren Kopien auf Festplatte wären allein schon wegen der immensen Datenmengen von manchmal 100 GByte pro Film nicht praktikabel – selbst wenn man Kopierschutz- und Urheberrechtsfragen außen vor lässt. Nicht zuletzt knausern die Streaminganbieter oft bei den Tonspuren und lassen Extras wie Audiokommentare weg, die auf den Discs zu finden sind.

Filmenthusiasten kommen auch in Zukunft nicht umhin, ihre Sammlungen sowohl mit ESTs als auch mit Discs zu bestücken. Denn manche Filme bekommt man nur als digitalen Stream, andere nur auf Disc. Insbesondere Titel von unabhängigen Filmemachern, kleineren Anbietern aus Europa oder inzwischen aufgelösten Studios sind bei den großen US-Streamingplattformen nicht zu finden.

kann ihnen bei My Movies einen passwortgeschützten Browserzugang geben, oder klassische PDF-Listen zum Ausdrucken zusammenstellen. Selbiges klappt auch mit dem DVD Profiler. Movie Connect von Collectorz kann darüber hinaus Doublets heraussuchen und detaillierte Statistiken anzeigen.

## Fazit

Die Qualität eines Verwaltungsprogramms steht und fällt mit der verknüpften Film-datenbank. Die Apps von iCollect Everything fallen hier stark ab und sind nicht konkurrenzfähig. Offensichtlich wurden sie primär für Leute entwickelt, die allen möglichen Kram auf eBay verkaufen wollen – auf die Bedürfnisse von Filmsamm-

lern gehen sie kaum ein. Da greift man besser zum kostenlosen Filmotech, das seine Grundfunktionen solide umgesetzt hat, wenn man auch für Formatangaben seiner Filme selbst in die Tasten greifen muss und die Mobil-App lediglich die Sammlung anzeigt.

Der DVD Profiler von Invelos wartet mit einer großen, sehr gut gepflegten Disc-Datenbank auf. Doch die Windows-Software ist veraltet und hat den Anschluss an die digitalen Filmangebote verpasst. Collectorz hält seine Apps zwar mit den Abo-Einnahmen up to date, die große Datenbank ist jedoch schlecht gepflegt und strotzt vor Fehleinträgen. Immerhin kann man im Browser die sieben-tägige Probezeit gut zum Im- und Export

seiner Filme nutzen, um Daten aus ver-schiedenen Quellen zusammenzu-führen.

Den mit Abstand besten Eindruck hinterlässt My Movies: Die Datenbank wird von den rund eine Million Kunden penibel gepflegt und der Support reagiert schnell auf Anfragen, Fehler und Ergän-zungen. Abgesehen von kleineren Feh-lern überzeugen die Apps mit übersicht-licher Bedienung und flexiblen Filter-funktionen sowie dem besten Scanner der zugehörigen Mobil-App, mit der wir eine Sammlung mit knapp 800 Discs in nicht mal zwei Stunden fehlerfrei einlesen konnten. Probieren Sie einfach mal die kostenlosen Probeversionen mit 50 Filmen aus. (hag@ct.de) ct

## Filmverwaltungsprogramme

Name	My Movies	Movie Connect	DVD Profiler 4.0	iCollect Movies	Filmotech
Hersteller	Binnerup Consult	Collectorz	Invelos	iCollect Everything	Pascal Pluchon
Webseite	mymovies.dk	collectorz.com	invelos.com	icollecteverything.com, sortitapps.com	filmotech.info
Sprachen	Deutsch, Englisch	Englisch	Deutsch, Englisch	Englisch	Deutsch, Englisch
Formate: Discs / Digital	✓ / ✓	✓ / ✓	✓ / –	✓ / ✓	✓ / ✓
Medien	alle Discformate, VHS, iTunes, Amazon, Google Play	alle Discformate, VHS, Apple, Amazon, Google Play, YouTube, Disney, Netflix	DVD, Blu-ray, UHD	alle Diskformate, digitale Kopien, VHS	alle
Synchronisation	Cloud	Cloud	eigener Server / Cloud	Cloud	eigener Server
Filmdatenbank	IMDb	IMDb	Invelos	iCollect Everything	TMDb
Testversion	bis 50 Filme, Windows-Vollversion	7 Tage	bis 50 Filme	bis 50 Titel, bis 21 Tage	Vollversion
Desktop-App	My Movies	Movie Connect	DVD Profiler	Collectors	Filmotech
Systeme	Windows, macOS, tvOS	Browser	Windows	Windows, macOS	macOS, Windows
Versionen	Windows: 5.40, macOS: 2.11	vom 7.7.2022	4.00 von 2017	1.9	3.100
Browser-Anzeige	✓	✓	✓	✓	–
Trailervorschau	aktuelle Filme	✓	✓	–	✓
Dateiordner-Scan	✓	–	–	–	✓
Importformate	andere Anwendungen (online), CSV/TXT (nur UPC/EAN-Nummern)	TXT, CSV, My Movies, DVD Profiler, IMDb, Movie Collector, Movie Connect, etc.	DVD Profiler	–	CSV, XML, Titelliste, AMC
Exportformate	XML, PDF (online), SQLite Datenbank	TXT, CSV, XML, PDF	XML, Access-Plug-in	–	CSV, XML, Media Center
Statistiken	flexible Kategorienfilter	Formate, Jahre, Genres, Regisseur, Darsteller	Genres, Studios, Disc-Formate, Bewertungen, Kaufdaten u. a.	–	Jahr, Laufzeit, Genre, Medium, Bewertung, Käufe u. a.
Besonderheiten	Wiedergabe per VLC-Player	Duplikatfinder	Plug-in Erweiterungen	Ablösung durch iCollect Everything	–
Mobil-App	My Movies 4 Pro	CLZ Movies - Movie Database	DVD Profiler	iCollect Movies, Movie Database: Blu-ray 4K DVD	Gest Films, Filmotech
Systeme	Android, iOS	Android, iOS	iOS	Android, iOS	Android, iOS
Version	Android: vom 28.12.2022, iOS: 4.08	Android vom 18.11.2022, iOS: 7.5.3	iOS: 4.04 von 2018	Android vom 24.11.2022, iOS: 6.7.2	Android vom 28.11.2022, iOS: 4.5.0
Strichcodescanner	✓	✓	(✓)	✓	–
Filme anzeigen / editieren / anlegen	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / – / ✓	✓ / ✓ / ✓	✓ / – / –
Bewertung	++	⊕	○	⊖⊖	○
Desktop-App	++	⊕	○	⊖⊖	○
Mobil-App	++	⊕	⊖	○	⊖⊖
Infos Filme / Discformate	⊕⊕ / ⊕	○ / ⊖	⊕ / ⊕⊕	⊖ / ⊖	⊖ / –
Strichcode-Scanner	++	⊕	⊖⊖	○	–
Import / Export	○ / ○	⊕⊕ / ⊕	⊖⊖ / ⊖	– / –	⊕ / ⊕
Filter & Statistiken	++	⊕	⊕⊕	⊖⊖	○
Preis Desktop	Windows: kostenlos, macOS: 24 €	3 €/Monat	15 US-\$	25 US-\$	kostenlos
Preis mobil	19 € oder 10,50 €/Jahr	1,49 €/Monat	3,50 €	12 €	kostenlos, ohne Werbung: 5 €
✓ vorhanden	– nicht vorhanden	(✓) funktionierte nicht mit iPhone 14 Pro	⊕⊕ sehr gut	⊕ gut	○ befriedigend
⊕ gut	⊖ befriedigend	⊖⊖ schlecht	⊖⊖⊖ sehr schlecht		

# Zahlen, Daten, Fakten

## Elektroschrott und Recycling

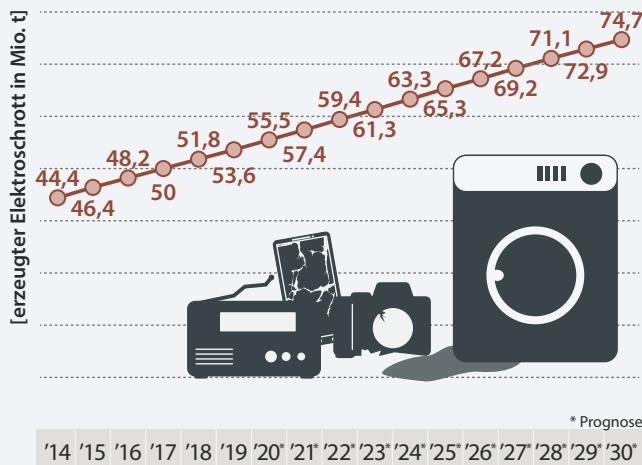
Ende 2022 befragte Bitkom Research im Auftrag des Digitalverbands Bitkom telefonisch 1003 Personen in Deutschland ab 16 Jahren zu ihrem Umgang mit ausrangierten Geräten und Elektroschrott. Die repräsentative Umfrage ergab: Aktuell horten die Deutschen daheim rund 210 Millionen ungenutzte Handys oder Smartphones sowie 49 Millionen ausrangierte Laptops und 26 Millionen Tablets.

Immerhin 44 Prozent der Befragten gaben an, ein Altgerät verschenkt oder verkauft zu haben. Bei Entsorgung und Recycling hapert es. Ab und an landet ein Altgerät sogar im Hausmüll. Durch sachgerechtes Recycling ließen sich seltene Erden, aber auch andere wertvolle Stoffe zurückgewinnen: Allein 3 Tonnen Gold liegen versteckt in den Altgeräten – laut Bitkom in deutschen Haushalten herum.

Die Grafiken auf dieser Doppelseite visualisieren Ergebnisse der Bitkom-Umfrage. Hinzu kommen Diagramme zum internationalen Vergleich von Recyclingquoten. Wichtiger Unterschied: In den letztgenannten Grafiken geht es um Elektroschrott allgemein, also ebenfalls um ausrangierte IT-Geräte, aber auch um Haushaltsgeräte wie Waschmaschinen und Geschirrspüler. (dwi@ct.de) **ct**

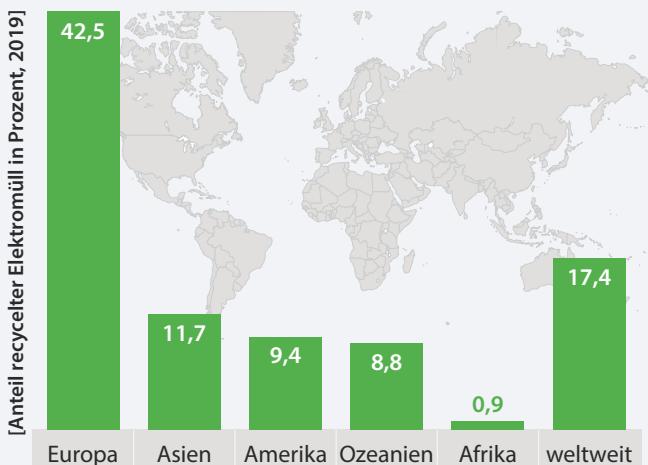
### ► Immer mehr E-Schrott

Für das Jahr 2030 wird eine Erzeugungsmenge von knapp 75 Millionen Tonnen Elektroschrott (IT- und HH-Geräte) weltweit prognostiziert.<sup>1</sup>



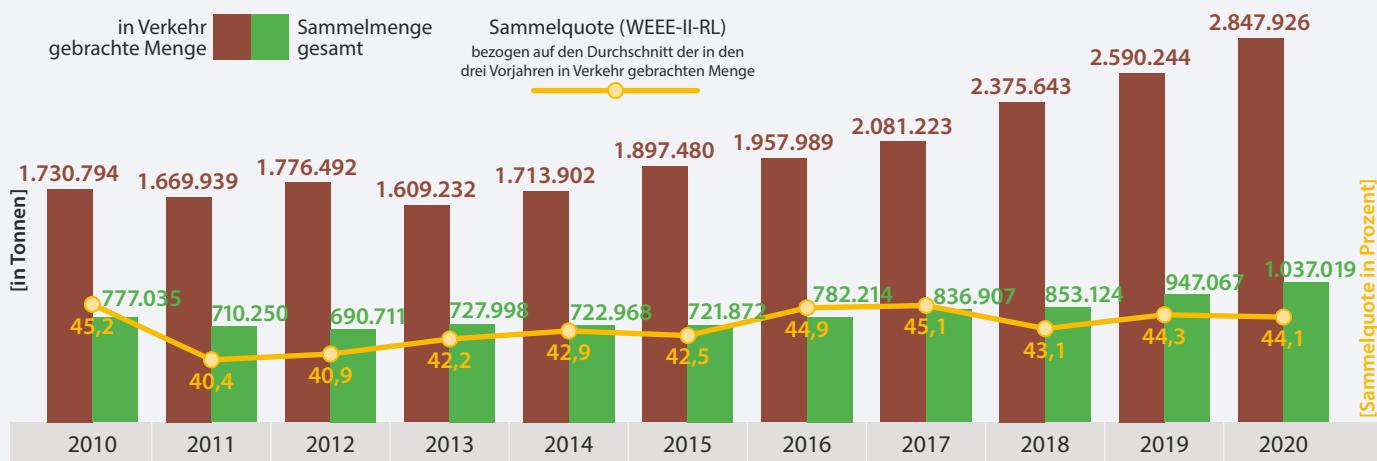
### ► Geringe Recyclingquote

Weltweit werden lediglich 17,4 Prozent des Elektromülls nachhaltig und umweltgerecht recycelt.<sup>1</sup>



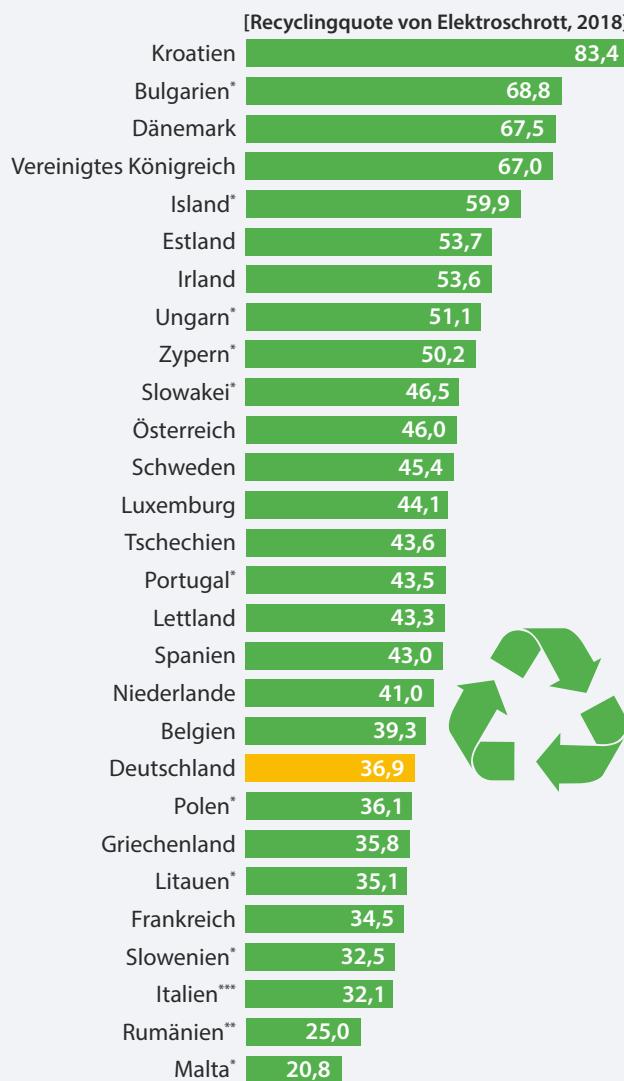
### ► Sammelquote in Deutschland

Für alle Elektro- und Elektronikaltgeräte gilt in der EU seit 2019: Die Menge gesammelter Altgeräten muss mindestens 65 Prozent der in den drei Vorjahren in Verkehr gebrachten Geräte entsprechen.<sup>2</sup>



## ► Quote nach Ländern

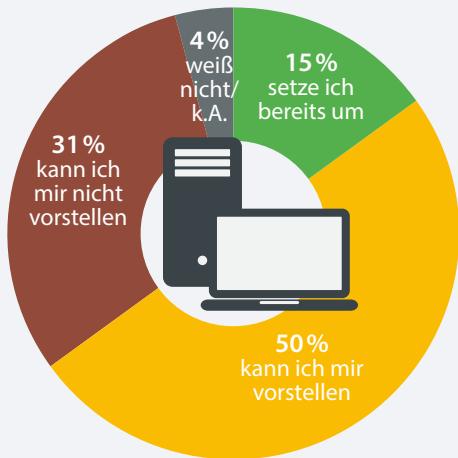
Zwischen den europäischen Ländern gibt es große Unterschiede bei der Recyclingquote von Elektro- und Elektronikschrott.<sup>3</sup>



\* Wert für 2017, \*\* Wert für 2016, \*\*\* Wert für 2015

## ► Refurbished IT

15 Prozent der Deutschen haben 2022 bereits aufbereitete Produkte statt Neuware gekauft, weitere 50 Prozent können sich dies vorstellen.<sup>4</sup>



## ► Ungenutzte Alt-Handys

Während 2014 rund 100 Millionen Alt-Handys in deutschen Schubladen lagen, waren es 2022 rund 210 Millionen Geräte.<sup>4</sup>



## ► Was steckt in Alt-Handys?

Aktuell liegen 210 Millionen Alt-Handys in deutschen Haushalten. Darin stecken allein 3 Tonnen Gold.<sup>4</sup>



## ► Wohin mit dem Altgerät?

Die neue Möglichkeit, ein ausrangiertes Handy beim Discounter abzugeben, wird noch nicht gut angenommen.<sup>4</sup>



# secIT

by Heise

HANNOVER 2023

meet.  
learn.  
protect.

14.–16. März 2023

Inklusive  
IT-Recruiting-Area

heise Jobs  
— IT KOMPAKT —



Aussteller

A<sup>1</sup> Digital

Aagon  
CLIENT MANAGEMENT PLATFORM

ALLGEIER  
CyRis

ALSO  
THE TECHNOLOGY PROVIDER

ARCTIC WOLF

baramundi

bintec elmeg  
infot GROUP

bitkom  
akademie

CONSIST  
Business Information Technology

CORDWARE  
INFORMATIONSCLOUDS

CYBER SAMURAI

»CYBERSENSE

DataGuard

Delinea

GRTNR  
MEET FOR YOUR BUSINESS

heylogin

HORNETSECURITY

IDEE

Infoblox

jamf

LANCOM  
SYSTEMS

Magelan

oneconsult  
together against cyberattacks

opentext™  
Security Solutions

radware

sonatype

SONICWALL

SOPHOS

sysdig

# DIE Kongressmesse für Security-Experten

Entdecken Sie aus erster Hand die neuesten Trends, Produkte und Sicherheitslösungen.

## HIGHLIGHTS

### VORTRÄGE:

**Die neuen quantensicheren Kryptoalgorithmen und die Tücken, sie zu implementieren**  
Klaus Schmeh

**AD-Sicherheit: Goldene Zertifikate für Pentester und Admins**  
Hans-Joachim Knobloch

**Wenn der Deepfake zweimal klingelt**  
Tobias Schrödel, Live-Demonstration

### WORKSHOPS\*:

**Pentest Top 10: Die häufigsten und schwerwiegendsten Lücken und was man dagegen tun kann**  
Jörg Schneider

**Malware und Ransomware – Hintergründe, Erkennung, Reaktion, Schutz**  
Stefan Strobel

\* in Kombination mit einem Tagesticket buchbar

## Jetzt Ticket sichern:



Offizieller Eventpartner



**Bare.ID** **BOSCH** CyberCompare

**energy net** econocom  
Autorisierte Händler

**eset** Digital Security  
Progress. Protected.

**FORTINET**

**FORESCOUT**

**FTAPI**

**ManageEngine**

**mimecast**

**netzlink**

**ninjaOne**

**SVA**

**TANIUM**

**Threema.Work**

**VECTRA** SECURITY THAT THINKS.<sup>®</sup>

**veeAM**

**wiz**

Partner der Recruiting-Area

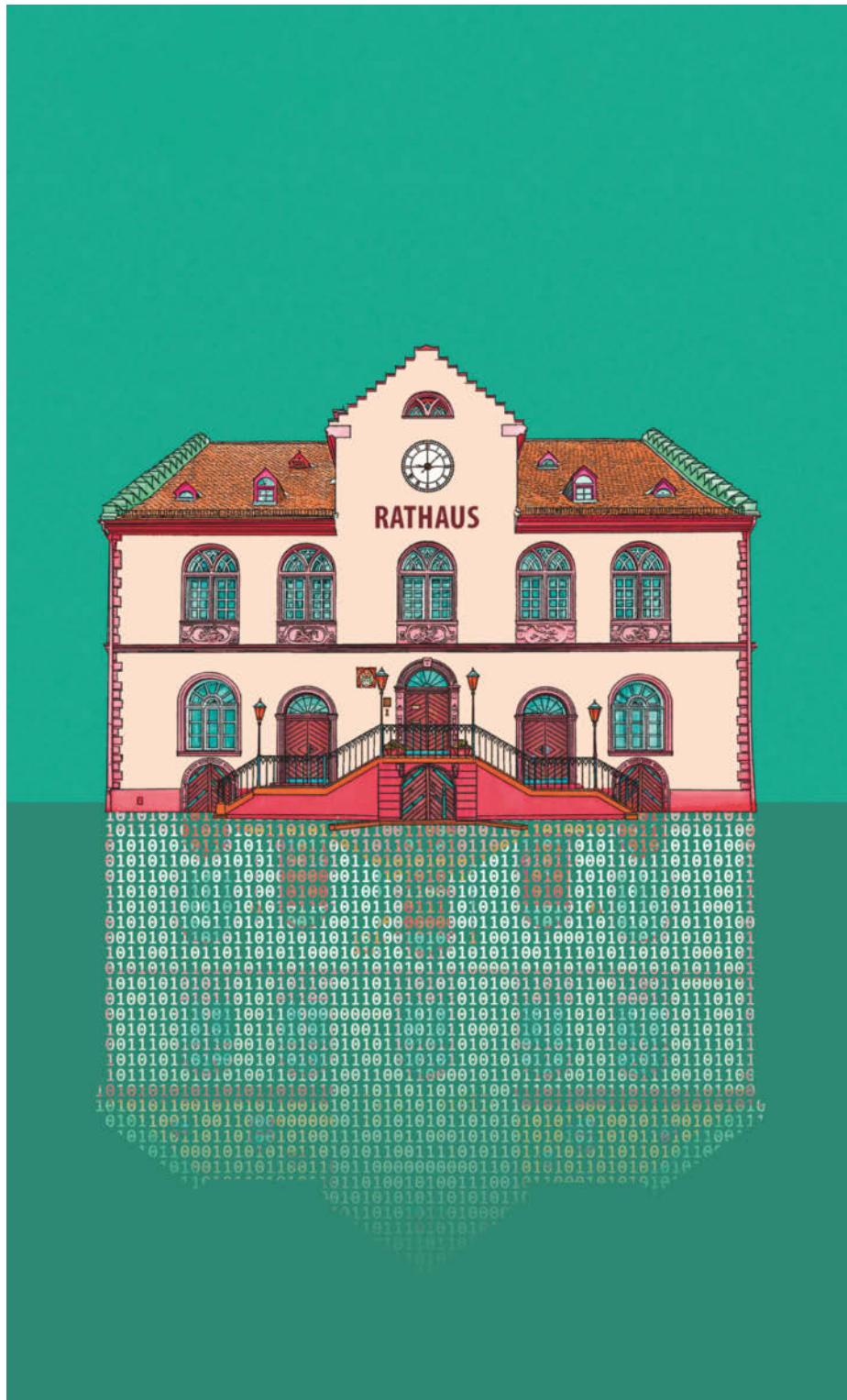
**BWI** IT für Deutschland **CONSIST** **Heise Gruppe** **Tutanota**  
privacy. done. right.

Kooperationspartner

**CISO** ALLIANCE

**NIEDERSACHSEN** DIGITAL

**UVN**  
Unternehmerverbände  
Niedersachsen e.V.



**Parkausweis, Führerschein, Ummeldung & Co.: Wir haben nachgeforscht, was man bei Deutschlands Behörden online erledigen kann und was nicht. Und sind dabei auf Vorreiter wie Nürnberg gestoßen, die beweisen, dass eine digitale, bürgerfreundliche Verwaltung auch in Deutschland möglich ist.**

**Von Jo Bager und Christian Wölbert**

**B**ei dem Stichwort Nürnberg denken die meisten Menschen spontan an Leckereien wie Lebkuchen und Rostbratwürste. Weniger bekannt ist, dass die Frankenmetropole auch beim Thema Digitalisierung glänzt: In einem c't-Ranking zur Digitalisierung der Verwaltung in 32 großen deutschen Städten steht sie ganz oben. Sie bietet 14 der 15 von uns ausgewählten Anträge über das Internet an und lässt damit deutlich größere Städte wie Hamburg und Berlin hinter sich.

Ganz unten in der Rangliste landet Potsdam mit nur einem einzigen Onlineantrag aus unserer Auswahl, der Kfz-Zulassung. Für die restlichen 14 Angelegenheiten gibt es laut Auskunft der Stadtverwaltung bestenfalls ein PDF-Formular zum Herunterladen, Ausdrucken, Unterschreiben und Mailen. Von Ende Dezember bis Mitte Januar war aber nicht einmal das möglich: Wegen „Hinweisen auf eine Cyberattacke“ hatte die Stadtverwaltung die meisten ihrer Server vom Netz getrennt und konnte keine Mails senden oder empfangen.

Die beiden Extrembeispiele Nürnberg und Potsdam zeigen: Wie viel Behördenkram man online erledigen kann, hängt in Deutschland immer noch stark vom Wohnort ab. Denn für den Großteil der Verwaltungsleistungen sind die Städte und Landkreise zuständig, nicht der Bund oder die Länder. Personalausweis, Führerschein, Geburtsurkunde, Wohngeld – für diese und zig andere Dinge muss sich der Bürger an seine Kommune wenden.

Den Anstoß für unser Ranking gab das Onlinezugangsgesetz (OZG): Das 2017 verabschiedete Regelwerk verpflichtete alle deutschen Behörden, ihre Dienstleistungen auch online anzubieten – und zwar

Bild: Thomas Kühnbeck

# Vorbild Nürnberg

**Digitalisierung der Verwaltung:  
32 Städte im c't-Ranking**

flächendeckend und spätestens bis zum 31.12.2022. Eigentlich dürfte es Digital-Nachzügler wie Potsdam nun also gar nicht mehr geben.

Doch schon vor Jahren zeichnete sich ab, dass die Behörden das OZG-Ziel nicht erreichen werden. Inzwischen ist das Scheitern amtlich bestätigt: Nach Auskunft des Bundesinnenministeriums (BMI) gab es Anfang Januar nur für 105 von insgesamt rund 580 sogenannten OZG-Leistungen „flächendeckend Onlineangebote“. Von 35 Leistungen, die eigentlich priorisiert werden sollten, haben es nur zwei bundesweit ins Netz geschafft, und zwar das BAföG und die Corona-Überbrückungshilfe.

### Was geht wo?

Doch was genau können Bürger nun online beantragen und wofür müssen sie weiterhin zum Amt rennen? Bei der Beantwortung dieser Frage helfen die BMI-Zahlen nicht weiter. Das Ministerium erfasst nicht, welche Städte welche Leistungen online anbieten. Für solche Statistiken seien die Bundesländer zuständig, heißt es beim BMI nur. Aber auch bei den meisten Ländern sucht man aktuelle Übersichten vergeblich.

Wir haben deshalb eine Liste von 15 Verwaltungsleistungen angelegt, die für Normalbürger besonders relevant sind: vom Bewohnerparkausweis über den Führerschein und die Kfz-Zulassung bis zur Wohnungsanmeldung. Dann haben wir die 25 größten deutschen Städte plus 7 Landeshauptstädte – damit aus jedem Bundesland mindestens eine Stadt dabei

ist – um Auskunft zum Digitalisierungsgrad bei diesen Leistungen gebeten. Alle Antworten haben wir, soweit möglich, durch Recherche auf den Webseiten der Städte überprüft.

Für unsere Rangliste (siehe Tabelle auf S. 120) haben wir jeweils einen Punkt vergeben, wenn Bürger die entsprechende Leistung über ein Onlineformular beantragen können. Anders als in unserer ersten Auswertung zur digitalen Verwaltung [1] gab es keinen halben Punkt mehr für Formulare, die man herunterladen, ausdrucken, unterschreiben, scannen oder fotografieren und per Mail einreichen kann.

Der Grund: Mit der Mail spart sich der Bürger zwar die Briefmarke und den Weg zum Briefkasten, doch ein Onlinedienst im Sinne des Onlinezugangsgesetzes ist die Methode nicht. Hinzu kommt, dass Mails fast immer unverschlüsselt übertragen werden. Bei der Hundesteueranmeldung mag das verschmerzbar sein, aber Einkommensnachweise, Gesundheitsinformationen, Ausweiskopien und Ähnliches sollte man nicht per Mail senden. Man würde solche Dokumente ja auch nicht in einem offenen Briefumschlag verschicken.

Im Vergleich zu unserer Analyse von Anfang 2022 bieten die meisten Städte inzwischen einen oder zwei Onlinedienste mehr. An der großen Kluft zwischen Voreitern wie Nürnberg und München sowie Nachzüglern wie Mainz und Potsdam hat sich jedoch kaum etwas geändert. Und erneut schneiden große Kommunen im Schnitt besser ab als kleine. Schließlich haben die Großen normalerweise auch größere Budgets und mehr Personal für Digitalisierungsprojekte.

Die Tabelle zeigt den Stand Ende 2022, also zum Ablauf der OZG-Frist. Zahlreiche Städte betonten uns gegenüber, dass sie in den nächsten Monaten weitere Dienste online stellen wollen. Manche davon erschienen sogar schon kurz nach Abschluss unserer Recherche Anfang Januar, etwa der digitale Wohngeldantrag in Hannover. In der Tabelle zeigen wir der Einheitlichkeit halber jedoch nur die Dienste, die zum 31.12.2022 online waren.

### Ursachenforschung

Betenen müssen wir, dass wir mit 15 Diensten nur einen Bruchteil der insgesamt 580 OZG-Leistungen berücksichtigen. Bei einer anderen Auswahl – etwa mit



Bild: Stadt Nürnberg

**Altes Rathaus, neue Technik: Schon im Jahr 2005 startete die Stadt Nürnberg ein großes E-Government-Projekt.**

einem Fokus auf Verwaltungsleistungen für Unternehmen – könnte die Rangfolge anders aussehen. Ein Großteil der OZG-Leistungen ist aber für die allermeisten Bürger und Firmen irrelevant. In der Liste stehen zig obskure Vorgänge wie „Abfallentsorgung in der Hohen See“ und „Frequenzzuteilung“.

Natürlich wollten wir auch genauer wissen, warum Nürnberg bei der Zahl der Dienste vorne liegt. Die Verantwortlichen aus der Stadtverwaltung erklären das in erster Linie mit der Tatsache, dass die Stadt schon relativ früh, im Jahr 2005, eine E-Government-Offensive gestartet und viele Dienste selbst entwickelt hat (siehe Interview auf S. 118).

Viele andere Städte haben hingegen einfach die Hände in den Schoß gelegt – keine Behörde musste Sanktionen befürchten, wenn sie die OZG-Pflicht ignorierte. Mittlerweile prüfen viele dieser Nachzügler immerhin, ob sie Dienste ihres Bundeslandes oder aus anderen Ländern übernehmen können. „Hier sind wir vom Land abhängig bezüglich der Umsetzung“, meldete uns zum Beispiel Magdeburg zu den Themen Unterhaltsvorschuss und Wohngeld.

### Spreu und Weizen

Die Übernahme fertiger Dienste von anderswo (im OZG-Jargon: „Einer-für-Alle-Prinzip“, EfA) ist grundsätzlich sinnvoll, damit nicht jeder das Rad neu erfinden muss. Nürnberg zum Beispiel will bald, als

## c't kompakt

- Für den Großteil der Verwaltungsleistungen in Deutschland sind die Kommunen zuständig. c't vergleicht deshalb das Angebot von Onlineanträgen in 32 Städten.
- Nürnberg und München bieten fast alle der von uns betrachteten Leistungen auch online an, Mainz und Potsdam nur wenige.
- Nürnberg fällt auch mit übersichtlichen Webseiten, einem bequemen Servicekonto und einer hohen Online-Nutzungsquote positiv auf.

eine der ersten bayerischen Kommunen, den in Hamburg entwickelten EfA-Dienst für die digitale Wohnsitzanmeldung einführen. Damit hätte die Stadt dann alle 15 von uns betrachteten Leistungen online. Doch bislang gibt es nur wenige fertige EfA-Dienste und häufig müssen die Kommunen diese dann noch an ihre bestehende Software anpassen, manchmal auch an landesrechtliche Eigenheiten.

Bei komplexen Themen wie dem aktuellen Mammutfprojekt Führerscheinumtausch trennt sich endgültig die Spreu vom Weizen. An den meisten Orten muss man dafür zweimal aufs Amt: Erst zum Beantragen des neuen Führerscheins und dann noch einmal ein paar Wochen später, um den alten Lappen gegen die neue Scheckkarte einzutauschen.

In einigen Städten wie Mönchengladbach oder München kann man den neuen Führerschein immerhin online beantragen und muss dann nur noch einmal aufs Amt. Unter anderem in Nürnberg ist gar kein Behördengang mehr nötig: Man beantragt den neuen Führerschein online, erhält sofort ein Ersatzdokument, schickt anschließend seinen alten Lappen an die Behörde und der neue Führerschein

## „Es bringt nichts, analoge Prozesse einfach digital nachzubauen“

Was hat Nürnberg anders gemacht als andere? Bremst der Datenschutz die Digitalisierung aus? Und ist es überhaupt sinnvoll, dass jede Stadt eigene Onlinedienste betreibt? Im Interview stehen uns zwei Vertreter der Stadt Nürnberg Rede und Antwort: Olaf Kuch, Leiter des Direktoriums Bürgerservice, Digitales und Recht sowie Matthias Latus, Chef des Amtes für Digitalisierung und Prozessorganisation.

**c't: Herr Kuch, Herr Latus, Nürnberg bietet viele Verwaltungsleistungen online an und schneidet deshalb im c't-Ranking unter 32 Städten am besten ab. Wie haben Sie das geschafft?**

**Olaf Kuch:** Nürnberg hat früh angefangen. Bereits ab 2005 sind Mitarbeiter des Organisationsamts mit einer Liste der Bürgerdienste bei den Dienststellen hausein gegangen und haben gefragt: Was wäre sinnvoll online zu machen? Was wird wirklich nachgefragt? Man hat auch von Anfang an zum Beispiel Bezahlverfahren mitgedacht. So haben wir über viele Jahre eine Struktur geschaffen. Jetzt haben wir so viele Leistungen auf der digitalen Straße, dass die Bürgerinnen und Bürger das auch spüren.

**c't: Wer gab damals den Impuls?**

**Kuch:** Digitalisierung war das Steckenpferd des damaligen Leiters des E-Government-Büros. Er hat die Dienststellen wirklich genervt, denn Digitalisierung bedeutet zunächst einmal Zusatzarbeit. Es bringt ja auch nichts, analoge Prozesse einfach digital nachzubauen. Man muss die Arbeitsweisen hinterfragen und dafür braucht man Durchhaltevermögen. Ich kann das aus erster Hand berichten, denn ich war damals

einer der Dienststellenleiter, die davon genervt waren. Jetzt bin ich vom Bedenkensträger zum Mitantreiber geworden.

**c't: Können Sie Beispiele für Prozesse nennen, die Sie im Rahmen der Digitalisierung verändert haben?**

**Kuch:** Nehmen wir den Bewohnerparkausweis. Behält man den alten Prozess bei, müsste ein Bürger online die gleichen Angaben machen wie am Schalter, dann würden wir die Daten manuell prüfen und ein Pappschildchen per Post zusenden. Das ist natürlich unzureichend. Wir verarbeiten den Onlineantrag automatisch und der Bürger kann sich den Parkausweis zuhause sofort ausdrucken. Dafür brauchen wir sogar eine Sondergenehmigung des zuständigen Ministeriums.

**c't: Datenschutz gilt ja häufig als Digitalisierungsbremse. Wie sehen Sie das?**



Bild: oh

**Matthias Latus: „Digitalisierung ist eine Mammutaufgabe.“**

**Matthias Latus:** Bürger und Unternehmen vertrauen uns sensible Daten an, damit wir Leistungen für sie erbringen können. Daher ist uns guter Datenschutz sehr wichtig. Das dürfen unsere Kunden auch von uns erwarten. Mit der Datenschutzgrundverordnung haben sich hier manche Standards für uns weiter geklärt. Das umzusetzen ist für uns durchaus komplex und zwingt auch zu mancher Schleife oder zu weiteren Zustimmungs-Klickboxen, die wir unseren Kunden aufzürden müssen. Gleichzeitig können wir mit klaren Standards aber gut umgehen. Als viel herausfordernder haben wir es erlebt, dass in vielen Fachgesetzen noch Digitalisierungsbremsen versteckt sind: beispielsweise im Melderecht, das oft zur persönlichen Vorsprache zwingt, oder in Vorschriften zu Verwaltungsverfahren. Hier wird oft noch die eigenhändige Unterschrift gefordert, wo es oft nicht mehr zwingend nötig wäre.

**c't: Sie haben viele Onlinedienste selbst entwickelt, statt auf fertige Software aus anderen Kommunen zu warten. Hatten Sie ein größeres Budget als andere Städte?**

**Kuch:** Nein, das war aus der Vision heraus geboren, dass wir es richtig machen wollten, statt nur Stückwerk abzuliefern. Es gab in den wenigsten Fällen passende Produkte auf dem Markt. Im Idealfall geht der Prozess digital vom Bürger zum Rathaus, dann aber auch digital in die Behördesoftware und noch besser auch digital wieder zurück zum Bürger. Deswegen haben wir viel selbst gemacht. Aber grundsätzlich bleibt die Idee richtig, Lösungen von anderen zu übernehmen.

kommt dann von der Bundesdruckerei aus Berlin direkt nach Hause. Das ist zwar noch lange nicht volldigital, aber mehr Service geht angesichts der rechtlichen Rahmenbedingungen kaum.

### Digitalquoten: mal top, mal Flop

Nürnberg fällt nicht nur bei der Zahl der Dienste positiv auf: Wir haben die 15 größten Städte auch gefragt, in wie vie-

len Fällen der Bewohnerparkausweis sowie die Kfz-Zulassung jeweils online und offline beantragt wurden. Schließlich nutzen Onlinedienste nichts, wenn niemand sie findet, oder sie so kompliziert sind, dass man doch lieber zum Bürgeramt marschiert. Die beiden Dienste eignen sich besonders gut als Indikatoren, weil sie fast überall online verfügbar sind und in großen Städten

jährlich Tausende bis Zehntausende dieser Anträge eingehen.

Nürnberg nannte uns für den Parkausweis eine sensationelle Digitalquote von 97 Prozent und verwies damit abermals den großen Konkurrenten München auf den zweiten Platz (95 Prozent). In anderen Städten liegt der Wert deutlich niedriger, unter anderem Duisburg und Dortmund meldeten sogar mehr Offline- als Online-

### c't: Gibt es bei Ihnen noch Prozesse, die nicht komplett durchdigitalisiert sind?

**Kuch:** Ja, auch die gibt es. Zum Beispiel haben wir zu Beginn der Ukrainekrise schnell einen Onlinedienst gebastelt, um allein die Schlangen vor den Ämtern zu vermeiden. Das war nichts komplett Durchdachtes, aber in der Not hilfreich. Andere Vorgänge dürfen wir aus rechtlichen Gründen nicht digitalisieren, zum Beispiel den Antrag auf den Personalausweis. Dann helfen wir eben, indem wir Abholautomaten für die Ausweise aufstellen. Damit ersparen wir immerhin den zweiten Gang zum Amt.

### c't: Sehen Sie Digitalisierung insgesamt als Mehrbelastung für die Stadtverwaltung oder als Entlastung?

**Latus:** Digitalisierung ist eine Mammutaufgabe. Wir müssen die IT-Infrastruktur bereitstellen, Prozesse optimieren, Fachverfahren anbinden, IT-Fachleute gewinnen und ausbilden. Auch das Veränderungsmanagement ist ein sehr großes Thema. Außerdem müssen wir Dienste mitunter aufgrund gesetzlicher Vorgaben digital und analog anbieten. Es fällt also erst einmal nichts weg, es kommt etwas dazu. Aber wenn man in Digitalisierung investiert, schafft man auch Entlastung.

### c't: Beim Parkausweis haben Sie eine Onlinequote von 97 Prozent. Sparen Sie damit nicht ordentlich Personal ein?

**Kuch:** Natürlich, in solchen Bereichen, wo es vollautomatisch läuft, kann man das

Personal anderweitig einsetzen. Das ist kein Personalabbau, sondern ein Freischafeln von Ressourcen.

### c't: Ist es aus Ihrer Sicht überhaupt sinnvoll, dass jede Stadt eigene Onlinedienste anbietet für Verfahren, die landesweit oder bundesweit einheitlich geregelt sind, etwa den Führerscheinantrag?

**Kuch:** Die ganz große Lösung ist natürlich in der Tat, solche Leistungen zentral in Portalen auf Bundeslandebene anzubieten. Das wäre absolut richtig.

### c't: Sie würden also freiwillig Kompetenzen und Gestaltungsmöglichkeiten abgeben?

**Kuch:** Das sind ja keine Kompetenzen, um die wir uns gerissen haben, sondern die der Gesetzgeber uns gegeben hat. Bei Dingen wie Baugenehmigungen, Ausweiswesen, Meldewesen haben wir auch keinen Gestaltungsspielraum. Daran hängt unser städtisches Selbstbewusstsein sicherlich nicht.

### c't: Was haben Sie sich für 2023 in Sachen Digitalisierung vorgenommen?

**Latus:** Wir werden unter anderem die Implementierung und Umsetzung digitaler Fachstrategien unserer Dienststellen und Eigenbetriebe vorantreiben. Darüber hinaus unser Angebot an Onlinediensten weiter ausbauen, insbesondere dort, wo hohe Fallzahlen liegen. Auch schauen wir, welche Prozesse wir automatisieren können. Zum Beispiel haben wir in der Führerscheinstelle ein Pilotprojekt, bei dem eine



Bild: Giulia Iannicelli / Stadt Nürnberg

**Olaf Kuch:** „Man muss die Arbeitsweisen hinterfragen und dafür braucht man Durchhaltevermögen.“

Software bestimmte Karteikartenabschriften für andere Führerscheinbehörden automatisch erledigt. Das ist im Moment ein „stupider“ Roboter, wir wollen uns aber hier auch zukünftig mit KI befassen.

### c't: Welche Unterstützung wünschen Sie sich dafür vom Land Bayern und vom Bund?

**Kuch:** Die rechtlichen Rahmenbedingungen zu verbessern, sodass wir mehr digitalisieren können. Die Paradebeispiele dafür sind Pass-, Ausweis- und Meldeweisen. Das sind echte Bringer, da reden wir von Zehntausenden Fällen im Jahr. Und wir wären auch dankbar, wenn mehr Onlinedienste von Bund und Ländern zur Verfügung gestellt werden.



Bild: Stadt Nürnberg

**Nicht digital, aber trotzdem bequem: Weil Personalausweise nicht per Post zugestellt werden dürfen, hat die Stadt Nürnberg Abholautomaten in Sparkassen-Filialen aufgestellt.**

weisen müssen und die dafür nötige PIN verlegt haben. Obendrein gilt die vom Bund entwickelte Antragssoftware „i-Kfz“ als hakelig.

Die hohe Parkausweis-Digitalquote in Nürnberg dürfte auch damit zusammenhängen, dass die Stadt ihre Webseiten niederschwellig gestaltet hat. Das Design mag ein wenig altbacken wirken, aber auf fast jeder Themenseite steht klipp und klar, wie man einen Antrag stellen kann. Behördenkauderwelsch findet man hier kaum. Auf vielen Seiten anderer Städte mussten wir hingegen lange herumrätseln, was nun online geht und was nicht.

### Ein Konto für alles

Einen weiteren Pluspunkt hätte Nürnberg für das Nutzerkonto „Mein Nürnberg“ verdient. Wer hier persönliche Daten hinterlegt, erhält bereits vorausgefüllte Antragsformulare. Nach Angaben der Stadt kann man mit dem Konto aber auch Bearbei-

anträge. Eine hohe Digitalquote ist auch eine Voraussetzung für die Entlastung der Behörden, denn Onlineanträge zu simplen Themen können zumindest theoretisch automatisiert bearbeitet werden.

Bei der Kfz-Zulassung fällt die Digitalquote allerdings durchweg desaströs aus,

sie liegt in allen Städten unter einem Prozent. Das erklärt sich zum Teil daraus, dass Unternehmen (wie Autohändler) den Onlinedienst aktuell noch nicht nutzen können. Viele private Antragsteller dürften daran scheitern, dass sie sich für die Zulassung mit ihrem E-Perso übers Netz aus-

## Digitale Antragsverfahren in Großstädten und Landeshauptstädten (Stand: 31.12.2022)

Stadt	Punkte	Abfallbehälter bestellen	Bauantrag	Bewohnerparkausweis	Bibliotheksanmeldung	Führerschein (Erstantrag)	Führerscheinumtausch	Anforderung Geburtsurkunde	Anmeldung eines Hundes
Nürnberg	14	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
München	13	⊕	⊖	⊕	⊕	⊕	⊕	⊕	⊕
Bonn	12	⊕	⊖	⊕	⊕	⊖	⊕	⊕	⊕
Düsseldorf	11	⊕	⊖	⊕	⊕	⊖	⊕	⊕	⊕
Mannheim	11	⊕	⊕	⊕	⊖	⊕	⊖	⊕	⊕
Wuppertal	11	⊕	⊖	⊕	⊖	⊕	⊕	⊕	⊕
Augsburg	10	⊕	⊕	⊕	⊖	⊖	⊖	⊕	⊕
Bielefeld	10	⊖	⊖	⊕	⊕	⊖	⊕	⊕	⊕
Hamburg	10	⊕	⊖ <sup>1</sup>	⊕	⊖ <sup>2</sup>	⊕	⊖	⊕	⊕
Mönchengladbach	10	⊕	⊖	⊕	⊖	⊖	⊕	⊕	⊕
Köln	10	⊕	⊕	⊕	⊖	⊖	⊕	⊕	⊕
Stuttgart	10	⊕	⊕	⊕	⊕	⊖	⊖	⊕	⊕
Bremen	9	⊖	⊖	⊕	⊕	⊖	⊖	⊕	⊕
Leipzig	9	⊕	⊖	⊕	⊕	⊖	⊖	⊕	⊖
Berlin	8	⊕	⊖	⊕	⊕	⊖	⊖	⊕	⊖
Bochum	8	⊕	⊖	⊕	⊖	⊖	⊖	⊕	⊕
Münster	8	⊖	⊕	⊕	⊖	⊖	⊖	⊕	⊖
Schwerin	8	⊕	⊕	⊕	⊕	⊕ <sup>6</sup>	⊖	⊕	⊕
Dortmund	7	⊖	⊖	⊕	⊖	⊖	⊖	⊕	⊕
Dresden	7	⊕	⊖	⊖	⊕	⊖	⊖	⊕	⊖
Duisburg	7	⊕	⊖	⊕	⊖	⊖	⊖	⊕	⊖
Hannover	7	⊕	⊖	⊕	⊖	⊖	⊖	⊕	⊕
Kiel	7	⊖	⊖	⊖	⊖	⊖	⊖	⊕	⊖
Saarbrücken	7	⊕	⊕	⊕	⊕	⊖	⊖	⊕	⊖
Wiesbaden	7	⊖	⊖	⊕	⊕	⊕	⊖	⊕	⊖
Frankfurt a. M.	6	⊖	⊖	⊕	⊕	⊖	⊖	⊕	⊖
Erfurt	6	⊖	⊖	⊕	⊕	⊖	⊖	⊕	⊖
Essen	6	⊖	⊕ <sup>4</sup>	⊖	⊖	⊖	⊖	⊕	⊕
Karlsruhe	6	⊕	⊖	⊖	⊖	⊖	⊖	⊕	⊕
Magdeburg	5	⊖	⊖	⊖	⊖	⊖	⊖	⊕	⊕
Mainz	3	⊖	⊖	⊕	⊕	⊖	⊖	⊕	⊖
Potsdam	1	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖

⊕ = Antrag kann online gestellt werden

⊖ = persönlich oder per Post / E-Mail

<sup>1</sup> Onlineantrag möglich, zusätzlich muss Antrag in Papierform übermittelt werden

<sup>2</sup> Zuständigkeit: Hamburger Bücherhallen

<sup>3</sup> nur für Unverheiratete, ohne minderjährige Kinder

<sup>4</sup> nur für einige Stadtteile

tungsstände verfolgen, mit Ansprechpartnern in den Behörden kommunizieren, Gebühren bezahlen (zum Beispiel per PayPal und Kreditkarte) sowie Bescheide und Rechnungen in digitaler Form empfangen.

Wer sich mit dem elektronischen Personalausweis bei „Mein Nürnberg“ anmeldt, kann auch Anträge mit Schriftformerefordernis (wie beim Unterhaltsvorschuss) digital einreichen. Die wenigsten anderen Kommunen betreiben ein solches Konto. Viele wollen das Nutzerkonto ihres jeweiligen Bundeslandes einbinden, stehen dabei aber erst am Anfang.

Doch mit Onlinediensten und Basisinfrastruktur wie Nutzerkonten ist es nicht getan, auch die Verwaltung im Hintergrund muss digital Schritt halten: Wenn Onlineanträge ausgedruckt und in Kladen von Abteilung zu Abteilung geschoben werden, haben weder die Bürger noch die Verwaltungsangestellten viel gewonnen [2]. Auch bei der internen Digitalisierung

sieht sich Nürnberg als Vorreiter: Ein Dokumentenmanagementsystem für die revisionssichere elektronische Aktenführung sei stadtweit eingeführt, im Amt für Migration und Integration habe man bereits fast alle Prozesse „Ende-zu-Ende“ digitalisiert.

Bis zur komplett digitalen Verwaltung ist es jedoch überall in Deutschland noch ein sehr weiter Weg – auch aufgrund rechtlicher Schranken. Eine Geburtsurkunde zum Beispiel muss hierzulande nach wie vor auf Papier ausgestellt werden.

## Fazit

Das Onlinezugangsgesetz gilt gemeinhin als Flop, aber Vorreiter wie Nürnberg beweisen, dass zumindest große Kommunen durchaus ein breites und auch nutzerfreundliches Onlineangebot aufbauen können. Man muss rechtzeitig damit anfangen, konsequent dranbleiben und gute Ideen haben. Außerdem zeigen die vieler-

orts hohen Digitalquoten beim Bewohnerparkausweis, dass kaum noch jemand zum Amt gehen will, wenn die Onlinedienste leicht auffindbar und verständlich gestaltet sind.

Allerdings gibt es außer den Onlinediensten noch viele andere Baustellen: Bund und Länder beschließen voraussichtlich bald das „OZG 2.0“, das auch die interne Verwaltungsdigitalisierung zur Pflicht machen soll. Und mit der Registermodernisierung läuft ein weiteres Mammutprojekt. Dabei wollen Bund und Länder die Datenbanken der Behörden miteinander vernetzen, sodass diese ihre Anträge einfacher gestalten können und Bürger nicht jedes Mal aufs Neue einen Stapel von Nachweisen einreichen müssen.

(cwo@ct.de) 

## Literatur

- [1] Jo Bager, Christian Wölbert, Halbdigital, Digitalisierung der Verwaltung – eine Bestandsaufnahme, c't 6/2022, S. 60
  - [2] Christian Wölbert, Im Land der Internetausdrucker, Warum das Gesetz zur Digitalisierung der Verwaltung scheiterte, c't 2/2023, S. 12

Weitere Infos: [ct.de/yagx](http://ct.de/yagx)

## Und auf dem Land?

Um auch Eindrücke aus ländlichen Gegend zu gewinnen, haben wir 13 Städte mit jeweils rund 30.000 Einwohnern – eine aus jedem Flächenland – zur Digitalisierung der Verwaltung befragt. Die Kleinstädte lassen wir im Ranking außen vor, weil sie für weniger Leistungen zuständig sind als die Großstädte und die Zuständigkeiten obendrein je nach Bundesland stark variieren.

Im Mittel bieten die Kleinen weniger Onlinedienste als die 32 großen Städte. Es gibt aber auch Ausnahmen: Andernach (Rheinland-Pfalz), Weil am Rhein (Baden-Württemberg) und Bad Hersfeld (Hessen) meldeten uns deutlich mehr eigene Onlinedienste als die anderen Kleinstädte. Zum Beispiel kann man dort Geburtsurkunden anfordern, einen Hund steuerlich anmelden und einen Kita-Platz finden. Bad Hersfeld nimmt sogar Bauanträge digital entgegen. Ziemlich analog ticken hingegen zum Beispiel Saarlouis (Saarland), Itzehoe (Schleswig-Holstein) und Altenburg (Thüringen).

Kfz-Neuzulassung	Schwerbehinder-tenparkausweis	Unterhalts-vorschuss	Gewerbe-anmeldung	Wohngeld	Vormerkung Kita-Platz	Wohnungs-anmeldung
+	+	+	+	+	+	-
+	+	-	+	+	+	+
+	+	-	+	+	+	+
+	+	-	+	+	+	-
+	+	+	-	+	+	-
+	+	+	-	+	+	-
+	+	+	-	+	+	-
+	+	-	+	+	+	-
+	-	+	+	+	-	+
+	+	-	+	+	+	-
+	-	-	+	+	+	-
+	-	-	+	-	+	+
+	+	+	+	-	+	-
+	-	+	+	+	+	-
+	-	-	+	+	+	-
+	-	-	+	-	+	-
+	-	-	+	-	+	-
+	-	-	+	+	+	-
+	-	-	+	-	+	-
+	-	-	+	+	+	-
-	-	+	-	-	-	-
+	-	-	+	+	+	-
+	-	-	+	+	+	-
+	-	-	+	+	+	-
+	-	-	+	-	+	-
+	-	-	+	-	+	-
-	-	-	+	-	-	-
+	-	-	-	+	+	-
+	-	-	-	-	+	-
-	-	-	-	-	-	-
+	-	-	-	-	-	-

<sup>5</sup> Änderung des Ausweisdokuments nachträglich vor Ort

<sup>6</sup> über Landkreis

<sup>7</sup> Zuständigkeit: Regionalverband Saarbrücken



# Renovierung erfolgreich

**Warum man mit Giropay nun besser zahlt als mit PayPal oder Kreditkarten**

**Giropay, das Bezahlsystem deutscher Banken und Sparkassen, hat sich neu erfunden. Es ist schneller, günstiger und vor allem datensparsamer als PayPal und Kreditkarten. Wir erklären die Vorteile des Systems und warum wir einen Umstieg empfehlen.**

**Von Tobias Weidemann**

**K**lick-klick. Ihre neuen Klamotten liegen im Warenkorb, nun geht es an die virtuelle Kasse. Aber welche Bezahlart soll es sein? Neben bekannten und komfortablen Vertretern wie PayPal und Kreditkarte oder auch Rechnung und Lastschrift steht in einigen Shops „Giropay“ zur Auswahl. Sie haben bisher einen Bogen um dieses Feld gemacht? Damit sind Sie nicht allein: Vielen Kunden war das Bezahlverfahren entweder zu umständlich oder sie kannten es nicht einmal. Denn nur vergleichsweise wenige Händler und Marktplätze bieten es bisher überhaupt an – während PayPal, Visa und Mastercard der Standard sind.

Das wollen viele deutsche Banken und Sparkassen nun ändern. Deshalb haben sie Giropay mit dem ebenfalls verschmähten hauseigenen Bezahldienst Paydirekt zusammengelegt und gründlich renoviert: Das Ganze firmiert jetzt nur noch unter dem Namen „Giropay“. Insbesondere den Bezahlprozess haben die Kreditinstitute stark vereinfacht und eine neue Smartphone-App dafür entwickelt. Damit können Kunden zukünftig sogar online per Girocard shoppen; bisher konnten sie mit der Karte nur an der Ladenkasse zahlen. Wir haben uns das neue Giropay angesehen und nach Hintergründen und weiteren Plänen gefragt.

## Bisher nur Nischenprodukte

Paydirekt und Giropay sind im Onlinehandel keine neuen Akteure. Die deutschen Banken und Sparkassen hatten deren Einführung jedoch so lange hinausgezögert, bis die Konkurrenz sich bereits etabliert hatte, und verwirrten ihre Kunden dann mit zwei unterschiedlichen Systemen nebst umständlicher Bedienung. Da half es auch nicht, dass die Daten bei beiden Verfahren auf deutschen Bankservern blieben.

All das schlug sich in den Marktanteilen nieder. Trotz millionenschwerer Werbezuschüsse für Onlinehändler, die ihren Kunden das Bezahlen per Paydirekt schmackhaft machen sollten, kam der Dienst 2020 gerade einmal auf 3,3 Millionen Zahlungen mit einem Volumen von rund 290 Millionen Euro. Zum Vergleich: Der Gesamtumsatz im deutschen Onlinehandel lag 2022 laut Handelsverband Deutschland (HDE) bei rund 100 Milliarden Euro, und diese Summe enthält noch nicht mal die Umsätze mit Konzerttickets oder Fahrkarten. Den Großteil des Umsatzes wickelten PayPal und Rechnungskauf ab (jeweils rund 28 Prozent im Jahr 2021), gefolgt von Lastschrift und Kreditkarten.

Seit Mai 2021 führen die deutschen Banken die beiden Systeme nun unter dem (passend zur Girocard eingängigen) Namen „Giropay“ zusammen, wobei die Bezeichnung „Paydirekt“ verschwindet. Giropay soll dabei zum einen „der

Brückenkopf für die digitalen Zahlungslösungen“ sein, wie es Henning vorm Walde als Geschäftsführer der für das neue Giropay verantwortlichen Paydirekt GmbH formuliert. Zum anderen soll das neue Giropay zum Wallet mit drei Autorisierungsmethoden werden: Zu den beiden alten aus Giropay und Paydirekt gesellt sich die digitale Girocard als neues Verfahren.

Damit verfolgen die Banken laut vorm Walde das Ziel, den Zukunftsmarkt der digitalen Zahlungslösungen nicht den US-Playern zu überlassen. Man wolle das Giropay-Ökosystem „zu einem Omnichannel-Zahlungssystem ausbauen“, heißt es in schönstem Marketingdeutsch – sprich: einem einheitlichen Verfahren für Online- und Offline-Einkäufe.

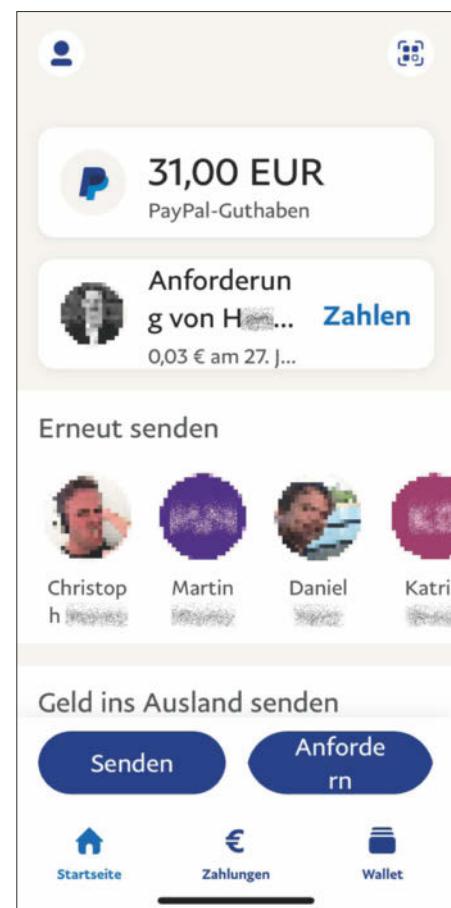
## Frischzellenkur

Auch die deutschen Banken sehen Onlinezahlungen einem Bankenvertreter zufolge mittlerweile als wichtigsten Zukunftsmarkt. Dabei wollen sie es den Kunden beim bargeldlosen Zahlen möglichst einfach machen. Und tatsächlich: Mit dem neuen Giropay zahlt es sich deutlich komfortabler als früher.

Die wichtigste Voraussetzung für den Kunden ist dabei, dass sein Kreditinstitut Giropay unterstützt. Dazu zählen insbesondere die Sparkassen, fast alle Genossenschaftsbanken, außerdem Postbank, Deutsche Bank, Commerzbank und Comdirect sowie ING und HypoVereinsbank. Es fehlen aber zum Beispiel DKB, Santander und Targobank, außerdem alle Neobanken wie N26 oder Tomorrow.

Zunächst muss man im Onlinebanking ein Giropay-Nutzerkonto anlegen. Einzig dieser Prozess ist noch etwas umständlich [1], die Mühe lohnt sich aber. Anschließend installiert man die Giropay-App für Android oder iOS und meldet sich an. Wählt man Giropay nun in einem Onlineshop am PC als Bezahlmethode, klickt man in der nachfolgenden Auswahl für den einfachsten Weg auf „Giropay-Login“ (die „Online-Überweisung“ als zweite Option kann man getrost ignorieren). Anschließend startet man die neue Giropay-App auf dem Handy und authentifiziert sich mit vierstelliger PIN, Fingerabdruck oder Gesichtserkennung.

Nun scannt man mit der App nur noch einen QR-Code auf dem PC-Bildschirm, fertig. Tempo und Komfort sind PayPal mehr als ebenbürtig. Kauft der Kunde via Handy ein, leitet der Onlineshop ihn zum



**PayPal ist für den Onlinehandel bislang die Referenz in Sachen Bedienkomfort und Funktionsumfang und den deutschen Bezahlarten weit überlegen. Beim Datenschutz macht der US-Konzern allerdings keine gute Figur.**

Bezahlen direkt in die neue Giropay-App. Im Modus „Giropay-Login“ gibt es die Zahlung nach der Authentifizierung per PIN, Fingerabdruck oder Gesichtserkennung ähnlich einfach frei.

Selbst ohne Smartphone ist das Verfahren komfortabler als früher. Je nach eigenen Einstellungen im Onlinebanking und in Giropay entfällt nun häufiger die Authentifizierung über die Bank; es genügen Giropay-Nutzername und Passwort.

Besonders ins Auge sticht auf Android-Handys jedoch ein dritter Weg: die digitale Girocard. Die Idee dahinter: Kunden bezahlen an der Ladenkasse und online mit demselben statt mit unterschiedlichen Mitteln. Die digitale Girocard steht zunächst Kunden von Sparkassen sowie Volks- und Raiffeisenbanken zur Verfügung. Auch dafür muss man zunächst das Giropay-Nutzerkonto einrichten und dann zusätzlich die institutseigene Bezahl-App „Mobiles Bezahlen“ respektive „Pay“ in-

## c't kompakt

- Im neuen Giropay haben deutsche Banken und Sparkassen ihre bisher schwerfälligen Dienste Paydirekt und Giropay zusammengelegt und de facto neu erfunden.
- Zahlungen funktionieren in Onlineshops nun sogar einfacher als mit PayPal & Co., bieten aber ein viel besseres Datenschutzniveau und zukünftig sogar eine digitale Girocard.
- Damit könnten die Deutschen auch die Abkündigung von Maestro teilweise auffangen, mit der Mastercard die Girocard unter Druck setzt – zumal Giropay weitere Funktionen bekommen soll.

Transaktionen Gutscheine Dienste

Hallo Markus!

Letzte Anmeldung:  13:10 Uhr

 Volksbanken  
Raiffeisenbanken

Dein Konto (DE\*\*\*)

Kontoinformationen

Kundenname

Markus Montz

Benutzername



Passwort

\*\*\*\*\*

Verknüpftes Konto

Bank: Hannoversche  
Volksbank

IBAN: 

BIC: VOHADE2H

[>Sie möchten giropay nicht mehr nutzen?](#)

E-Mail-Adressen

Freunde können an Ihre E-Mail-Adressen  
Geld senden.

Standard-E-Mail-Adresse 



[+ E-Mail-Adresse hinzufügen](#)

Newsletter

Sie sind mit Ihrer  
Standard-E-Mail-Adresse für unseren  
Newsletter angemeldet:

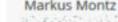
[Newsletter abbestellen](#)

Ich stimme dem personalisierten  
Newsletter-Tracking zu, damit die  
Inhalte für mich optimiert werden  
können.

[Informationen zum Datenschutz](#)

Adressen

Markus Montz

 Hannover  
Deutschland

[+ Neue Adresse hinzufügen](#)

**Giropay schaltet man im Online-banking seines Kreditinstituts frei. Anschlie-ßend passt man seine Einstellun-gen im Nutzer-portal von Giro-pay an [1].**

und Mastercard langfristig kaum konkurrenzfähig bleiben, denn mit diesen kann man bereits im Internet einkaufen. Dass die deutschen Banken nun nachziehen, hilft aber keineswegs nur den Kreditinstituten, sondern entlastet auch das Portemonnaie der Verbraucher. Denn für Zahlungen mit der digitalen Girocard müssen Händler geringere Gebühren an ihre Zahlungsdienstleister entrichten als beim Einsatz von Debit- und insbesondere Kreditkarten von Visa und Mastercard [3].

Während Händler für den Einsatz der Girocard je nach Zahlungsdienstleister meist rund 0,2 bis 0,4 Prozent Provision plus einen Sockelbetrag von einigen Cent entrichten, können es bei einer der beiden großen Kreditkarten je nach Vertragsgestaltung zwischen einem und zwei Prozent sein. Im Internet ist es meist noch mehr. Die reine Visa- und Mastercard-Debitcard ist für den Handel zwar etwas günstiger, liegt aber oftmals ebenfalls noch oberhalb von einem Prozent. Verbraucher sehen diese Kosten zwar nicht auf dem Kassen-

stallieren. Darin hinterlegt man eine Girocard (wie das technisch funktioniert und weshalb es sicher ist, erklären wir in [2]). Beim Bezahlen wählt man dann die „Digitale Girocard“. Anschließend leitet GiroPay in die Bezahl-App weiter, in der man sich per PIN, Fingerabdruck oder Gesichtserkennung authentifiziert.

Ob, wann und wie die ersten Privatbanken wie die Deutsche Bank oder Direktbanken wie die Comdirect ihr Giropay-Angebot um die digitale Girocard erweitern, ist indes noch offen. Auch iOS-Nutzer müssen fürs Erste noch auf die digitale Girocard als dritte Option in ihrem Giropay verzichten. Grundsätzlich wären iPhone & Co. aber dazu fähig, schließlich kann man als Sparkassenkunde schon seit Mitte 2021 über Apple Pay in Onlineshops mit der Girocard zahlen.

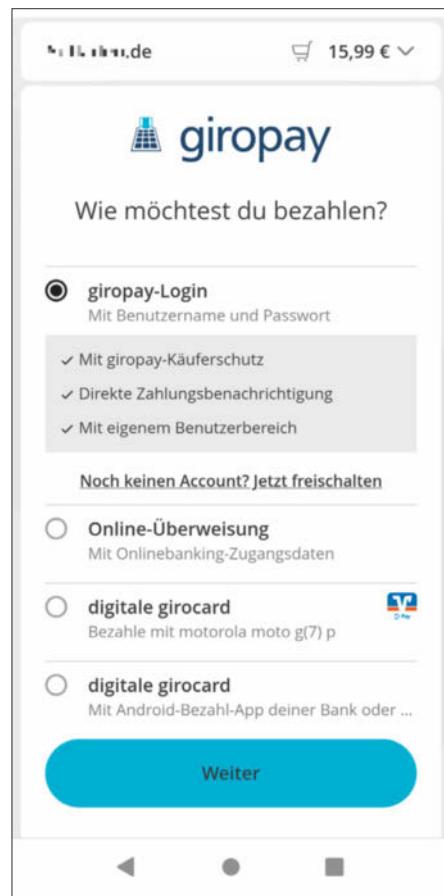
## Die Konkurrenz schl鋑t nicht

Die digitale Girocard ist eine Antwort auf Mastercards Schritt, sein Zweitsystem Maestro ab Juli 2023 abzukündigen, über das viele Girocard-Nutzer bislang im Ausland bezahlten. Die reine Girocard funktioniert hingegen nur in Deutschland. Viele Beobachter sehen in Mastercards Entscheidung daher auch die Absicht, der

Girocard langfristig Marktanteile zugunsten der eigenen Mastercard-Debitkarten abzunehmen. Dabei dürften Mastercard und quasi nebenbei auch Visa darauf hoffen, dass die Banken entweder nur noch deren reine Debitkarten ausgeben oder die Girocard zukünftig mit diesen Debitkarten anstelle von Maestro oder Visas V-Pay kombinieren (mehr zu diesen Debitkarten und dem Unterschied zu Girocard und Kreditkarte unter [3]).

Bei der Euro Kartensysteme, einem Dienstleister der Banken und Sparkassen für die Vermarktung und Technik der Girocard, gibt man sich nach außen jedoch entspannt. „Was Maestro angekündigt hat, macht uns jetzt keine Angst“, so Geschäftsführer Oliver Hommel. „Denn zum einen ist die Kooperation ja erst einmal nur bei ab Mitte 2023 ausgegebenen Karten nicht mehr dabei und läuft erst nach und nach über die nächsten vier Jahre aus. Zum anderen sehen wir, dass die meisten Institute ihre Girocards mit einer Debit-Mastercard oder mit Visa Debit kombinieren und die Girocard damit im Ausland weiterhin einsetzbar bleibt.“

Dennoch: Ohne die jetzt nachgerüstete Online-Bezahlfunktion dürfte Girocard gegenüber den Debitkarten von Visa



Die digitale Girocard kommt auf Android-Handys. Den Anfang machen die Sparkassen sowie die Volks- und Raiffeisenbanken.

kostenfreie Online Marketing Webinare

# Erfolgreich online

Wir zeigen Ihnen, wie Sie mit Online Marketing  
neue Kunden, Klienten oder Patienten  
gewinnen.

Alle Themen und aktuelle Termine  
finden Sie hier:  
[www.heise-regioconcept.de/webinare](http://www.heise-regioconcept.de/webinare)



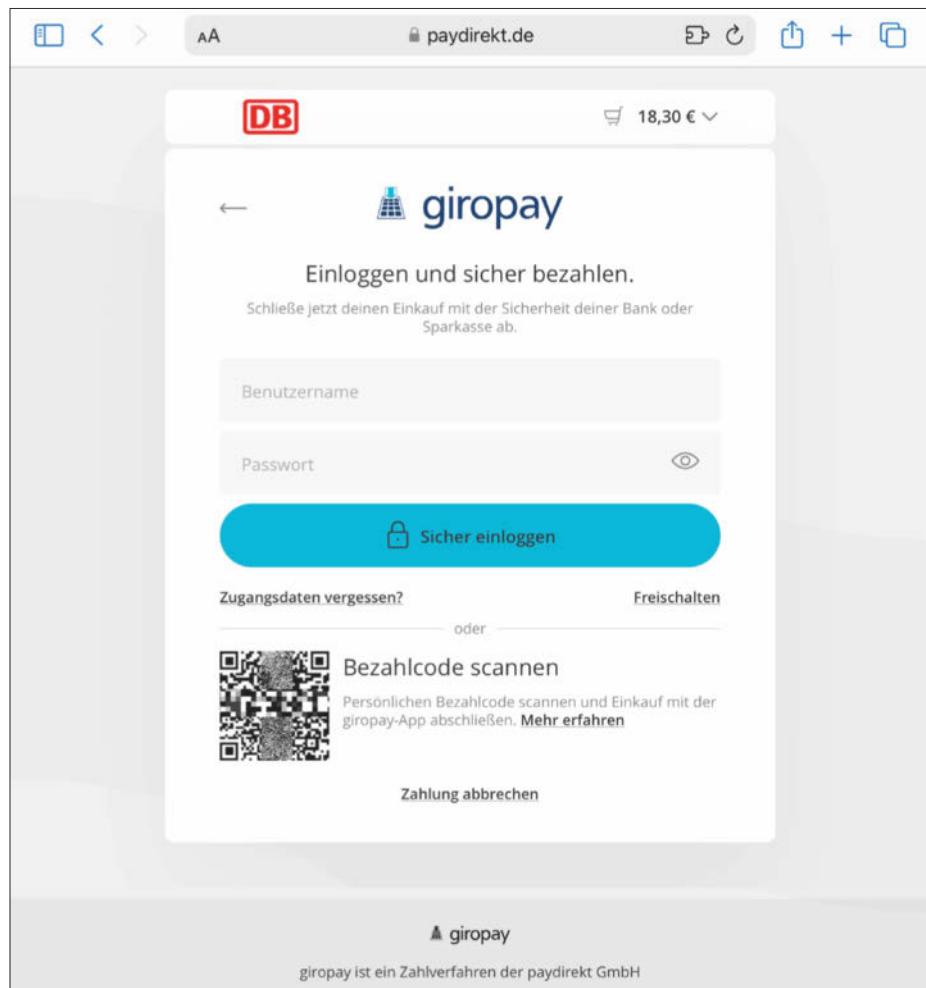
Profitieren Sie  
von unserem  
Experten-  
wissen!

Erfolgreiches  
Marketing  
vor Ort.



 Heise RegioConcept

Telefon 0511 80 90 89 43  
[www.heise-regioconcept.de](http://www.heise-regioconcept.de)



**Bezahlen, wie man es sich 2023 im Netz vorstellt: Einfach Giropay-App öffnen, mit Fingerabdruck oder Face-ID authentifizieren, QR-Code scannen und fertig ist die Laube.**

bon, die Händler legen sie aber auf ihre Endpreise um.

### Weiteres Ausbaupotenzial

Bei der Umgestaltung von Giropay haben die deutschen Banken mehr denn je mit den Onlinehändlern zusammengearbeitet, wie ein Vertreter eines großen Handelskonzerns berichtet. Für Handelsunternehmen (auch stationäre) bedeutet dies eine bisher nicht bekannte Dynamik, wenn sie neue Funktionen in Giropay vorschlagen. Hinzu kommt, dass vor allem das Girocard-System dem stationären Handel schon lange weitgehende Sicherheit vor nicht gedeckten und zurückgewiesenen Zahlungen bietet. Das macht die Kombination aus Girocard und Giropay für den Handel attraktiver. Die deutsche Kreditwirtschaft setzt also einige Hebel in Bewegung, damit ihr neues, komfortables Zahlungsverfahren auch in den (Online-)Shops ankommt: Kunden können

sich berechtigte Hoffnungen machen, dass es sich etabliert und mehr und mehr Funktionen hinzukommen.

So wünscht sich die Wirtschaft beispielsweise eine Zusammenarbeit mit Bonusprogrammen, damit Kunden einfacher Treuepunkte sammeln können. Auch eine Altersverifikation für den Handel steht im Raum, etwa in kassenlosen Supermärkten oder bei Lieferdiensten, die Spirituosen und Tabakwaren anbieten. Auf der Liste stehen außerdem In-App-Käufe und regelmäßig wiederkehrende Zahlungen; die Tourismusbranche wünscht sich, mit Giropay zusätzliche Nächte vor Ort buchen zu können. All das geht bislang eleganter über die Kreditkarte.

Das Ende der technisch möglichen Entwicklung wäre damit noch lange nicht erreicht: Die Banken könnten pro Girokonto beliebig viele digitale Girocards ausgeben, sodass nicht nur der Kunde, sondern auch einige Systeme in seinem ver-

netzten Gerätetanz eine eigene Karte bekommen. Beispielsweise könnte das E-Auto mit seiner eigenen Girocard automatisch an der Ladesäule oder im Parkhaus bezahlen – „Seamless Payment“ nennt sich dieses Bezahlen ohne explizite Kassenzone.

Lässt Giropay damit womöglich PayPal und Kreditkarten hinter sich? Ralf Gladis vom Zahlungsabwickler Computop ist der Meinung, dass sowohl die Kreditkarten als auch die Girocard, respektive Giropay, in Zukunft ihre Daseinsberechtigung haben. „Die Kreditkarte ist eindeutig teurer für den Handel, aber sie bietet zumindest bisher auch deutlich mehr Funktionen, die im Girocard-Lager erst nach und nach entwickelt werden müssen.“ Der Handel könnte daher bestimmte Bezahlösungen wie Upgrades, regelmäßig wiederkehrende Transaktionen für Abonnements oder internationale Lösungen bislang einfacher über Visa- und Mastercard abwickeln. Kreditkarten lohnen sich für den Handel auch noch aus einem anderen Grund: „Kunden geben mit der Kreditkarte oftmals mehr Geld aus, da sie die Abbuchung erst im nächsten Monat haben“, so Gladis.

Computop und andere Zahlungsabwickler binden derzeit die Shop-Systeme zahlreicher Onlinehändler an die Giropay-Welt an und müssen parallel auch ihre eigenen Schnittstellen an die neue API anpassen. Das ist zunächst mit Aufwand verbunden, lohnt sich aber aus Gladis' Sicht: „Die gute Nachricht aus Sicht der Händler ist, dass sich das in Zukunft sowohl technisch als auch vertraglich einfacher umsetzen lassen wird. Denn mit dem neuen Giropay haben auch die Zahlungsdienstleister nur noch einen Ansprechpartner. Der funktioniert wie ein Acquirer [Vertragspartner des Händlers, die Red.] und macht einen Preis und Vertrag.“

### Vorteil Datenschutz

Die Themen Datenschutz und Privatsphäre waren und sind aus Kundensicht ein großer Vorteil gegenüber den US-Konzernen. Denn die Kundendaten bleiben ausnahmslos in Deutschland. Doch auch technisch verfolgt das Girosystem einen datensparsameren Ansatz als die US-Anbieter. Dieser stützt sich auf Unique User IDs (UUID). Diese tauschen der Zahlungsdienstleister oder die Bank des Händlers und die Kundenbank verschlüsselt als Platzhalter (Token) aus, wenn sie die Zah-

lung autorisieren und auslösen. Nur die Kundenbank kann sie dem Kunden zuordnen. Abgesehen vom Zahlungsvorgang prüfen die Beteiligten die Daten ansonsten lediglich auf Muster für Geldwäsche und Betrug.

Auch die Konzeption des Giropay-Systems selbst verhindert, dass jemand die Transaktionen analysieren und für weiterreichende Marktforschung oder Datenhandel zweckentfremden kann. „Im Gegensatz zu anderen Bezahldiensten ist so kein externer Dritter involviert, wir nutzen die Daten weder für Werbezwecke noch für Warenkorbanalysen“, erklärt Paydirekt-Geschäftsführer Henning vorm Walde. Eine Besonderheit ist nämlich der dezentrale Ansatz: Giropay verrechnet die Zahlung der Kunden nicht selbst, vielmehr wickeln Händler und Kundenbank sie direkt miteinander ab. „Kurzum: Wir auto-

risieren direkt gegen das Konto, die Daten liegen bei der einzelnen Bank“, so vorm Walde. Die Bank wiederum darf die Daten nur mit ausdrücklichem Einverständnis des Kunden für weitergehende Zwecke verwenden, ebenso der Händler.

### Ausblick:

#### Guter Start, offene Fragen

Das neue Giropay wirkt verheißungsvoll, auch aus Kundensicht. Zum Glück sind sich die deutschen Privatbanken, Genossenschaftsbanken und Sparkassen inzwischen weitgehend einig, dass Girocard und Giropay über ihre zukünftige Rolle im Zahlungsverkehr mitentscheiden. Allerdings handelt auch weiterhin jedes Institut für sich, sprich: Jede Privatbank und jede der 370 Sparkassen und 770 Genossenschaftsbanken bestimmt selbst, ob, wie und zu welchen Konditionen sie

ihren Kunden das digitale Zahlungsverfahren anbieten. Welche Möglichkeiten der Kunde abseits der Basisfunktionen erhält, liegt also in den Händen seiner jeweiligen Bank. Dabei ist Kwitt, der P2P-Zahlungsdienst im Giropay-System, noch gar nicht einbezogen (siehe Kasten und [3]).

Am Ende werden die Banken aber nur erfolgreich sein, wenn sie ihre Kunden und den Handel mit Komfort, Einheitlichkeit und einem kompletten Angebot für alle Lebenslagen überzeugen. Denn gerade die Kunden dürften ihre eingespielten Zahlungswege wie Rechnungskauf, PayPal oder Kreditkarte nur aufgeben, wenn es ihnen spürbare Vorteile bringt. Bei der Bedienung haben die Banken ein Zwischenziel erreicht: Das neue Giropay ist nicht mehr nur datenschutzfreundlich, sondern funktioniert für Kunden sogar komfortabler als PayPal & Co. Wir können es daher (endlich!) ausdrücklich empfehlen.

Die Branche ist aber noch lange nicht am Ziel, weder an der Ladenkasse noch im Onlinehandel. Insbesondere bei P2P-Zahlungen könnte sie sich mehr von den europäischen Nachbarn abgucken und dort Angebote schaffen, wo PayPal, Visa und Mastercard für Verkäufer – vor allem kleingewerbliche und private – zu teuer und zu aufwendig sind (siehe Kasten).

Auch den Datenschutztrumpf könnten Banken und Sparkassen stärker ausspielen und viel deutlicher mit ihrem vorbildlichen, hohen Maß an Privatsphäre werben. Anders ausgedrückt: Ein Zahlungsdienst wie Klarna analysiert Käufe und Warenpräferenzen, um Marktforschung zu betreiben; das ist Teil seines Geschäftsmodells. Bei PayPal und Konsorten kann man sich nie ganz sicher sein, welche Daten in den USA landen. Die deutschen Banken setzen dem mit Giropay ein System entgegen, das die sensiblen Daten ihrer Kunden schützt. Sie besinnen sich damit bewusst oder unbewusst auf einen alten Wert: Vertraulichkeit.

(mon@ct.de) ct

### Literatur

- [1] Markus Montz, Geld hin, Geld her, PayPal, Paydirekt, Kwitt: Bezahl-Apps im Vergleich, c't 18/2022, S. 120
- [2] Markus Montz, Digitale Zahlmeister, Sicher und datensparsam mit dem Smartphone bezahlen, c't 3/2023, S. 20
- [3] Markus Montz, Kleines Logo, große Wirkung, Mit welcher Debitkarte Sie besser bezahlen: Girocard oder Visa und Mastercard, c't 22/2022, S. 114

## Kwitt: Haste mal 'ne Mark?

Ebenfalls zur Dachmarke Giropay gehört das P2P-Bezahlsystem Kwitt, über das sich Privatpersonen mithilfe ihrer Handynummern Geld schicken können. Kwitt ist bisher Teil von Onlinebanking-Apps für Smartphones; lange Zeit boten es vor allem die Sparkassen und Volks- und Raiffeisenbanken an. Auch Kwitt soll mit Giropay zusammenwachsen. Will man bargeldlos Geld für ein Geburtstagsgeschenk einsammeln, sich unterwegs gegenseitig Geld leihen und zurückzahlen oder auf dem Flohmarkt kleine Beträge an andere Privatleute schicken, regelt man das hierzulande vorrangig über PayPal – während dafür beispielsweise in der Schweiz Twint, in Spanien Bizum und in Schweden Swish die Mittel der Wahl sind.

In der Giropay-App ist eine rudimentäre P2P-Zahlungsfunktion bereits implementiert. Doch genau wie bei Kwitt kann das System Geld nur an Kontakte aus dem eigenen Adressbuch im Smartphone übertragen – eine Einschränkung, die beispielsweise für Zahlungen auf dem Flohmarkt unpraktischer ist als die Abwicklung per PayPal [1]. Hinzu kommt, dass Sparkassen-Kunden bisher mit der Giropay-App kein Geld senden können. Wann und in welchem Umfang weitere P2P-Funktionen in Giropay einfließen, beispielsweise Zahlungen an Personen ohne Adressbucheintrag, ist noch offen.



**Kwitt gehört nominell zu Giropay, es bleibt aber vorerst Teil der Onlinebanking-Apps der Banken, die es anbieten.**



Bild: Michael Vogt

# Virenzensur

## Malware filtern per TLS-Inspektion

**Das Protokoll HTTPS schützt den Webverkehr durch Verschlüsselung vor Manipulation und Ausforschung. Es verhindert aber auch, dass Firewalls in Downloads versteckte Trojaner entdecken. Mit TLS-Inspektion kommen die Firewalls der Malware dennoch auf die Schliche. Wir zeigen, wie das funktioniert und welche Vor- und Nachteile die Technik hat.**

Von Markus Stubbig

**U**nverschlüsseltes Internet ist passé: Webdienste haben längst von HTTP (Hypertext Transfer Protocol) auf HTTPS (HTTP Secure) umgestellt, das den Kundenverkehr mit Ende-zu-Ende-Verschlüsselung (Transport Layer Security, TLS, früher Secure Sockets Layer, SSL) gegen Angriffe durch Manipulation und Abhören schützt.

Die großen Anbieter von Security-Lösungen betreiben schon länger HTTPS-Filter in ihren Geräten, doch inzwischen wird dieses Feature auch zum Standard in kostenfreien Open-Source-Firewalls. Die Arbeitsweise ist überall gleich: Die Firewall fungiert als gewollter Man-in-the-

Middle. Unterschiede liegen darin, wie gründlich die Engines im Datenstrom nach Trojanern und anderer Malware suchen.

Dieser Artikel beschreibt, wie eine Firewall die verschlüsselte Session „aufbricht“, die Inhalte scannt und dabei dem Webbrowser trotzdem eine gültige HTTPS-Verbindung präsentiert. Dazu gibt es

eine Übersicht von Firewall-Distributionen, die man auf eigener Hardware für kleine Netze gratis nutzen darf. Auf Seite 132 folgt eine Anleitung, wie man die Open-Source-Firewall OPNsense um einen HTTPS-Filter erweitert.

**ct Hardcore**

Doch bevor Sie sich auf TLS-Inspektion stürzen: Die Technik ist durchaus umstritten [1]. In Firmen ist die Analyse des Webverkehrs schon dann zustimmungspflichtig, wenn der Arbeitgeber der Belegschaft auch nur stillschweigend gestattet hat, den Internetanschluss in Pausen für private Zwecke wie beispielsweise Online-Banking zu nutzen.

## Aller Proxy Anfang

Der klassische Web-Proxy ist ein für den Internetsurfer im Regelfall unsichtbarer Vermittler zwischen dem Client (Browser etwa auf dem Notebook) und dem Internetserver, der die Webinhalte bereitstellt. Der Client redet mit dem Proxy, der wiederum mit dem Server.

Solche Proxies wurden eingeführt, um in der Internetanfangszeit Webinhalte lokal zwischenzuspeichern. Das hat die seinerzeit langsam Anschlüsse von unnötig doppelt übertragenen Inhalten verschont. Schon damals lag es nahe, die ohnehin durch den Proxy fließenden Daten gleich auf Malware oder unangemessene Inhalte zu untersuchen und dem Websurfer im Zweifelsfall eine warnende Webseite zu präsentieren.

Inzwischen läuft Webverkehr fast ausnahmslos über verschlüsselte Verbindungen, erkennbar am „https://“ vor der Serveradresse oder am Schlosssymbol. Solchen Verkehr müssen Firewalls und Webfilter als Man-in-the-Middle entschlüsseln, damit sie die Inhalte prüfen können. Sie verschlüsseln ihn anschließend wieder, damit der Client die Sitzung nicht abbricht. Das läuft im Einzelnen so ab:

- Der Client startet eine HTTPS-Verbindung zu einem Webserver.
- Der Proxy fängt die Anfrage ab und baut selbst eine HTTPS-Verbindung zum Ziel auf.
- Der Server erhält die Verbindungsanfrage; woher sie kommt, ist ihm egal, er antwortet.
- Jetzt hat der Proxy eine HTTPS-Verbindung zum Server.
- Der Proxy erzeugt spontan ein neues TLS-Zertifikat, das wie das des Ziels aussieht, sodass der Clientbrowser nichts bemerkt und den Proxy als Server akzeptiert.
- Der Proxy antwortet seinem Client im Namen des Servers und die verschlüsselte Verbindung zwischen Client und Proxy entsteht, ohne dass der Surfer – im Idealfall – davon etwas mitbekommt.

Damit hält der Proxy zwei TCP-Verbindungen pro Webzugriff: eine zum Client

und eine zum Server. Im Proxy liegen die Daten im Klartext vor, sodass er sie auf Malware untersuchen, oder wenn gewünscht, auch Inhalte nach Kategorien sperren kann.

## Zertifikate, Zertifikate

Kryptografische Schlüssel und Zertifikate bilden die Grundlage für das Vertrauen in HTTPS-Verbindungen. Deshalb hat der Proxy das geheime Kryptomaterial des Servers nicht – und normalerweise auch sonst niemand auf der Welt. Folglich muss der Proxy die HTTPS-Kommunikation mit seinem Client auf ein anderes Zertifikat stützen. Das fällt dem Browser auf, der seinem Anwender eine Zertifikatswarnung präsentiert.

Damit die ausbleibt, muss der Clientbrowser allen vom Proxy vorgelegten Serverzertifikaten vertrauen. Das klappt, indem der Proxy selbst zur Stamzzertifizierungsstelle wird (Certificate Authority, CA). Dafür erzeugt man ein selbstsigniertes Root-CA-Zertifikat oder eines für eine Unterzertifizierungsstelle, beispielsweise mit einem Tool wie XCA oder bei manchen Firewall-Distributionen auch über deren Konfigurationsseiten. Dieses Zertifikat kommt per Import in den Zertifikatspeicher der Client-Betriebssysteme; in Anwendungen, die ihren eigenen Zertifikatspeicher führen, muss man es separat einspielen.

Wer seine Computer per Gruppenrichtlinien und die Smartphones per Mobile Device Management verwaltet, spielt das CA-Zertifikat über deren Funktionen automatisch an alle betreuten Clients aus. Ob das geklappt hat, lässt sich mit dem Aufruf einer verschlüsselten Webseite wie ct.de prüfen.

## c't kompakt

- TLS-Verschlüsselung schützt Ihre Daten vor dem Ausgespähtwerden, aber verhindert auch, dass Virensucher in Downloads verborgene Malware entdecken.
- Mit TLS-Inspektion in der Firewall kann man einen Virensucher einschleifen, der verschlüsselte Downloads untersucht und vor Schädlingen warnt.
- Die Funktion gibt es in kommerziellen Firewall-Distributionen ebenso wie in Open-Source- und Community-Projekten.

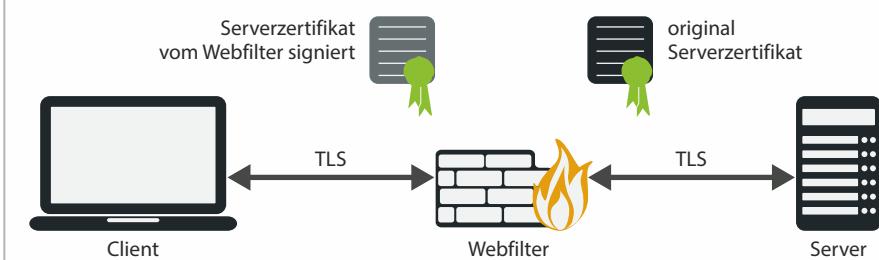
Beim Aufruf bekommt der Browser ein Zertifikat serviert, das zwar aufs Ziel – hier nach Umleitung www.heise.de – lautet, aber von der Zertifizierungsstelle des Webfilters signiert ist. Für den Webbrowser ist es ein gültiges Zertifikat bezogen auf die Webadresse, die ausstellende CA und das Ablaufdatum. TLS-Schwächen des Webfilters, etwa Fehlverhalten bei selbstsignierten Zertifikaten, ungültigen Hostnamen oder schwachen Protokollen, kann man über www.badssl.com untersuchen.

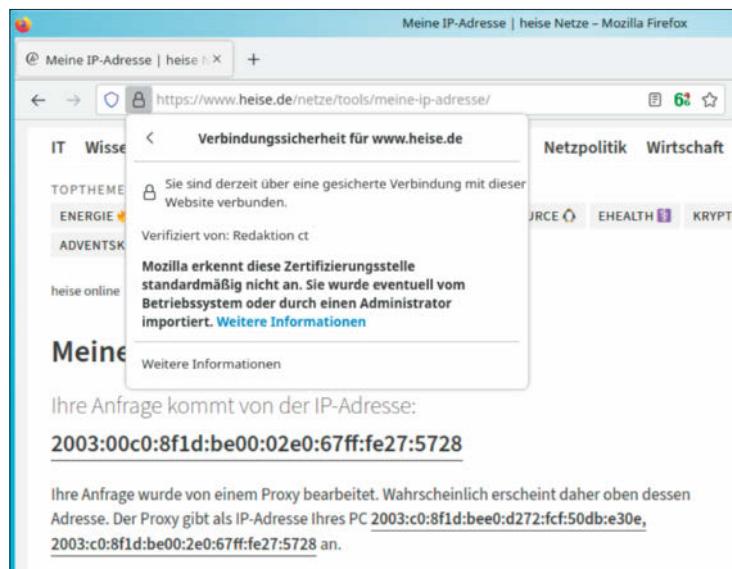
## Grenzen

Wer einen bunt gemischten EDV-Zoo betreibt, wird beim Verteilen des neuen CA-Zertifikats das Fluchen neu lernen. Denn dort stößt man auch auf harte Nüsse, die den Import in ihren Zertifikat-Store ver-

## Inspektion von TLS-Datenströmen

Ein in die Firewall integrierter Webfilter für verschlüsselte TLS-Datenströme sitzt als Proxy zwischen Client und Internetserver. Er weist sich dem Client mit spontan erzeugten Zertifikaten als angesteuertes Ziel aus und kann so den Datenverkehr entschlüsseln. Wenn man dem Client eine eigene Certificate Authority (CA) implantiert, bleiben Browser- und App-Warnungen aus.





**Der TLS-Inspektor erzeugt für alle aufgerufenen Webseiten im Flug eigene Zertifikate, die er als Root-CA selbst signiert. Deren Zertifikat muss man in die Clientbetriebssysteme und die Browser importieren.**

weigern, beispielsweise EC-Karten-Terminals, von der Belegschaft mitgebrachte private Smartphones, Smart-TVs oder IoT-Geräte.

Ein Zertifikat für Zwischenzertifizierungsstellen, das von einer bereits in den Geräten hinterlegten CA signiert ist, würde solche Probleme lösen. Dafür scheidet das bei Betreibern eigener Webserver beliebte Let's Encrypt aus, weil es sinnvollerweise nur übliche Serverzertifikate liefert. Denn andernfalls könnte sich jeder selbst Zertifikate beispielsweise für \*.microsoft.com ausstellen und Windows-Rechnern in seinem Netz beliebige Fake-Updates unterschieben. So endet hier das Gedankenexperiment der eigenen öffentlichen CA, denn der finanzielle und zeitliche Aufwand dafür ist enorm.

Anwenden mit Sachverstand beschert die TLS-Inspektion ein mulmiges Gefühl, denn „Feind hört mit“ und versteht jedes Datenpaket. Wenigstens lässt sich vergleichsweise leicht herausfinden, ob ein TLS-Inspektor in der Leitung sitzt: In diesem Fall sind die Zertifikate aller besuchten Webseiten von derselben CA signiert, was in der ungefilterten HTTPS-Praxis nie vorkommt. Es bleibt ein offensichtlicher Weg um den Filter herum: Nutzer könnten aus dem Firmennetz durch ein VPN zum Heimrouter tunnen. Das sollte der Admin in der Firmenfirewall unterbinden.

## Risiken und Nebenwirkungen

Der gewollte Man-in-the-Middle unterbricht die Ende-zu-Ende-Verschlüsselung und liefert mit der als vertrauenswürdig eingestellten Certificate Authori-

ty signierte, spontan erzeugte Zertifikate. Die Clients verlassen sich darauf und genau da liegt ein neues Risiko: Die Verantwortlichen müssen ihre selbst gebaute CA wie ein rohes Ei behandeln, damit deren Sicherheit zumindest ansatzweise der einer öffentlichen CA entspricht. Leicht gesagt, denn eine CA ist mit ein paar OpenSSL-Befehlen erstellt und wird ruckzuck zum Teil der produktiven Infrastruktur. Wer es richtig machen will, orientiert sich an den Richtlinien und Best Practices beim Aufbau einer Public-Key-Infrastruktur (PKI, [2]).

Eine weitere Unsicherheit liegt darin, dass ein Client nicht mehr die Vertrauenswürdigkeit bis zum Zielserver bewertet, sondern nur die kurze Strecke zum Proxy. Ob der weitere Weg sauber und sicher ist, validiert der Proxy. Wenn beispielsweise der Server ein ungültiges, selbst signiertes oder abgelaufenes Zertifikat serviert, muss der Proxy das bemerken und seinem Client ein Zertifikat generieren, das absichtlich fehlerhaft ist. Nur so kann der Nutzer sehen, dass die Kommunikation mit dem angesteuerten Ziel fragwürdig ist, und die Sitzung im Zweifel beenden, bevor Schaden entsteht.

Apropos ungültiges Zertifikat: Wenn Proxy und Client unterschiedliche Mengen an CA-Zertifikaten gespeichert haben, werden einzelne TLS-Verbindungen für den Proxy gültig sein, nicht aber für den Client, und umgekehrt. In der Folge surft der Anwender arglos auf einer Webseite, die sein Browser ohne TLS-Inspektion angemeckert hätte.

Admins bekommen Mehrarbeit, denn außer den Browsern verwenden auch Be-

triebssysteme und Anwendungen HTTPS für ihre Updates. Einige davon, wie beispielsweise das Windows-Update, vertragen sich nicht mit der TLS-Untersuchung. Diese muss man folglich per Liste von der TLS-Inspektion ausnehmen und diese Liste jedes Mal auffrischen, wenn sich am Update-Prozess der verschiedenen Betriebssysteme etwas ändert.

Weil der extern verschlüsselte Webverkehr in der Firewall im Klartext durchläuft, ist in der Firewall das Ausleiten und Analysieren der Daten trivial. Vertrauen in die Infrastruktur und ihre Admins ist unabdingbar, wird aber trotzdem in Einzelfällen enttäuscht werden.

Für Nutzer solcher Netze gilt deshalb: Unterlassen Sie auf Firmengeräten tunlichst alle privaten Internetdinge, vor allem solche, bei denen es um vertrauliche Informationen und um Geld geht (Online-Banking, Zahlungen per Kreditkarte). Falls der Arbeitgeber ein ungefiltertes Gast-WLAN anbietet, nutzen Sie dieses mit dem privaten Smartphone. Oder weichen Sie gleich auf Mobilfunk oder Ihr vertrauenswürdiges VPN aus.

## Mehr Dampf bitte

Nicht zu unterschätzen ist die in der Firewall erforderliche, zusätzliche Prozessorleistung für die doppelte Krypterei, also das gleichzeitige TLS-Ent- und Verschlüsseln jedes einzelnen Pakets. Wenn die Firewall-CPU dadurch an den Anschlag kommt, wird der Proxy zum Flaschenhals und bremst große Downloads aus, obwohl die Internetverbindung mehr könnte.

Als Beispiel dazu ein Vorgriff auf den folgenden Artikel: Ein Celeron-J3160-Prozessor lieferte im c't-Labor als transparenter HTTP-Proxy unter OPNsense beim Download einer großen Datei von einem Server in der vorgelagerten Netzwerkzone rund 330 Mbit/s. Dabei waren zwei seiner vier Kerne voll beschäftigt (rund 50 Prozent Gesamtlast auf dem Prozessor). Mit HTTPS blieben zirka 190 Mbit/s übrig. Wer eine schnellere Internetanbindung hat, braucht also auch einen schnelleren Prozessor, um unbremst surfen zu können.

Bei Appliances bietet eventuell der Hersteller oder der Zubehörhändel Kryptobeschleuniger als nachrüstbare Steckkarte. Ein Upgrade auf ein leistungsstärkeres Modell (vertikale Skalierung) oder eine zusätzliche Firewall (horizontale Skalierung) sind oft die sinnvollere Option.

## Alternative

TLS-Inspektion ist unter anderem umstritten, weil sie die Sicherheit von TLS und Zertifikaten untergräbt. Sicherheit geht aber auch ohne TLS-Inspektion, wenn man die Malware-Analyse à la Virenscanner auf die Clients verschiebt. Der Vorteil liegt in der verfügbaren Leistung: Hierbei muss keine zentrale Firewall alle Verbindungen prüfen, sondern die Aufgabe verteilt sich.

Wenn der Client einen Verstoß bemerkt, informiert er optional ein zentrales Dashboard und handelt nach einer vorgegebenen Richtlinie: blockieren, erlauben oder warnen. Problematisch wird dieser Ansatz, wenn es Geräte gibt, die der Administration des Unternehmens nicht unterstehen, zu alt sind oder schlicht zu wenig Leistung haben. Und klar, solche Software-Lösungen sind nicht gratis zu haben.

## Eigenheiten

Die Open-Source-Firewalls setzen auf den Proxyserver Squid und den Virenscanner ClamAV. OPNsense entstand als Abspaltung von pfSense und seitdem schwinden die Ähnlichkeiten. In der Web-GUI fasst pfSense den Web-Proxy und AV-Scanner zusammen, was die Konfiguration einheitlicher wirken lässt. Beide Dienste kommunizieren zwar über das Internet Content Adaptation Protocol (ICAP), aber die bei OPNsense noch nötige Fummeli (siehe folgenden Artikel) versteckt pfSense im Hintergrund.

Die Endian-Firewall nutzt dieselben Tools, reicht aber deutlich weniger Einstellungsoptionen über die Konfigurationsseiten zum Admin durch. So funktioniert Endian

zwar gut als Web-Proxy, ist aber nicht flexibel in allen Netzarchitekturen einsetzbar und auch noch nicht für IPv6 bereit.

OpenWrt geht den minimalistischen Weg und erwartet, dass der Admin über die Browzeroberfläche eine vollständige Squid-Konfiguration zufügt. Das garantiert maximale Flexibilität, erfordert aber tiefgehendes Squid-Wissen. Etwas mehr Komfort wäre schön und so ist OpenWrt als TLS-Inspektor allenfalls erste Wahl, wenn es ohnehin schon als Router arbeitet [3].

Sophos liefert mit seinen Security-Produkten UTM und XG den erwarteten Komfort, auch wenn sich die Konfigurationsseiten der beiden Produkte grundlegend unterscheiden. Als Proxy fungiert eine Eigenentwicklung. Da Sophos mit Virenscannern groß wurde, stammt dieser Teil ebenfalls aus eigenem Haus.

Bei der XG-Firewall gestaltet sich die Einrichtung am einfachsten: Sobald man in einer Regel die Webfilterung aktiviert, springt der Web-Proxy an. Eine weitere Checkbox startet die TLS-Inspektion. Das Konfigurieren der UTM ist nur wenig aufwendiger: Ihre Web-GUI verzahnt Filter, Profile, HTTPS, Kategorien, Benutzer und Aktionen. Das Ergebnis ist ein sehr granuläres Regelwerk, mit dem das HTTPS-Filtern umfassend gelingt, IPv6 inklusive.

## Zusammengefasst

Eine Firewall kann eine verschlüsselte Verbindung zwischen Client und Server öffnen und die übermittelten Daten auf Viren und Malware untersuchen. Damit das klappt, ist Vorarbeit nötig und alle Beteiligten auf der Clientseite müssen der

Firewall vertrauen. Wenn die Admins alle Randbedingungen erfüllen, entsteht in Summe ein Sicherheitsgewinn, denn dann schaut die TLS-Inspektion in die HTTPS-Verbindungen, ohne deren Klartextinhalte zu gefährden.

Prinzipiell kann man einen TLS-Inspektor mit den Linux-Tools Squid und iptables/nftables selbst zusammenstöpseln, aber der Aufwand dürfte für die meisten Interessenten zu groß sein. Mit fertigen Firewall-Appliances ist die Lernkurve leichter erklimmen. Sie nutzen dieselbe Software und legen eine Weboberfläche darüber, über die Admins das Procedere anhand verständlicher Regler und Einstellungen festlegen.

Für den praktischen Einsatz auf eigener Hardware eignen sich Kandidaten der Open-Source-Welt sowie kommerzielle Vertreter, die die Verwendung ihres Produkts für kleine Netze kostenfrei gestatten. Die nebenstehende Tabelle stuft die verschiedenen Firewall-Distributionen hinsichtlich ihrer Tauglichkeit als Webfilter und TLS-Inspektor ein. Auf den folgenden Seiten schildern wir, wie Sie das mit pfSense verwandte, FreeBSD-basierende OPNsense zum transparenten Webfilter machen. Die anderen Vertreter weichen in den dort gezeigten Schritten ab, funktionieren aber technisch ähnlich.

(ea@ct.de) ct

## Literatur

- [1] TLS-Interception: Kontroverse um HTTPS-Überwachung in Unternehmen, ct.de/-7330578
- [2] BSI TR-03145, Secure Certification Authority operation Version 1.1, Kapitel 6
- [3] Andrian Möcker, Mitroutelegenheit, OpenWrt virtualisiert auf Synology-NAS betreiben, c't 16/2022, S. 158

## Firewall-Distributionen mit TLS-Inspektion für kleine Netze

Produktnam	Endian	OpenWrt	OPNsense	pfSense	Sophos UTM	Sophos XG
Version	3.3.15	21.02.3	22.7.9	2.6.0	9.711-5	19.0.0
verfügbar seit	2005	2004	2015	2006	2011	2014
Herkunft	Italien	Community	Niederlande	USA	UK	UK
basiert auf	angepasstes Linux	angepasstes Linux	FreeBSD	FreeBSD	angepasstes Linux	angepasstes Linux
Open Source	✓	✓	✓	✓	—	—
eingeschränkt auf	—	—	—	—	50 Nutzer	4 CPU-Kerne, 6 GByte RAM
Transparenter Proxy auf Layer 2 / 3	— / ✓	✓ / ✓	— / ✓	— / ✓	✓ / ✓	✓ / ✓
auch für IPv6	—	✓	✓ <sup>1</sup>	✓	✓	✓
Proxy versteckbar / erkennbar	— / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / —	— / ✓
Viren/Malware-Scanner	✓	—	✓	✓	✓	✓
Kategorienfilter	✓	—	✓	✓	✓	✓
reicht ungültiges Zertifikat durch	✓	— <sup>2</sup>	✓	✓	✓	✓
Support für TLS 1.3	—	✓	✓	✓	—	✓
Support für HTTP/3 (QUIC)	—	✓	—	—	—	✓ <sup>3</sup>
Komplexität beim Einrichten	gering	hoch	mittel	mittel	gering	mittel

<sup>1</sup> Anpassungen per Kommandozeile nötig

<sup>2</sup> Seite wird blockiert (keine Auswahl möglich)

<sup>3</sup> abschaltbar

✓ vorhanden

— nicht vorhanden

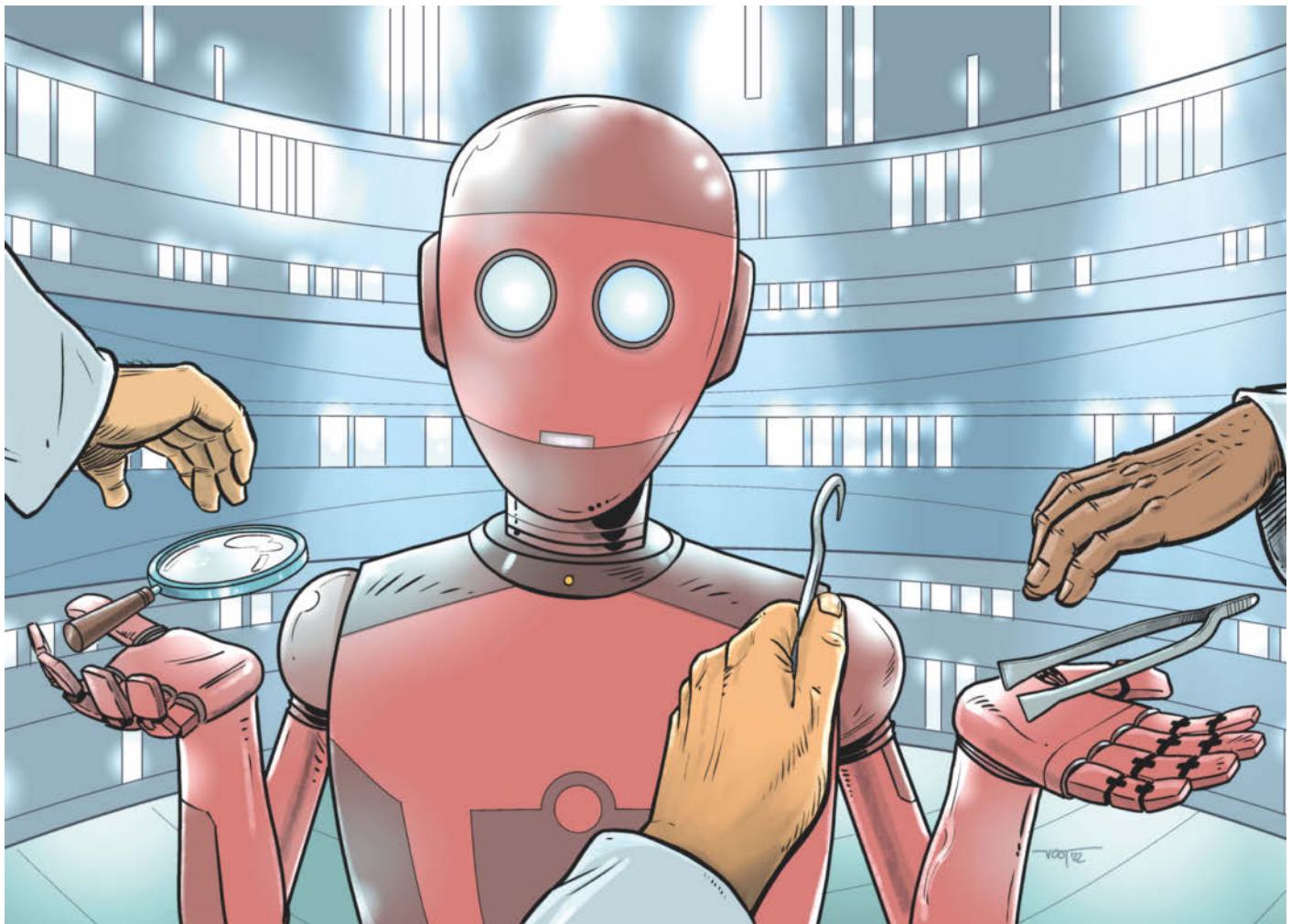


Bild: Michael Vogt

# Virenensor rüsten

## OPNsense-Firewall als TLS-Inspektor einrichten

**Firewall-Distributionen wie OPNsense können verschlüsselten Webverkehr analysieren und so das LAN vor Trojanern und anderer Malware schützen. Die Funktion lässt sich mit einer Handvoll Klicks an einem Nachmittag anwerfen.**

**Von Markus Stubbig**

Wer Webdownloads auf Malware prüfen möchte, muss die HTTPS-Verschlüsselung aufbrechen. Diese TLS-Inspektion ist technisch zwar nicht trivial,

aber zum Glück bringen moderne Firewall-Distributionen (siehe Seite 128) die dafür nötigen Funktionen bereits mit.

Wir zeigen am Beispiel von OPNsense, wie man einen Web-Proxy mit TLS-Inspektion einrichtet. Dabei gehen wir davon aus, dass OPNsense bereits installiert und für den Betrieb als Dualstack-Router eingerichtet ist. Sichern Sie diesen Zustand über System/Konfigurationen/Sicherungen auf Ihren PC. Das macht den Neuanfang leichter, falls Sie im Folgenden an irgendeiner Stelle versehentlich falsch abbiegen.

Das Modem hängt an einer der Netzwerkschnittstellen der Firewall und stellt

die Internetverbindung her; alternativ kommt sie von einem vorgelagerten Router wie etwa einer Fritzbox. Die zweite Firewall-Schnittstelle führt über einen Switch ins LAN und versorgt die dortigen Clients mit dem Internetzugang, gegebenenfalls auch drahtlos über WLAN-Access-Points.

Weitere LAN-Ports, wahlweise in der Firewall oder im nachgelagerten Switch, ermöglichen logisch getrennte Subnetze (Netzwerkzonen, etwa für Gäste oder Smart-Home- und Internet-of-Things-Geräte). Wenn das LAN aus konfigurierbaren Switches und Multi-SSID-fähigen Access-Points besteht, kann man solche zusätzlichen Netz-

**ct Hardcore**

ct kompakt

- Mit TLS-Inspektion kann eine Firewall HTTPS-verschlüsselte Downloads auf Malware filtern.
  - Die Firewall-Distribution OPNsense braucht dafür zwei Erweiterungen und ein wenig Handarbeit auf der Kommandozeile, um die Browserkonfiguration zu ergänzen.
  - Für Update-Quellen gängiger Betriebssysteme lassen sich Ausnahmen anlegen, die ungefiltert durchlaufen.

werkzonen auch per VLAN-Tagging über einen Trunk-Port gebündelt aus der OPNsense-Firewall ausleiten.

Wir gehen im Folgenden von einer vor-geschalteten Fritzbox aus, die der Firewall per DHCPv4 eine IPv4-Adresse und per DHCPv6 mit Präfixdelegation einen /62-IPv6-Adressblock übergibt. LAN-seitig muss man in der Firewall einen IPv4-Adress-bereich einstellen, der sich von dem der Fritzbox (typischerweise 192.168.178.0/24) unterscheidet, damit Network Address Translation (NAT) funktioniert. Da OPN-sense standardmäßig den IPv4-Adressblock 192.168.1.0/24 verwendet, ist normaler-weise nichts zu ändern. IPv6-seitig verwen-det OPNsense in seinem LAN standard-mäßig das erste /64-Netz aus dem delegier-ten IPv6-Block.

Die Browserkonfiguration von OPNsense lauscht auf der Adresse des Default-Gateway (typisch 192.168.1.1), die OPNsense per DHCP im LAN verbreitet. Falls sie nicht antwortet, hängt man zwecks Diagnose Bildschirm und Tastatur an den Firewall-Rechner. Hat der nur eine serielle Schnittstelle, brauchen Sie einen USB-zu-RS232-Adapter für den PC, eventuell ein Nullmodem-Kabel sowie ein Terminalprogramm wie etwa PuTTY. Über diese Konsolezugänge zeigt OPNsense die Zustände der Netzadapter und ihre IP-Adressen an. Per Textmenü kann man Logdateien einsehen oder eine Shell aufrufen.

## Langlebiges Zertifikat

Im ersten Schritt erstellen Sie ein eigenes CA-Zertifikat. Die neue „interne Zertifizierungsstelle“ entsteht mit einem Klick auf den „+“-Knopf in der Weboberfläche bei System/Sicherheit/Aussteller. Die

Voreinstellungen sind weitgehend akzeptabel, aber die Lebenszeit sollten Sie deutlich höher setzen als die vorgegebenen 27 Monate, um häufige Stammzertifikatswechsel zu vermeiden. 10 Jahre sollten für die Lebensdauer der Hardware genügen.

Laden Sie das frisch erstellte CA-Zertifikat über den Exportieren-Knopf in der Listenzeile herunter. Doch Vorsicht: Die sehr ähnliche Schaltfläche direkt rechts daneben spuckt zusätzlich den privaten Schlüssel der CA aus, der tunlichst unter Verschluss bleiben sollte.

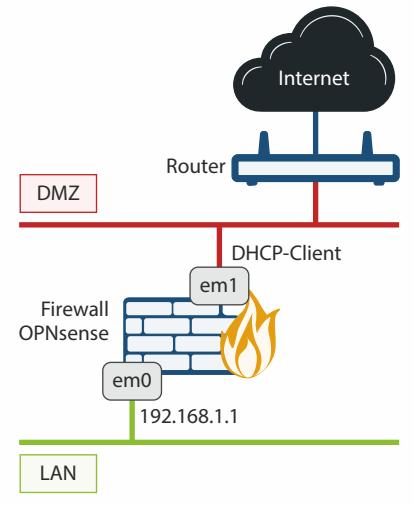
Wer beim späteren Import des CA-Zertifikats sicher gehen will, dass es korrekt eingespielt wurde, erstellt vorab einen Fingerprint. Kommandozeilenartisten nehmen zum Berechnen des Fingerprints den Befehl `openssl x509 -noout -fingerprint -in $dateiname`, alle anderen bedienen sich einer Webseite [1] oder des Tools XCA [2].

Clientseitig gehts einfacher: Bei Windows startet ein Doppelklick auf die Zertifikatsdatei einen Importassistenten. Weisen Sie ihn an, das Zertifikat nicht nur für den aktuellen Benutzer, sondern für „Lokaler Computer“ zu übernehmen. Bei der Frage nach dem Zertifikatsspeicher schalten Sie auf „Alle Zertifikate...“ um und wählen als Ziel „Vertrauenswürdige Stammzertifizierungsstellen“. Nach dem Import können Sie im Reiter „Details“ ganz unten den Fingerabdruck vergleichen. Nur bei Übereinstimmung hat es die Zertifikatsdatei unbeschadet zum Client geschafft.

Damit ist praktischerweise auch schon der Windows-Standardbrowser Edge abgehandelt. Anderen Browsern

## Firewall-Platzierung

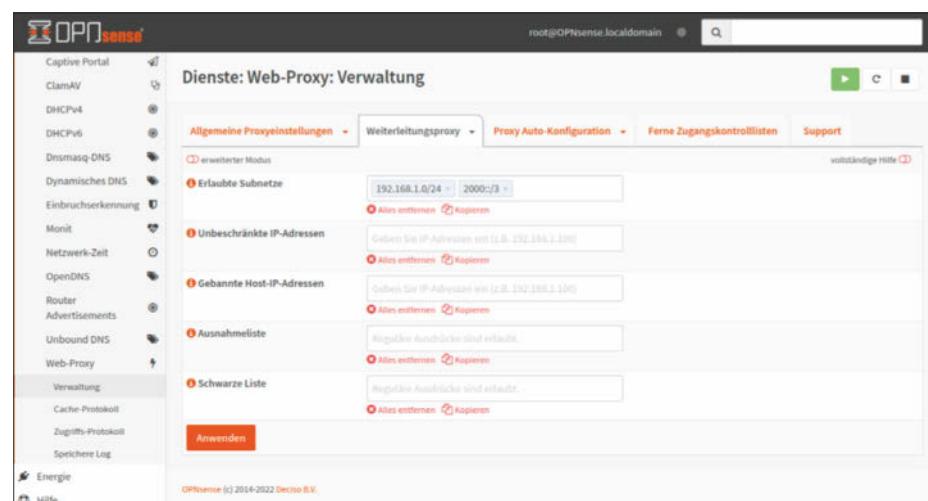
Damit eine Firewall mit TLS-Inspektion allen Verkehr erwischt, setzt man sie zwischen das (W)LAN und den Router. Das Netz zwischen Router und Firewall wird so zur De-Militarized Zone (DMZ).



müssen Sie das Zertifikat separat implantieren. Bei Firefox finden Sie die Funktion weit unten im Einstellungen-Menü unter „Datenschutz & Sicherheit“. Setzen Sie beim Importieren ein Häkchen, damit Firefox dieser CA zum Authentifizieren von Webseiten vertraut.

## TLS inspizieren

Jetzt kann OPNsense endlich den Webfilter anwerfen, und zwar im ersten Schritt nur die Proxy-Funktion. Die Malware-Analyse folgt, wenn der Proxy läuft, was



Bei OPNsense's Proxy-Einstellungen verbirgt sich die „Zugangskontrollliste“ zum Freigeben der internen IP-Adressen hinter dem kleinen Dreieck des Reiters „Weiterleitungsproxy“.

die eventuelle Fehlersuche erleichtert. Die Proxy-Einstellungen liegen im OPNsense-Menü bei Dienste/Web-Proxy/Verwaltung. Schalten Sie hier den Proxy ein.

Im zweiten Reiter „Weiterleitungsproxy“ bekommen die Optionen „Transparenten HTTP-Proxy aktivieren“ und „Aktiviere SSL-Untersuchung“ ein Häkchen, beim „Proxy Interface“ der Loopback- und der LAN-Adapter. Als „zu verwendende CA“ wählen Sie das eben erzeugte Zertifikat aus.

Klappen Sie nach dem „Anwenden“ mit einem Klick auf das kleine Dreieck das Reiter-Submenü aus. In der „Zugangskontrollliste“ tragen Sie als „Erlaubte Subnetze“ den IPv4-Bereich des LANs ein (192.168.1.0/24) sowie für IPv6 alle globalen Adressen (2000::/3). Denn diese verwenden die LAN-Clients für ihre IPv6-Verbindungen ins Internet.

Der nächste Schritt ist spezifisch für OPNsense und pfSense: Die Client-Anfragen aus dem LAN gelangen erst zum Webfilter, wenn man eine Weiterleitungsregel manuell einrichtet. Andere Firewalls erstellen sie automatisch.

Legen Sie bei Firewall/NAT/Portweiterleitung insgesamt vier Umlenkregeln an, jeweils zwei für HTTP und HTTPS auf IPv4 und zwei entsprechende auf IPv6. Als Schnittstelle wählen Sie „LAN“, als Protokoll „TCP“, als Quell- und Zieladressen sowie Quellports „jeglich“ und als Zielport jeweils den passenden, 80 für HTTP, 443 für HTTPS. Das Umleitungsziel wird ein „Einzelner Host“, der für IPv4 127.0.0.1 und für IPv6 fd01::1 heißt; HTTP geht an Port 3128, HTTPS an 3129.

Die übliche IPv6-Localhost-Adresse ::1 funktioniert bei OPNsense wegen des zugrunde liegenden FreeBSD nicht, weswegen wir eine Unique Local Address (ULA) eingesetzt haben.

Beim Erstellen der Weiterleitungsregeln legt OPNsense automatisch unter Firewall/Regeln/LAN Pendants an, die den gewünschten Verkehr akzeptieren. Weil die übergeordneten Standardregeln schon alles hereinlassen, können Sie diese vier Einträge löschen.

## Extra adressiert

Nun braucht der Proxy seine ULA. Klicken Sie bei Schnittstellen/Virtuelle IPs/Einstellungen“ auf den „+“-Knopf und tragen Sie für die LAN-Schnittstelle die Adresse „fd01::1“ ein.

Leider bot die OPNsense-Browserkonfiguration beim Erstellen dieser Anleitung keine Einstellmöglichkeit, mit der

man Squid diese Adresse beibringen kann. Der folgende Workaround auf der Root-Shell schiebt dem Web-Proxy drei zusätzliche Konfigurationszeilen unter, damit er auf HTTP- und HTTPS-Anfragen über IPv6 lauscht:

```
cat <<EOF >/usr/local/etc/squid/auth/4
lsquid_ipv6_lan.conf
http_port [::]:3128 intercept
https_port [::]:3129 intercept ssl-4
bump cert=/var/squid/ssl/ca.pem dyna-4
mic_cert_mem_cache_size=10MB genera-4
te-host-certificates=on
acl localnet src 2000::/3
EOF
service squid restart
```

Mit der Listen-Adresse [::] müssen Sie diese Einstellung nicht anfassen, falls Sie den ULA-Präfix (fd01::/64) ändern. Die acl-Zeile sorgt dafür, dass der Proxy Webverkehr von den globalen IPv6-Adressen (Globally Unique Addresses, GUA) der LAN-Clients akzeptiert.

Jetzt sollte der Webfilter die HTTP(S)-Verbindungen abfangen. Rufen Sie auf einem Client im Firewall-LAN mit dem Webbrowser https://ct.de/ auf und klicken Sie sich über das Schlosssymbol zu den Zertifikatseigenschaften durch. Dort muss der im selbst erstellten CA-Zertifikat eingetragene Name als Aussteller auftauchen.

Falls nicht, verrät die Logdatei unter Dienste/Web-Proxy/Zugriffsprotokoll, ob Webanfragen der LAN-Clients beim Proxy ankommen. Vergleichen Sie in der OPNsense-Konfiguration, ob alle bisher genannten Schritte übernommen wurden

und holen Sie eventuell fehlende Einstellungen nach. Vielleicht hatten Sie an einer Stelle vergessen, auf den Speichern-Knopf oder auf „Änderungen übernehmen“ zu klicken. Ein Neustart der Firewall zwischendurch wirkt manchmal auch Wunder.

## Filterleistung

Schon das reine HTTPS-Ent- und Verschlüsseln braucht einige Rechenleistung, wie sich im c't-Labor zeigte: Dort lief OPNsense 22.7.9 auf dem Celeron-J3160-Prozessor (vier mit maximal 2,2 GHz getaktete x86-Kerne) eines Yanling-Kompakt-PCs (NUC-C3, Test in c't 22/2021, S. 106).

HTTP-Verkehr reichte das Kästchen mit rund 330 Mbit/s bei knapp über 50 Prozent CPU-Last weiter. Mit HTTPS ohne Filterung blieben zirka 190 Mbit/s übrig. War der ClamAV-Filter zugeschaltet, sank der Durchsatz noch mal ein Stückchen auf gut 170 Mbit/s. An einem 100 Mbit/s schnellen Internetanschluss bremst solche ein Kästchen also noch nicht, bei der nächstschnelleren Tarifstufe (200/250 Mbit/s) aber schon etwas.

OPNsense bringt im Lobby-Menü wie andere Firewalls sein Dashboard mit, das die aktuelle Hardwareauslastung anzeigt. Wenn dort bei längeren HTTPS-Downloads 50 oder mehr Prozent CPU-Last erscheinen, sollten Sie die weiteren Indikatoren im Reporting-Bereich der Weboberfläche in Augenschein nehmen.

Unter Berichterstattung/Gesundheit erscheinen aktuelle und historische Werte, gemittelt über 10 Minuten. Wann die Firewall die meiste Arbeit hat, deckt Traffic/

	Quelle	Ziel	NAT				
	Schnittstelle	Protokoll	Adresse	Ports	IP	Ports	Beschreibung
1	LAN	TCP	-	80	127.0.0.1	3128	Anti-Aussperregel
2	LAN	TCP	-	443	127.0.0.1	3129	
3	LAN	TCP	-	80	fd01::1	3128	
4	LAN	TCP	-	443	fd01::1	3129	

Legend: Aktivierte Regel, Deaktivierte Regel, Alias (zur Betrachtung/Bearbeitung klicken), Keine Weiterleitung, Deaktiviere keine Umleitung, Verknüpfte Regel, Verknüpfte Regel deaktiviert.

**Web-Anfragen der LAN-Clients landen beim Proxy, wenn man in der Firewall vier Weiterleitungsregeln anlegt, jeweils für HTTP und HTTPS sowie IPv4 und IPv6.**

LAN auf. Klicken Sie bei CPU und Arbeitsspeicher auch die längeren Intervalle durch. Wenn zu Bürozeiten die 70-Prozent-Marke die meiste Zeit überschritten wird, sollten Sie über ein Hardware-upgrade nachdenken.

## Schutz erweitern

Mit den HTTPS-Verbindungen über den Proxy ist die Grundlage für den Webschutz per TLS-Inspektion gelegt. Dafür bietet OPNsense einen VirensScanner (ClamAV) und einen Kategoriefilter, der externe Sperrlisten im Reiter „Ferne Zugangs-kontrolllisten“ des Proxys einbindet.

Den VirensScanner holen Sie unter System/Firmware/Erweiterungen mit Klicks auf das Plus-Zeichen bei den Plug-ins os-clamav und os-c-icap ins Boot. ClamAV gehört mittlerweile zu Cisco, wird aber als Open-Source weiterentwickelt. C-ICAP verbindet den Scanner mit dem Web-Proxy.

Nach der Installation setzen Sie unter Dienste/C-ICAP/Konfiguration das Starter-Häkchen sowie im „Antivirus“-Reiter eines bei „Aktiviere ClamAV“. Entsprechend schalten Sie bei Dienste/ClamAV/Konfiguration den clamd- sowie den fresh-clam-Dienst ein und lassen bei der Gelegenheit die Virensignaturen herunterladen. Das wird je nach Geschwindigkeit Ihres Internetanschlusses wenige bis viele Minuten dauern.

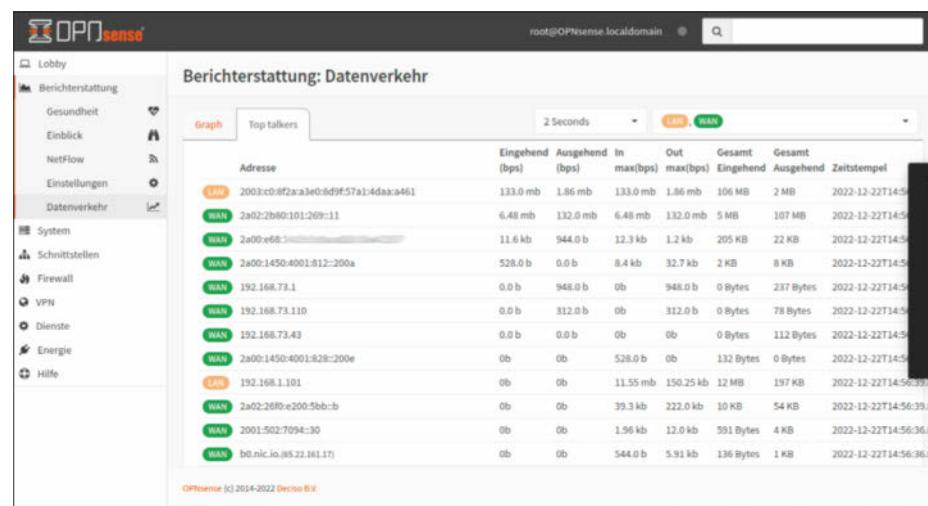
Die komplette Signaturdatenbank machte sich auf unserem System mit rund 1,5 GByte im Arbeitsspeicher breit. Die Firewall-Appliance sollte also mindestens vier GByte RAM haben.

Im letzten Schritt weisen Sie den Web-Proxy an, den VirensScanner zu verwenden. Dafür muss nur ein Häkchen an die Option „ICAP aktivieren“ im Untermenü „ICAP-Einstellungen“ des Reiters „Weiterleitungsproxy“. Starten Sie nun die Firewall im Menü unter Energie neu und warten Sie ein paar Minuten, bis sich alles zurechtgerückelt hat.

Ob der Virenschutz greift, zeigt ein Browserzugriff auf die EICAR-Testdatei [3]. Ihr Inhalt ist harmlos und als Funktionstest für alle VirensScanner gedacht. Der Browser sollte auffällig vor Win.Test.EICAR\_HDB-1 warnen.

## Finger weg!

Zwar lässt sich jede TLS-Verbindung mit solch einer Middle-Box untersuchen. Aber manche Anwendungen stellen ihren Betrieb ein, wenn sie den Schnüffler im Datenpfad entdecken. Prominente Beispiele



**OPNsense liefert im Reporting-Bereich, was Fritzboxen vermissen lassen: Die Top-talkers-Statistik mittelt über bis zu 10 Sekunden, welche Hosts wie viele Daten ziehen. Oben steht, wer gerade die Leitung zustopft.**

sind das Windows-Update und Googles Play Store. Ersteres gab bei uns trotz eingespieltem CA-Zertifikat mit dem Fehler 0x801901f7 auf. Auf einem Android-12-Gerät meinte Letzterer, er habe keine Internetverbindung und möchte nicht mal Updates herunterladen, die bereits in seiner Liste standen.

Für solche Fälle können Sie in der Web-Proxy-Konfiguration Ausnahmen anlegen, von denen Squid die Finger lässt. Im Reiter „Weiterleitungsproxy“ wartet ganz unten ein Eingabefeld für „Nicht abzufangende SSL-Seiten“. Es akzeptiert Domänennamen, Subdomains, Teile davon und auch Wildcards wie \*.microsoft.com.

Welche Servernamen einzutragen sind, beantwortet die Dokumentation oder ein Blick in die Logdatei des DNS-Resolvers kurz nach dem Updateversuch. Weitere Hinweise gibt die Squid-FAQ-Seite [4].

## Mehr erkennen

ClamAV ist dafür bekannt, nicht die beste Erkennungsrate zu haben. Es fällt sogar bei ein paar der bekannten Tests [5] durch. Wer mehr Schutz wünscht, kann auf inoffizielle Definitionsdateien von Nutzergruppen zurückgreifen oder eine kostenpflichtige Signaturquelle anzapfen.

Ein paar inoffizielle Signatur-Provider listet OPNsense bereits in seiner Web-oberfläche, sie werden in der Grundeinstellung jedoch nicht genutzt. In der ClamAV-Szene sind ferner die Signaturen von Sanesecurity beliebt. Die Site finanziert sich durch Spenden, pflegt eigene Signa-

turdatenbanken und bündelt sie mit dem Content anderer Anbieter. Wer die Datenbank-URLs nicht händisch in OPNsense einfügen möchte, kann das Installer-Skript von eXtremeSHOK nutzen [6].

## Unsichtbar

Der entstandene Web-Proxy sitzt zwar transparent im Datenpfad, ist aber mit traceroute leicht als Layer-3-Gerät auf IP-Ebene erkennbar. Andere Firewall-Produkte, etwa die von Sophos (siehe vorigen Artikel), bieten einen Inline-Modus. Dabei verhält sich das Gerät wie ein Layer-2-Ethernet-Switch mit IP-Filter und TLS-Inspektor.

Das Netz kann damit ohne IPv4-Umadressierung durch das Firewall-NAT weiterlaufen und die Admins müssen die bestehende Infrastruktur nicht auf Links drehen. Solch ein Layer-2-Filter braucht eine IP-Adresse im LAN allein für seine Konfiguration. So kann der transparente TLS-Inspektor wieder spurlos aus dem Netz verschwinden, falls seine Anwesenheit unerwartete Probleme bereitet.

(ea@ct.de) ct

## Literatur

- [1] SAML X.509 Certificate Fingerprint, SHA1 Decoder (alle Links auch über ct.de/y599)
- [2] XCA, X Certificate and Key management
- [3] EICAR Anti-Virus Test File
- [4] FAQ zum Web-Proxy Squid
- [5] WICAR.org, Test Your Anti-Malware Solution
- [6] eXtremeSHOK, Basic guide to Installing and Updating on pfSense 2.5+

**Literaturlinks:** ct.de/y599

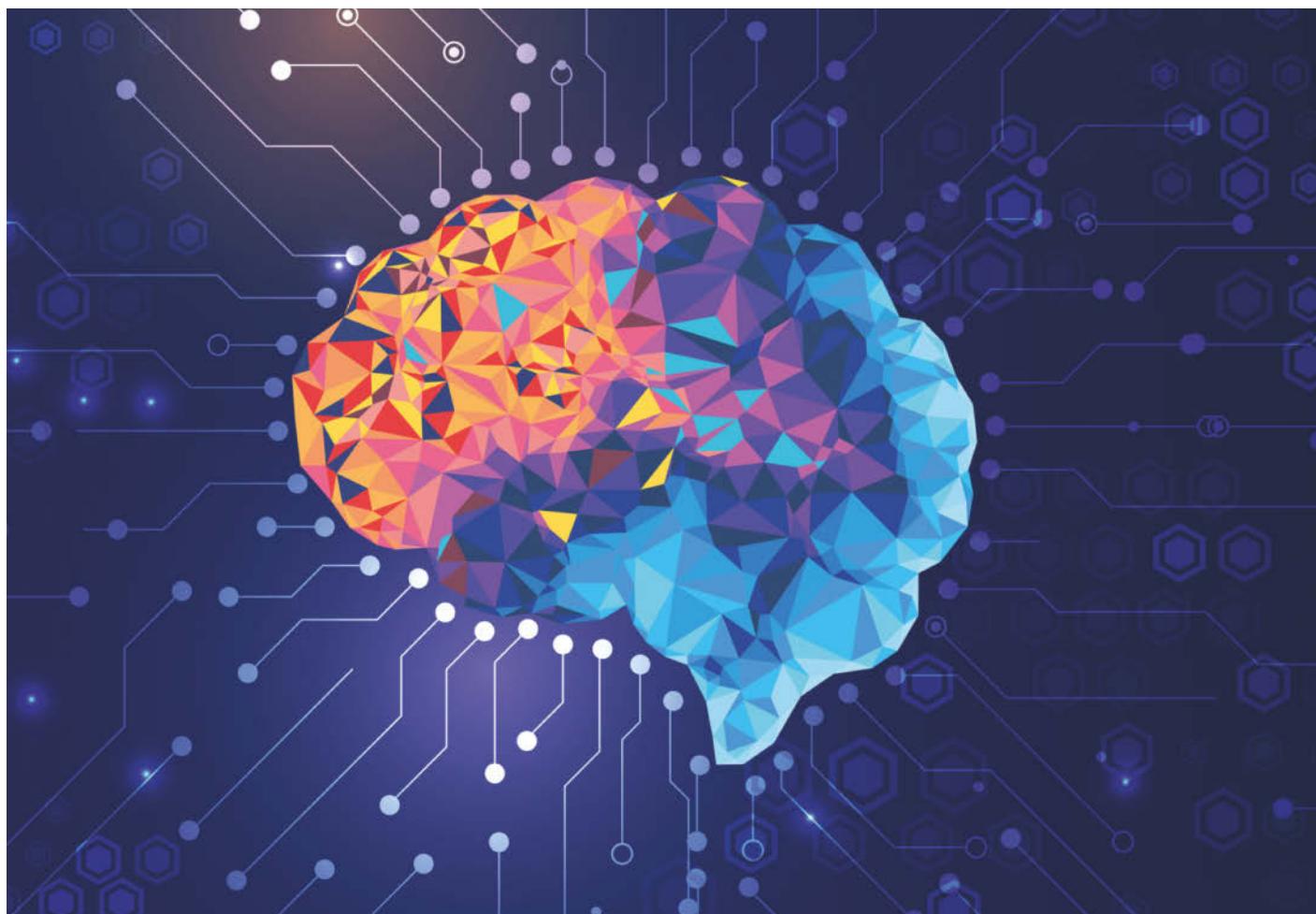


Bild: kras99 | stock.adobe.com

# Das Gehirn als Vorbild

## Neuromorphe Computer: Biologisch inspirierte Datenverarbeitung

**Die Menschheit giert nach immer mehr Rechenleistung, doch die gängigen Computerarchitekturen stoßen zunehmend an physikalische Grenzen. Auf der Suche nach neuartigen Konzepten orientieren sich Computerwissenschaftler deshalb am menschlichen Gehirn und versuchen, die Funktionsweisen biologischer Nervensysteme technisch nachzuahmen.**

Von Thomas Brandstetter

Was kommt nach Moore? Diese Frage treibt Forscher und Tech-Konzerne gleichermaßen um. Gemeint ist das Mooresche Gesetz, das seit Beginn des Computerzeitalters mit erstaunlicher Zuverlässigkeit beschreibt, wie sich die Anzahl der in einen Chip integrierten Baulemente alle ein bis zwei Jahre verdoppelt. Doch die dafür nötige Verkleinerung von Transistoren stößt langsam, aber sicher an knallharte, physikalische Grenzen. Dabei trägt jeder von uns eine Rechenmaschine auf den Schultern, die im Laufe von Millionen Jahren Evolution eine enorme Effizienz ausgebildet hat: das Gehirn. Es würde gleich mehrere Probleme lösen, diese Prozesse technisch nachzubauen.

Im Alltag kommt das Gehirn mit lediglich 25 Watt aus und erledigt Aufgaben, die jedes KI-System hoffnungslos überfordern. Während Prozessoren im strengen Takt der Systemuhr Nullen und Einsen durch Register, Caches und Speicher schieben, arbeitet das Gehirn ohne Hauptspeicher und ohne fixen Rhythmus auf Basis sogenannter Spikes. Diese elektrischen Impulse entstehen, wenn eines der knapp 86 Milliarden zu einem Netzwerk verbundenen Neuronen feuert, um Information an Tausende andere Neuronen zu übertragen. Wird ein Neuron wiederum von genügend solcher Spikes angeregt, beginnt es seinerseits zu feuern und die Datenverarbeitung ist in vollem Gang.

## **Effiziente Vorgaben**

„Im Gehirn sind nie mehr als ein Prozent der Neuronen gleichzeitig aktiv. Deshalb ist es auch so energieeffizient“, erklärt Christian Mayr, Professor für Hochparallele Systeme und Neuromikroelektronik der Technischen Universität Dresden. „Es verdichtet Informationen extrem, ist auf Neuigkeiten ausgelegt und versucht ständig, auf seine Umwelt zu reagieren und sie vorherzusagen.“ Nur wenn etwas nicht der Vorhersage entspricht, wird Aufmerksamkeit darauf gelenkt.

In einer Zusammenarbeit mit der University of Manchester war Mayr an der Entwicklung des Supercomputers SpiNNaker2 (Spiking Neural Network Architecture) beteiligt. Während man sich beim Vorgängermodell SpiNNaker1 noch mit dem Zusammenschluss einer Million Smartphoneprozessoren des Typs Arm968E-S begnügte, soll der SpiNNaker2 mit 10 Millionen Prozessorkernen die nötige Rechenleistung für die nächste Generation von künstlicher Intelligenz bereitstellen. Auch er läuft zwar wie herkömmliche Computer auf Basis digitaler Transistoren, seine Architektur ist aber bereits teilweise an die Funktionsweise des Gehirns angepasst.

„So wie das Gehirn Informationen auf das absolut Wesentliche reduziert, verwenden auch wir Codierungsprinzipien, die redundante Informationen weglassen“, sagt Mayr. Allein die Netzhaut im Auge mit ihren vier Zellschichten reduziert die permanent einströmenden visuellen Informationen bereits auf ein Hundertstel. Dementsprechend sind in der Regel auch bis zu 95 Prozent eines Videostreams redundant und damit verzichtbar, wenn sich von Bild zu Bild wenig ändert. „Herkömmliche Computerhardware läuft streng synchron und immer auf der gleichen Betriebsspannung und Taktfrequenz“, sagt Mayr. „Damit ist es ihr egal, wie viele Informationen darüber laufen. Sie wird immer gleich viel Energie verbrauchen.“ Die Prozessoren und Recheneinheiten des SpiNNaker2 dagegen können abhängig vom Informationsaufkommen hinauf- und hinuntergefahren werden, um weniger Energie zu verschwenden. Aktuell arbeiten Mayr und seine Kollegen in ihrem Start-up SpiNNcloud Systems daran, ihren neuromorphen Prototypen zur Marktreife zu bringen.

## Künstliche Synapsen

Ein weiteres Problem klassischer Computerarchitekturen ist die strikte Trennung

zwischen dem Speichern und dem Verarbeiten von Daten. Für jeden Rechenschritt muss das System zunächst die Ausgangswerte aus dem Arbeitsspeicher holen, zum Prozessor leiten und das Ergebnis anschließend wieder zurück in den Speicher transferieren. Dieser zeitaufwendige Vorgang wird immer mehr zum Flaschenhals der digitalen Technik, da die Prozessoren zwar immer schneller werden, das Auslesen der Speicher damit allerdings nicht mithält.

„Hier kann man vom Nervensystem viel lernen“, sagt Hermann Kohlstedt, der am Institut für Elektrotechnik und Informationstechnik der Universität Kiel die Arbeitsgruppe Nanoelektronik leitet. „Dort gibt es diese Trennung zwischen Verarbeitung und Speicher nicht.“ Wenn das Gehirn Informationen verarbeitet und einzelne Neuronen feuern, verstärken sich dadurch gleichzeitig die Synapsen, also die Verbindungen zwischen diesen Neuronen. Das Netzwerk passt sich also während der Verarbeitung an die aktuelle Aufgabe an, lernt dazu und speichert die Daten gewissermaßen in Form der synaptischen Veränderungen gleich mit.

Wie sich eine Synapse durch das Feuer der anliegenden Neuronen verändert, verstehe man schon sehr gut, sagt Kohlstedt. „Das lässt sich zum Beispiel mit memristiven Bauelementen bereits gut nachbilden.“ Memristoren – ein Kofferwort aus Memory (Speicher) und Resistor (Widerstand) – sind im Wesentlichen elektrische Widerstände mit einer veränderlichen Leitfähigkeit. Wenn Strom durch sie fließt, verändert sich die Stärke des Widerstandes – ähnlich wie bei der Synap-

ct kompakt

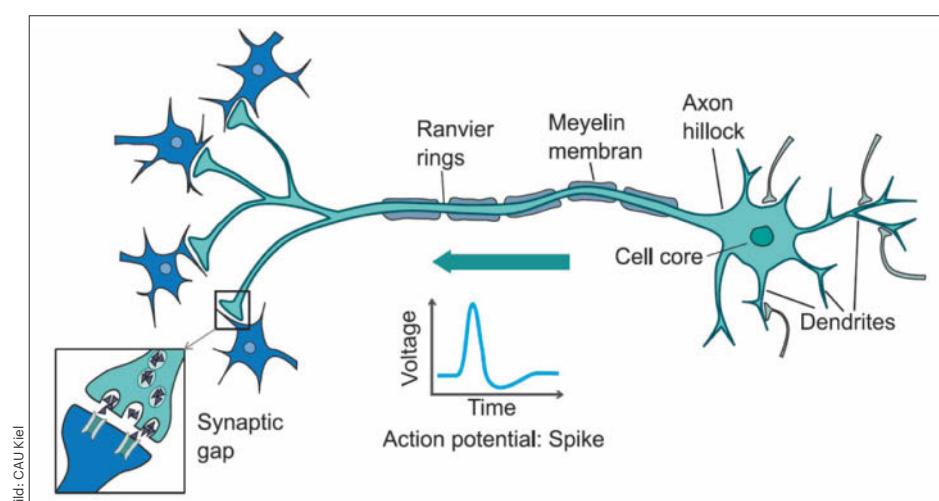
- Bislang gebräuchliche elektronische Bauelemente lassen sich nicht mehr beliebig verkleinern und optimieren.
  - Mit starren Taktfrequenzen und Betriebsspannungen verbrauchen sie unnötig viel Energie.
  - Architekturen, die das menschliche Gehirn zum Vorbild nehmen, rechnen vielleicht effizienter und schneller.

se, deren Leitfähigkeit durch die Anzahl der Spikes verändert wird, die über sie laufen. Diesen Wert erhält der Memristor auch nach dem Ausschalten des Stroms.

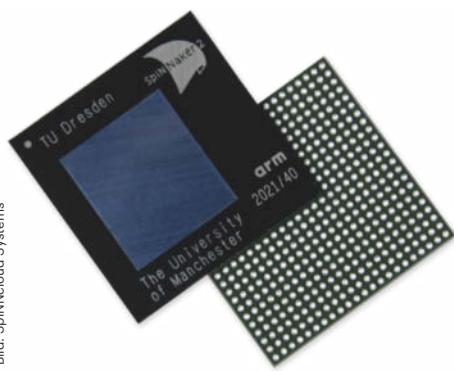
Einfache Memristor-Netzwerke mit 1000 oder mehr Bauelementen wurden bereits erfolgreich zur Mustererkennung eingesetzt und könnten herkömmliche Hardware in Zukunft bei speziellen, sich wiederholenden Rechenoperationen unterstützen, um das Gesamtsystem zu beschleunigen. „Der Aufbau von größeren Memristor-Netzwerken, die wirklich so ähnlich funktionieren wie das Nervensystem, steckt allerdings noch in den Kinderschuhen“, sagt Kohlstedt.

## Das Gehirn als Ganzes

Im Rahmen des Sonderforschungsbereiches „Neuroelektronik: Biologisch inspirierte Informationsverarbeitung“ der CAU Kiel loten Kohlstedt und seine Kollegen



Neuronen sind die elementaren Bauelemente des Nervensystems. Sie inspirieren Forscher unter anderem an der Universität Kiel zur Entwicklung neuromorpher Computersysteme.



**Für SpiNNaker 2 verbaut das Start-up SpiNNcloud Systems an der TU Dresden knapp 66.000 dieser neuromorphen Chips, von denen jeder 152 ARM-Prozessorkerne enthält. Das Gesamtsystem soll über 10 Millionen Kerne verfügen und damit den größten neuromorphen Supercomputer der Welt bilden.**

diverse Möglichkeiten aus: Sie wollen nicht nur die lokalen Eigenschaften wie die Funktionsweise von Synapsen auf die technische Informationsverarbeitung übertragen, sondern auch die Eigenschaften des gesamten Gehirns. „Deep Learning etwa funktioniert bereits recht gut“, sagt Kohlstedt. „Dabei hat man dafür eigentlich nur rudimentäre Eigenschaften von Neuronen übernommen.“

Das Grundprinzip dafür stammt noch aus den 1960er Jahren und hat seinen aktuellen Höhenflug vor allem verbesserter Hardware, der massenhaften Verfügbarkeit von Trainingsdaten aufgrund der voranschreitenden Digitalisierung und der Entwicklung neuer, im Detail immer ausfeilterer Software zu verdanken. „Viele andere Aspekte des Gehirns hat man aber

komplett vernachlässigt, weshalb man für Deep Learning auch sehr viele Bauelemente und somit auch sehr viel Energie braucht“, sagt Kohlstedt. „Unser Ansatz ist es deshalb, noch tiefer in die Biologie reinzuschauen.“

Dabei stützen sich die Forscher vor allem auf Erkenntnisse aus Neurobiologie und Medizin. Dort liefern Messmethoden wie die Elektroenzephalografie (EEG), die die elektrischen Aktivitäten des Gehirns aufzeichnet, oder Magnetresonanztomographie (MRT) Anhaltspunkte darüber, welche Funktion das Gehirn an welcher Stelle hat. „Wenn jemand zum Beispiel eine andere Person erkennt, dann wirken die Neuronen über weite Bereiche des Gehirns wie ein Orchester zusammen“, erklärt Kohlstedt. „Das sind globale Effekte, die man messen kann, die wir gerne in unsere Schaltungen aufnehmen würden.“

### Neuronen am kritischen Punkt

Derzeit haben Kohlstedt und sein Team die sogenannte Kritikalität im Visier. Einer Modellvorstellung aus der Neurobiologie zufolge arbeitet das Gehirn am besten, wenn sich die Aktivität der Neuronen auf einem optimalen Niveau befindet. Unterhalb dieses kritischen Punktes herrscht zu viel Ruhe im Gehirn, darüber ist es zu sehr angeregt. „In beiden Fällen läuft die Informationsverarbeitung schlecht“, erklärt Kohlstedt. „Wenn sich das Gehirn dagegen nahe am kritischen Punkte befindet, reagiert es besonders gut auf äußere Einflüsse.“ Ein Beispiel aus der Physik: Wird ein ferromagnetisches Material wie Eisen erwärmt, geht die ursprüngliche Ordnung der Elementarmagneten nach und nach verloren. Bei der kritischen Temperatur

erreicht es schließlich einen Zustand der Unordnung. An diesem Punkt reicht ein kleines Magnetfeld, um das System zu beeinflussen.

Um dem Kritikalitätseffekt auf die Spur zu kommen, haben die Forscher Netzwerke aus elektronischen Oszillatoren untersucht, die ebenfalls als Kandidaten für künftige, neuromorphe Computersysteme gelten. Dabei werden die Spikes eines biologischen neuronalen Netzwerkes durch Schwingungen miteinander vernetzter Oszillatoren nachgebildet, die sich wie die Neuronen im Gehirn gegenseitig beeinflussen. Und obgleich solche Oszillatoren-Netzwerke noch nicht sehr weit gediehen sind und noch keine praktisch nutzbaren Berechnungen ausführen können, halfen sie den Forschern zu verstehen, wie Kritikalität entstehen kann. „Unsere mathematischen Modellierungen haben gezeigt, dass auch die Umgebung, also die Steuerung von außen dafür zuständig sein könnte, dass das Gehirn diesen optimalen Arbeitszustand erreicht“, sagt Kohlstedt.

Das scheint durchaus plausibel, denn wenn die Hypothese stimmt und das Gehirn durch bestimmte äußere Einflüsse auf einem optimalen Niveau arbeitet, ist das schließlich ein Resultat von Millionen Jahren Evolution, in denen die Umgebung ständigen Einfluss auf die Entwicklung des Gehirns hatte. „In unserer Arbeit haben wir gezeigt, wie man äußere Einflüsse nutzen kann, um damit auch ein technisches System an diesen optimalen, kritischen Punkt zu bringen“, sagt Kohlstedt. „Das ist ein weiterer Schritt auf dem Weg zu einer biologisch inspirierten Informationsverarbeitung.“



**Der neuromorphe Großrechner SpiNNaker1 (Spiking Neural Network Architecture) simuliert mit einer Million Smartphone-Chips Aspekte des Gehirns. Er entstand in Kooperation der TU Dresden und der Uni Manchester.**

## Wachstum und Entwicklung

Anders als künstliche Rechner verändert sich das menschliche Gehirn. Im Schnitt wächst es bis zum zweiten Geburtstag um etwa 2000 Neuronen beziehungsweise stolze zwei Millionen synaptische Verbindungen – pro Sekunde. Die Gesamtlänge seiner Axonen, also der Bahnen, über die die elektrischen Nervenimpulse laufen, wachsen in diesem Zeitraum mit einer Rate von zehn Metern pro Sekunde. „Mit unserer Forschung wollen wir ausloten, wie sich dieses Wachstum für die Informationstechnik nutzen lässt“, sagt Kohlstedt.

So wären etwa Oszillatoren-Netzwerke denkbar, in denen gewisse Oszillatoren zunächst ruhen und nicht an der Informationsverarbeitung teilnehmen. Erst wenn das System aktiv wird und Schwingungen austauscht, schaltet es diese Oszillatoren und die zugehörigen Verbindungen dazu. „Dann hätte man gewissermaßen ein wachsendes System nachgebildet“, sagt Kohlstedt. „Das ist zwar noch Zukunftsmusik, aber es erscheint mir durchaus realistisch, dass man so etwas irgendwann hinbekommen könnte, um den faszinierenden Prozess der Ontogenese zumindest teilweise technisch nachzubilden.“

## Simuliertes Gehirn

Um die Funktionsweise des Gehirns für die Technik nutzbar zu machen, muss man sie erst einmal verstehen. Biologen können zwar die räumliche Verteilung von Nervenzellen messen und statistische Aussagen über ihre Verbindungen treffen. Wie genau das neuronale Netz funktioniert, erschließt sich aus diesen Daten allerdings nicht. Hier kommen Neuroinformatiker ins Spiel, beispielsweise Prof. Wolfgang Maass vom Institut für Grundlagen der Informationsverarbeitung der Technischen Universität Graz. Ihm ist es gemeinsam mit seinem Team kürzlich gelungen, einen Teil des Gehirns einer Maus im Computer zu simulieren und so die Funktion des Sehens nachzubilden.

Grundlage für die Simulation ist das Modell des visuellen Kortex einer Maus. Dieses 51.978 Neuronen umfassende Stück der primären Sehrinde sei eines der am genauesten untersuchten Teile eines Gehirns, sagt Maass. Dahinter stehen mehrere Jahre intensiver Forschungsanstrengungen, unter anderem des 2003 gegründeten Allen-Instituts, das auf eine Spende von Microsoft-Mitgründer Paul Allen zurückgeht.



Bild: Allen-Institut

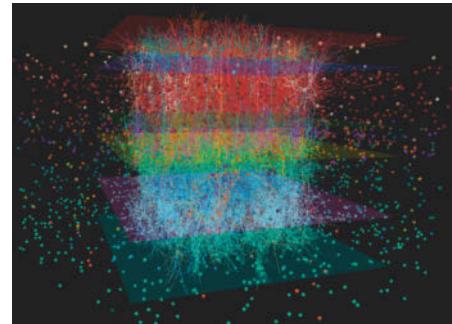


Bild: Allen-Institut

**Forscher des US-amerikanischen Allen-Instituts haben aus Tausenden digitalen Neuronen den Bereich des Mäusegehirns simuliert, der die visuellen Eindrücke verarbeitet.**

Als Input für ihre Simulation haben die Forscher in Graz die gleichen Bilder gewählt, die auch die lebende Maus gesehen hat. Das Spektrum reichte von einem einfachen Streifenmuster bis hin zu Bildern von Hunden oder Papageien. Der Vergleich zwischen statistischen Messungen an den Neuronen der Maus während des Betrachtens der Bilder und Messungen im simulierten Gehirnmodell zeigte schließlich, dass die Simulation erfolgreich war. Bei einer Aufgabe sah die Maus etwa eine Folge von Bildern und musste reagieren, wenn ein Bild sich vom vorhergehenden unterschied. Die Forscher testeten also nicht bloß das reine Sehen, sondern auch die Fähigkeit der Maus, mit visuellen Informationen umzugehen. „Eine Maus schafft diese Aufgabe mit einer Trefferquote von etwa 80 bis 90 Prozent“, sagt Maass. „Und unser Computermodell hat in etwa dieselbe Trefferquote erzielt.“

## Robustes Sehen

Zusätzlich haben die Forscher auch die Fehleranfälligkeit des simulierten Gehirns untersucht und mit einer künstlichen Intelligenz verglichen. Dazu haben sie absichtlich dieselben Störungen sowohl in einem künstlichen neuronalen Netzwerk als auch im Mausmodell erzeugt. Der Input enthielt also jeweils ein paar falsche Pixel und wie sich herausstellte, war das Mausmodell diesen Fehlern gegenüber robuster als das KI-Modell. „Das ist zum Beispiel wichtig für technologische Anwendungen wie das autonome Fahren, wo viele fatale Unfälle passieren, weil das Sehen nicht richtig funktioniert“, sagt Maass.

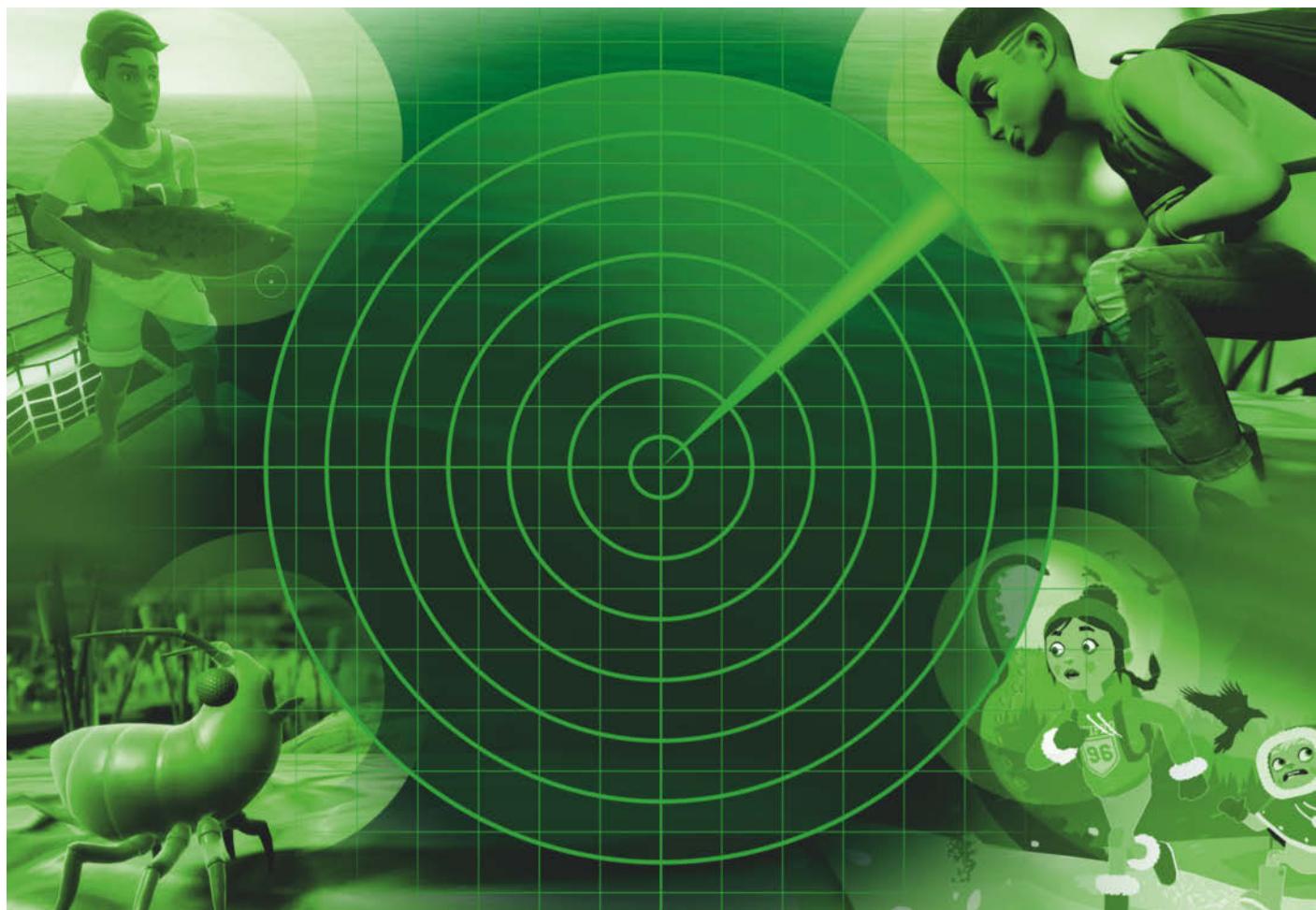
Außerdem sind in einem künstlichen neuronalen Netz für die Bildverarbeitung

**Neuroinformatiker an der Universität Graz haben ein digitales Mäusegehirn auf Bilderkennung getrimmt. Das Computermodell erkannte unterschiedliche Bilder mit einer ähnlichen Trefferquote wie eine echte Maus.**

fast alle Neuronen aktiv, was sehr ineffektiv ist. „Man kann sich das vorstellen, wie ein wildes Durcheinander in einer großen Gesprächsrunde“, erklärt Maass. Das menschliche Gehirn schafft es, wichtige Gesprächsinformationen zu filtern. Dafür gibt es eine eigene Klasse von Neuronen, die inhibitorisch wirken, andere Neuronen also vom Feuern abhalten. Dieser von der Evolution raffiniert ausgeklügelte Prozess findet in der künstlichen Intelligenz in der Regel noch keine Anwendung. „Aktuell versuchen wir in Projekten mit Partnern aus der Industrie, diese komplexen Schaltkreise mit Inhibition aus dem biologischen Modell zu abstrahieren und überlegen, wie man das auf künstliche, neuronale Netzwerke übertragen könnte“, sagt Maass.

## Fazit

Der Siegeszug des maschinellen Lernens mit seinen vage an biologische Nervensysteme angelehnten neuronalen Netzen scheint erst am Anfang zu stehen. Unermüdlich suchen Forscher und Industrie nach Anregungen aus der Biologie, um Informationstechnik leistungsfähiger und effizienter zu gestalten. Ihre Bemühungen reichen von der kleinsten Ebene, wo elektronische Bauelemente die lokale Funktion von Synapsen nachbilden sollen, bis hin zu den globalen Abläufen zwischen Milliarden von Neuronen, die als Vorbilder für neue Software und Computerarchitekturen dienen sollen. Und auch wenn das große Ziel, die Funktionsweise des Gehirns vollständig zu verstehen und nachzubilden, noch unerreichbar scheint, verspricht alleine der Weg dorthin bereits wertvolle Erkenntnisse und Innovationspotenzial. (akr@ct.de) **ct**



# Unter dem Radar

## Die besten Spiele, die 2022 unbeachtet blieben

**Bei all den Spielen, die im zurückliegenden Jahr 2022 veröffentlicht wurden, blieben viele gute Titel fast unbemerkt. Wir reichen die besten Geheimtipps nach.**

**Von Dominik Schott**

**E**in Blick zurück auf die Spiele des Jahres 2022 zeigt ein ausgesprochen buntes Bild: Außer dem japanischen Action-Rollenspiel Elden Ring und dem kinoreif in-

szenierten God of War: Ragnarök zählte auch das niedliche Katzenabenteuer Stray zu den größten Verkaufshits der letzten zwölf Monate. Auch manche Indie-Titel haben es unerwartet zu einiger Bekanntheit gebracht, darunter Vampire Survivors. Der pixelige Überlebenskampf gegen gigantische Gegnerhorden zählte 2022 zu den meistgespielten Games überhaupt. Oder das Tower-Defense-Game Dome Keeper, ein Familienprojekt aus Deutschland, das schon nach 24 Stunden über eine Million Verkäufe verbuchen konnte[1].

Trotzdem bleiben die meisten Jahresrückblicke unvollständig, denn viele hervorragende Neuerscheinungen aus dem letzten Jahr sind in der Menge der Veröf-

fentlichungen untergegangen und haben nicht das Publikum erreicht, das sie eigentlich verdient hätten. In diesem Artikel bereiten wir deshalb einigen hervorragenden Spielen eine Bühne, die 2022 unter dem Radar flogen – quer durch die Genres und Plattformen.

### ABRISS

Ein kleines deutsches Entwicklerteam steht hinter **ABRISS** (Windows ab 7,15 Euro), das ein simples Spielprinzip in Abrisskunst verwandelt. Die einzige Aufgabe im Spiel ist es, möglichst effizient Gebäude abzureißen. Doch die Bautätigkeiten inszeniert das Spiel mithilfe hochauflösender Voxel-Grafik außerordentlich spektakulär. Wenn

## ct kompakt

- Viele gute Spiele aus dem Jahr 2022 sind in der Flut der Neuerscheinungen untergegangen.
- Gerade Indie-Titel, die ohne aufwendiges Marketing veröffentlicht werden, finden oft nicht ihr Publikum.
- 15 Games vorwiegend aus der Indie-Ecke beleuchten die dunklen Ecken des vergangenen Spielejahres.

Hochhäuser kollidieren, sorgsam platzierte Sprengladungen in einer gigantischen Kettenreaktion explodieren und Stahlträger kontrolliert ineinanderkrachen, dann ist das eine wahre Freude – und nur auf den ersten Blick so leicht, wie es klingt.

ABRISS stellt für jede Aktion nur wenige Werkzeuge bereit. Untermalt wird das Spektakel mit hintergründig wummernden Elektroklängen, die auf den Tanzflächen von Berliner Klubs entstanden sind und punktgenau zum desaströsen Spielerlebnis passen.

### Against the Storm

Auf den ersten Blick hat **Against the Storm** (Windows ab 7,20 Euro) nicht viel mit unserer echten Welt zu tun: Biber, Eidechsen und Menschen siedeln Seite an Seite in einer feindseligen Welt, kämpfen gegen Monster und harte Wetterbedingungen ums Überleben. Doch das Fantasy-Aufbaustrategiespiel hat viele Parallelen zu den großen Themen unserer Zeit: Wetterkatastrophen sind ebenso wichtige Spielmechaniken wie der Raubbau an der Natur. Wenn wir zu rücksichtslos vorgehen, blindlings Wälder roden und allzu viele Ressourcen abbauen, steigt bald der Unmut unserer Bewohner, die sich die Besiedlung einer neuen Welt ganz anders vorgestellt haben.

Zusätzlich ist Against the Storm vollgepackt mit interessanten Spielmechaniken, die teilweise aus anderen Genres entlehnt sind. Das Ergebnis ist eine fordernde Simulation, die viele Stunden vor den Monitor fesseln kann.

### As Dusk Falls

**As Dusk Falls** (Windows ab 7, Xbox One, 30 Euro) ähnelt in seiner Inszenierung einer Netflix-Serie: In zwei Staffeln und einem Dutzend spielbarer Episoden erzählt das Spiel die Geschichte zweier Familien, deren

Schicksale irgendwann im Jahr 1998 zufällig ineinander verwoben werden. Das Spiel begleitet das Geschehen über einen langen Zeitraum mit handgezeichneten Szenen. In wichtigen, oft hochdramatischen Momenten kann man selbst eingreifen, um Entscheidungen zu fällen, Gespräche zu führen oder kleinere Areale zu erkunden.

Das Besondere an diesem Spiel ist eine Erzählung, die ihre Themen aus dem Leben greift: Es geht um komplizierte Familienverhältnisse, Gewalt, Untreue, Zukunftsängste. Ein Spiel, das unter die Haut geht und noch lange nach dem Abspann im Kopf verweilt.

### Blank Frame

Zugegeben: Wirklich hübsch ist **Blank Frame** (Windows 10, 4 Euro) mit seiner körnigen, verwaschenen Grafik nicht. In

diesem surrealen Horrorspiel irren Spielfiguren durch einen Wohnblock, in dem Seltsames passiert. Um herauszufinden, was vor sich geht, muss der Protagonist Henri das eigene Apartment Zentimeter für Zentimeter erkunden.

Die Hommage an das Horrorgenre der frühen 2000er Jahre zitiert fleißig bekannte Elemente des Monster-Horrors und Thrillers. Zwischen den groben Pixeln entsteht aber auch etwas Eigenes: Blank Frame ist nicht einfach gruselig, sondern schaurig. Langsam bekommt man eine Gänsehaut, während die eigene Spielfigur ganz langsam begreift, welcher Horror nur eine Tür weiter lauert.

### Diplomacy is not an Option

In **Diplomacy is not an Option** (Windows ab 7,21 Euro) zieht man als frisch gekürter



In ABRISS geht es darum, Gebäude möglichst effizient einzurütteln. Das ist häufig kniffliger als gedacht.



Das Spielprinzip von Against the Storm ist ungewöhnlich und setzt stark auf ineinander greifende Systeme. Wer gern optimiert, wird sich hier wohlfühlen.



Der grobkörnige Grafikstil von Blank Frame mag abschreckend wirken, doch hinter der Retrofassade verbirgt sich ein fesselndes Horrorspiel.



Ein ganz besonderer Look, eine dramatische Geschichte und mehrdimensionale Charaktere: As Dusk Falls hat alle Zutaten für ein paar unterhaltsame Stunden.

Burgherr eine Festung hoch, baut Bauernhöfe und holzt Wälder ab. Doch alle paar Minuten müssen Hunderte Gegner abgewehrt werden, die sich kopflos gegen die Stadtmauern werfen. Wie der Titel verspricht, ist Diplomatie keine Option und so liegt es am Burgherrn, dafür zu sorgen, dass mit den Gegnerhorden auch die eigenen Stadtmauern stetig wachsen.

Aus diesem Spielprinzip ergibt sich ein kurzweiliges Aufbaustrategiespiel, das mit seiner Inszenierung einen ganz eigenen Stil verfolgt. Dank der texturarmen Polygongrafik tut es das sowohl grafisch als auch erzählerisch, denn die Geschichte des Spiels nimmt sich selbst nicht allzu ernst.

### Faith: The Unholy Trinity

Der Entwickler und Künstler, der sich selbst Airdorf nennt, hat sich 2022 mit

seiner Horror-Trilogie **Faith: The Unholy Trinity** (Windows ab 7, 13 Euro) ein Denkmal geschaffen. Das Spiel ist nach jahrelanger Arbeit an den einzelnen Teilen als Gesamtwerk erschienen und begeistert vor allem mit überbordender Kreativität. Faith sieht aus, als hätte es eigentlich vor über 40 Jahren erscheinen müssen, schafft es aber trotz der extrem altbackenen Grafik, Horror auf den Bildschirm zu zaubern.

Das gelingt dem Macher einerseits mithilfe eines ausgeklügelten Sounddesigns, das in genau den richtigen Momenten Akzente setzt. Andererseits schreckt Airdorf auch nicht davor zurück, Gewalt, Gemetzel und Blutfontänen in Vollbild auf dem Bildschirm zu zeigen – dank des Pixellooks ausreichend entschärft, aber immer noch so intensiv, dass sich der Horror voll entfalten kann. Das

Spiel ist nichts für sanfe Gemüter, für Horrorfans dafür umso mehr.

### How Fish is Made

Eine Sardine geht auf eine Reise und stellt sich dabei die ganz großen Fragen des Lebens. Klingt skurril, ist aber die Essenz von **How Fish is Made** (Windows ab 7, gratis), einem Adventure, das im Innern einer großen Fabrik spielt. Oder ist es doch ein Magen? Das Spiel ist hier nicht eindeutig. In seiner Präsentation verzichtet es auf zeitgemäße Grafik und greift stattdessen auf technische Standards der Playstation-1-Zeiten Ende der 1990er Jahre zurück.

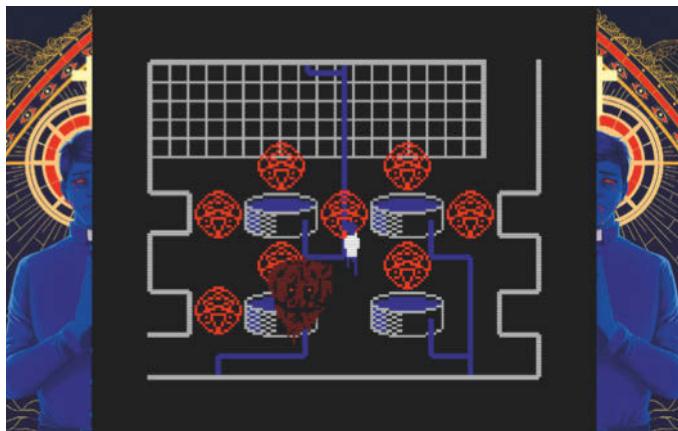
Die ominöse Selbstbeschreibung auf der Steam-Seite („Are sardines trustworthy? Are you? Do you want to be?“) klingt etwas abschreckend, doch das Dreierteam hinter How Fish is Made nimmt den Mund nicht zu voll. Am Ende löst das Spiel alle offenen Fragen auf. Dafür braucht man eine Portion Grips und wird nicht nur mit einem ungewöhnlichen Spielerlebnis (gratis!) belohnt, sondern darf auch die beste Gesangseinlage in einem Game der letzten 15 Jahre miterleben.

### Letters: A Written Adventure

Drei Schweizerinnen fanden sich im Studium zusammen, gründeten ein Studio und arbeiteten jahrelang an ihrem Debut namens **Letters: A Written Adventure** (Windows ab Vista, 15 Euro). Das Spiel begleitet ein junges Mädchen durch die Pubertät und schließlich bei ihren ersten Schritten ins Erwachsenenleben. Das Besondere: Das Spiel erzählt die sehr berührende, nahbare Geschichte in den Tagebüchern der Protagonistin, durch die wir Zeile um Zeile hüpfen, dabei Hindernisse



Stress, und trotzdem Spaß dabei: In Diplomacy is not an Option klopfen die Gegnerhorden im Minutentakt am Burgtor an. Gute Vorbereitung ist überlebensnotwendig.



Das Horrorspiel **Faith** wirkt wie ein Computerspiel aus den 1980er Jahren, erzählerisch aber ungemein kreativ und überraschend. Das Spiel schockt auch Genre-Kenner.



Nur wenige Spiele machen uns zum Fisch und lassen uns noch dazu in dieser Form den großen Sinnfragen des Lebens nachjagen.

überspringen und kleinere Wortsätsel lösen müssen.

Letters ist kein schwieriges, dafür ein umso gemütlicheres Spiel, das eine in diesem Medium selten gehörte Geschichte erzählt: Die einer jungen Frau, die erst noch ihren Weg finden muss und dabei von den Lebensgeschichten ihrer drei Schöpferinnen inspiriert wurde.

### Pentiment

Eigentlich steckt mit Obsidian hinter **Pentiment** (Windows ab 7, Xbox One, 20 Euro) ein echter Spielestudio-Promi. Doch selbst die Branchenveteranen hatten Probleme damit, die Entwicklung eines Spiels wie Pentiment zu rechtfertigen: Das Spiel setzt auf einen ungewöhnlichen Grafikstil und nimmt sich viel Zeit, bis die Geschichte in Fahrt kommt.

Alles dreht sich um einen Mordfall in einem hochmittelalterlichen Kloster, den der Spielheld lösen muss. Dazu spricht er lange mit möglichst vielen Menschen. Klingt trocken und das ist es anfangs auch. Doch das Spiel gewinnt mit der Zeit an Dramatik und vor allem: an Charme. Wesentlich trägt dazu die Grafik bei, die den Illustrationen in mittelalterlichen Büchern nachempfunden und damit in dieser Form nahezu einzigartig in der Spielewelt ist. Ein besonderes Detektivspiel also, mit klassischem Mordfall, aber innovativer Präsentation.

### Shotgun King: The Final Checkmate

Es ist wohl eine der ungewöhnlichsten Genre-Kombinationen auf dieser Liste: **Shotgun King: The Final Checkmate** (Windows ab 7, 10 Euro) bringt den unendlichen

Reiz eines Schachspiels mit dem Wieder-spielwert eines modernen Roguelites zusammen, das prozedurale Level generiert und auf Speicherstände verzichtet, die man im Falle des Versagens laden könnte. Mit Shotgun King hat das französische Indie-Studio Punkcake Delicieux ein Abenteuer mit einer neuartigen Spielidee erschaffen.

Hauptfigur dieses Abenteuers ist die Schachfigur des schwarzen Königs, der sich am weißen König rächen will, deswegen zur Schrotflinte greift und gegen die Spielfiguren seines Widersachers antritt. Die einzelnen Runden erinnern dabei nur wenig an Schach: Zwar bewegen sich alle Figuren, wie es das traditionelle Vorbild vorsieht, davon abgesehen nutzt Shotgun King aber ein eigenes Regelwerk. Der Spieler kann beispielsweise Karten ausspielen, die besondere Fähigkeiten für die

eigene Figur freischalten, seine Schrotflinte abfeuern oder übersinnliche Hilfe herbeirufen. Ein Titel, der vertraute Spiel-elemente zu etwas Neuem kombiniert.

### Signalis

Aus der Feder des Hamburger Indie-Studios rose-engine stammt das Horrorspiel **Signalis** (Windows, 20 Euro) im Pixellook, das in einer dystopischen Zukunftsvision angesiedelt ist: Inmitten einer Welt fest im Griff eines strengen Regimes strandet die Protagonistin namens Elster auf dem unwirtlichen Planeten und muss als Helden dort um ihr Überleben kämpfen.

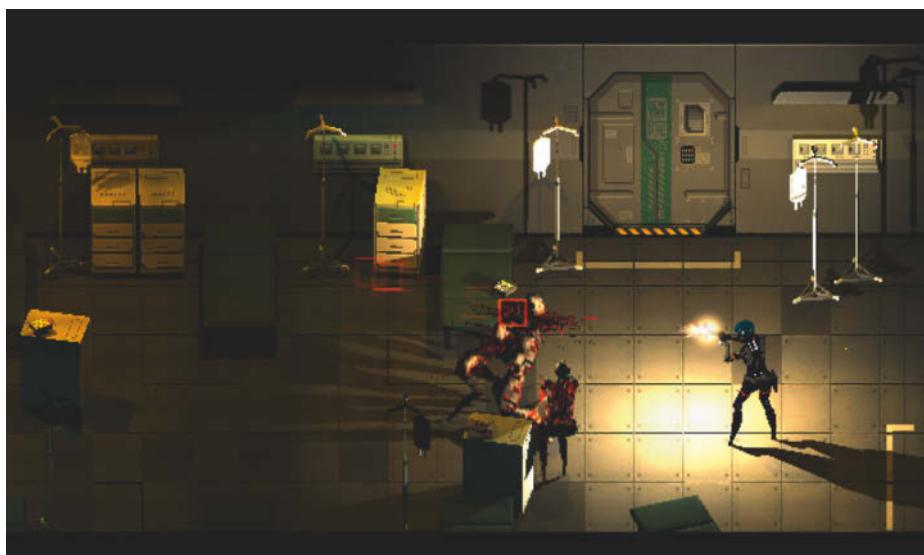
Bedrohungen gibt es reichlich, Herausforderungen auch – und die über allem schwelende große Frage, was das Leben mit Elster noch vorhat. Zwischen Ressourcen-suche und unheimlichen Erkundungs-trips stellt sie sich großen Themen: Es geht



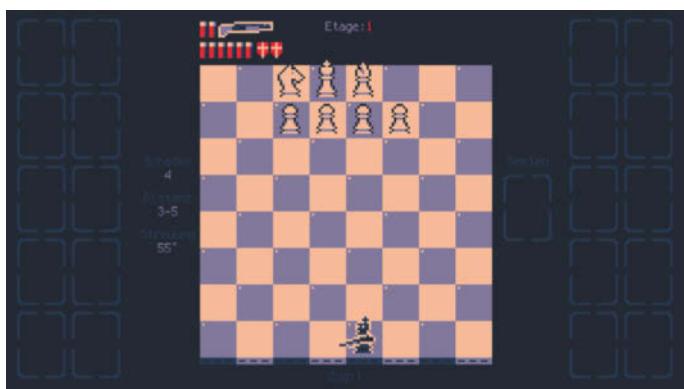
Verträumt, entspannend und berührend ist die Geschichte der jungen Frau, die Letters als ungewöhnliches Jump-&-Run-Adventure erzählt.



„Der Name der Rose“ lässt Grüßen: In einem Kloster geschieht ein Mord und man muss all seinen spätmittelalterlichen Grips bemühen, um den Mörder zu stellen. Großer Bonus: der mittelalterliche Look.



Survival-Horror im Pixellook: Mit Signalis hat das Hamburger Indie-Team rose-engine einen internationalen Erfolg gelandet.



Ein Hauch Schach trifft auf eine große Portion Taktik und ein bisschen Wahnsinn: Shotgun King hat nur noch wenig mit dem Spiel der Könige gemein, aber das ist alles andere als schlimm.



Das Aufbaustrategiespiel Stacklands ersetzt knuffige Siedlungen durch Karten und Zahlen. Doch die tollkühne Idee der Entwickler hat sich ausgezahlt.

um Identität, Zugehörigkeit und Zukunfts-hoffnung, garniert mit einem Horror, der an die besten Tage von Stanley Kubrick und David Lynch erinnert.

## Stacklands

Ein Grund, warum Wirtschaftssimulationen beliebt sind, ist ihre Inszenierung: Nur zu gerne verlieren sie sich in Details, zeigen einfachste Handgriffe jedes Arbeiters in voller Länge und bemühen sich darum, die Realität möglichst glaubwürdig abzubilden. **Stacklands** (Windows ab 7, macOS ab 10.13, 4 Euro) entfernt absichtlich all diese Elemente und ersetzt liebevoll gestaltete Dioramen durch Spielkarten.

Diese Karten werden nach und nach ausgespielt und symbolisieren dabei das, was andere Games des Genres versuchen, realitätsgerecht nachzubilden: Ressourcen, Häuser, Landschaften, Menschen. Trotz der extremen Abstraktion macht Stacklands nach kurzer Eingewöhnung viel Spaß: Die schön illustrierten Karten haben ihren eigenen Reiz und es dauert nicht lange, bis man sie nicht mehr nur als Karten auf dem Spielfeld, sondern als Dorf sieht. Stacklands bietet mit seiner minimalistischen Inszenierung ein besonderes Erlebnis (nicht nur) für alle, die glauben, in diesem Genre schon alles gesehen zu haben.

## The Case of the Golden Idol

Das wohl außergewöhnlichste Detektivspiel der jüngeren Spielegeschichte haben zwei Entwickler mit **The Case of the Golden Idol** (Windows ab 7, macOS ab 10.13, 18 Euro) hervorgebracht: Die Geschichte um ein sagenhaftes goldenes Idol wird in zwölf Kriminalfällen mit Standbildern inszeniert erzählt. So was hat es noch nicht gegeben.

Jedes Standbild zeigt eine oftmals dramatische Szene, von der spontanen Entzündung eines Menschen über einen Giftmord bis hin zum erdolchten Mann im Bett. Was hier passiert und wer der Täter ist, das müssen die Spielerinnen und Spieler herausfinden, indem sie via Mausklick in den Taschen der Anwesenden wühlen, Dokumente lesen und schließlich alle Hinweise zusammentragen. Und weil das Spiel in zwölf Einzelfälle aufgeteilt ist, kann man es auch häppchenweise durchspielen, ohne zu viel Zeit am Stück investieren zu müssen. Und ja, der grobe Look ist Gewöhnungssache.

### The Plague Doctor of Wippa

Eigentlich spielt the **The Plague Doctor of Wippa** (Windows ab 7, macOS ab 10.13, Linux ab Ubuntu 18.04, CentOS 7 oder SteamOS, 8 Euro) in einer mittelalterlichen Kleinstadt und die Geschichte begleitet einen jungen Arzt bei der Suche nach einem Heilmittel gegen die in der Stadt wütende Pest. Und doch ist das Point-&-Click-Adventure aktuell, erzählt von Vorurteilen und Grüppchenbildung inmitten einer Pandemie, von sozialer Ausgrenzung und der Suche nach Sündenböcken.

All das macht The Plague Doctor of Wippa gerade jetzt spieltenswert: Während es augenscheinlich um Themen der Vergangenheit geht, hält das Spiel unserer Gesellschaft den Spiegel vor. Zwischen den Zeilen lernen wir mehr über unsere Gegenwart, als die mittelalterliche Pixelkulisse vermuten lässt.

### Zero Sievert

Eigentlich sieht **Zero Sievert** (Windows ab 10, 20 Euro) ungemein knuffig und sym-



Das Indie-Team hinter **The Case of the Golden Idol** bereichert mit seinem Spiel das Detektiv-Genre um ein paar neue Ideen und fordert den Grips mit einigen sehr kniffligen Fällen heraus.

pathisch aus: Der Pixellook lässt selbst ein so grausiges Szenario wie die Postapokalypse einer radioaktiv verstrahlten Welt – daher der Titel – beinahe angenehm aussehen. Doch der Eindruck täuscht: Zero Sievert simuliert den Überlebenskampf in einer Welt, in der es keine soziale Norm, keine Gesetze und keine Rechte mehr gibt.

Gemeinsam mit anderen Überlebenskämpfern oder allein ziehen die Pixelfiguren in eine abwechslungsreiche Welt hinaus. Dort sammeln sie Ausrüstung und Nahrung und planen nur von einem Tag zum nächsten. Der Reiz des Spiels ist dabei der Faktor des Unbekannten: So ist nie ganz klar, was als Nächstes passiert, wer in dieser Welt Freund und Feind ist und ob sich radioaktiv verstrahlte Tiere genauso verhalten, wie man es von ihren gesunden Artgenossen erwarten würde. In Zero Sievert gibt es viel herauszufinden, zu entdecken und zu erkunden. Wer gern der eigenen

Nase und dem eigenen Bauchgefühl folgt, wird hier viele spannende Stunden erleben.

### Schatzkiste ohne Boden

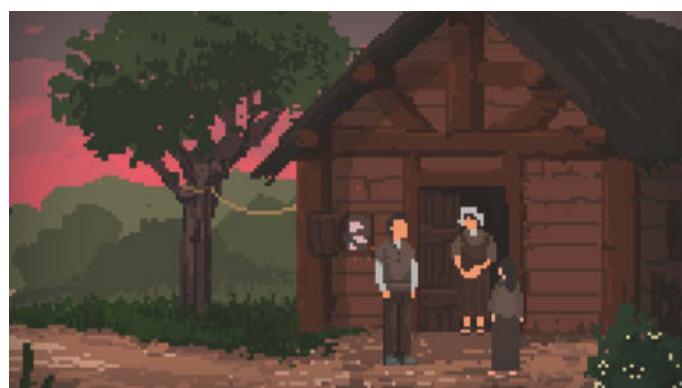
Fünfzehn Empfehlungen aus ganz unterschiedlichen Genres – und doch lässt auch dieses Schlaglicht auf die weniger gut ausgeleuchteten Ecken des Spielejahres 2022 noch viele hervorragenden Spiele unerwähnt. Der Blick zum Seitenrand der Spiele-Releases lohnt: Abseits von Scheinwerfern und dröhndem Hype warten noch viele weitere Geheimtipps darauf, endlich entdeckt und gespielt zu werden.

(lmd@ct.de) ct

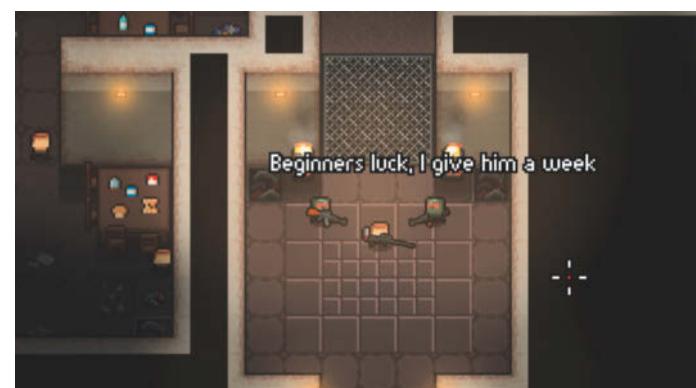
### Literatur

[1] Dominik Schott, Wohl oder Übel, Über die Jagd nach Spiele-Errungenschaften, ct 26/2022, S. 140

Links zu den Spielen: [ct.de/yr4](http://ct.de/yr4)



Auf den ersten Blick ist dieses Point-&-Click-Adventure eine Zeitreise ins Mittelalter. Der Kampf gegen die Pest im Spiel zeigt allerdings viele Parallelen zur Pandemie der letzten Jahre.



Der Überlebenskampf in Zero Sievert ist härter, als es der liebenswerte Pixel-Look vermuten ließe: Die knallharte Spielwelt fordert auch Kenner des Survival-Genres.

# Mastodon Maschinenraum

**chaos.social-Admin Leah Oswald berichtet über ihre Erfahrungen**



Bild: Leah Oswald

**Leah Oswald hat die Mastodon-Instanz `chaos.social` mit aufgebaut, die mit über 10.700 Usern zu den Schwergewichten im dezentralen sozialen Netzwerk gehört. Im Gespräch mit c't erklärt sie, wie `chaos.social` funktioniert und warum beim Wachstum Kontrolle wichtig ist.**

**Von Niklas Dierking**

**D**as dezentrale soziale Netzwerk Mastodon ist seit der Übernahme von Twitter durch Elon Musk schnell gewachsen. Anders als andere soziale Netzwerke wird Mastodon nicht von einem Unternehmen kontrolliert, sondern setzt sich aus vielen großen und kleinen Instanzen zusammen, die miteinander kommunizieren können. Grundsätzlich kann jeder eine eigene Mastodon-Instanz aufsetzen und damit einer Community ein Zuhause geben. Leah Oswald administriert `chaos.social` und erklärt im c't-Interview, worauf man beim Aufsetzen einer eigenen Instanz achten sollte.

**c't: Du hast 2017 die Mastodon-Instanz `chaos.social` mit aufgebaut und bist dort Administratorin. Was ist das für eine Gemeinschaft?**

**Leah Oswald:** Die Community hat sich in den letzten Monaten sehr dynamisch entwickelt. Ursprünglich haben wir die Instanz aufgesetzt, um den Menschen rund

um den Chaos Computer Club im Fedi-verse ein Zuhause zu geben, weil es das noch nicht gab. Mein Admin-Kollege rixx hat damals gesagt: „Es gibt da diese coole neue Software Mastodon, hast du nicht Lust, dass wir das für die Chaos-Community aufsetzen?“ Wir haben das zur GPN 2017 (Gulaschprogrammernacht, ein CCC-Event, Anm. d. Red.) fertigbekommen und vorgestellt. Seitdem sind immer mehr Leute dazu gekommen. Irgendwann wurden es aber zu viele Menschen und wir haben auf ein Einladungssystem umgestellt, also konnten nur bestehende Mitglieder neue Mitglieder hinzufügen. Das hat bis vor Kurzem noch gut funktioniert.

Seit der Übernahme von Twitter durch Elon Musk hat sich die Entwicklung der Mitgliederzahlen sehr beschleunigt. Das waren teilweise bis zu 200 neue Accounts am Tag und sicher nicht mehr nur Freunde-Freunde. An diesem Punkt haben wir vorerst die Registrierung geschlossen, damit sich wieder ein Gemeinschaftsgefühl entwickeln kann.

**c't: Wie viele User sind aktuell auf eurer Instanz registriert?**

**Oswald:** Wir haben circa 10.700 registrierte Mitglieder. Das hatte sich bis zur Ankündigung von Musks Twitter-Plänen sehr linear entwickelt. Plötzlich haben sich in ein paar Tagen 1500 Menschen registriert. Ende Oktober gab es den nächsten großen Schwung mit 2500 neuen Usern. Außerdem sind viele inaktive User wieder aktiv geworden. Die tatsächliche Zahl aktiver Accounts ist von 2000 auf 7000 angestiegen.

**c't: Ihr administriert die Instanz zu zweit. Wie sieht eure Arbeitsteilung aus?**

**Oswald:** Ich kümmere mich vorrangig um die Technik und rixx übernimmt die Moderation und Kommunikation nach außen, beispielsweise in unserem Admin-Blog, und er macht die Dokumentation.

**c't: Wie seid ihr vorgegangen, als ihr eure Instanz aufgesetzt habt?**

**Oswald:** Ich arbeite im Bereich IT-Infrastruktur als Leiterin eines Operation-Teams, deswegen konnte ich eine Menge Vorerfahrung einbringen. Mastodon haben wir mit einem Ansible-Playbook (ein Open-Source-Werkzeug zur Automatisierung und Konfiguration, Anm. d. Red.) installiert, das rixx gefunden hatte. Das Playbook haben wir über die Jahre weiterentwickelt. Anfänglich lief Mastodon noch in einer kleinen virtuellen Maschine mit vier Kernen und 8 GByte RAM. Die VM ist jedoch über die Jahre größer geworden. Bis Anfang 2022 war der Server schon auf 20 GByte-RAM, zehn CPU-Kerne und eine Reihe NVMe-SSDs angewachsen. Die flotten SSDs sind wichtig, weil sonst alles sehr langsam wird. Bis auf wenige Probleme mit Updates lief unsere Instanz ziemlich wartungsarm vor sich hin.

Nach dem großen Ansturm waren wir gezwungen, unsere Architektur zu überdenken und haben die Datenbank auf einen separaten Server ausgelagert. Jetzt haben wir eine VM mit dem Webinterface, dem Streaming-API und Redis als Cache sowie eine weitere VM, wo die Sidekiq-Worker laufen,

die alle Jobs verarbeiten, die von intern oder extern kommen. Dazu gibt es einen externen Speicher, auf dem wir die Mediendateien ablegen. Das war eine Bedingung, um die Sidekiq-Worker auslagern zu können. Sonst hätte man ein geteiltes Dateisystem nutzen und Performanceabstriche machen müssen. Die Mediendateien liegen jetzt in einem S3-kompatiblen Object-Storage (ein skalierbarer Cloud-Speicher, Anm. d. Red.). Da setzen wir auf Minio.

**c't: Mastodon ist also keine Anwendung aus einem Guss. Welche Aufgaben erfüllen die einzelnen Komponenten?**

**Oswald:** Der sichtbare Teil ist die Webkomponente, ein Webserver namens Puma, der in Ruby geschrieben ist. Dann gibt es das Streaming-API. Das kümmert sich darum, dass ich nicht immer die ganze Seite neu laden muss, wenn ich als Nutzer neue Toots sehen will, sondern das automatisch via WebSocket gestreamt wird. Die Redis-Datenbank dient als Cache für die Timeline und Benachrichtigungen, speichert und verwaltet aber auch Jobs für Sidekiq. Die Sidekiq-Worker verarbeiten Aktionen wie Likes und Toots, komprimieren Media-Uploads, holen Toots fremder Instanzen und generieren Link-Previews. All diese Aktionen werden in Warteschlangen eingesortiert, die dann von Workern abgearbeitet werden. Dazu kommt unser S3-kompatibler Storage, also ein Webserver mit definiertem API, auf den ich Dateien hochladen und runterladen kann.

**c't: Ist ein externer Object-Storage Pflicht oder kann man auch das lokale Dateisystem nutzen?**

**Oswald:** Ja, das geht, aber man sollte vorher nachdenken, wohin man mit der Instanz möchte. Bei einer Instanz bis 1000



**Administratoren einer Mastodon-Instanz müssen die Daten Ihrer Nutzer schützen. Der Admin-Account sollte durch eine Zwei-Faktor-Authentisierung gesichert sein.**

Leuten sollte das lokale Dateisystem ausreichen. Wenn ich aber eine Community habe, von der ich glaube, dass sie schnell wächst, dann sollte man das von Beginn an mitdenken. Die Architektur später umzubauen, ist schwierig. Bis Oktober letzten Jahres haben wir Dateien noch lokal gespeichert. Dann mussten wir im laufenden Betrieb umbauen und 2,4 Millionen Dateien synchronisieren. Das hat zwei Tage gedauert und währenddessen war die Instanz sehr langsam.

**c't: Hast du noch mehr Tipps, die man beachten sollte, wenn man eine große Instanz aufziehen will?**

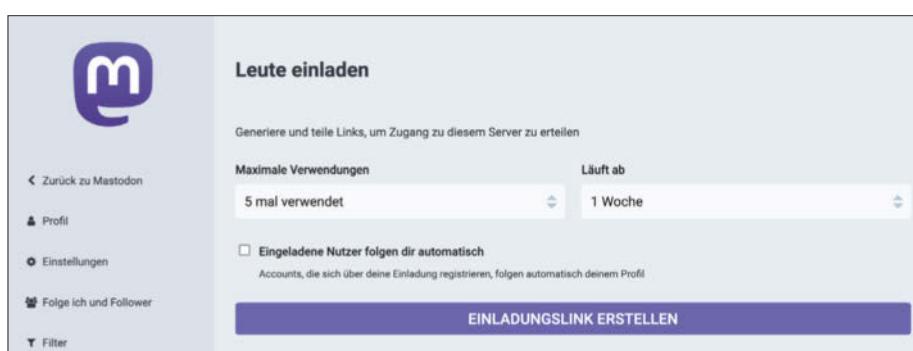
**Oswald:** Wie bei jeder Software, die viele Menschen benutzen, sollte man auch bei Mastodon wissen, was man tut und sich der großen Verantwortung bewusst sein. Als Admin hat man Zugriff auf sensible Daten, und die Nutzer vertrauen einem. Deswegen sollte man unbedingt darauf

achten, die Instanz sicher zu betreiben und regelmäßig Backups anlegen. Dazu sollten Security-Basics erfüllt werden, beispielsweise Zwei-Faktor-Authentifizierung für Admin-Accounts, SSH-Zugang nur mit passendem Schlüssel und man sollte darauf achten, Mastodon und die restliche Software auf dem Server aktuell zu halten.

Abgesehen vom technischen Aspekt ist die Moderation sehr wichtig. Ich würde niemandem empfehlen, eine Instanz mit mehr als hundert Leuten allein zu betreiben. Das kann dazu führen, dass die Moderation nicht hinterherkommt und die Instanz beispielsweise eine Anlaufstelle rechter Trolle wird. Wenn daraufhin andere Instanzen deinen Server blocken, war all die Arbeit umsonst. Ab 1000 aktiven Nutzerinnen und Nutzern sollte man sich Hilfe holen, beispielsweise um sich bei Moderationsentscheidungen eine zweite Meinung einzuholen. Grundsätzlich würde ich von Instanzen mit mehr als 20.000 Accounts abraten, auch weil dann der dezentrale Ansatz an seine Grenzen stößt.

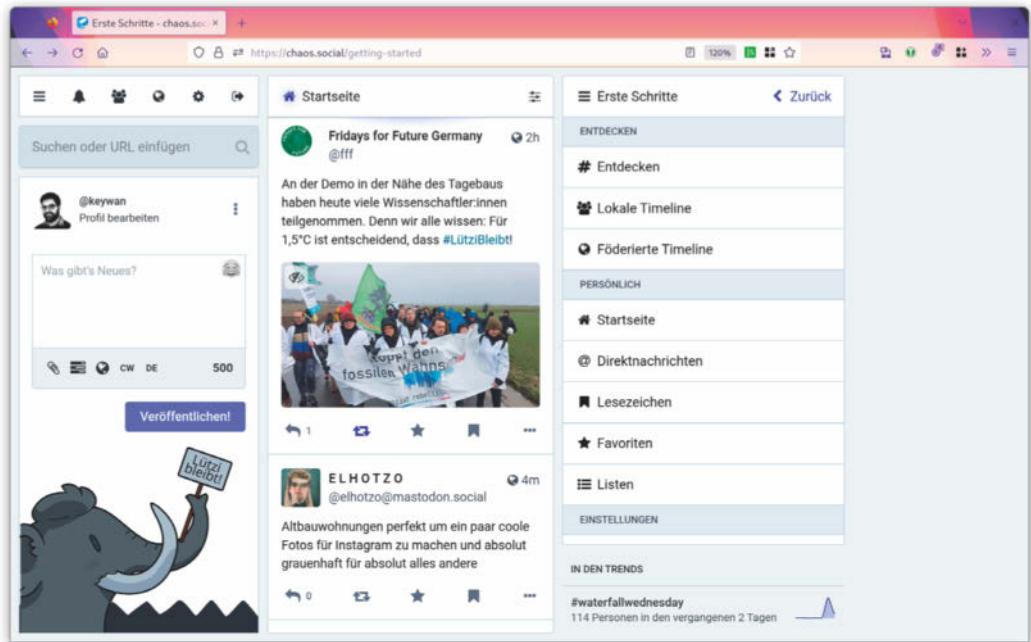
**c't: Wie kann man für ein gutes Wohlfühlklima auf seiner Instanz sorgen?**

**Oswald:** Wo viele Menschen zusammenkommen müssen unterschiedliche Wünsche und Ansprüche vermittelt werden. Das zu moderieren ist schwierig und man kann sich als Admin sicher sein, dass irgendwer immer mit einer Entscheidung unzufrieden ist. Als Nutzer kann man den Admins das Leben leichter machen, indem man die Instanzregeln liest und sich daran



**Administratoren können mit ablaufenden Einladungslinks dafür sorgen, dass ihre Instanz in kontrollierbarem Tempo wächst.**

**Das Mastodon-Webinterface** ist der sichtbare Teil von `chaos.social`. Im Hintergrund arbeiten weitere Komponenten wie eine Datenbank, ein Media-Server und das Streaming-API im Verbund, um die Postings in die Timeline zu spülen.



hält. Wenn ein Post klar gegen die Instanzregeln verstößt, dann sollte man ihn melden und eine Beschreibung des Problems mitliefern. Wenn es kein gravierendes Problem ist, dann reicht es meistens auch, den betreffenden Account einfach selbst zu blocken oder stumm zu schalten.

**c't: Ihr mietet für eure Instanz eine Menge Rechenleistung und steckt viel Zeit in Administration und Moderation. Wie finanziert ihr den Betrieb von `chaos.social`?**

**Oswald:** Wir finanzieren uns hauptsächlich über Spenden. Dafür haben wir den Verein `chaos-social e.V.` gegründet. Ab einem gewissen Punkt des Wachstums mussten wir den Betrieb formalisieren,

auch damit wir nicht mehr als Privatpersonen haften. Der Verein ist nicht als gemeinnützig eingetragen, dafür sind die Hürden sehr hoch und es bedeutet mehr Aufwand. An den Verein können User spenden, beispielsweise per Banküberweisung, PayPal und Liberapay. Andere Instanzen haben ähnliche Modelle und es ist durchaus gängig, dass sich User freiwillig an den Kosten beteiligen.

**c't: Du hast ja von dem großen Ansturm nach der Übernahme von Twitter durch Elon Musk gesprochen. Welche Stellschrauben hat Mastodon, damit eine Instanz kontrolliert wachsen kann?**

**Oswald:** Eine Option ist, Registrierungen nur mit einer Einladung zuzulassen. Die

Einladungslinks können bei uns von der Administration oder von Usern generiert werden. Das sorgt auch dafür, dass sich ein gewisses Vertrauensverhältnis entwickelt. Man kann potenzielle User auch einen Grund angeben lassen, warum sie Mitglied werden wollen, so wie eine „Mini-Bewerbung“. Registrierungen generell zu öffnen ist risikoreich. Ich kenne Instanzen, die innerhalb weniger Tage 30.000 neue Accounts hatten. Das ist ein Rezept für ein Desaster. Wir haben unsere Instanz außerdem so modifiziert, dass generierte Einladungslinks nur einmal benutzt werden können.

**c't: Viele Mastodon-Instanzen werden von Ehrenamtlichen gehostet. Was kann ich denn als Nutzer tun, wenn die keine Zeit mehr für ihre Instanz habe oder ich die Instanz aus anderen Gründen wechseln möchte? Kann ich als User meine Daten retten und umziehen?**

**Oswald:** Ja, im Mastodon-Webinterface gibt es die Option, die eigenen Daten zu exportieren, beispielsweise als CSV-Tabelle, die Follows, geblockte Accounts und gefolgte Accounts enthalten. Diese Dateien braucht man, um auf eine andere Instanz umzuziehen. Sie lassen sich über das Mastodon-Webinterface importieren. Man kann aber nicht alle Daten mitnehmen. Alte Posts und angelegte Listen ziehen beispielsweise nicht mit um.

([ndi@ct.de](mailto:ndi@ct.de))

```
ssh
It is also saved within this container so you can proceed with this wizard.

Now that configuration is saved, the database schema must be loaded.
If the database already exists, this will erase its contents.
Prepare the database now? Yes
Running 'RAILS_ENV=production rails db:setup' ...

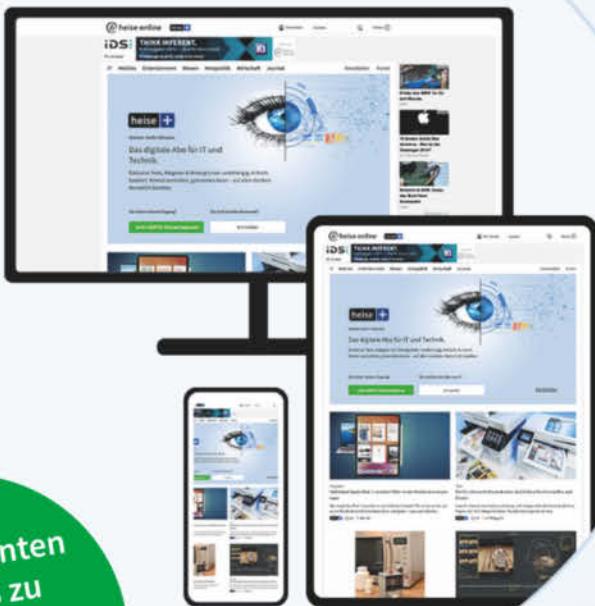
Database 'postgres' already exists
Done!

All done! You can now power on the Mastodon server

Do you want to create an admin user straight away? Yes
Username: admin
E-mail: mail@example.com
```

Bei der Einrichtung von Mastodon auf einem Linux-Server unterstützt ein Installationsskript.

c't-Abo-  
nenten  
lesen bis zu  
**75%**  
günstiger



## Das digitale Abo für IT und Technik.

**Exklusives Angebot für c't-Abo-  
nenten:**  
Sonderrabatt für Magazinabonnenten

- ✓ Zugriff auf alle Artikel von heise+
- ✓ Alle Heise-Magazine online lesen:  
c't, iX, MIT Technology Review,  
Mac & i, Make und c't Fotografie
- ✓ Jeden Freitag exklusiver Newsletter  
der Chefredaktion
- ✓ 1. Monat gratis lesen – danach jederzeit kündbar

Sie möchten dieses Exklusiv-Angebot nutzen? Jetzt bestellen unter:

[heise.de/plus-testen](http://heise.de/plus-testen)

✉ [leserservice@heise.de](mailto:leserservice@heise.de) ☎ 0541 80009 120

# Der Untergang der Zivilisation

**Das Jahr-2000-Problem:  
c't klärte auf**

**1999 befürchtete man unerkannte EDV-Probleme beim Jahrtausendwechsel. Manche Auguren prognostizierten sogar das Ende der Zivilisation durch amoklaufende Atomwaffen. Die c't informierte 1999 in der ersten Ausgabe.**

**Von Rudolf Opitz**

Viele Programme stammten Ende des zwanzigsten Jahrhunderts noch aus Zeiten, als Speicher ein knappes Gut war und an jedem Byte gespart wurde. Daher ließen viele Entwickler die ersten zwei Ziffern „19“ der Jahreszahl einfach weg, wodurch der Wechsel auf „00“ als 1900 fehlinterpretiert werden konnte. Das würde nicht nur zu falschen Rechnungen führen, auch wichtige Steuerungssysteme drohten fehlerhaft zu funktionieren.

Das Jahr-2000-Problem war der c't bereits in der ersten Ausgabe 1999 ein Titelthema wert. Der Einstiegsartikel zitierte Zeitzeugen wie den früheren Softwareentwickler Alan Greenspan, damals Vorsitzender der US-Zentralbank:

**„Und es kam uns nie in den Sinn, daß diese Programme, welche die Eins und Neun [...] weglassen, immer noch laufen, wenn wir uns dem Jahrtausend nähern.“**

Die Tricks zum Speichern eines Datums sind so vielfältig wie die Betriebssysteme und Entwicklungsplattformen: MS-DOS zählte beispielsweise die Jahre ab 1980 binär, was nur ein Byte belegte – eine speichersparende Technik?

**„Das klingt einleuchtend, aber die volle Wahrheit liegt auf halber Strecke.“**

**cke zwischen Tradition und Schlampelei.“**

Viele Verwaltungs- und Finanzprogramme für Banken und Ämter entstanden in der Sprache Cobol, die traditionell ein Datum als sechsstellige Dezimalzahl abspeicherte – mit zweistelliger Jahresangabe. Diese belegte als ASCII-Zeichenkette satte sechs Byte – alles andere als sparsam. Moderne Cobol-Versionen nutzen aber acht Byte mit vierstelliger Jahreszahl.

In der c't-Ausgabe 23/1999 wiederholten wir die Kritik an den Vorbereitungen auf den Jahrtausendwechsel für kritische Infrastruktur. Für den PC-Anwender gab es Tipps, wie die verschiedenen Betriebssysteme bei Fehlern reagieren und wie man ihnen mit einem simplen DATE-Befehl das richtige Datum vermitteln konnte.



**c't informierte in der Ausgabe 1/1999 ausführlich über die Jahr-2000-Probleme. Befürchtete Katastrophen blieben glücklicherweise aus.**



**„Wenn der private Rechneranwender am Neujahrsmorgen seine Rechner einschaltet, bleibt vielleicht der Bildschirm dunkel. Weil der Strom ausgefallen ist.“**

Die c't-Redaktion stellte 1999 kostenlose PC-Tests und Korrektursoftware inklusive Quelltext bereit. Das hinderte jedoch selbsterkannte Spezialisten wie die Microtech 2000 GmbH nicht, das Jahr-2000-Problem mit überteuerter Software (250 D-Mark pro PC) „für jedermann“ lösen zu wollen. Die Software wurde nur vorgeführt, Testmuster gab es nicht. Die c't äußerte sich skeptisch (c't 5/1999, S. 16), der Pressevertreter verlangte eine Gegendarstellung, bis im Mai 1999 eine Haussuchung der Microtech-Geschäftsäume bekannt wurde: **„Für die Firma Microtech 2000, die im Februar großen Rummel um ihre Jahr-2000-Software gemacht hatte, interessiert sich jetzt der Staatsanwalt.“**

Ermittelt wurde gegen den Geschäftsführer Tanju Karabunar, der pikanteweise mit einem Wahlkampfbrief des damaligen Kanzlerkandidaten Gerhard Schröder für seine wertlose Software warb.

In der Nachschau wirkte sich der Jahrtausendwechsel dann nicht so dramatisch aus wie befürchtet: Es gab lediglich Störungen bei Kreditkartentransaktionen. Ein Autofahrer soll eine Kfz-Steuer nachforderung für die letzten 100 Jahre erhalten haben. Im Kernkraftwerk Fukushima meldete eine Anzeige für Steuerstäbe den 6. Februar 2036, was aber den Betrieb nicht beeinträchtigte. Dem Marktforscher Gartner zufolge kosteten die Jahr-2000-Maßnahmen weltweit rund 600 Milliarden US-Dollar. Die nächste Zeitmessungskrise wird 2038 erwartet – dann läuft die 32 Bit breite Unix-Zeit über.

(rop@ct.de) **c't**

**c't-Artikel zum Jahr-2000-Problem:  
[ct.de/y7bx](http://ct.de/y7bx)**

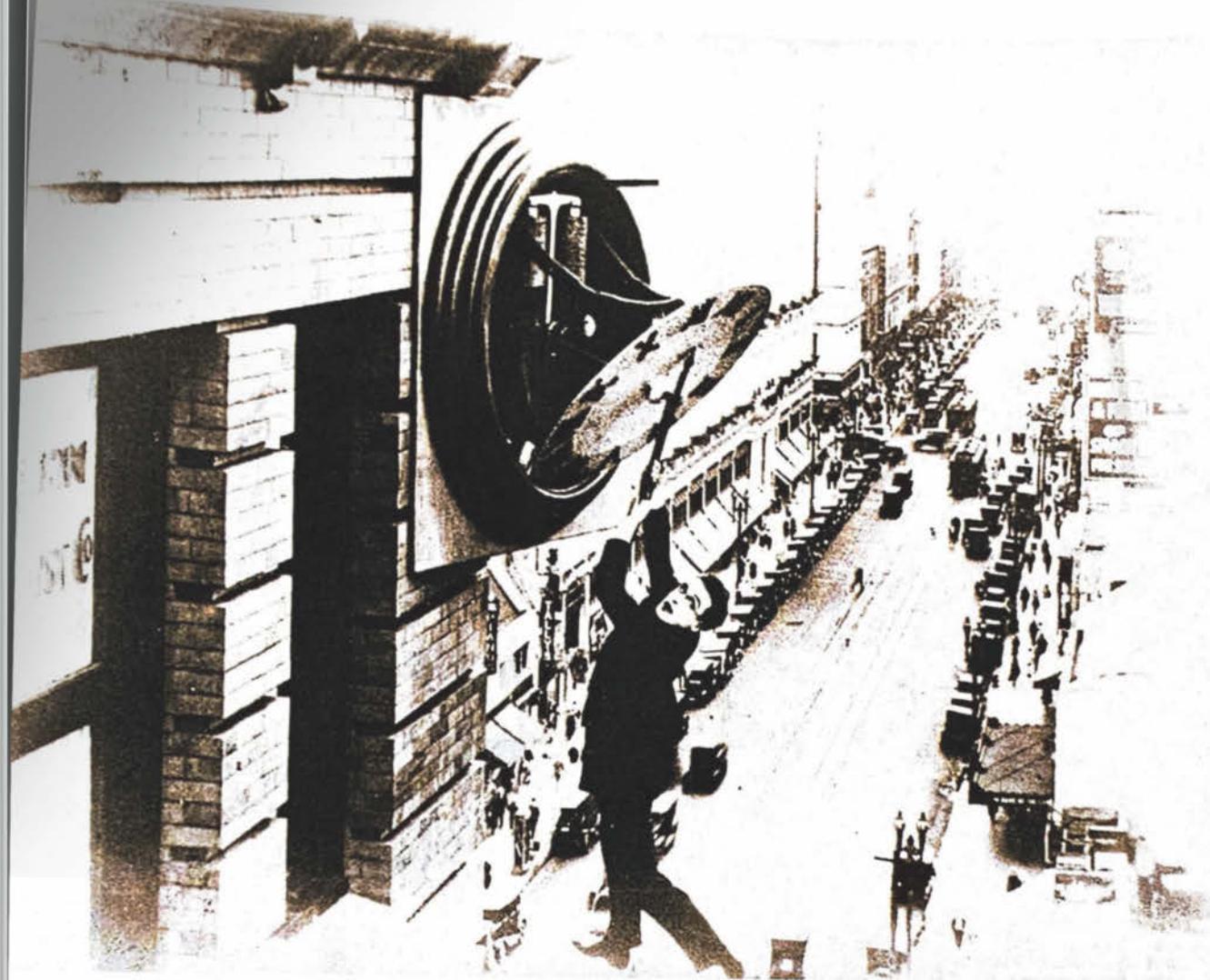


Bild: Ipo

Dr. Jörn Loviscach, Dr. Wolfgang Stieler

# Zeitbombe

## Das Jahr-2000-Problem nimmt Gestalt an

**Kassandrauer prophezeien den Untergang der Zivilisation durch Amok laufende Atomwaffen und Reaktoren; die Industrie- und Handelskammer Köln führt an, daß bis zu zehn Prozent der Unternehmen das Jahr 2000 nicht überleben – und das nur, weil Rechner oder Steuerungssysteme sauer auf die Jahreszahl 00 reagieren. Wenn der private Rechneranwender am nächsten Neujahrsmorgen seinen Rechner einschaltet, bleibt vielleicht der Bildschirm dunkel. Weil das Stromnetz ausgefallen ist.**

Noch 360 Tage bleiben bis zum magischen Datum 1. Januar 2000. [1] Die letzte Frist ist angebrochen, Fehler zu suchen und auszumerzen oder immerhin ihre Auswirkungen zu begrenzen. Kraftwerke und Krankenhäuser sind ebenso betroffen wie PC-Systeme. Doch alle Augen tappen im dunkeln. Welche Hard- und Software wird tatsächlich lahmgelegt? Welche Systeme verarbeiten Daten jenseits vom 31. Dezember 1999 nicht korrekt? Anwender und Hersteller fahnden nach Bugs – und werden fündig ...

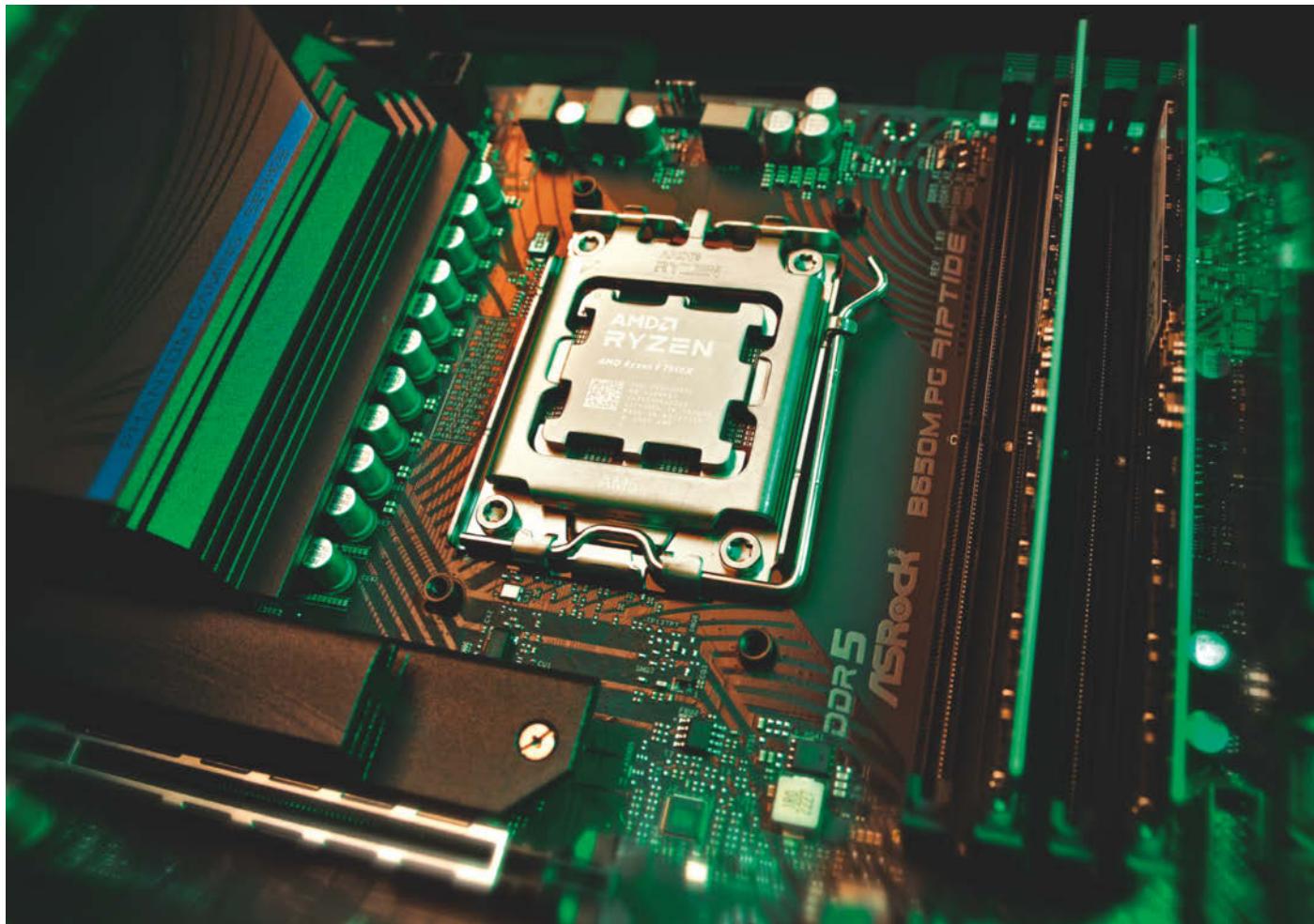
Eine klare Auskunft vom Hersteller erhielt die Notrufzentrale in Hannover: Die Software des Rechners, der die Gefahrenpunkte kennt und die Einsätze der Feuerwehr koordiniert, ist

nicht 2000-fest. Ohne Update müßten die Beamten wieder Bleistift und Papier zücken und den Stadtplan wälzen.

Alan Greenspan, einst Entwickler und nun der Vorsitzende der US-Zentralbank, mahnte vergangenen September vor einem Kongreßkomitee: 'Ich erinnere mich nicht daran, eine nennenswerte Dokumentation zu den Programmen gehabt zu haben, die ich schrieb. Und es kam uns nie in den Sinn, daß

### Jahr 2000 und Euro

PC-Systemuhr	S. 66
Machen umgehen	S. 70
Softwarereparatur	S. 76
Euro-Umstellung	S. 82



# Runtergedreht

## Praxistipps zum Energiesparen bei Ryzen-7000-Prozessoren

**AMDs High-End-Desktopprozessoren rechnen besonders schnell, schlucken aber auch viel Strom. Wir geben Tipps, wie Sie aktuelle Ryzen-CPUs sparsamer betreiben. Das hilft auch, Lärm zu reduzieren.**

Von Christian Hirsch

Die Ryzen 7000 bringen nicht nur eine überarbeitete Plattform mit neuer CPU-Fassung, DDR5-RAM und PCI Express 5.0, sondern setzen auch neue Maßstäbe bei der Rechenleistung. Leider gilt das auch für die Leistungsaufnahme unter Last,

denn ein Teil der Performance-Steigerungen gehen aufs Konto der höheren Power-Limits. Bei den Vorgängern Ryzen 5000 war bei 105 Watt Thermal Design Power (TDP) beziehungsweise 142 Watt Package Power Tracking (PPT) Schluss, die Ryzen 9 7900X und 7950X dürfen bis zu 170 Watt TDP beziehungsweise 230 Watt PPT schlucken. Das verteuren alle AM5-Mainboards, weil kräftigere Spannungswandlerschaltungen notwendig sind [1]. Zudem lassen sich die CPUs unter Volllast nicht leise kühlen.

Als Abhilfe bieten die Ryzen-7000-Prozessoren mehrere Möglichkeiten, den Energiebedarf der Prozessoren zu reduzieren. Auf den ersten Blick mag überraschen, dass das oft mit geringen oder gar ohne Performance-Einbußen einhergeht. Zur Auswahl stehen klassisches Undervolting, der dynamische Curve Optimizer

sowie der Eco-Modus. Mit der High-End-CPU Ryzen 9 7950X und unserem Bauvorschlag für einen High-End-PC [2] haben wir getestet, welche Methoden sich lohnen.

### Undervolting mit mehr Performance

Bei Prozessoren hängen Taktfrequenz und Kernspannung direkt voneinander ab. Je höher der Takt, desto schneller müssen die Transistoren schalten. Damit das fehlerfrei klappt, brauchen sie eine höhere Spannung. Das führt allerdings wiederum dazu, dass die Abwärme überproportional ansteigt, weil die Leistungsaufnahme quadratisch von der Spannung abhängt.

Zudem ist die Spannungs-Frequenz-Kurve nicht linear. Ein Taksprung von 4 auf 5 GHz erfordert höhere Spannungs-zuschläge als von 3 auf 4 GHz. Der genaue

## c't kompakt

- Sie können die hohe Leistungsaufnahme der Ryzen 7000 reduzieren.
- Das klappt vor allem mit dem Eco-Mode.
- Undervolting kann die Performance sogar leicht steigern.

Verlauf hängt von Faktoren wie dem Fertigungsverfahren, dem Schaltungsdesign und dem Aufbau der Rechenwerke ab. Diese individuelle Kennlinie ermitteln die CPU-Hersteller und hinterlegen sie im Prozessor. Moderne CPUs passen abhängig von der Auslastung dynamisch ihre Taktfrequenz an, um möglichst viel Energie zu sparen. Die für den aktuellen Takt notwendige Spannung ergibt sich dann aus der hinterlegten Kurve.

Vom Board erhalten Ryzen-Prozessoren eine einheitliche Spannung für alle Kerne (VDDCR\_CPU). Weil die einzelnen Kerne mit verschiedenen Taktfrequenzen arbeiten können, gibt es für jeden Kern im Prozessor-Package einen separaten digitalen Low-Dropout-Regler (LDO), der aus der VDDCR\_CPU die jeweils benötigte Spannung erzeugt.

In der Praxis spendieren die CPU-Hersteller der Frequenz-Spannungs-Kurve einen Sicherheitsaufschlag, damit es nicht zu Rechenfehlern kommt. Allerdings gleicht kein Prozessor dem anderen, sodass man beim Undervolting versucht, diesen Sicherheitsspielraum abzuschmelzen. Kommt die CPU bei gleicher Taktfrequenz mit weniger Spannung aus, produziert sie weniger Abwärme. Weil moderne Prozessoren die Kernspannung ständig verändern, empfehlen wir mit einem sogenannten Offset zu arbeiten. Das bedeutet, dass man keine feste VDDCR\_CPU vorgibt, was die LDO-Regler außer Kraft setzt, sondern die gesamte Kennlinie absenkt.

Bei unserem Bauvorschlag müssen Sie im BIOS-Setup des Asrock B650M PG Riptide unter „OC Tweaker/External Voltage Settings/VDDCR\_CPU Voltage“ den Offset Mode aktivieren. Dann erscheint ein weiteres Auswahlfeld: „Offset Voltage mV“. Wir empfehlen, schrittweise vorzugehen und die Spannung zuerst einmal um 25 Millivolt abzusenken. Anschließend

müssen Sie die Stabilität prüfen. Das klappt mit dem kostenlosen Lastprogramm Prime95, das es unter anderem für Windows und Linux gibt. Es berechnet große Primzahlen und nutzt dafür die Vektoreinheiten moderner CPUs mit AVX2- und AVX512-Befehlen.

Prime95 heizt den Prozessor nicht nur auf, sondern prüft die Ergebnisse zugleich auf Richtigkeit. Nicht jeder Rechenfehler äußert sich gleich durch einen Reboot oder den Absturz des Systems, kann aber dennoch Dateien beschädigen. Den Stabilitäts-Test rufen Sie in Prime95 unter „Options/Torture Test“ auf. Maximale Leistungsaufnahme generieren je nach CPU die ersten beiden Auswahlmöglichkeiten Smallest und Small FFTs. Treten nach rund 20 bis 30 Minuten keine Fehlermeldungen auf, wechseln Sie erneut ins BIOS-Setup und senken die Spannung um weitere 25 Millivolt ab. Bei Stabilitätsproblemen setzen Sie den Offset auf den vorherigen Wert zurück.

Bei unserem Testsystem konnten wir die Zulieferspannung vom Board um maximal 100 Millivolt absenken, ohne dass Probleme aufraten. Negative Auswirkungen auf die Performance konnten wir nicht feststellen, im Gegenteil gab es sogar ein kleines Geschwindigkeitsplus, weil die CPU etwas kühler bleibt. Bei Volllast auf allen 16 Kernen erreicht der Ryzen 9 7950X selbst mit dem riesigen CPU-Kühler Noctua NH-D15 schnell die Drosseltemperatur von 95 Grad Celsius. Das ist kein Bug, sondern von AMD bewusst so angelegt: Der Prozessor darf und soll für einen höchstmöglichen Turbotakt den thermischen Spielraum voll ausschöpfen.

## Eco-Modi AMD Ryzen 7000

TDP	PPT Limit	TDC Limit	EDC Limit
65 W	88 W	75 A	150 A
105 W	142 W	110 A	170 A
170 W	230 W	160 A	225 A

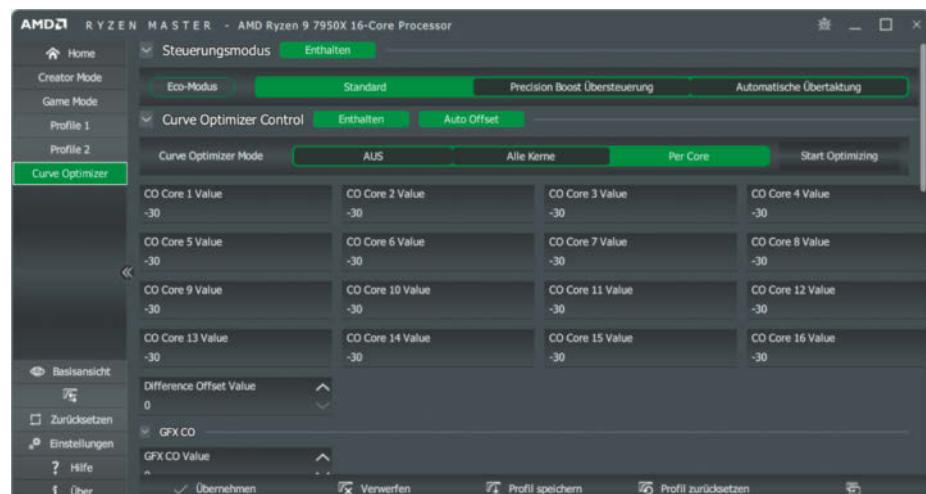
TDP: Thermal Design Power, PPT: Package Power Tracking, TDC: Thermal Design Current, EDC: Electrical Design Current

Im Rendering-Benchmark Cinebench R23, der hochoptimierten Code mit Vektorbefehlen (AVX) verwendet, rechnete die CPU mit Undervolting ein Prozent schneller. Bei anderen Anwendungen wie dem Packprogramm 7-Zip, dem Office-Benchmark PCMark 10 und dem 3D-Spiel Shadow of the Tomb Raider trat keine messbare Differenz auf. Bei Verarbeitung des Cinebench R23 nahm das Gesamtsystem 32 Watt weniger Leistung auf, was einer Ersparnis von rund elf Prozent entspricht.

## Curve Optimizer

Mit den Ryzen-5000-Prozessoren hat AMD den Curve Optimizer als automatisierte Undervolting-Methode eingeführt, die auch bei den Ryzen 7000 funktioniert. Diese bietet mehrere Vorteile: Zum einen muss man nicht mehr von Hand die Spannung schrittweise absenken und jeweils die Stabilität prüfen. Das erledigt die Übertaktungssoftware AMD Ryzen Master (ct.de/ycs2) vollautomatisch und in viel feineren Schritten.

Statt eines festen Offsetes verändert der Curve Optimizer zudem den gesamten Verlauf der Frequenz-Spannungskurve. Beigeringer und mittlerer Auslastung und Taktfrequenz senkt der Prozessor die



Zum Optimieren der Frequenz-Spannungs-Kurve benötigt man im Ryzen Master Tool nur ein paar Mausklicks.

## Undervolting AMD Ryzen 9 7950X

Modus	Cinebench R23 1T [Punkte]	Cinebench R23 MT [Punkte]	7-Zip komprimieren [MByte/s]	PCMark 10 [Punkte]	Shadow of the Tomb Raider <sup>1</sup> [fps]	Leistungsaufnahme Cinebench R23 MT [W]	Effizienz [Cinebench pro W]
nominal (170 W TDP, 230 W PPT)	► besser 2031	► besser 38147	► besser 143,3	► besser 7358	► besser 220	◀ besser 297	► besser 129
Eco-Modus (105 W TDP, 142 W PPT)	2046	36349	140,5	7309	222	200	182
Eco-Modus (65 W TDP, 88 W PPT)	2022	30084	137,7	7266	221	128	234
Eco-Modus (45 W TDP, 61 W PPT)	2030	24525	129,9	7112	219	93	263
nominal mit Curve Optimizer	2042	39821	142,5	7394	222	303	131
Eco-Modus 105 W mit Curve Optimizer	2035	36188	141,2	7325	221	199	182
nominal mit 85 °C Temperaturlimit	2032	37611	143,6	7347	223	255	148
nominal mit -100mV Kernspannung	2041	38588	143,4	7361	221	266	145
Eco-Modus 105 W mit -100mV Kernspannung	2052	37866	143,4	7384	223	196	193

TDP: Thermal Design Power, PPT: Package Power Tracking <sup>1</sup> Full HD, High, SMAA

Spannung beispielsweise stärker ab, als wenn er voll ausgelastet ist.

Im Ryzen-Master-Tool müssen Sie als Erstes unten links in die „Erweiterte Ansicht“ umschalten. Lassen Sie sich nicht von den zahlreichen Messwerten abschrecken. Klicken Sie in der linken Spalte auf „Curve Optimizer“. Nun können Sie auswählen, ob Sie die Kurve wahlweise für alle CPU-Kerne oder für jeden Kern einzeln absenken wollen.

Wir haben uns für die zweite Variante entschieden. Damit dauert die Optimierung zwar deutlich länger, beim 16-Kerner waren das rund zwei Stunden, aber eventuelle Unterschiede in der Güte der Kerne werden so berücksichtigt. Wir empfehlen vor dem Klick auf „Start Optimizing“ alle offenen Programme zu schließen, denn beim Austüfteln der korrekten Werte kann sich das System neu starten.

Der Curve Optimizer wirft am Ende keine Spannungsdifferenz aus, sondern Werte von 0 bis -30. Eine Stufe entspricht laut AMD einer Absenkung von 3 bis 5 Millivolt. Bei unserem Ryzen 9 7950X hatten wir anscheinend viel Glück, denn für alle Kerne schlug das Ryzen-Master-Tool eine Anpassung von -30 vor, was dem maximalen Einspareffekt und einer Absenkung von 90 bis 150 Millivolt entspricht.

Anschließend müssen Sie die Werte im Ryzen-Master-Tool noch übernehmen und den Rechner neu starten. Die Übertaktungssoftware überträgt die ermittelten Werte dabei selbst in die Firmware, sodass Sie im BIOS-Setup nichts umstellen müssen und der Curve Optimizer permanent aktiv ist. Trotz der integrierten Stabilitätstests des Ryzen-Master-Tools empfehlen wir zusätzlich Prime95 für mindestens eine halbe Stunde laufen zu lassen.

Die Ergebnisse unseres Ryzen 9 7950X verblüfften uns: Statt einer Einsparung lag die Leistungsaufnahme mit 303

Watt minimal über dem Ursprungswert von 299 Watt. Zugleich legte die Multithreading-Rechenleistung um vier Prozent zu. Durch die geringe Spannung wird die CPU weniger heiß, kann also höher takten, bis das 95-Grad-Limit erreicht ist. Höherer Takt bedeutet aber immer auch mehr Spannung, weshalb die Leistungsaufnahme leicht steigt.

### Überdurchschnittlicher Spareffekt

Bereits im Testbericht der Ryzen-7000-Prozessoren sind wir auf den Eco-Modus eingegangen [3]. Dahinter verbirgt sich nichts anderes, als mit offiziellem Segen von AMD die Power-Limits der CPU abzusenken. Im BIOS-Setup sowie im Ryzen-Master-Tool gibt es dafür einen Schalter, der die Ryzen-7000X-CPUs auf 65 Watt Thermal Design Power einbremst, egal ob es sich um Modelle mit 105 oder 170 Watt TDP handelt. Die tatsächliche CPU-Leistungsaufnahme liegt bei 65 Watt TDP unter Volllast jedoch bei 88 Watt, denn AMD gestattet den Ryzen 7000 ihre TDP dauerhaft um 35 Prozent zu überschreiten. Diese Grenze bezeichnet der Chiphersteller auch als Processor Power Tracking Limit (PPT).

Außer der bereits angesprochenen Drosseltemperatur ( $T_{JunctionMax}$ ) von 95 Grad und dem PPT Limit gibt es noch zwei weitere Kenngrößen, die den aktuellen CPU-Takt mitbestimmen: Das Thermal Design Current Limit (TDC) legt die maximale Stromstärke fest, die bei  $T_{JunctionMax}$  fließen darf. Das höhere Electrical Design Current Limit (EDC) begrenzt kurzzeitige Stromspitzen. In der Tabelle auf Seite 91 haben wir die Grenzwerte für die unterschiedlichen TDP-Klassen zusammengestellt.

Um diese Variablen einzustellen, müssen Sie in die Tiefen des BIOS-Setups hinabsteigen. Beim Asrock-Board unseres

Bauvorschlags finden Sie die Optionen für TDP, PPT, TDC und EDC Limit unter „Advanced/AMD CBS/SMU Common Options“. Abhängig vom Board-Hersteller sind diese in andere Menüpunkte eingesortiert.

In unseren Experimenten haben die Ryzen 9 7950X nicht nur auf 65 Watt, sondern alternativ auch auf 105 und 45 Watt heruntergeregt. Als praxistauglichster Kompromiss zwischen Effizienz und Performance hat sich beim 16-Kerner die 105-Watt-Einstellung mit 142 Watt PPT Limit herausgestellt. Die CPU verliert in der Multithreading-Wertung des Cinebench lediglich fünf Prozent Rechenleistung, das System schluckt aber 33 Prozent beziehungsweise 97 Watt weniger Energie.

Mit noch niedrigeren Power-Limits nimmt die Effizienz, also die Performance pro Watt, weiter zu. Allerdings geht das stärker zu Lasten der absoluten Geschwindigkeit. Mit einer für Desktop-CPUs extrem geringen TDP von 45 Watt benötigt unser High-End-Bauvorschlag unter Volllast unter 100 Watt. Jedoch halbiert das fast das Ergebnis im Cinebench R23. Dann kann man sich die 630 Euro für den Ryzen 9 7950X auch sparen und stattdessen eine preiswerte CPU kaufen. Die Preisdifferenz zum Achtkerner Ryzen 7 7700X von 250 Euro wird man bei üblicher Nutzung niemals wieder hereinholen, denn dazu müsste man bei einem Strompreis von 40 Cent pro Kilowattstunde insgesamt 625 kWh einsparen.

Als Bonus haben wir ausprobiert, verschiedene Energiespartechniken miteinander zu kombinieren. Bei einer Thermal Design Power von 105 Watt konnten wir mit zusätzlich zugeschaltetem Curve Optimizer keinen weiteren Spareffekt messen. Mit manuellem Undervolting von -100 mV holten wir im Cinebench R23 ein leichtes Performanceplus von vier Prozent bei vier Watt weniger Leistungsaufnahme heraus.

Alternativ bietet AMD bei den Ryzen 7000 die Option, im BIOS-Setup die Drosseltemperatur abzusenken. So regelt der Prozessor seinen Takt beispielsweise schon bei 85 Grad Celsius Kerntemperatur ab. In unseren Messungen lag der Spar-Effekt und die Rechengeschwindigkeit dabei ungefähr in der Mitte zwischen 105 und 170 Watt TDP. Allerdings schwanken die Werte, je nachdem, ob der Kühler durch vorherige Last schon aufgeheizt wurde oder nicht.

Auf die Leerlaufleistungsaufnahme haben sämtliche genannte Energiesparmethoden übrigens keinen Einfluss. Denn bei ruhendem Windows-Desktop legen sich alle CPU-Kerne so weit schlafen, dass sie von der Kernspannung getrennt werden. In diesem Zustand geht der Energiebedarf aufs Konto von Mainboard, SSD, eventuell vorhandener Grafikkarte und Wandlerverlusten von Board und Netzteil.

Zudem wirken sich die Energiesparmaßnahmen nicht auf Anwendungen aus,

die nur einen oder wenige Kerne auslassen, weil der Prozessor dabei sein Energiebudget nicht ausschöpft. Das gilt für Office-Anwendungen, wie sie der PCMark 10 misst, aber auch für 3D-Spiele wie Shadow of the Tomb Raider. 7-Zip nutzt zwar alle Kerne eines Prozessors, verwendet jedoch hauptsächlich Integer-Code. Diese Recheneinheiten benötigen deutlich weniger Energie als Gleitkommaeinheiten. Deshalb reduziert sich die Performance bei 7-Zip nur mäßig bei sehr geringer Thermal Design Power.

## Fazit

Mit abgesenkten Power-Limits lässt sich die Leistungsaufnahme der High-End-Prozessoren der Serie AMD Ryzen 7000 in akzeptable Gefilde holen, ohne nennenswert Performance einzubüßen. Undervolting, sei es manuell oder per Curve Optimizer, lohnt sich eher für Anwender, die die CPUs für maximale Rechenleistung mit voller Thermal Design Power betreiben wollen.

Unsere Experimente zeigen, dass Desktop-Prozessoren außerhalb von High-End-Workstations mit mehr als 150 Watt Maximalleistungsaufnahme nur wenig Sinn ergeben. Wir hätten uns gewünscht, dass AMD die Ryzen 9 7900X und 7950X mit 105 Watt TDP vorgestellt hätte. Das würde den meisten Käufern preisgünstigere Mainboards bescheren und AMD könnte im Konkurrenzkampf mit Intel mit deutlich besserer Effizienz glänzen. Wer mehr Leistung benötigt, kann ja die Power-Limits erhöhen. (chh@ct.de) **ct**

## Literatur

- [1] Christian Hirsch, Premiumaufschlag, AM5-Mainboards für Ryzen-7000-Prozessoren im Test, c't 24/2022, S. 90
- [2] Christian Hirsch, Leiser Riese, Bauvorschlag für einen starken Rechner mit Ryzen 7000, c't 26/2022, S. 30
- [3] Carsten Spille, Fünf ist Trümpf, Ryzen 7000: Vier Desktop-Prozessoren für die Fassung AM5, c't 22/2022, S. 56

**Ryzen Master herunterladen:** [ct.de/ycs2](http://ct.de/ycs2)

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

3 x als Heft

**Chatbots:** Entwicklung, Strukturen, Hersteller  
Rugged Server  
Docker-Container verne  
Ceph als iSCSI-Storage  
Payment Request API  
Post-Quantum-Kryptogr

**KI schnell und einfach**

MACHINE LEARNING AS A SERVICE, NEURO-CHIP  
Kubernetes-Deployment mit Rancher 2.0  
Small Things Monitoring  
Schwachstellen systematisch bewerten  
ZUGFERD 2.0  
Docker-Container verne  
Post-Quantum-Kryptogr

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

[www.ix.de/testen](http://www.ix.de/testen)



# Daten-Jongleur

## Fitnessdaten unter Android App-übergreifend synchronisieren

**Alle Gesundheitsdaten in einer App – unabhängig vom Hersteller der Sportuhr. Das verspricht Google Health Connect. Die App synchronisiert schon in der Beta-Phase zuverlässig, doch an einigen Stellen hakt es noch.**

Von Stefan Porteck

**F**itness-Tracker und Gesundheitsgadgets gibt es wie Sand am Meer – und deshalb auch fast genauso viele Apps, die die Daten von den diversen Uhren, Brustgurten, Armbändern oder Schlafmatten einsammeln und in die Cloud des jeweiligen Herstellers befördern. Das ist ein Problem: Viele tragen im Alltag eine Smart- oder Hybridwatch, aber beim Sport legen sie eine Sportuhr oder einen Brustgurt eines anderen Herstellers um. Hat man mal eine Analoguhr am Handgelenk, protokolliert nur noch das Handy selbst die Schritte. So landen Körper- und Fitnessdaten auf unterschiedli-

chen Portalen und lassen sich nur mühevoll wieder zusammenführen.

Übersichtlicher wäre es, wenn alle Fitness-, Trainings- und Körperdaten automatisch synchronisiert würden und alle genutzten Fitness-Apps den gleichen Bestand hätten. Zwar bieten namhafte Hersteller wie Fitbit, Google Fit, Samsung, Withings oder Garmin eine Export- und teilweise auch eine Importfunktion an, aber da liegt die Krux: Kaum jemand hat die Muße, sich jeden Monat aufs Neue hinzusetzen, um die Körperdaten manuell zu übertragen.

Für dieses Problem hat Google eine App entwickelt, die nahezu alle Körperdaten aus kompatiblen Apps ausliest, in einer lokalen Datenbank aggregiert und ausgewählte Daten auf Wunsch auch in Apps zurückschreibt. Seit dem vergangenen Herbst steht „Health Connect“ im Play Store als öffentliche Beta-Version für Android zum Download bereit.

Wir haben Health Connect auf einem Pixel-Smartphone unter Android 13 mit Fitness-Daten von Withings, Google Fit und Fitbit traktiert und erklären, wie man sie einrichtet und was für Ergebnisse sie liefert.

### Hin- und hergeschoben

Damit Health Connect funktioniert, müssen die korrespondierenden Fitness-Apps die dafür von Google bereitgestellte Programmierschnittstelle unterstützen. Sie erlaubt Health Connect den Zugriff auf die Rohdaten der Apps. Bislang unterstützen noch nicht viele Anbieter das API, obgleich sich Google bemüht hat, schon zur Beta-Phase mit einigen Big Playern zu kooperieren. Mit von der Partie sind außer Health Mate, Google Fit und Fitbit die Dienste Samsung Health, MyFitnessPal, Oura sowie die Apps Perioden Kalender Flo, Lifesum, Outdooractive und Proov Insight.

Aufgrund der vielen verschiedenen Fitness-Apps müssen diverse Daten und unterschiedliche Datentypen unter einen Hut gebracht werden. Health Connect passt die Körper- und Gesundheitsdaten an ein eigenes Format an. Die App unterteilt die Daten in die Bereiche Aktivität, Ernährung, Körpermaße, Schlaf, Vitalparameter und Zyklustraining. Unter Aktivität speichert die App unter anderem Werte für verbrannte Kalorien, den Grundumsatz, die zurückgelegte Strecke, die bewältigte Steigung, die Geschwindigkeit und die Anzahl der Schritte. Im Bereich Körpermaße legt Health Connect Körperfett, Knochenmasse, Größe und Gewicht

## Letzte Zugriffe

Hier siehst du, welche Apps in den letzten 24 Stunden auf deine Daten zugegriffen haben

Zeit	App	Aktion
11:13	Health Mate	Schreiben: Aktivität, Körpermaße, Vitalparameter
11:13	Fit	Lesen: Aktivität, Vitalparameter, Körpermaße, Ernährung
10:49	Health Mate	Schreiben: Vitalparameter
10:39	Health Mate	Schreiben: Aktivität, Vitalparameter
10:36	Health Mate	Schreiben: Aktivität, Körpermaße, Vitalparameter
10:07	Fit	Schreiben: Schlaf, Vitalparameter

**Health Connect liest regelmäßig Körperdaten anderer Apps aus und führt sie in einer eigenen lokalen Datenbank zusammen.**

ab, während Blutdruck, Körpertemperatur, Herzfrequenz, Sauerstoffsättigung und Atemfrequenz Eingang in die Vitalparameter finden.

Alle ausgelesenen Daten speichert Health Connect in einer internen Datenbank im Systemspeicher des Smartphones. Andere Apps kommen nicht an die Daten heran und selbst einem Dateimanager bleibt der Zugriff ohne Root-Rechte verwehrt.

Health Connect wertet die Daten nicht selbst aus, sondern synchronisiert sie nur im Hintergrund zwischen den verbundenen Diensten. Stattdessen überlegt man sich, welcher seiner Fitness-Apps man die Auswertung überlassen möchte und von welchen anderen Apps Health Connect dazu die Daten einsammeln soll.

### Aufgezeichnet, fertig, los!

In der frühen Beta-Phase der App ist alles noch ein wenig inkonsistent und rumpelig. Das fängt damit an, dass Health Connect kein Icon in der App-Übersicht zeigt. Um die App zu starten, muss man deshalb die Android-Einstellungen aufrufen, dort in den Bereich Apps wechseln und sich im Eintrag „Alle installierten Apps“ bis zu

Health Connect durchscrollen und die App dort auswählen.

Obgleich man Health Connect nach der Ersteinrichtung nur noch selten öffnen muss, bietet es sich an, eine App-Kachel in den „Quick Settings“ von Android (die Leiste, über die man schnell Funktionen wie Flugmodus oder Hotspot aktiviert) abzulegen.

Im nächsten Schritt sind die gewünschten Fitness-Apps mit Health Connect zu verknüpfen und deren Datenexport -Import einzurichten. Bei unseren Tests mit Google Fit, Health Mate von Withings und Fitbit mussten wir dafür stets die jeweilige App nach der Installation von Health Connect einmalig aufrufen und wurden von einem Hinweis oder einem Pop-up gefragt, ob wir die Integration in Health Connect aktivieren möchten.

Für jede App lässt sich individuell festlegen, ob und welche Körperdaten Health Connect auslesen und in die App hineinschreiben darf. Das ermöglicht es, mehrere Apps parallel und mit identischem Datenbestand zu betreiben, komplexe Master-Slave-Synchronisationen einzurichten oder einen Datenbestand von App A zu App B umzuziehen.

Im Folgenden erklären wir die Rechte anhand eines Beispielszenarios, bei dem der Anwender einen Tracker und eine Waage von Withings nutzt und seinen Schlaf von einem Nest Hub Display überwacht und über Google Fit protokolliert. Alle Daten sollen bei Google Fit landen, während Withings nur als Datenquelle dient.

Die Einrichtung von Health Connect ist nicht besonders intuitiv. Das ist auch der Tatsache geschuldet, dass aufgrund einer missverständlichen Übersetzung ins Deutsche zunächst unklar bleibt, ob sich die Lese- und Schreiberlaubnis auf Health Connect oder die Fitness-App beziehen und man zunächst rätseln muss, in welche Richtung der Datenaustausch überhaupt abläuft.



**Dank Health Connect landen auch die Daten einer Withings-Uhr in Apps wie Google Fit.**

Tatsächlich beziehen sich die Rechte nicht auf Health Connect selbst, sondern auf die verknüpfte Fitness-App. Erlaubt man Google Fit beispielsweise das Lesen der Schritte, landen alle Schritte aus der Datenbank von Health Connect als getrackte Schritte in Google Fit. Aktiviert man das Schreiben der Schritte für Google Fit, werden alle damit aufgezeichneten Schritte zusätzlich auch in der Datenbank von Health Connect gespeichert.

Um Google Fit als Senke und die Sportuhr von Withings als Quelle einzurichten, öffnet man Health Connect und wechselt im unteren Bereich der App auf „App Berechtigungen“. Dort listet Health Connect alle kompatiblen Apps auf und unterscheidet in erster Instanz zwischen Apps mit und ohne Zugriff.

Tippt man nun auf Google Fit, öffnet sich eine Liste aller Körperdaten und Vitalparameter, die Health Connect verarbeiten kann. Für unseren Anwendungsfall haben wir alle Schreibzugriffe deaktiviert und Lesezugriffe eingeschaltet. Einige Ausnahmen: der Grundumsatz und das Schlaftracking – letzteres berechnet Google Fit selbstständig und die Schlafdaten soll die App über das Nest Hub Display weiterhin selbst erheben.

Im zweiten Schritt wechselt man zu den Berechtigungen der App von Withings. Da Health Mate die Daten der Uhr liefern, aber keine externen Daten übernehmen soll, müssen Sie alle Lesezugriffe für Health Mate ausschalten. Den Schreib-

### c't kompakt

- Google Health Connect aggregiert Fitness-Daten anderer Apps.
- Die Android-App verarbeitet Daten lokal auf dem Smartphone.
- Das Einrichten ist in der aktuellen Beta-Version noch etwas kompliziert.

zugriff haben wir bei allen Daten, wieder mit Ausnahme des Schlafes, erlaubt.

Nachdem alles eingestellt war, mussten wir die Benutzeroberfläche von Health Connect nicht mehr aufrufen. Die App verrichtete im Anschluss im Hintergrund zuverlässig ihren Dienst.

## Hohe Hürden und kleine Probleme

Health Connect wird nur dann aktiv, wenn man eine der verbundenen Apps startet. Das soll Strom sparen, bringt aber den Schönheitsfehler mit sich, dass die Daten nicht in Echtzeit von einer App in die andere wandern. Dabei handelt es sich aber nur um ein kosmetisches Problem. Wer seine Daten in Echtzeit überwachen will, kann jederzeit in die App des Fitnesstrackers schauen. In unserem Dauertest von rund zwei Monaten wurden unterm Strich die Daten korrekt übernommen, auch wenn es manchmal ein halbes Stündchen dauerte, bis die jeweilige App sie korrekt anzeigte.

Stromsparend ist das Prozedere allerdings nicht: Praktisch alle Fitness-Apps starten in regelmäßigen Abständen einen Hintergrunddienst, der die neuesten Aufzeichnungen von der Hardware ausliest und speichert. Das interpretierte Health Connect auf unserem Pixel 6 als aktives Öffnen der App und startete seine Lese- und Schreibvorgänge. Der Vorteil ist, dass die App alle Daten auch dann zuverlässig

synchronisiert, wenn man weder Health Connect noch eine Fitness-App regelmäßig aktiv öffnet. Dadurch steigt aber auch der Stromverbrauch deutlich, wie ein Blick in die Akku-Statistik unseres Testgeräts zeigte, jedoch nicht in dem Maße, dass wir eine spürbare Verkürzung der Laufzeit des Smartphones bemerkten.

In unserem Test kam es selten zu doppelten Datensätzen: Da alle Werte mit einem genauen Zeitstempel versehen sind, ignorierte Health Connect beispielsweise doppelt aufgezeichnete Schritte sehr zuverlässig und verwarf den zweiten Datensatz. Welcher Wert gespeichert und welcher verworfen wird, entscheidet Health Connect laut Google anhand der bisherigen Nutzung, sprich: Die App, die sonst den Großteil der Daten liefert, wird von Health Connect bevorzugt. Ist man mit der Vorauswahl nicht zufrieden, stellt man in Health Connect manuell ein, welche Apps bei welchen Daten den Vorzug bekommen. So vermieden wir größtenteils doppelte und inkonsistente Einträge. Sollte es doch mal Doubletten geben, lassen sich einzelne Datensätze aus Health Connect löschen, verbleiben dann aber weiterhin in den verknüpften Fitness-Apps.

## Doppelläufer

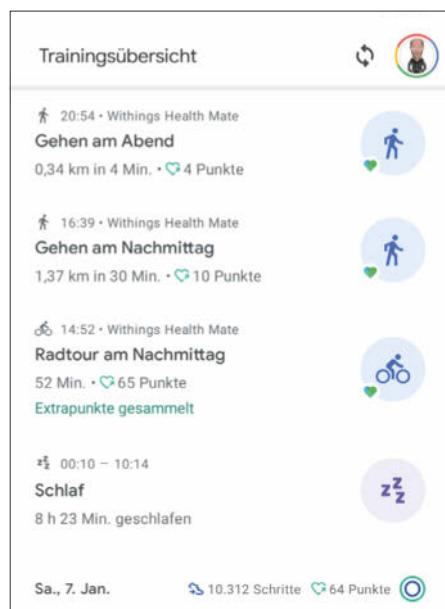
Praktisch jeder Fitness-Tracker erkennt, wenn die Nutzer längere Zeit gehen, laufen oder Rad fahren und zeichnet dann nach einigen Minuten automatisch ein Workout auf. Das Problem dabei: Jeder Tracker startet zu einer unterschiedlichen Zeit. Health Connect erkennt dann nicht, dass die um 14 Uhr gestartete Radtour der Fitnessuhr dieselbe ist, die das Smartphone ab 14:03 Uhr protokolliert hat. In der Folge landen zwei Radtouren in allen verknüpften Apps.

Ein weiterer Wermutstropfen: Health Connect fehlt zumindest in der Betaphase eine Exportfunktion. Das hat den Nachteil, dass man beim Umzug auf ein neues Telefon seinen historischen Datenbestand verliert und die App mit einer leeren Datenbank bei null startet – zumindest, wenn man nicht vorsorgt. Für den Umzug auf ein anderes Smartphone empfiehlt Google deshalb, in den Android-Einstellungen das App- und Datenbackup einzuschalten.

Obgleich Health Connect alle Daten an zentraler Stelle sammelt und alle Werte dort zu sehen sind, taugt sie nicht zur Analyse der Daten. Es gibt keine Statistiken, Filter oder gar Diagramme oder Trends.



**Trainings und Aktivitäten synchronisiert**  
**Health Connect zuverlässig, oft zusammen mit korrespondierenden Metadaten, etwa der Dauer und der Pulsfrequenz. Die Standortdaten und die Entfernung wurden jedoch nicht von der Withings-App zu Google Fit geschoben.**



**Google Fit kennzeichnet deutlich, welche Daten die App via Health Connect aus anderen Apps übernommen hat.**

Stattdessen zeigt die App eine schnöde Listenansicht für jeden einzelnen Tag. Das sieht in Apple Health deutlich schicker aus.

## Fazit

Bei der Unterstützung seitens der Hersteller von Fitness-Apps hat Google zum Start schon etliche große Anbieter ins Boot geholt und gegenüber Apple Health die Nase vorn. Sportler dürften dennoch enttäuscht sein, dass Garmin, Polar, Strava und Runkeeper nicht mit von der Partie sind.

Trotz der frühen Beta-Phase funktionierte Health Connect in unseren Tests bereits größtenteils zuverlässig: Wir erlebten weder Abstürze noch schredderte die App die Gesundheitsdaten, wenn durch das parallele Aufzeichnen mehrerer Apps Konflikte entstanden. Health Connect sammelt nur Daten, die sie aus anderen Apps erhält. Man kann Daten weder manuell eintragen noch über andere Wege von weiteren Geräten einlesen wie beispielsweise von autonomen Fahrradcomputern, Uralt-Messgeräten oder einem Zweithandy. Das muss man also weiterhin manuell in der jeweils genutzten Fitness-App erledigen.

(spo@ct.de)

# KANBAN DAY

Kanban im Unternehmen –  
mehr als nur Projektmanagement



Online-Konferenz – 28. Februar 2023

## Kanban als Veränderungsmethode

Der Kanban Day legt einen Schwerpunkt auf Kanban als Veränderungsmethode. Er gibt einen fundierten Einblick in die Vielfalt von Kanban, wie sich die Methode gewinnbringend einsetzen lässt und welche Metriken für eine Veränderung und kontinuierliche Verbesserung sinnvoll sind.

### Highlights aus dem Programm:

- ✓ Kanban und Selbsterkenntnis – **Markus Hippeli**
- ✓ Kanban-Grundlagen entmystifiziert – **Mathias Schröder**
- ✓ Physisches Whiteboard oder elektronisches Tool? – **Mathias Tölken**
- ✓ Holokratische Ansätze und Kanban – **Heike Röttgers & Gerhard Wagler**
- ✓ Kanban in SAFe – **Sebastian Nickel**
- ✓ Kanban im Kontext einer Organisation – **Thomas Epping**

Jetzt  
Frühbucher-  
rabatt  
sichern!

Veranstalter

 **heise Developer**

 **dpunkt.verlag**

in Kooperation mit

 **it-agile**

 **leanovate**  
beyond product



# Konserviertes Wissen

## Backup- und Exportmöglichkeiten populärer Notizprogramme

**Notiz- und Wissensmanagementprogrammen vertraut man schnell sein halbes Leben an – der Verlust dieser Daten wäre katastrophal. Wir haben uns angesehen, wie man in den populärsten Programmen eigene Backups anlegt und wichtige Inhalte in allgemein lesbare Formate exportiert.**

**Von Stefan Wischner**

Sie werden oft einfach als Notizprogramm bezeichnet, in ihnen sammelt sich aber meist viel mehr als Einkaufslisten oder Urlaubspacklisten: Evernote, OneNote, Notion, Joplin, Obsidian, Google Notizen, Apple Notizen und UpNote dienen oftmals als zentrale Sammelstelle für das private und berufliche Leben, speichern komplett Projekte, Niederschriften ganzer Semester oder alles für die nächste Steuererklärung. Der Verlust solcher Datensätze tut weh.

Dummerweise gibt es kein einheitliches Speicherformat für diese Art von Informationen. Dafür unterscheiden sich die Organisationskonzepte und Inhaltsformate der genannten Programme viel zu sehr. Also speichern die meisten in einem eigenen Format, das zu nichts kompatibel ist und das oft auch noch in tief im System vergraben Datenbanken oder völlig transparent in der Cloud des jeweiligen Anbieters.

Lokale Dateien sind immer Risiken wie Hardwarefehlern oder Malware-Angriffen ausgesetzt. Beim Hersteller gespeicherte Daten genießen zwar meist einen deutlich besseren Schutz. Dafür kann es Probleme mit dem Konto und damit dem Zugang zu den eigenen Daten geben – man denke nur an die Kontensperren seitens Microsoft wegen vermeintlicher Verstöße gegen Nutzungsbedingungen. Und was, wenn ein Hersteller eines Tages beschließt, sein Programm nicht mehr weiterzuentwickeln, gar einzustellen und die Online-Datenspeicher zu schließen?

Um ruhig schlafen zu können, muss ein Backup her, oder noch besser zwei: Eines, aus dem man die gesicherten Daten inklusive Organisationsstruktur im Ernstfall wieder zurückspielen kann und eines, das die wichtigsten Inhalte auch in

## ct kompakt

- Notizprogramme speichern Daten oft versteckt oder in proprietären Formaten.
- Nicht alle Anbieter ermöglichen ein verlustfreies Backup mit Restore-Option.
- Man kann jedoch wichtige Inhalte zumindest in einem allgemein lesbaren Format exportieren.

unabhängig vom Ursprungsprogramm lesbare Dateien sichert. Also am besten in einem allgemeinen Format wie PDF oder HTML. Um den Schutz vor Rechnerausfällen, Malware-Befall, Brand- und Wasserschäden muss man sich natürlich dann selbst kümmern – zum Beispiel mit Hilfe externer Datenträger an verteilten Orten.

Die gute Nachricht: Zumindest der Export von Text- und Bildinhalten in Standardformaten geht bei allen, wenn auch unterschiedlich flexibel und komfortabel. Wir haben uns die Backup- und Exportmöglichkeiten der acht populärsten Programme für Notiz- und Wissensmanagement angesehen.

### Apple Notizen

Das zu macOS und iOS gehörende Programm „Notizen“ speichert Inhalte wahlweise in der iCloud oder lokal („Auf meinem Mac“). Im ersten Fall gibt es keine Zugriffsmöglichkeiten auf Dateiebene; eine separate Komplettsicherung ist nicht möglich. Lokal gespeicherte Notizen liegen hingegen in einer SQLite-Datenbank. Die zugehörigen Dateien finden sich im versteckten Ordner `~/Library/Group Containers/group.com.apple.notes/` und liegen somit in Reichweite von Backupprogrammen wie der Time Machine. Aus einem Komplettbackup lassen sich im Notfall aber nur alle Notizen auf einmal wiederherstellen.

Apple Notizen rückt Inhalte nur ungern in allgemein nutzbaren Formaten heraus. Sie können lediglich einzelne Notizseiten als PDF-Datei exportieren. Deutlich besser geht das mit einem externen Tool: Das Programm „Exporter“ aus dem App Store sichert die Inhalte, egal ob lokal oder in der iCloud gespeichert, wahlweise

als HTML- oder Markdown-Dateien und legt angehängte Dateien separat ab. Die kostenlose Version exportiert immer alle Ordner auf einmal; wer knapp 6 Euro bezahlt, erhält eine Funktion zur Auswahl von Ordnern.

### Evernote

Die Entwickler des populären Notizprogramms Evernote haben vor rund zwei Jahren einen radikalen Schnitt gemacht, indem sie die nativen Clients für Windows, macOS und Mobsysteme auf Basis des Web-App-Frameworks Electron von Grund auf neu geschrieben und als Version 10 veröffentlicht haben.

Dabei blieben einige Funktionen auf der Strecke, die auch die Möglichkeiten, Notizen zu archivieren, zu sichern und zu exportieren, betreffen. Der Hersteller bietet jedoch bis auf weiteres Windows- und Apple-Nutzern auch eine leicht angepasste alte 6er-Version an („Evernote Legacy“), die sich parallel zu Evernote 10 installieren und nutzen lässt.

Nur diese Legacy-Version erlaubt es, Notizen alternativ zum Cloudspeicher des Herstellers (bei Google gehostet) auch lokal auf dem eigenen Rechner zu speichern. Die Daten stecken je nach System in einer SQLite-Datenbank (Windows) oder in einer Kombination aus Datenbank, Dateien und Ordnern (macOS). Sie sind somit für Backupprogramme erreichbar und lassen sich zur Not auch datei- und ordnerweise kopieren.

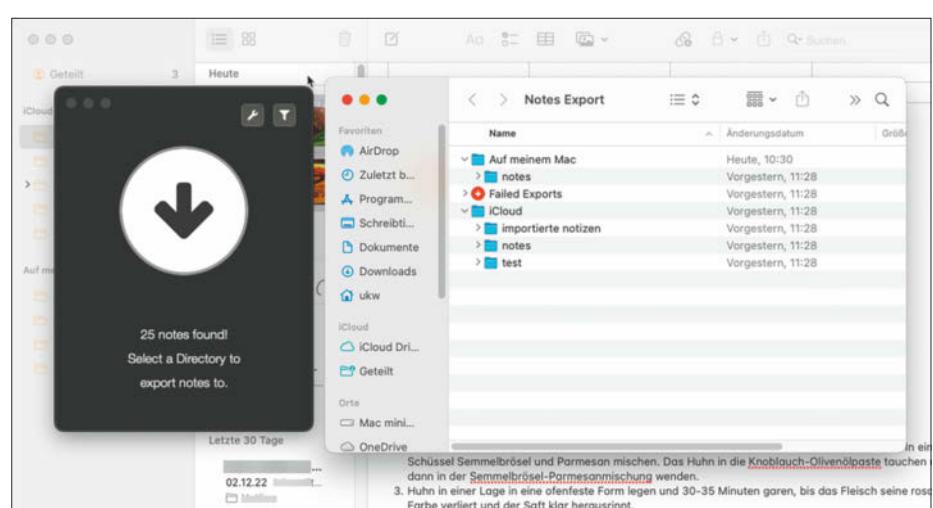
Auf der Cloud gespeicherte Notizen gibt es hingegen keinen direkten Zugriff;

ein dateigestütztes 1:1-Backup ist nicht möglich. Zwar werden zuletzt geöffnete Inhalte für einen temporären Offlinezugriff lokal zwischengespeichert; diese Cache-Dateien eignen sich aber auch nicht zur Datensicherung.

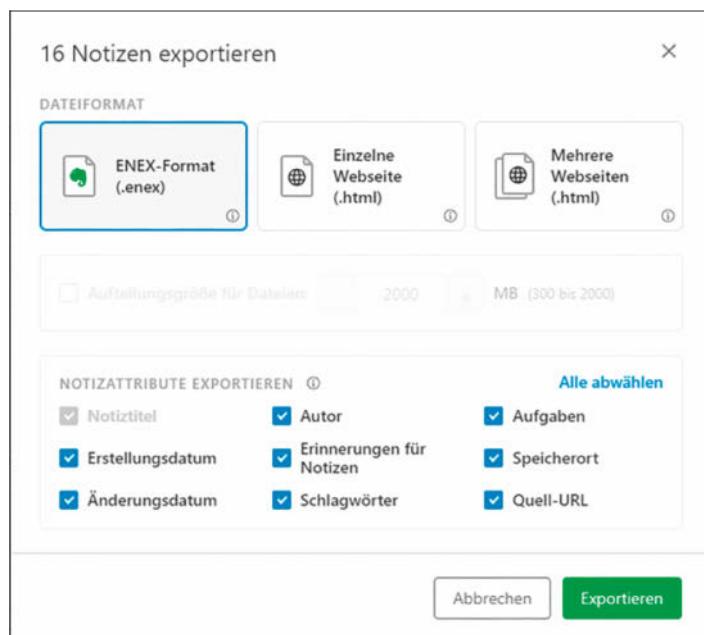
Die beste Methode dafür ist der Export der Notizen – egal, ob lokal gespeichert oder aus der Cloud geladen – in ENEX-Dateien. Das ist ein Evernote-eigenes Format, das auf XML aufbaut. Das ENEX-Format ist eine gute Wahl, weil es nahezu alle Inhalte (auch Metadaten und Tags) enthält und sich Daten somit verlustfrei zurückspielen lassen. Lediglich die Zuordnung von Notizseiten zu Notizbüchern geht verloren. Das ist nicht ganz so tragisch, weil man ohnehin nur notizbuchweise exportieren kann, also für jedes Notizbuch eine eigene Datei entsteht.

Komplette Notizbücher lassen sich mit dem alten und dem aktuellen Evernote gleichermaßen einfach in ENEX-Dateien exportieren. Der zugehörige Befehl findet sich im Kontextmenü nach einem Rechtsklick auf den jeweiligen Notizbuchnamen. Möchte man hingegen eine manuell bestimmte Auswahl von Notizen speichern, empfiehlt sich Evernote Legacy. Die 10er-Version beschränkt nämlich die maximale Zahl gleichzeitig exportierbarer, manuell selektierter Notizseiten auf 100.

ENEX-Dateien können Sie zwar mit jedem Texteditor öffnen, sie sind aber nur mühsam zu lesen – vor allem wenn angehängte Dateien in base64-Kodierung enthalten sind. Daher empfiehlt es sich, wichtige Inhalte zusätzlich in einem allgemein



**Apple Notizen kann nur einzelne Notizen im PDF-Format exportieren. Erst das externe Tool „Exporter“ speichert komplett Sammlungen im HTML- und Markdown-Format.**



nutzbaren Format zu exportieren. Evernote bietet als Formate dafür HTML und PDF an. Wählt man HTML, darf man zudem entscheiden, ob alle Notizen in einer Datei landen oder für jede eine eigene HTML-Datei entstehen soll. Dateianhänge werden formatbedingt immer in separaten Dateien abgelegt.

Ein weiterer Vorteil von Evernote Legacy für Windows, der mit der neuen Version weggefallen ist, ist das beigelegte Kommandozeilentool ENscript.exe. Damit können Sie den Export auch mehrerer Notizbücher zum Beispiel per Batch-Datei steuern. Eine umfangreiche Anleitung zum Export aus Evernote nebst Beispiel-Batchdatei für ENscript finden Sie in [1].

## Google Notizen

Google Notizen (auch bekannt als Google Keep) ist ein sehr einfaches, rein cloud-gestütztes Notizprogramm für Webbrowser und Mobilgeräte. Jeder mit einem Google-Konto kann es kostenlos nutzen.

Eine echte Backup-Funktion für Komplettsicherungen mit Restore-Option fehlt. Immerhin gibt es zwei Möglichkeiten, Notizinhalte in ein lesbares Format zu exportieren, um sie cloudunabhängig zu archivieren oder anderweitig weiterzuverarbeiten.

Am einfachsten ist es, Notizen inklusive der Bilder in Googles Onlinetextverarbeitung Docs zu kopieren. Dazu klicken Sie in der betreffenden Notiz auf das Dreipunktemenü und wählen „In Google Docs kopieren“. In der mobilen App unter An-

droid und iOS tippen Sie zuvor auf „Senden“ und können für Einzelnotizen auch andere Apps als Google Docs als Ziel wählen. Das funktioniert auch mit mehreren selektierten Notizen auf einmal, auf Mobilgeräten dann aber nur noch mit Google Docs als Ziel. Mehrere Notizen landen hintereinander ohne Trennung oder Seitenteilung in der Textverarbeitung und lassen sich in unterschiedlichen Formaten, zum Beispiel PDF, DOCX, RTF, ODT und HTML auf Ihren Rechner herunterladen.

Die zweite Methode nutzt Googles Takeout-Dienst, der es erlaubt, allerlei persönliche Google-Daten auf den eigenen Rechner zu laden, darunter auch Notizen – jedoch nur alle auf einmal.

Öffnen Sie dazu in einem Webbrowser die Seite [takeout.google.com](https://takeout.google.com), heben dort

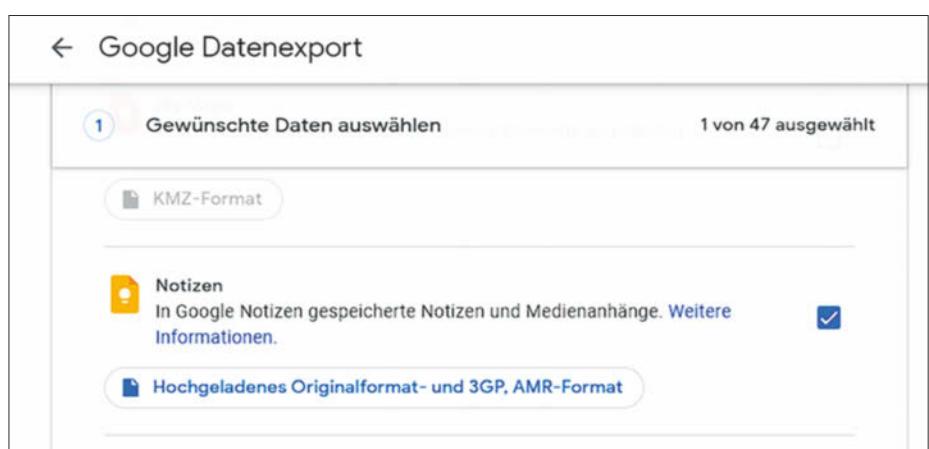
**Evernotes ENEX-Exportformat**  
enthält optional auch alle wichtigen Metadaten, nur nicht die ursprüngliche Zuordnung zu Notizbüchern.

die Auswahl für alle gewählten Dienste auf und setzen dann ein Häkchen nur beim Eintrag „Notizen“. Klicken Sie unten auf „Nächster Schritt“ und im folgenden Fenster auf „Export erstellen“. Wenn Sie alle Standardeinstellungen belassen haben, erhalten Sie nach einer gewissen Zeit eine Mail mit einem Downloadlink an Ihr Google-Postfach. Der Hinweis, das könne bisweilen Tage dauern, hat sich in unseren Tests nicht bestätigt; die Mail kam nach wenigen Minuten. Die darüber heruntergeladene Zip-Datei enthält alle Notizen als Einzeldateien in zwei Formaten: einmal als HTML, einmal im JSON-Format mit Metadaten. Bilder und Audiodateien liegen einzeln in der Zip-Datei.

## Joplin

Joplin ist ein vor allem unter technikaffinen Nutzern beliebtes Open-Source-Notizprogramm, das im Editor Markdown nutzt und Daten in lokalen Datenbanken speichert. Eine Synchronisation der Daten mit der herstellereigenen Cloud oder auf NextCloud, Dropbox, OneDrive oder per WebDAV ist optional.

Der beste Weg, Backups von Joplin-Inhalten zu erzeugen, ist der Export in JEX-Dateien. Das ist ein Archiv im TAR-Format, das sich mit Programmen wie 7-Zip problemlos öffnen lässt. Darin stecken alle Inhalte in einzelnen Markdown-Textdateien und in einem Ordner mit Dateianhängen. Zuordnungen und interne Verlinkungen sind durch die kryptische Namensgebung der Dateien gewährleistet und der Anwender kann sie verlustfrei zurückspielen – sofern er nichts an den Bezeichnungen manipuliert hat. Der alternativ verfügbare Raw-Export verzichtet



**Das simple Notizprogramm von Google bietet selbst nur wenige Exportfunktionen. Über Googles Takeout-Dienst kann man aber per Webbrowser alle Notizen auf einmal als JSON- oder HTML-Dateien herunterladen.**

auf die Archivdatei und schreibt direkt Einzeldateien und Ordner.

Zusätzliche Export-Formate für den gesamten Datenbestand oder markierte Einzelnotizen sind Markdown (im Gegensatz zu JEX und RAW mit „sprechenden“ Dateinamen) und HTML mit oder ohne Ordnerstruktur. Selektierte Notizen kann man zudem als PDF-Dateien exportieren.

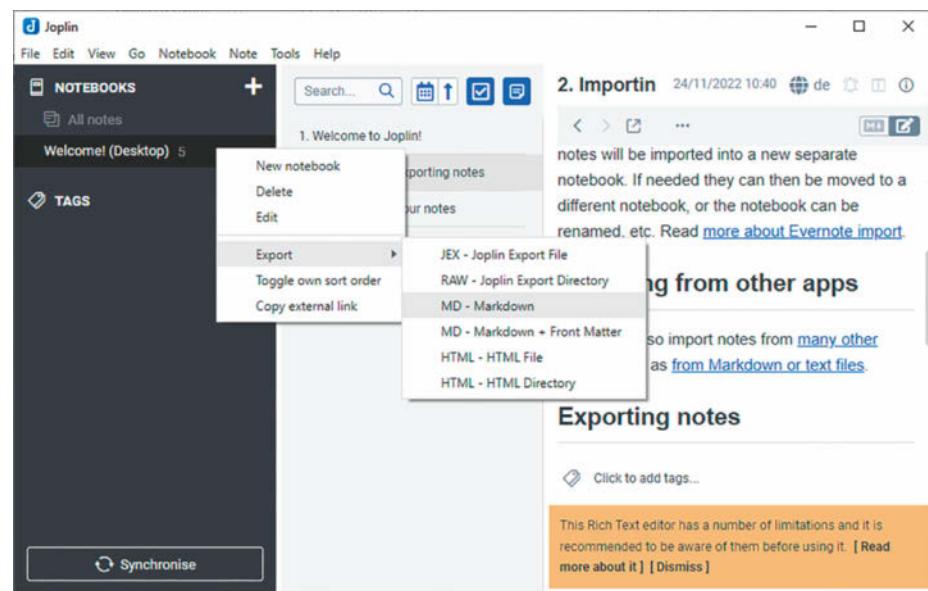
Eine automatische Backup-Funktion enthält Joplin nicht. Das Programm unterstützt aber von der Community geschriebene Plug-ins. Im zugehörigen Verzeichnis („Tools/Options/Plugins/Manage your plugins/Browse all plugins“) findet sich auch „Simple Backup“ von JackGruber, mit dem man bei laufendem Programm automatische Sicherungen in beliebigen Zeitintervallen und mit mehreren Revisionen einrichtet.

## Notion

Das rein cloudestützte Wissensmanagement-Programm Notion zeichnet sich durch eine komplexe Strukturierbarkeit der Inhalte und die Integration von Datenbanken aus.

Der Anbieter versichert, dass vom gesamten Workspace – das ist die oberste Hierarchieebene – minütlich eine Sicherheitskopie in dessen Cloud abgelegt wird. An die kommt man aber als Nutzer nicht selbst heran. Sollte einmal ein Zurückspielen der Daten notwendig werden, weil die Seitenversionsverwaltung und der Papierkorb ein Malheur nicht beheben können, muss man sich an den Support wenden.

Was man aber selbst erledigen kann, ist ein Export aller Daten, also des kompletten Workspaces, oder der von ausgewählten Inhalten in einem allgemein lesbaren Format. Nutzer der kostenlosen oder der Plus-Version von Notion exportieren wahlweise in Markdown- oder HTML-Dateien. Markdown eignet sich besser, um es in andere Programme zu importieren und dort weiterzubearbeiten; HTML bildet jedoch die originalen Layouts meist besser ab. Datenbanktabellen werden im CSV-Format exportiert. Nur Inhaber eines teureren Abos (Business oder Enterprise) dürfen auch im PDF-Format exportieren. All diese Formate erhalten zwar die Inhalte, lassen sich aber nicht ohne Strukturverlust wieder in Notion importieren. Exporte kann man nur manuell anschließen; eine Backup-Automatik gibt es in Notion nicht – „derzeit“, wie sich der Hersteller dazu äußert.



Aus dem Open-Source-Programm Joplin exportiert man Inhalte wahlweise als restaurierbare Markdown-Dateien (RAW und JEX) oder in klassische Markdown- oder HTML-Files. Den kompletten Datenbestand kann man auch als PDF speichern.

## Obsidian

Nutzer des zunehmend beliebten kostenlosen Notiz- und Wissensmanagementprogramms Obsidian (Test in [2]) müssen sich kaum Sorgen um ihre Daten machen. Ein besonderes Merkmal des Programms ist nämlich, dass es kein proprietäres Datei- und Speicherformat verwendet, sondern direkt mit herkömmlichen Markdown-Dateien arbeitet. Ihre Organisation erfolgt über das Dateisystem in Ordnern und Unterordnern.

Das hat eine Reihe von Vorteilen: Sie können jedes Backup-Programm nutzen und müssen lediglich die Obsidian-Verzeichnisbäume in die Sicherung einschließen. Eine simple Kopie der Ordner auf einen externen Datenträger, Server oder Cloudspeicher reicht auch. Außerdem steckt in Obsidian eine Backupfunktion, die in einstellbaren Zeitintervallen selbstständig Sicherungskopien an einem wählbaren Ort anlegen.

Die Dateien lassen sich direkt wieder in Obsidian, aber auch mit jedem Texteditor öffnen. Ist der Markdown-fähig, bleiben weitestgehend auch die Formatierungen erhalten. Es gibt aber einige Unterschiede bei Markdown-Dialekt. Zudem sind Markdown-Dateien ein guter Ausgangspunkt für die Konvertierung in andere Formate wie PDF oder DOCX mit separaten Tools wie Pandoc (ct.de/y1yj).

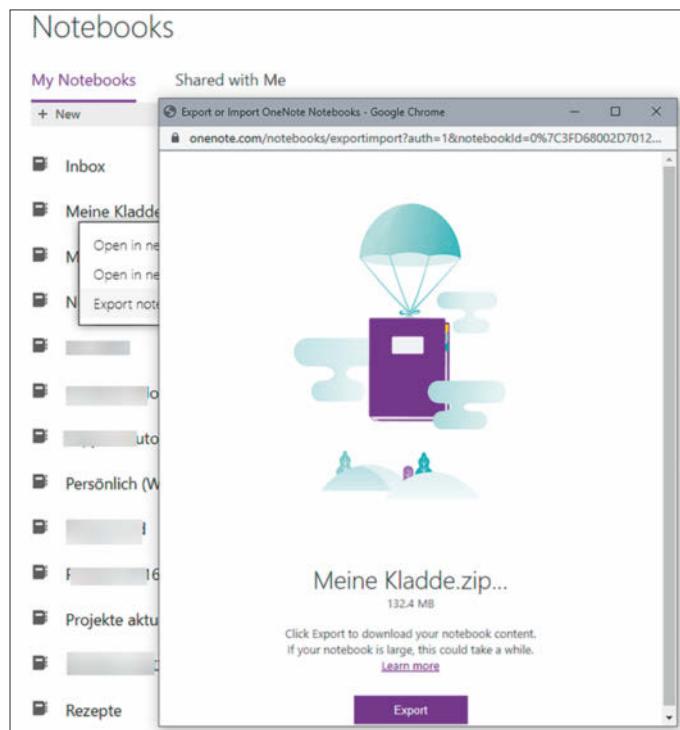
Außerhalb von Obsidian gehen jedoch einige organisatorische Strukturen verlo-

ren. Die Notiztitel werden zu den Dateinamen, finden sich aber nicht mehr in den Markdown-Dateien selbst, interne Links und Backlinks funktionieren nicht mehr und auch Bildzuordnungen können verschwinden. Da externe Programme auch mit den Livedaten und Komplett Sicherungen arbeiten können, ist Umsicht angebracht. Besser, man fertigt separate Kopien an.

## OneNote

In Microsofts Notizprogramm OneNote ist alles etwas anders und die Erklärung umfangreicher. Ein Grund ist Microsofts Zickzackkurs bei der Produktpflege und -politik. Sie hat zu einem Wildwuchs von zwar weitgehend untereinander daten-, aber nicht funktionskompatiblen OneNote-Varianten für die unterschiedlichen Desktop- und Mobilbetriebssysteme geführt. Unter Windows gibt es sogar zwei Versionen mit gelegentlich wechselnden Namen (zur Zeit: „OneNote“ und „OneNote für Windows 10“).

Alle OneNote-Inhalte liegen grundsätzlich auf OneDrive. Lediglich das „Ur-OneNote“, die Desktopversion für Windows (vormals „OneNote 2016“, nun nur noch „OneNote“) erlaubt es, Notizen alternativ lokal abzuspeichern – allerdings nur dann, wenn man eine MS-Office-Lizenz besitzt. Sie sind dann abschnittsweise – ein OneNote-Abschnitt ist eine hierarchische Strukturinheit – in binär kodierten XML-Datei-



**Auf OneDrive für Privatkonten gespeicherte Notizbücher exportiert man über die Weboberfläche von OneNote. Damit das klappt, muss man die erst auf englische Sprache umstellen.**

seit Jahren nicht behobenen Skriptfehlers funktioniert das Folgende sonst nicht.

Nach einem Rechtsklick auf das zu exportierende Notizbuch wählen Sie „Export Notebook“. Bestätigen Sie den Export im nächsten Fenster. Bleibt das komplett leer, haben Sie die Sprache nicht umgestellt. Sie erhalten eine Zip-Datei mit den einzelnen ONE-Dateien des Notizbuchs. Um sie unabhängig von Ihrer verwendeten OneNote-Version wieder zu OneDrive hochzuladen, besuchen Sie die Webseite <https://www.onenote.com/notebooks/exportimport?toImport=true>.

Nutzen eines Geschäfts- oder Schulkontos ist diese Option verwehrt. Ihnen bleiben bislang nur die Windows-Desktopversion und die genannte Backupfunktion oder der manuelle Export.

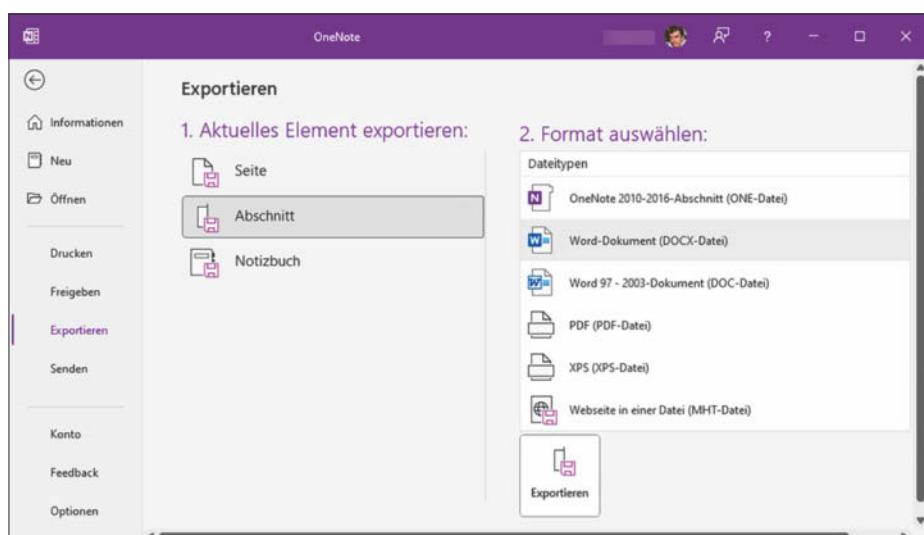
Nur in der Windows-Desktop-Version von OneNote gibt es nämlich zusätzlich die Möglichkeit, Notizen entweder im OneNote-eigenen ONE-Format oder in ein allgemein les- und nutzbares Format zu exportieren („Datei/Exportieren“).

Die aktuelle Notizseite oder den kompletten Abschnitt exportieren Sie wahlweise im PDF- oder HTML-Format, für komplett Notizbücher bietet das Programm nur PDF an. Ist auf dem Rechner MS Office (insbesondere Word) installiert, können Sie auch DOCX-Dateien erzeugen. Notizbücher lassen sich zudem auch als ONEPKG-Dateien sichern. Das ist nicht mehr als ein ZIP-Archiv, das alle ONE-Dateien des Notizbuchs zusammenfasst.

en mit der Endung .ONE gespeichert und gemäß der Zuordnung zu Notizbüchern mit einer Indexdatei in Dateisystemordnern organisiert. Das ONE-Format ist nur von OneNote lesbar, lässt sich aber problemlos in Dateibackups einschließen oder auf Sicherungsdatenträger kopieren. Die Desktopversion von OneNote enthält zudem eine Backupfunktion („Datei/Optionen/Speichern und Sichern/Sicherung“), die an einem definierbaren Ort Kopien der ONE-Dateien anlegt, allerdings ohne Indexdatei. Beim Zurückspielen muss man einige Zuordnungen per Hand wiederherstellen. Diese Backupfunktion sichert auch auf OneDrive gespeicherte Notizbücher, wenn unter „Datei/Optionen/Speichern und Sichern/Sicherung“ ein Häkchen bei „In SharePoint gespeicherte Notizbücher sichern“ gesetzt ist. Stören Sie sich nicht am Begriff „SharePoint“, gemeint ist „OneDrive“.

Neuerdings besitzt auch OneNote für macOS eine ähnliche Backupfunktion. Sie dient nur zum Sichern und Zurückspielen von in der Cloud gespeicherten Notizen, eine lokale Speicherfunktion existiert auf dem Mac nach wie vor nicht. Sie aktivieren die Backups über „OneNote/Einstellungen/Sicherungen...“ Die Restore-Funktion finden Sie unter „Datei/Sicherungskopien öffnen“.

In der Cloud gespeicherte Notizbücher liegen zwar ebenfalls im ONE-Format auf OneDrive, sind dort aber versteckt. Sichtbar sind nur Platzhalterdateien mit



**Nur die Windows-Desktopversion (nicht „OneNote für Windows 10“) gestattet den Export von Notizen im HTML- oder PDF-Format. Ist Office installiert, kann man auch in Wordformaten speichern.**

Bedingt durch das ungewöhnliche Format von OneNote-Notizen mit auf einer endlos großen Seite frei platzierbaren Inhaltsobjekten kann beim Export in HTML-, PDF- oder Worddateien ein ziemlicher Layoutsalat entstehen. Teilweise versucht das Programm, Inhalte so zu verkleinern, dass sie auf eine reguläre Textseite passen, teils entstehen unvermittelte Seitenumberüberschreitungen mit Teileinhalten der Vorseite. Immerhin bleiben Text- und Bildinhalte und externe Links erhalten. Vektorgrafiken (Handschrift) werden meist in Bitmaps umgewandelt, eingebettete Dateien gehen verloren.

Für wichtige Inhalte empfiehlt sich eine duale Sicherungsstrategie: Eine Kopie im OneNote-eigenen ONE-Format und zusätzlich eine in HTML, PDF oder DOCX.

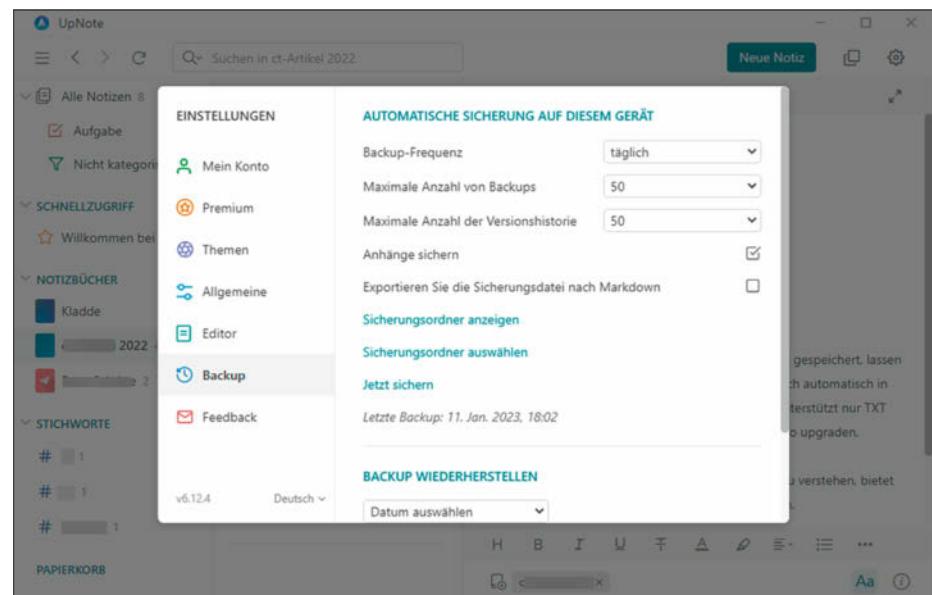
## UpNote

Das noch nicht ganz so bekannte Upnote (Kurztest in [3]) orientiert sich in Sachen Bedienung und Oberfläche stark an Evernote, unterscheidet sich von diesem aber unter anderem dadurch, dass es außer der Synchronisation über die Cloud des Anbieters auch die lokale Speicherung von Notizen erlaubt.

Außerdem enthält es eine sehr gute halbautomatische Backupfunktion, mit der man sowohl lokal als auch in der Cloud gespeicherte Inhalte nicht nur an einem beliebigen Ort sichert, sondern auch ohne Schäden an Inhalt und Struktur wieder zurückspielt – allerdings immer den gesamten Datenbestand auf einmal. Dazu muss Upnote aber laufen. Die Restore-Funktion kann man immerhin auf aus dem Papierkorb gelöschte Notizen begrenzen.

Über das Zahnradsymbol und „Backup“ stellt man Speicherpfad, Backupfrequenz und Anzahl der Revisionen ein. Die Originaldaten lokaler Notizbücher liegen in einer SQLite-Datenbank, cloudgespeicherte bei Googles Firebase-Dienst. Die Backups im herstellereigenen Format bilden die Inhalte nur ab und sollten nicht manipuliert werden. Man kann aber einstellen, dass das Backup zusätzlich Markdown-Dateien sichert.

Die kann man auch aus selektierten Notizen erzeugen, jedoch nur in der bezahlten Version, auch im PDF- und Markdown-Format. Im Gratis-Upnote stehen nur TXT und HTML als Exportformate zur Verfügung. Bei einzelnen Notizen wählt man aus dem Dreipunktemenü im Editor



**UpNote bietet umfangreiche Backup- und Exportmöglichkeiten, auch halbautomatisch, mit mehreren Revisionen und verlustfreier Restore-Option.**

„Exportieren“; hat man mehrere Notizen ausgewählt, erscheint ein passendes Menü im Editorbereich automatisch. Formatbedingt geht bei diesen Einzelexports manche Strukturinformation (interne Links, Notizbuchzuordnung, Tags) verloren, weshalb sie ein Vollbackup nicht ersetzen.

## Fazit

Es ist schon ziemlich überraschend: Nur zwei der untersuchten Notiz- und Wissensmanagementprogramme erlauben ein Komplettbackup aller Inhalte, das sich verlustfrei im Bedarfsfall wieder zurückspielen lässt, nämlich UpNote und Joplin. Bei allen anderen verliert man zumindest strukturelle Informationen und muss diese nach einem Restore mühsam manuell wiederherstellen.

Ein Sonderfall ist Obsidian: Das Programm arbeitet mit den Ordnerstrukturen des Dateisystems und Markdown-Dateien. Eine Sicherungskopie der kompletten Dateibäume nebst Inhalten erhält deshalb auch alle Link- und Organisationsstrukturen. Das muss man aber extern per Skript oder Backupprogramm erledigen. Ein halbautomatisches Backup, das zumindest dann läuft, wenn das jeweilige Programm gestartet ist, bieten nur die Desktopversionen von UpNote, Obsidian und OneNote, aber nicht die Universal-Windows-Plattformversion „OneNote für Windows 10“. In Joplin kann man das Backup per Plug-in nachrüsten.

Alternativ extrahiert man aus allem Programmen mehr oder weniger komfor-

tabel zumindest Text- und Bilddaten in einem allgemein lesbaren Format wie Markdown, HTML oder PDF. Die lassen sich nicht ohne Weiteres wieder zurückspielen, taugen also weniger als Vollbackup. Aber auf diesem Weg legt man sich vom jeweiligen Programm und Hersteller unabhängige Archivkopien an.

Das Evernote-eigene ENEX-Format ist ein guter Kompromiss zwischen vollständigem Inhalt und programmunabhängiger Lesbarkeit. Zudem hat es sich als Quasi-Standard etabliert und wird von manch anderem Programm als Importformat akzeptiert. Leider fehlen Evernote automatische Backup-Mechanismen und die neue Version 10 schränkt die Speicheroptionen gegenüber den Vorgängern ein.

Aber egal, wie umständlich es einem die Programme machen. Wenn der Gedanke, von heute auf morgen alle Inhalte zu verlieren, mehr als nur ein Schulterzucken auslöst, ist das bisschen Arbeitszeit für einen gelegentlichen Datenexport an einen sicheren und selbst kontrollierten Ort sinnvoll investiert. (swi@ct.de) **ct**

## Literatur

- [1] Stefan Wischner, In Sicherheit gebracht, Daten aus Evernote exportieren und sichern, c't 6/2021, S. 160
- [2] Stefan Wischner, Hirnbrausen, Markdown-Notizprogramm, c't 25/2022, S. 100
- [3] Stefan Wischner, Schlanke Notizprogramme, c't 23/2022, S. 81

**Pandoc-Konverter: [ct.de/y1yj](http://ct.de/y1yj)**



# Gnome mit Kacheln

## Linux-Desktop Gnome für große Bildschirme einrichten

**Wer einen übergroßen Monitor nutzen will, stößt mit den Voreinstellungen von Gnome schnell an Grenzen. Wir zeigen, welche Einstellungen und Erweiterungen auch Pixelmonster optimal bespielen.**

Von Keywan Tonekaboni

Der neue Monitor für den Linux-Rechner ist da! Endlich genug Fläche für all die vielen Fenster. Doch mehr Pixel allein lösen nicht alle Probleme und schaffen neue, denn Gnome hilft kaum dabei, Fenster effizient auf einer großen Bildschirmfläche zu verteilen. Zwar gibt es

eine Einrasthilfe, die Fenstergrößen automatisch anpasst. Doch während Windows oder KDE Plasma das Fenster auch auf ein Viertel der Displayfläche reduzieren, kann Gnome sie nur auf eine der beiden Hälften schieben.

Mit den richtigen Hilfsmitteln glänzt der Gnome-Desktop auch auf der großen Bildschirmfläche. Allerdings schießen in manchen Situationen Tools quer, die sonst gute Dienste leisten. Wir stellen daher sinnvolle Einstellungen und praktische Erweiterungen vor für übergroße oder überbreite Monitore.

### Optimieren ohne Tweaks

Seit Gnome-Version 41 enthält „Einstellungen“ den Abschnitt „Multitasking“, der eine Handvoll Optionen listet, die das Verhalten der Gnome-Bedienoberfläche beeinflussen. Die meisten davon gibt es seit

Einführung der Gnome-Shell, nur waren sie bislang versteckt. Ändern ließen sich diese Optionen unter anderem über das Zusatzprogramm „Gnome Optimierungen“. Das besser als Tweak-Tool bekannte Werkzeug ist jetzt weitgehend überflüssig.

### ct kompakt

- Die Desktopumgebung Gnome schöpft das Potenzial übergroßer Bildschirme nicht aus.
- Erweiterungen für die Gnome-Shell rüsten Komfortfunktionen nach.
- Mit der Erweiterung Tiling Assistant arbeiten Sie auf großen Displays besonders produktiv.

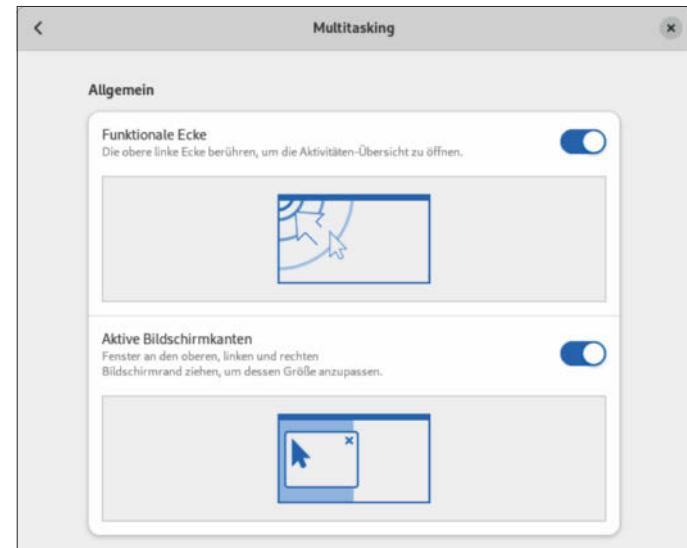
Falls abgeschaltet, können Sie unter „Multitasking“ die aktiven Bildschirmkanten einschalten, worauf sich die Größe eines Fenster anpasst, wenn Sie es an den Bildschirmrand ziehen. So eine Funktion heißt auf Englisch „Tiling“ oder „Snap Layout“. Die Gnome-Einrasthilfe kann Fenster nur auf die rechte beziehungsweise linke Hälfte des Bildschirms zwingen oder sie auf die gesamte Displayfläche maximieren. Später im Text stellen wir Erweiterungen vor, die ein flexibleres und ausgefeilteres Tiling erlauben. Solche Erweiterungen deaktiviert die Funktion der aktiven Bildschirmkanten von Gnome, um Wechselwirkungen damit zu vermeiden.

Ab Werk besitzt Gnome außer dem sichtbaren Desktop noch weitere virtuelle Arbeitsflächen, zwischen denen Sie über die Aktivitätenübersicht oder mit Tastenkombination Super+Alt+Pfeiltaste links/rechts wechseln. Verwenden Sie mehrere Monitore, dann richtet Gnome normalerweise die virtuellen Arbeitsflächen nur für den primären Bildschirm ein. Das ist der Monitor, der auch die Menüleiste und das Dock anzeigt. Unter „Multitasking“ können Sie bei der Nutzung mehrerer Monitore Gnome anweisen, auf allen Bildschirmen virtuelle Arbeitsflächen einzurichten.

Der Vorteil der Gnome-Vorgabe: Auf dem zweiten Monitor mit statischer Arbeitsfläche platziert man Fenster, die man stets im Blick haben möchte, wie ein Mailprogramm, Chatfenster oder Systemanzeigen. Tauscht man beispielsweise zwei 16:9-Bildschirme gegen einen überbreiten 21:9-Monitor, fällt die statische Arbeitsfläche weg. Als Workaround können Sie Fenster, die Sie immer im Blick haben müssen, auf alle Arbeitsflächen pinnen. Klicken Sie dazu mit der rechten Maustaste auf die Titelleiste des gewünschten Programmfensters, beispielsweise der Messenger-App. Wählen Sie im Fenstermenü den Eintrag „Immer auf der sichtbaren Arbeitsfläche“. Dann nimmt Gnome beim Wechsel der Arbeitsfläche das Fenster mit. Bei manchen Programmen wie Microsoft Teams fehlt die Titelleiste. Hier öffnen Sie das Fenstermenü, indem Sie beim Rechtsklick zusätzlich die Super-Taste (Windows-Taste) gedrückt halten.

Mit einem Hack können Sie die Arbeitsflächen-Einstellungen nutzen, um ohne zusätzliche Erweiterungen das Tiling auf extrabreiten Monitoren zu verfeinern. Verfügt Ihr Monitor über mehrere Display-

**Das Verhalten des Gnome-Desktops ändern Sie in den Einstellungen unter Multitasking, etwa um Fenster am Bildschirmrand einschnappen zu lassen.**



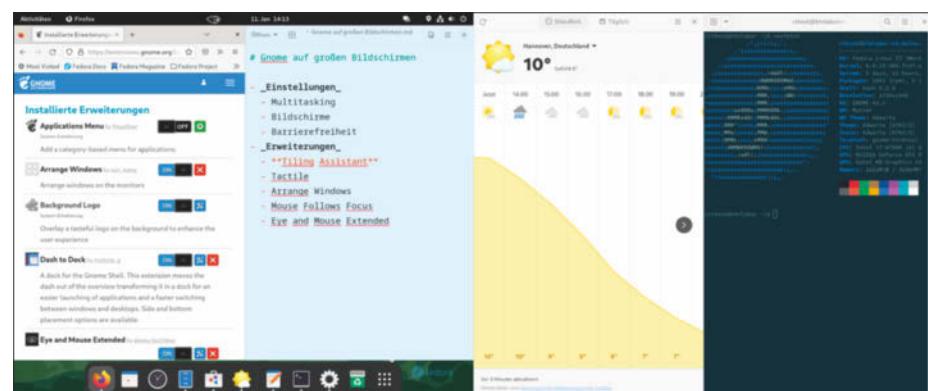
eingänge und unterstützt die Funktion Picture-by-Picture, schließen Sie ihn mit zwei Kabeln an den Computer an. Gnome behandelt die erkannten Displayflächen wie eigenständige Monitore. Platzieren Sie unter „Bildschirme“ (Ubuntu: „Anzeigegeräte“) beide Anzeigen nebeneinander. Dadurch erhalten Sie vier Spalten, an denen Sie Fenster ausrichten können. Es sieht etwas merkwürdig aus und funktioniert prinzipiell, lohnt sich aber nur, wenn man partout keine Erweiterungen installieren möchte.

## Gnome-Desktop mit Erweiterungen tunen

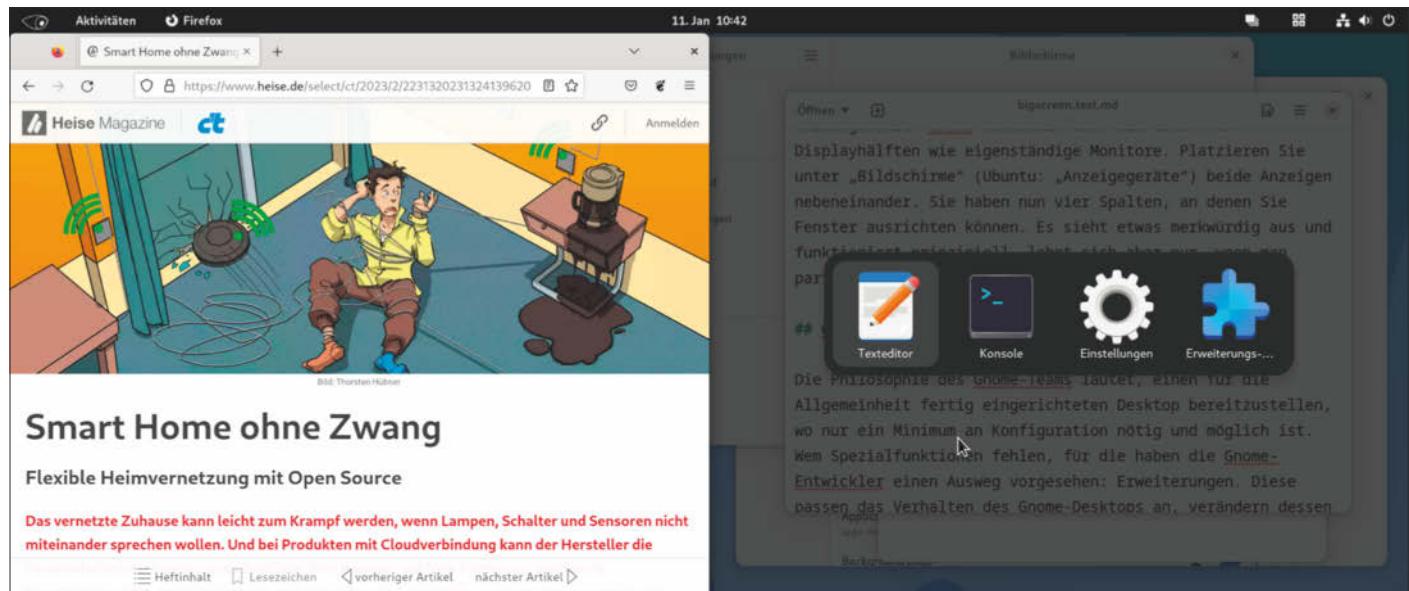
Die Philosophie des Gnome-Teams lautet, einen Desktop bereitzustellen, der nur ein Minimum an Konfiguration braucht und ermöglicht. Für Spezialfunktionen haben die Gnome-Entwickler einen Ausweg vorgesehen: Erweiterungen. Diese passen das Verhalten des Gnome-Desktops an, ver-

ändern sein Layout und fügen neue Funktionen hinzu oder integrieren jene anderer Anwendungen in die Bedienoberfläche. Dazu modifizieren Erweiterungen den Programmcode der Gnome-Shell, was Einfluss auf die Stabilität des Desktops haben kann. Deshalb kann es auch vorkommen, dass sich Extensions gegenseitig in die Quere kommen.

Daher ein Wort der Warnung: Erweiterungen sind dafür gedacht, den Gnome-Desktop punktuell anzupassen, nicht dazu, das ganze Bedienkonzept auf den Kopf zu stellen. Verwenden Sie daher nur benötigte Erweiterungen oder greifen Sie gleich zu einer anderen Desktop-Umgebung. Deinstallieren Sie außerdem nicht benötigte Erweiterungen, da diese auch im deaktivierten Zustand beim Start der Gnome-Shell initialisiert werden. Wer diese Hinweise beachtet, kann mit einer Handvoll Erweiterungen viel Spaß haben.



**Beherrscht Ihr überbreiter Bildschirm den Picture-by-Picture-Modus, trotzten Sie Gnome ein vierseitiges Tiling ab, wenn Sie Ihren Monitor mit zwei Kabeln parallel anschließen.**



Die Erweiterung Tiling Assistant baut die Einrastfunktion aus. Sie gruppiert die Fenster, woraufhin Sie diese gemeinsam in den Vordergrund heben oder deren Größen simultan ändern können.

## Teilen und herrschen

Mitunter die erste Frage, die sich bei übergroßen und extrabreiten Bildschirmflächen stellt: Wie platziere ich die Fenster möglichst effizient? Auf einem 21:9-Display will man selten Fenster auf die ganze Fläche maximieren. Hier kommt das Tiling ins Spiel, also das Einrasten und Unterteilen der Fenster anhand eines festen Rasters – zum Beispiel vier Viertel – oder nach einem Muster zu teilen, etwa die Fläche dynamisch durch die Anzahl der geöffneten Fenster. Interessanterweise greift das Tiling teils auf Konzepte von sehr nerdigen Bedienoberflächen zurück, wie den Tiling-Window-Managern [1]. Zahlreiche Erweiterungen ersetzen oder ergänzen die Tiling-Funktion von Gnome.

Eine sehr flexible und umfangreiche Erweiterung ist der „Tiling Assistant“, der trotzdem relativ intuitiv zu bedienen ist. Den Eintrag zu dieser Erweiterung auf extensions.gnome.org (siehe Kasten „Shell-Erweiterungen installieren“) und die für alle weiteren Extensions haben wir für Sie unter ct.de/ys28 verlinkt. Der Tiling Assistant ändert zunächst zwei Dinge: Wenn Sie ein Fenster an den Rand ziehen, gibt es zusätzliche Optionen, wie das Fenster einrasten kann, beispielsweise in der oberen Bildschirmhälfte oder in einer Ecke. Lassen Sie Fenster in einer dieser Zonen einrasten, öffnet sich ein Pop-up mit Icons aller weiteren geöffneten Programme. Wählt man ein Icon aus, platziert der Tiling Assistant das zugehörige Fenster

auf der freien Fläche. Zusätzlich gruppiert es die Fenster. Wird ein Fenster der Gruppe angehoben, also vor andere Fenster gezeichnet, dann hebt der Tiling Assistant alle anderen Fenster mit an. Wechselt man die Arbeitsfläche, visualisiert eine kleine Animation, welches Fenster den Fokus hat.

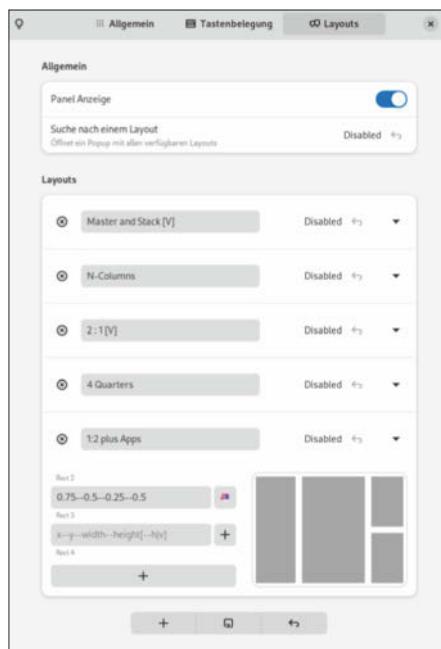
Verschieben Sie ein Fenster mit der Maus und halten dabei die Strg-Taste ge-

drückt, dann rastet das Fenster nicht nur im Monitorrand ein, sondern auch bei bereits eingerasteten anderen Fenstern. Beide Fenster teilen sich dann die Fläche. Wenn Sie die Größe des einen Fensters ändern, zieht das andere Fenster mit. Probieren Sie es einfach aus; Tiling Assistant zeigt in einer Animation, wo das Fenster einrastet.

Zusätzlich zur Mausbedienung gibt es Tastenkombinationen, um die Fenster zu platzieren. Wie bei der Gnome-Tiling-Funktion verschiebt die Tastenkombination aus Super-Taste und der linken Pfeiltaste das Fenster beispielsweise auf die linke Hälfte. Darüber hinaus kann man die Super-Taste aber auch mit einer Taste des Ziffernblocks kombinieren. Bei Super+9 vom Ziffernblock landet das ausgewählte Fenster in der oberen, rechten Ecke.

Viele dieser Vorgaben können Sie nach Belieben anpassen – etwa das Kachel-Pop-up abschalten oder die Tastenkombinationen verändern. Öffnen Sie dazu in der Erweiterungsverwaltung die Einstellungen des Tiling Assistant. Die meisten Optionen sind selbsterklärend.

Wenn Sie den Gnome-Desktop im Wayland-Modus nutzen, kann es Darstellungsfehler mit der Fokus-Animation geben. Deaktivieren Sie in diesem Fall die Animation unter „Active Window Hint“. Verlieren Sie oft die Übersicht, welches Fenster den Fokus hat, können Sie mit der Einstellung „Always“ den Tiling Assistant anweisen, dauerhaft einen blauen Rand um das fokussierte Fenster zu zeichnen.



Passen Sie in den Einstellungen von Tiling Assistant die Layouts an und legen Sie fest, welche Apps automatisch mit dem Layout starten sollen.

Auch diese Einstellung kann im Wayland-Modus Probleme verursachen.

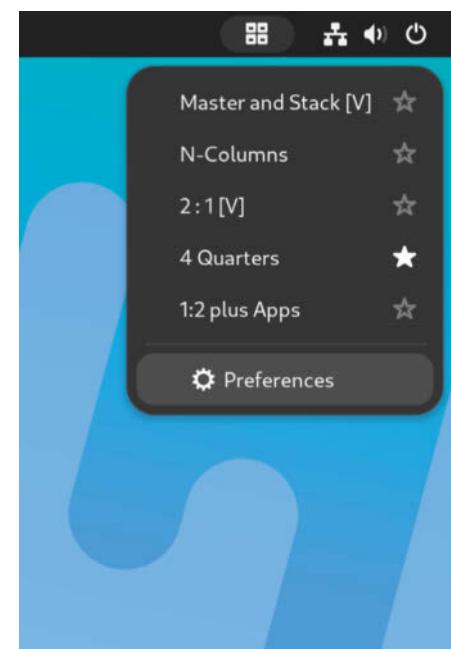
Der Abschnitt „Dynamisches Tastenbelegungsverhalten“ verändert das Verhalten von Tastenkombinationen abhängig vom Zustand des geteilten Fensters. Bei „Fester Fokus“ wechseln die Tastenkombinationen das aktiv ausgewählte Fenster, wenn es schon im Raster platziert ist. Ein links eingeschnapptes Fenster springt dann mit Super+6 (vom Ziffernblock) nicht nach rechts, sondern wechselt den Fokus, wenn rechts ein anderes eingerastetes Fenster vorhanden ist. Mit der Auswahl „Kachelzustand“ ändern Tastenkombinationen die Größe des eingerasteten Fensters. Befindet sich das ausgewählte Fenster auf der linken Hälfte und Sie drücken Super+2, wechselt das Fenster in die untere linke Ecke; ohne „Kachelzustand“ würde das Fenster die gesamte untere Hälfte belegen. Wenn Sie diese Beschreibung verwirrt und Sie nicht vorhaben, Fenster mit Tastenkombinationen wild hin und her zu scheuchen, belassen Sie das dynamische Tastenbelegungsverhalten in der Grundeinstellung, also deaktiviert.

### Layouts mit Tiling Assistant

Die wohl spannendste Funktion versteckt der Tiling Assistant als experimentelles Feature: Layouts. Damit legen Sie individuelle Raster an, die von der schnöden Verteilung abweichen und sich optional dynamisch erweitern. Ein Layout könnte etwa rechts zwei kleine Kacheln für Chatfenster vorsehen und links eine große Fläche für den Browser, ein Office-Programm oder die Entwicklungsumgebung. Wenn Sie ein Layout aktivieren, dann bietet Tiling Assistant an, mit dem Kachel-Pop-up alle geöffneten Fenster anhand des Layouts anzuordnen.

Um die Layout-Funktion freizuschalten, öffnen Sie die Einstellungen des Tiling Assistant und klicken links in der Titelleiste auf die Glühbirne (Ubuntu: Info-Icon). Daraufhin öffnet sich ein Menü. Wählen Sie den Eintrag „Fortgeschrittene ...“ aus und aktivieren Sie dort den Schalter „Erweiterte/Experimentelle Einstellungen“. Wenn Sie mit dem Pfeil in der Titelleiste in das Menü „Einstellungen“ zurückkehren, sehen Sie einen neuen Tab namens „Layouts“. Vier Layouts sind in Tiling Assistant bereits definiert: „Master and Stack [V]“, „N-Columns“, „2:1 [V]“, „4 Quarters“. Das letzte verhält sich wie das Standardlayout mit zwei Spalten und zwei Zeilen.

Bei „Master and Stack [V]“ gibt es ein Hauptfenster auf der linken Bildschirmhälfte. Die andere Hälfte teilt Tiling Assistant horizontal unter den Fenstern auf, die Sie über das Kachel-Pop-up auswählen. Bei vier Fenstern wären diese so aufgeteilt: links eine Spalte mit einer Zeile und rechts eine Spalte mit drei Zeilen.



Wechseln Sie blitzschnell über das Panelmenü das Raster-Layout, nach dem Tiling Assistant die Fenster anordnet.

Bei vier Fenstern wären diese so aufgeteilt: links eine Spalte mit einer Zeile und rechts eine Spalte mit drei Zeilen.

Das Layout „N-Columns“, also N-Spalten, teilt die Fläche vertikal anhand der ausgewählten Fenster auf. Die Spaltenbrei-

## Shell-Erweiterungen installieren

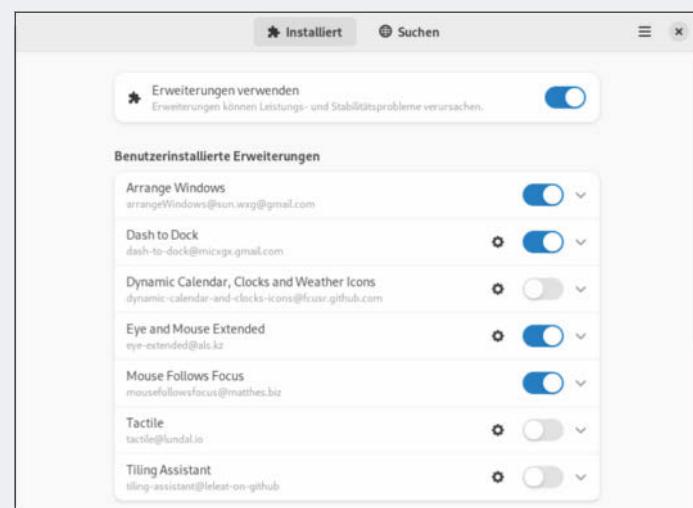
Am einfachsten installieren Sie Gnome-Shell-Erweiterungen mit dem „Erweiterungs-Manager“ (Extension Manager), den Sie via FlatHub beziehen. Diese App sucht im Extension-Repository des Gnome-Projektes nach Erweiterungen und bietet an, diese zu installieren und zu verwalten. Einziges Manko: Nachdem Sie eine Erweiterung installiert haben, müssen Sie von der Suche wieder zum Tab „Installiert“ wechseln, um sie zu verwalten.

Alternativ installieren Sie Erweiterungen mit dem Webbrowser über die Webseite [extensions.gnome.org](https://extensions.gnome.org). Rüsten Sie dazu zunächst über die Paketverwaltung Ihrer Distribution das Paket `chrome-gnome-shell` oder `gnome-browser-connector` sowie im Browser die Erweiterung „GNOME Shell-Integration“ nach[2], was die Webseite von sich aus anbietet.

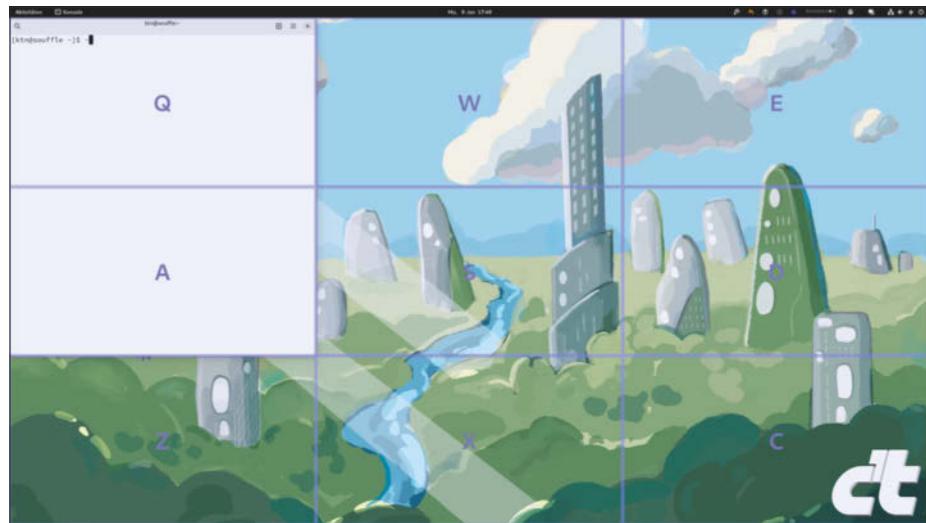
Die Einstellungen der Erweiterungen öffnen Sie, soweit vorhanden, in der App

Erweiterungs-Manager über den Tab „Installiert“ oder im Browser auf der Webseite für Gnome-Erweiterungen im Abschnitt „Installed Extensions“, indem Sie

jeweils in der Liste auf das Zahnrad- oder Werkzeug-Icon neben dem Namen der Erweiterung klicken. Es öffnet sich ein separates Fenster mit den Optionen.



**Der unabhängig von Gnome entwickelte Erweiterungs-Manager vereinfacht die Suche, Installation und Verwaltung von Gnome Shell Extensions.**



Die Erweiterung „Tactile“ blendet ein Raster ein, um darin Fenster zu platzieren. Dazu reicht es für die gewünschten Kacheln die angezeigten Buchstaben zu drücken.

te entspricht der Bildschirmbreite geteilt durch die Anzahl der ausgewählten Fenster. Während N-Columns dynamisch agiert, verhält sich das Layout „2:1 [V]“ statisch: eine zweidrittel große Kachel links und eine weitere Kachel rechts im dritten Drittel bieten Platz für insgesamt zwei Fenster. Der Zusatz „[V]“ ist ein Hinweis auf die vertikale Aufteilung.

Die Layouts wechseln Sie über ein Panel-Menü, das Sie in den Layout-Einstellungen aktivieren. Alternativ oder zusätzlich können Sie einem Layout eine eigene Tastenkombination zuweisen. Jedes Mal, wenn Sie ein Layout aktivieren, öffnet Tiling Assistant das Kachel-Pop-up, mit dem Sie die geöffneten Programmfenster im Layout anordnen. Sie können ein Layout durch Anklicken des Sternchens im Panel-Menü als Favorit festlegen. Halten Sie anschließend die Alt-Taste gedrückt, wenn Sie ein Fenster verschieben, dann bietet Tiling Assistant an, das Fenster anhand des favorisierten Layouts einzurasten. Halten Sie zusätzlich zu Alt noch die Super-Taste gedrückt, um das Fenster über mehrere Kacheln aufzuziehen.

### Raster-Layouts selbst gemacht

Ein eigenes Layout zu erzeugen ist machbar, aber mangels komfortablem Interface etwas umständlich. Es hilft, wenn Sie ein fertiges Layout als Vorlage verwenden. Klicken Sie zunächst in den Layout-Einstellungen unter der Liste der verfügbaren Layouts auf das Plus-Symbol, um ein neues Layout anzulegen. Vergeben Sie dann einen Namen, der idealerweise dem Layoutkonzept entspricht („6 Sechstel“ statt „Mein Layout“). So müssen Sie später

nicht grübeln, welches das gesuchte Layout ist.

Die erste Kachel definieren Sie mit dem Textfeld „Rect 0“ unterhalb des Namens, wobei Sie Größe und Position als Zeichenkette eintragen. Die Syntax setzt sich aus der Position auf der X- und Y-Achse sowie der Breite und Höhe der Kachel zusammen, jeweils getrennt durch zwei Bindestriche: x--y--Breite--Höhe, wobei Breite die Kachel nach rechts zeichnet und Höhe nach unten. So definiert 0--0.5--0.33--0.5 eine Kachel in der unteren linken Ecke, die ein Drittel der Bildschirmbreite breit und die Hälfte der Bildschirmhöhe hoch ist. Die Werte sind Dezimalbrüche, also 0.5 für die Hälfte, 1.0 für die ganze Breite beziehungsweise Höhe, relativ zur Monitorgröße. Der Koordinatenursprung (x=0, y=0) befindet sich in der oberen linken Bildschirmecke. Mit der großen Plus-Schaltfläche unter dem Textfeld fügen Sie zusätzliche Textfelder hinzu, mit dem Sie die weiteren Kacheln definieren.

Für ein Layout mit sechs Sechsteln sehen die Angaben dann so aus:

```
Rect 0: 0--0--0.33--0.5
Rect 1: 0--0.5--0.33--0.5
Rect 2: 0.33--0--0.33--0.5
Rect 3: 0.33--0.5--0.33--0.5
Rect 4: 0.66--0--0.33--0.5
Rect 5: 0.66--0.5--0.33--0.5
```

Die Kacheln dürfen sich nicht überlappen. Sie können, müssen aber nicht die ganze Fläche dem Layout zuteilen. Eine Grafik visualisiert die Aufteilung der Fläche und warnt bei Syntaxfehlern oder überlappen-

den Kacheln. Speichern Sie die Layoutdefinitionen über den Speichern-Knopf unterhalb der Liste.

Damit eine Fläche wie bei N-Columns dynamisch auf die ausgewählten Fenster verteilt wird, ergänzen Sie am Ende --v für eine vertikale oder --h für eine horizontale Aufteilung. So definiert 0.5--0--0.5--1--h eine Kachel in der rechten Hälfte, worin alle zugewiesenen Fenster übereinander gestapelt werden, also die Fläche unter ihnen horizontal aufgeteilt ist.

Rechts neben den Textfeldern gibt es je Zeile eine weitere Schaltfläche mit einem Plussymbol. Hier können Sie der Kachel eine Anwendung zuweisen, die Tiling Assistant startet, sobald Sie das Layout aktivieren. Möchten Sie das Layout über eine Tastenkombination aktivieren, weisen Sie diese über die Schaltfläche („Disabled“) neben dem Layoutnamen zu.

Im GitHub-Repository von Tiling Assistant finden Sie eine umfangreiche englischsprachige Dokumentation zu dynamischen Tastenkürzeln, verschiedenen Tiling-Modi und Layouts. Sie erreichen diese über die Info-Schaltfläche im Einstellungsfenster. Wählen Sie im Menü das Benutzerhandbuch aus.

Neben Tiling Assistant gibt es unter den Gnome-Erweiterungen weitere Extensions, die die Anordnung der Fenster erleichtern – beispielsweise gTile, gSnap oder Material Shell. Falls Ihnen das Prinzip gefällt, aber Tiling Assistant nicht zusagt, probieren Sie eine der genannten anderen Erweiterungen aus. Aktivieren Sie besser nicht mehrere Tiling-Erweiterungen gleichzeitig, um Wechselwirkungen zwischen ihnen zu vermeiden.

### Raster mit Tactile

Wenn Sie nur die Fenster per Tastenkombination an einem simplen Raster ausrichten wollen, ist die Erweiterung „Tactile“ eine bescheidene Alternative. Mit Super+T öffnen Sie ein Raster ein, beispielsweise 4×2 Felder, die jeweils mit einem Buchstaben beschriftet sind. Um das fokussierte Fenster auf dem Raster zu positionieren, drücken Sie zwei der angezeigten Buchstaben. Daraufhin zieht Tactile das Fenster zwischen beiden Feldern auf. Da die angezeigten Buchstaben passend zur Tastaturbelegung verteilt sind – zum Beispiel Q, W, E, R und A, S, D, F – klappt das flott und intuitiv. Die Tastenfolge Super+T, Q, A zieht das Fenster von der oberen linken Ecke bis zur unteren linken Ecke auf, wobei es nur ein Viertel der Bildschirmbreite ein-

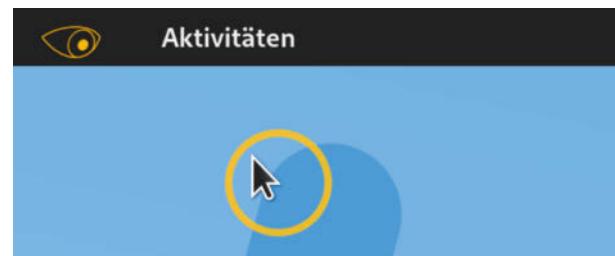
nimmt. Wollen Sie das Fenster auf nur ein Feld verkleinern, drücken sie zweimal den gleichen Buchstaben (Super+T, Q, Q).

In Tactile stehen für das Raster bis zu vier Layouts zur Verfügung. Drücken Sie nach Super-T eine Ziffer zwischen 1 und 4, wechselt das Raster zur jeweiligen Vorlage. Die Layouts können Sie in den Einstellungen der Erweiterung ändern. Sie lassen sich viel einfacher anpassen als bei Tiling Assistant, dafür sind sie weniger flexibel. Tactile arbeitet mit vier Spalten und drei Zeilen. Deren Größenverhältnis bestimmen Sie, indem Sie diesen jeweils eine Ganzzahl größer oder gleich Null zuweisen. Mit dem Wert gewichten Sie die Breite der Spalte beziehungsweise die Höhe der Zeile. Eine Spalte mit dem Wert 2 ist doppelt so breit wie eine mit dem Wert 1. Bei 0 blendet Tactile die Zeile oder Spalte aus. Die konkrete Spaltenbreite oder Zeilenhöhe ergibt sich aus der Gesamtfläche geteilt durch die Summe der vergebenen Gewichte und multipliziert mit dem Wert für die Spalte oder Zeile.

### Fenster automatisch arrangieren

Wenn Ihnen gar nicht danach ist, die Fenster händisch zu verteilen, assistiert Ihnen die Erweiterung „Arrange Windows“. Sie platziert alle geöffneten Fenster einer Arbeitsfläche nach einem vorgegebenen Muster, etwa alle nebeneinander als Spalten. Nach der Installation von Arrange Win-

Wie Saurons Auge verfolgt die Erweiterung „Eye and Mouse Extended“ den Mauszeiger auf Schritt und Tritt und hebt diesen auf Wunsch auch farblich hervor.



dows finden Sie rechts oben im Panel ein neues Icon, das einem Kartenstapel ähnelt. Ein Klick darauf öffnet ein Menü. Darüber bestimmen Sie, wie Arrange Windows die geöffneten Programmfenster, nun ja, arrangiert. Zur Auswahl stehen: Cascade (Fenster übereinander mit leichtem Versatz), Tile (Raster), Side by Side (als Spalten nebeneinander), Stack (als Zeilen übereinander), sowie Maximieren, wahlweise auch nur in der Höhe (Maximize Vertical) oder Breite (Maximize Horizontal).

Die Aktion wendet Arrange Windows immer auf alle Fenster der sichtbaren Arbeitsfläche simultan an. „Restoring“ soll die ursprünglichen Positionen und Ausmaße der Fenster wiederherstellen, allerdings unzuverlässig. Für die ersten vier Aktionen – Cascade, Tile, Side by Side und Stack – gibt es auch Tastenkombinationen (Strg+Alt+1...4).

### Maus-Cursor aufstöbern

Übergroße Monitore werfen nicht nur die Frage auf, wie man die Fenster am besten organisiert. Suchen Sie manchmal auf den unendlichen Weiten des Bildschirms nach dem Mauszeiger? Dann hilft eine Option aus den Gnome-Einstellungen. Aktivieren Sie im Abschnitt Barrierefreiheit unter „Zeigen und Klicken“ die Einstellung „Mauszeiger finden“. Wenn Sie die Strg-Taste drücken, hebt eine kreisförmige Animation die Position des Mauszeigers hervor. Unter Barrierefreiheit können Sie auch die Größe des Mauszeigers ändern.

Die Erweiterung „Eye and Mouse Extended“ löst die Sichtbarkeit des Mauszeigers auf eine Weise, die langjährigen Linux-Usern vertraut vorkommen dürfte: Es platziert im Panel ein Auge, das ununterbrochen auf den Mauscursor blickt. Wollen Sie wissen, wo der Mauscursor steckt, müssen Sie nur dem Blick des Panel-Augen folgen. Klicken Sie auf das Auge, zeichnet die Erweiterung dauerhaft einen farbigen Kreis um den Mauszeiger und steigert so dessen Sichtbarkeit. Die Position des Auges im Panel und die Farbe sowie das

Erscheinungsbild der Mauszeigermarkierung ändern Sie in den Einstellungen.

Falls Sie oft per Tastenkürzel zwischen Programmen wechseln und Ihnen die langen Mauswege zum ausgewählten Fenster lästig sind, verkürzt die Erweiterung „Mouse Follows Focus“ die Strecke. Die Extension „beamt“ den Mauszeiger stets in die Mitte des Fensters, das den Fokus hat. Die Funktion ist gewöhnungsbedürftig, da der Mauszeiger auch unerwartet wegspringen kann, wenn sich plötzlich irgendwo ein neues Fenster öffnet. Probieren Sie aus, ob die Erweiterungen Ihnen Arbeit abnimmt oder zusätzlichen Kummer bereitet.

### Weniger ist mehr

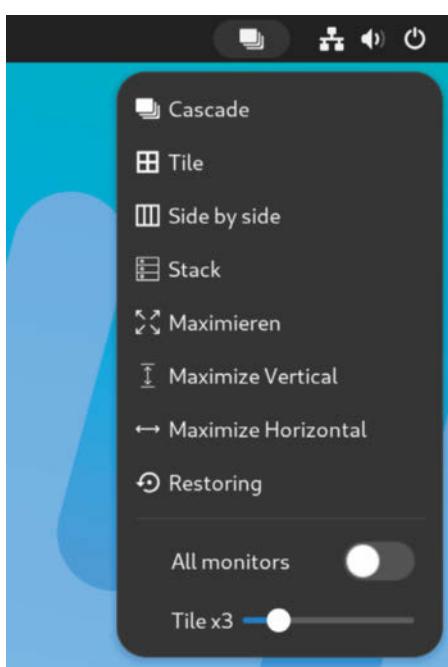
Die Suche mit Begriffen wie „Snap“ oder „Tiling“ im Erweiterungskatalog bringt weitere praktische Extensions hervor. Die leistungsfähigste Erweiterung auf großen Bildschirmen bleibt wohl der Tiling Assistant, wobei es die praktische Layout-Funktion vor unbedarften Nutzern verbirgt. Aber auch Tactile und Arrange Windows helfen, Fenster schnell auf der Bildschirmfläche zu platzieren.

Achten Sie bei Erweiterungen auf die Kommentare und Bewertungen im Katalog und prüfen Sie auf der jeweiligen Projekt-Homepage (meist ein GitHub-Repository), ob die Erweiterung gepflegt wird. Auch wenn Sie auf dem großen Bildschirm nicht so asketisch agieren wollen, wie es das Gnome-Projekt vorgibt, sollten Sie es mit den Zusatzfunktionen nicht übertreiben. Am effizientesten bleibt am Ende ein stabiler Desktop. (ktn@ct.de) ct

### Literatur

- [1] Anna Simon, Dynamisches Raster, Awesome: effizienter Unix-Desktop nach Maß, c't 15/2020, S. 152
- [2] Keywan Tonekaboni, Desktop-Modding, Gnome- und Ubuntu-Desktop durch Erweiterungen individuell anpassen, c't 4/2020, S. 152

**Links zu Erweiterungen und Extensionen**  
Webseite: [ct.de/ys28](http://ct.de/ys28)



Wenn Sie viele Fenster blitzschnell umsortieren möchten, leistet die Erweiterung „Arrange Windows“ gute Dienste.

# Für Wissenshungrige...

## Ausgewählte Fachliteratur



Wolfram Gieseke

### Windows 11 – Das Praxisbuch

Der ideale Begleiter für den PC-Alltag mit Windows 11. Mit Schritt-für-Schritt-Lösungen, direkt umsetzbaren Praxisrezepten sowie zahlreichen Tipps und Tricks führt es Sie durch alle wichtigen Themen und erleichtert Ihnen so die Arbeit mit Windows.

19,95 €



Brian Svidergol, Bob Clements, Charles Pluta

### Microsoft 365 Mobilität und Sicherheit

Bereiten Sie sich auf die Microsoft-Prüfung MS-101 vor und zeigen Sie, dass Sie die erforderlichen Fähigkeiten und Kenntnisse für die Verwaltung von Mobilität und Sicherheit in Microsoft 365 sowie die damit verbundenen Verwaltungsaufgaben in der Praxis beherrschen. Dieses Prüfungstraining wurde für erfahrene IT-Profis entwickelt.

49,90 €



Eric Amberg, Daniel Schmid

### Hacking – Der umfassende Praxis-Guide (2. Auflage)

Dies ist ein Leitfaden für angehende Hacker, Penetration Tester, IT-Systembeauftragte, Sicherheitsspezialisten und interessierte Poweruser. Mithilfe vieler Workshops sowie Tipps und Tricks lernen Sie die Vorgehensweise eines professionellen Hacking-Angriffs kennen.

49,99 €



Michael Weigend

### Python 3 für Studium und Ausbildung

Alle wichtigen Grundlagen der Python-Programmierung werden erklärt. Es sind keine Vorkenntnisse notwendig und die Themen werden fachunabhängig erläutert.

19,99 €



Christian Immler

### Haus und Wohnung smart vernetzt

Ob Sie Daten, Musik und Medien im ganzen Haus nutzen, Ihr WLAN optimieren oder per App aus der Ferne Ihre Heizung anstellen, diese und weitere relevante Themen rund um Ihr vernetztes Zuhause werden in diesem Buch ausführlich besprochen.

19,95 €

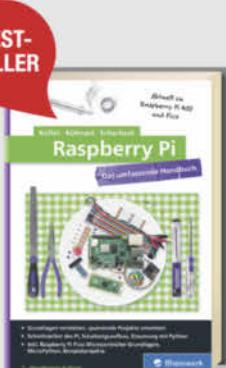


Thomas Kaffka

### 3D-Druck – Praxisbuch für Einsteiger (3. Auflage)

Entdecken Sie die nahezu unbegrenzten Möglichkeiten des 3D-Drucks in allen Varianten: vom Einsatz des eigenen 3D-Druckers zu Hause über die Verwendung von öffentlich zugänglichen Druckern bis hin zur Nutzung von 3D-Druckservices.

29,99 €



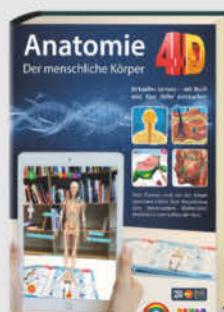
BEST-SELLER

Michael Kofler, Charly Kühnast, Christoph Scherbeck

### Raspberry Pi (7. Auflage)

Das Standardwerk in 7. Auflage, aktuell zum Raspberry Pi Pico. Die RasPi-Experten Michael Kofler, Charly Kühnast und Christoph Scherbeck bieten Ihnen auf über 1.000 Seiten das komplette Wissen, damit Sie mit dem Raspberry Pi richtig durchstarten.

44,90 €



Anatomie 4D –

### Der menschliche Körper

Mithilfe einer kostenlosen App und bahnbrechender Augmented Reality kann der Aufbau der Knochen, die Muskeln in Aktion, das Nerven- und Kreislaufsystem sowie das größte menschliche Organ, die Haut, beobachtet werden.

14,95 €



[shop.heise.de/highlights2022](https://shop.heise.de/highlights2022)

PORTOFREI AB 20 € BESTELLWERT INNERHALB DEUTSCHLANDS



## Zubehör und Gadgets



### ParkLite

ParkLite denkt mit. Die elektronische Park-scheibe stellt automatisch nach ca. 20 Sekunden die Parkzeit ein. Damit ist Schluss mit Bußgeldern! Hitze- und kältebeständig, inklusive Reinigungstuch und Klebefpads.

29,90 €



### Aluminium-Case FLIRC

Das hochwertige Gehäuse aus stabilem Aluminium ist ideal, um den Raspberry Pi 4 als Media Center zu verwenden. Das elegante Design integriert sich optimal in jede Wohnumgebung. **Auch im Set mit Raspi 4 Model B 2GB erhältlich.**

23,90 €

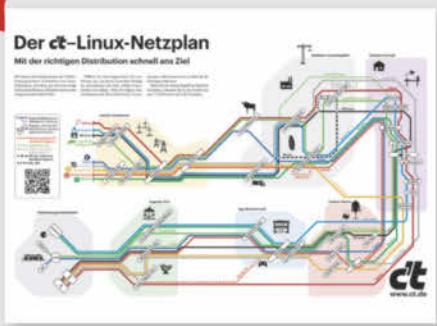


### musegear® finder Version 2

Finden Sie Schlüssel, Handtasche oder Geldbeutel bequem wieder statt ziellos zu suchen. Mit dem Finder können Sie z.B. das Smartphone klingeln lassen oder Wertgegenstände einfach tracken und noch mehr.

24,90 €

NEU



### c't-Linux-Netzplan

Entdecken Sie Linux auf eine ganz neue Art – als Netzfahrplan im A2-Format. Die verschiedenen Linux-Distributionen fahren wie U-Bahn-Linien durch die Landschaft und halten an Stationen, die für unterschiedliche Eigenschaften und Features stehen. Verfolgen Sie die Fahrt Ihrer Lieblings-Distribution durch das Hardware-Gewerbegebiet über das Fashion-Viertel bis zum Upgrade-Park.

9,90 €



### PoKitMeter – Multimeter, Oszilloskop und Logger

PoKit misst, zeigt und protokolliert eine Vielzahl von Parametern wie Spannung, Strom, Widerstand und Temperatur mittels Verbindung via Bluetooth mit Ihrem Smartphone oder Tablet.

109,90 €



BEST-SELLER

### Tasse „Kein Backup? Kein Mitleid!“

Wer kennt es nicht? Die lieben Kollegen haben wieder mal die Datensicherung vergessen und betteln bei Ihnen in der IT-Abteilung um Hilfe. Sie denken sich dabei nur: „Kein Backup? Kein Mitleid!“ Platzieren Sie die schicke Keramiktasse, außen matt-schwarz und innen rot, einfach demonstrativ auf Ihrem Schreibtisch. Der praktische Holzdeckel kann gleichzeitig als Untersetzer verwendet werden und verhindert somit nervige Kaffeeflecken auf dem Schreibtisch.

17,90 €



### Joy-IT OR750i: Freifunk- & OpenWrt-Dual-Band-Router

Der Einstieg in die Freifunk- und OpenWrt-Welt kann oft schwierig sein. Deshalb hat Joy-IT in Zusammenarbeit mit Freifunk Hannover und c't den OR750i entwickelt.

Dank Webinterface kann man beliebige Firmwares einfach hochladen – ohne komplizierte Kommandos oder inkompatible Hardware-Revisionen; ideal für OpenWrt-Einsteiger und solche, die Freifunk einfach nur nutzen wollen.

39,90 €



### REINER SCT Authenticator

Der REINER SCT Authenticator speichert die elektronischen Schlüssel für die Logins sicher in seiner Hardware und generiert die TOTP-Einmalpasswörter hochgenau alle 30 Sekunden. Er arbeitet **ohne Internetverbindung** und kann deshalb online nicht angegriffen werden. Zusätzlich kann seine Funktion noch mit einem **PIN-Schutz** abgesichert werden.

44,90 €



### „No Signal“ Smartphone-Hülle

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

39,90 €

# Datensparsam ausweisen

## Was Sie beachten sollten, bevor Sie eine Perso-Kopie weitergeben

**Oft soll man im Onlinealltag eine Ausweiskopie zur Identifizierung senden. Der Personalausweis enthält aber persönliche Informationen und kann Identitätsdieben als Vorlage dienen. Wann muss man das Dokument vorzeigen oder kopieren, und wann kann man dies guten Gewissens verweigern?**

Von Joerg Heidrich

Sie kennen es vielleicht vom Hotelresen: Bisweilen genügt es nicht, die Nummer des Personalausweises auf dem Check-in-Bogen einzutragen. Manche Hotels wollen unbedingt eine Kopie anfertigen, die dann auf unbestimmte Zeit zusammen mit der Anmeldung im Aktenordner verschwindet – datenschutzrechtlich eine mehr als zweifelhafte Praxis.

Dennoch hat sich diese aus der Offlinewelt bekannte Absicherung der Identität längst auch online etabliert – ein Ausweis lässt sich im Flachbettscanner schnell digital kopieren und via E-Mail versenden. Zudem gelten alternative Verfahren als aufwendiger, wenig verbreitet (E-Perso) oder nicht ausreichend sicher (Videoident). Und gerade im Onlinebusiness wollen Anbieter ihre Zugangsschwellen so niedrig wie möglich halten. Doch auf dem Personalausweis finden sich einige Informationen, mit denen man nicht allzu freizügig umgehen möchte und sollte. Deshalb geben wir Ihnen im Folgenden einen Überblick, wo und wie Sie off- und online Ausweiskopien weitergeben können und mitunter sogar müssen.

Der Gesetzgeber hat viele Fragen im „Gesetz über Personalausweise und den elektronischen Identitätsnachweis“ (kurz: „Personalausweisgesetz“ oder PAuswG) beantwortet. Demnach muss jeder deutsche Staatsangehörige ab dem Alter von 16 Jahren einen Personalausweis besitzen. Die Ausweise bleiben allerdings Eigentum der Bundesrepublik. Grundsätzlich gilt: Niemand darf vom Ausweisinhaber verlangen, das Dokument zu hinterlegen oder in sonstiger Weise „den Gewahrsam aufzugeben“. Folglich verbietet das PAuswG beispielsweise, den Ausweis als Pfand für eine Leih oder Miete einzuziehen.

Bis 2010 war es verboten, Ausweiskopien anzufertigen. Seitdem gestattet das PAuswG grundsätzlich diese Praxis – allerdings nur, wenn der Inhaber selbst die Kopie anfertigt oder dem zumindest explizit zustimmt. Empfänger der Kopie dürfen diese keinesfalls an Dritte außerhalb der eigenen Organisation weitergeben.

Die Kopie muss laut Gesetz „eindeutig und dauerhaft als Kopie erkennbar“ sein. Mit allzu realitätsnahen Ablichtungen bewegt man sich sogar schnell im strafrechtlich relevanten Bereich. Gleich vier Vorschriften im Strafgesetzbuch (StGB) stellen



Im aktuellen Layout der Perso-Vorderseite (2021) sollen Sie umfangreich schwärzen, bevor Sie eine Kopie versenden.

das Verändern, Fälschen, Verschaffen oder Missbrauchen von Ausweispapieren unterteils rigide Strafen. So steht auf das Verschaffen von amtlichen Ausweisen nach Paragraph 276 StGB eine Freiheitsstrafe bis zu zwei Jahren oder eine Geldstrafe.

### Perso und Datenschutz

Mit Namen, Geburtsdatum und Wohnort sowie biometrischen Informationen wie Augenfarbe und Körpergröße enthält der Personalausweis zahlreiche personenbezogene Daten, die in den Anwendungsbereich des Datenschutzrechts fallen. Sie lassen die Identifikation des Ausweisinhabers zu. Auch die Seriennummer und das Lichtbild gehören in diese Kategorie. Logisch also, dass die strengen Vorschriften der Datenschutz-Grundverordnung (DSGVO) einen allzu freigiebigen Umgang mit dem Dokument einschränken.

Ohnehin ist es nur sehr selten nötig, mit der Kopie alle Angaben auf einem Personalausweis zu erfassen und weiterzugeben. Sie sollten deshalb in jedem Einzelfall prüfen, welche Daten für das Gegenüber tatsächlich erforderlich sind, um Sie für den konkreten Anlass zu identifizieren. Muss etwa wirklich der Geburtsort, die Augenfarbe und Größe oder die Seriennummer des Ausweises vorhanden sein? Falls nicht, sollten Sie die Angaben auf der Kopie schwärzen – und zwar irreversibel.

Nutzen Sie dazu nicht etwa einen PDF-Editor, sondern drucken Sie die Kopie aus, schwärzen Sie die Zeilen mit einem schwarzen Filzstift und scannen Sie das Ergebnis nochmals. Gerade wenn Sie die Kopie an Ihrer Arbeitsstätte fertigen, sollten Sie im Hinterkopf behalten, dass moderne Bürosanner und Kopierer die Ablichtung oft dauerhaft auf ihrer internen Festplatte speichern.

Im europäischen Datenschutz gilt, dass personenbezogene Daten nur dann verarbeitet werden dürfen, wenn dafür eine Rechtsgrundlage existiert. Den Umgang mit Informationen in Personalausweisen regelt nicht nur das PAuswG, sondern es greifen auch viele andere Gesetze, die für besondere Situationen Regeln definieren. Im Folgenden finden Sie die häufigsten Anwendungsfälle.

### Kredit- und Finanzwirtschaft

Im Finanzbereich sieht das Geldwäschegesetz (GwG) umfangreiche Pflichten zur Identitätsprüfung der Kundschaft vor. Die gilt insbesondere, wenn man eine Geschäftsbeziehung begründet. Neben Fi-

Bild: Bundesregierung

nanzdienstleistern müssen unter anderem auch Versicherungsunternehmen, Steuerberater und Immobilienmakler ihre Klienten hinreichend identifizieren.

Dafür holen sie eine Reihe von Informationen ein. Bei natürlichen Personen sind das Name, Geburtsort, Geburtsdatum, Staatsangehörigkeit sowie eine postalische Anschrift. § 11 GwG legt fest, dass die Überprüfung „anhand eines gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird“, erfolgen muss. Den strengen Anforderungen des GwG genügt außer persönlichem Erscheinen auch das Postident-Verfahren oder die Ausweis-App. Eine Ausweiskopie zu übermitteln reicht nicht und ist deshalb unnötig.

## Telekommunikationsanbieter

Anbieter von Telekommunikationsleistungen, etwa Zugangsanbieter, verlangen bei Vertragsschluss von Neukunden oft, dass sie einen amtlichen Ausweis vorlegen. Das ist legitim und ergibt sich aus § 7 des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG). Fragt der Anbieter online nach einer Kopie, sollten Sie Teile daraus schwärzen, denn laut Gesetz sind für den Vertragsschluss nur Vorname, Nachname, Anschrift und Geburtsdatum nötig.

Etwas weiter gehen die Pflichten, wenn Sie einen Prepaid-Mobilfunkvertrag abschließen. Anbieter trifft die Registrierpflicht; sie müssen die von ihnen erhobenen Daten vor der Freischaltung überprüfen und dauerhaft speichern. Dieser Pflicht können sie nach § 172 des Telekommunikationsgesetzes (TKG) unter anderem nachkommen, indem der Kunde persönlich einen Personalausweis vorlegt oder mittels Postident. Eine elektronisch übermittelte, teilgeschwärzte Ausweiskopie genügt den Anforderungen nicht.

## Check-in im Hotel

Das Bundesmeldegesetz (BMG) sieht vor, dass Hotels und „vergleichbare Beherbergungsstätten“ persönliche Angaben zu den Gästen in einem Meldeschein dokumentieren müssen. Daraus ergibt sich aber weder eine Rechtsgrundlage noch gar eine Pflicht dazu, dass Kunden ihnen den Personalausweis oder ein anderes Bilddokument vorlegen müssen.

Hotels müssen keineswegs kontrollieren, ob die Angaben der Gäste korrekt sind. Bei Gästen aus dem Ausland gelten andere Regeln. Hier muss das Hotel gemäß BMG die Angaben anhand eines vorgelegten Iden-

titätsdokuments prüfen. Allerdings darf es auch in diesem Fall keine Kopie anfertigen.

## Jugendschutz

Auch das Jugendschutzgesetz (JuSchG) enthält Pflichten zur Überprüfung von Daten. Nach § 2 JuSchG muss ein Verkäufer oder ein Veranstalter im Zweifelsfall das Alter einer Person prüfen. Diese Pflicht besteht für ihn dann, wenn er nachvollziehbare Zweifel am Alter der Person hegt. Solche Zweifel existieren naturgemäß immer, wenn sich die Vertragsparteien nicht persönlich begegnen, etwa an Zigarettenautomaten. In derartigen Fällen kann die elektronische Altersvalidierung mittels Personalausweis helfen.

Bei Onlinegeschäften genügt es keinesfalls, dass der Händler eine Ausweiskopie via Mail oder Upload anfordert – diese Methode gilt nicht als hinreichend fälschungssicher. Das hat der Bundesgerichtshof (BGH) bereits 2007 festgestellt (Az. IZR 18/04). Möchte ein Händler beispielsweise jugendgefährdende Schriften vertreiben, muss er anders validieren, dass seine Kunden erwachsen sind. Als rechtssicher gelten etwa Prüfungen mit Videoident-Verfahren, nicht aber die bloße Eingabe von Ausweisdaten oder eine Kopie des Dokuments.

## Vermietung von Wohnraum

Bei der dauerhaften Vermietung von Wohnraum besteht ein berechtigtes Interesse des Vermieters, die angegebene Identität des Mieters zu kontrollieren. Hierfür kann ein Blick auf einen Lichtbildausweis erforderlich und erlaubt sein. Allerdings: Der Vermieter darf die Ausweisdaten nicht erfassen, schon gar nicht darf er eine Kopie des Ausweises verlangen und dauerhaft aufbewahren.

## Selbstauskünfte

Nach Art. 15 DSGVO kann jede Person bei Unternehmen Auskünfte bezüglich der Daten einholen, die dieses über sie gespeichert hat. Um eine solche Auskunft erteilen zu können, muss das Unternehmen als „Verantwortlicher“ im DSGVO-Sinn allerdings sicherstellen, dass es die Daten tatsächlich an den Betroffenen herausgibt, nicht etwa an einen Stalker. Die DSGVO sieht daher vor, dass der Verantwortliche bei begründeten Zweifeln an der Identität des Anfragenden zusätzliche Informationen anfordern muss.

Ein begründeter Zweifel dürfte beispielsweise dann vorliegen, wenn die An-



Bild: Bundesgesetzblatt

Auch die Rückseite des Persos enthält jede Menge Daten, die zur Identifizierung nicht benötigt und vorm Versenden entfernt werden sollten.

frage lediglich via E-Mail eintrifft und neben dem Namen keine zusätzlichen Angaben wie eine Kundennummer enthält. Die niedersächsische Datenschutzbehörde etwa bestätigte für diesen Fall, dass das Unternehmen eine Kopie des Personalausweises erbeten kann. Hier sollten Sie nicht erforderliche persönliche Daten wie Augenfarbe, Größe, Seriennummer und Unterschrift schwärzen. Das Unternehmen muss die Kopien unmittelbar nach einmaliger Sichtung löschen.

## Mahnung des Ministeriums

Auf Anfrage von c't äußerte sich das für Ausweisangelegenheiten zuständige Bundesinnenministerium (BMI) übrigens sehr skeptisch, was den Onlineversand von Ausweiskopien angeht: „Die Authentifizierung von Personen im Rahmen von Onlinedienstleistungen auf Basis einer Ausweiskopie – ungeachtet von geschwärzten Angaben auf der Kopie – wird vom Bundesministerium des Innern und für Heimat nicht empfohlen“, teilte eine Sprecherin mit.

Wenn es denn aber einmal sein muss, empfiehlt auch das BMI, möglichst umfangreich zu schwärzen. Außerdem „sollte berücksichtigt werden, dass in diesen Fällen Kommunikationswege über das offene Internet vermieden werden sollten“. Sprich: Das BMI legt nahe, Ausweiskopien nur Ende-zu-Ende-verschlüsselt zu versenden.

Die Bürger sollen der Antwort des BMI zufolge außerdem berücksichtigen, dass das PAuswG im Ausland nicht gilt und deshalb Vorsicht walten lassen, wenn sie Kopien an ausländische Anbieter senden. „Zudem wird darauf hingewiesen, dass ein gleichwertiger Datenschutzstandard grundsätzlich nur zwischen den EU-Mitgliedsstaaten besteht“, mahnt das Ministerium. (hob@ct.de) **ct**

## Tipps & Tricks

# Sie fragen – wir antworten!

### Mac mit aktiviertem Inhaltscaching aufspüren

Ich befinde mich in einem großen Netzwerk mit vielen Macs. Ein Kollege hat offenbar das Inhaltscaching aktiviert. Das bewirkt, dass einige Macs ein Problem beim Installieren von Updates haben. Wie finde ich heraus, auf wessen Mac der Caching-Server aktiviert ist?

Es gibt unter macOS einen Terminal-Befehl, der alle Geräte im Netzwerk mit aktiviertem Inhaltscaching auflistet:

AssetCacheLocatorUtil

Geben Sie das im Terminal ein und drücken Sie die Return-Taste. Die Ausgabe ist etwas unübersichtlich: Suchen Sie mit Cmd+F nach Zeilen, die „guid“ enthalten. Dort steht weiter vorn die IP-Adresse des Macs im Netzwerk. Eventuell gibt es mehrere Macs mit aktiviertem Inhaltscaching. Dann ist folgende Befehlskette praktischer, weil sie ausschließlich die gefundenen IP-Adressen ausspuckt:

```
AssetCacheLocatorUtil 2>&1 | grep ↵
  guid | cut -w -f 4 | cut -d : -f 1 | ↵
  uniq
```

Falls Ihnen die IP-Adresse zur Identifikation des Geräts nicht ausreicht, können Sie mit folgendem Kommando den zugehörigen Freigabenamen ermitteln:

```
dig +short -x <IP> -p 5353 @<IP>
```

Ersetzen Sie dabei <IP> durch die ermittelte IP-Adresse (ohne den dahinter mit Doppelpunkt angegebenen Port), sodass die Befehlszeile etwa so aussieht:

```
dig +short -x 192.168.178.79 -p 5353 ↵
@192.168.178.79
```

Das Kommando `dig` fragt den mit dem @-Symbol gekennzeichneten DNS-Server, welcher Name für die mit -x angegebenen IP-Adresse dort hinterlegt ist. Weil hier ein Mac mit der Port-Nummer 5353 als DNS-Server angegeben ist, verrät dessen Bonjour-Dienst (Multicast DNS) den vergebenen lokalen Domainnamen. Idealerweise ist der so gewählt, dass er den jeweiligen Nutzer identifiziert.

(Wolfgang Kreutz/bkr@ct.de)

### Groß- und Kleinschreibung unter Windows

Wenn Sie in c't-Artikeln über Windows schreiben, stehen da Pfadangaben und Registryschlüssel meistens mit großen Anfangsbuchstaben („C:\Windows“) und manchmal sogar mit Binnenmajuskel („C:\User\ct\AppData“). Nun habe ich beim Abtippen eines solchen Pfades versehentlich „c:\windows“ geschrieben, doch es hat trotzdem funktioniert.

Anders als unter Linux spielt die Groß- und Kleinschreibung unter Windows bei Pfaden und Ähnlichem normalerweise keine Rolle. Sie können alles kleinschreiben.

ben, alles groß, irgendeinen Mischmasch daraus, wie Sie wollen. In unseren Artikeln handhaben wir das zwar anders, doch hat das keine technischen Gründe, sondern es dient nur der Lesbarkeit.

Das bedeutet auch, dass sich unterschiedliche Bezeichnungen in der Zeichenfolge unterscheiden müssen: Dateien und Ordner, deren Namen sich jeweils nur durch Groß- und Kleinschreibung unterscheiden, duldet Windows nicht im selben Verzeichnis. Sie können also keine Datei unter dem Namen `Manuscript.txt` speichern, wenn sich im selben Ordner bereits eine `manuscript.txt` befindet.

Es gibt eine Ausnahme von der Regel. Die hat mit Linux zu tun, genauer mit dem Windows-Subsystem für Linux (WSL). Damit können Sie Linux-Binärdateien direkt unter Windows ausführen, wobei unter der Haube eine Linux-Distribution hilft (es stehen mehrere zur Auswahl). WSL gibt es in zwei Versionen, und bei WSL 1 speicherte Windows die Linux-Distribution direkt auf C. Dabei landen auch Dateien auf der Platte, die sich nur durch Groß- und Kleinschreibung unterscheiden (beispielsweise „axv.txt“ und „Axv.txt“). Das kann zu Problemen mit Programmen führen, die darauf nicht vorbereitet sind, sowie mit Skripten, die solche Programme

```
zsh
2022-12-01 21:44:02.375 AssetCacheLocatorUtil[43918:1443210] Finding refreshed content caches supporting shared caching
...
2022-12-01 21:44:02.376 AssetCacheLocatorUtil[43918:1443210] Found 1 content cache
2022-12-01 21:44:02.377 AssetCacheLocatorUtil[43918:1443210] 192.168.178.79:60750, rank 1, not favored, healthy, guid 2
3FAE025-61CA-4ABF-B457-A50085BE77D7, valid until 2022-12-01 22:44:04; supports personal caching: yes, and import: yes, shared caching: yes
2022-12-01 21:44:02.377 AssetCacheLocatorUtil[43918:1443210] Determining refreshed configured public IP address ranges.
.
2022-12-01 21:44:02.377 AssetCacheLocatorUtil[43918:1443210] No public IP address ranges are configured.
2022-12-01 21:44:02.377 AssetCacheLocatorUtil[43918:1443210] Determining refreshed favored server ranges...
2022-12-01 21:44:02.377 AssetCacheLocatorUtil[43918:1443210] No favored server ranges are configured.
2022-12-01 21:44:02.403 AssetCacheLocatorUtil[43918:1443210] Testing at found content caches for reachability...
2022-12-01 21:44:02.403 AssetCacheLocatorUtil[43918:1443210] This computer is able to reach all of the above content caches.
Wolfgang@MacBook-Pro-16: ~ % dig +short -x 192.168.178.79 -p 5353 @192.168.178.79
Wolfgang@MacBook-Pro-16: ~ %
```

Mit dem Terminal lässt sich herausfinden, bei welchen Macs in einem Netz das Inhaltscaching aktiviert ist.

nutzen. Das trifft auch Microsoft-eigene Software. Beispiel: Unser Sicherungsskript c't-WIMage nutzt unter der Haube das Windows-eigene Programm Dism.exe zum Erstellen der Backups, doch das kann mit derart unterschiedlichen Schreibweisen nicht umgehen. Daher scheitert das Sichern mit c't-WIMage, wenn eine WSL-1-Distribution installiert ist.

Immerhin hat Microsoft das Problem bei WSL 2 gelöst: Damit landen die Distributionen nicht mehr als einzelne Dateien und Ordner direkt auf der Platte, sondern auf einer virtuellen Festplatte, also in einer VHDX-Datei, die keine Probleme verursacht.

Das WSL-1-Problem macht übrigens auch deutlich, dass das Dateisystem NTFS entgegen anderslautenden Gerüchten sehr wohl mit Groß- und Kleinschreibung umgehen kann.

(axv@ct.de)

## Web Serial mit Chromium-Snap

Ich habe versucht, ein Smart-Home-Gerät (ein ESP8266 in einem Shelly1) mit der quelloffenen Firmware Tasmota zu bespielen. Dafür betreiben die Entwickler unter tasmota.github.io/install einen Installer, der direkt im Browser funktionieren soll. Ich musste nur einen USB-Serial-Adapter anschließen und ein Image auswählen. Das klang praktisch, funktionierte aber auf meinem Ubuntu mit Chromium nicht. Was läuft da schief?

Der Installer von Tasmota nutzt die recht neue Technik Web Serial, die noch nicht alle Browser unterstützen und die ausdrücklich experimentell ist. Aktuell funktioniert sie nur mit Browsern, in denen die Chromium-Engine steckt (Google Chrome, Chromium und Edge). Wenn Sie mit Chromium unter Ubuntu Probleme haben, liegt das vermutlich daran, dass Ubuntu den Browser automatisch per Snap installiert hat. Snaps laufen jedoch in einer Sandbox, die den experimentellen Zugriff auf USB-Geräte nicht automatisch erlaubt. Mit dem folgenden Befehl können Sie dem Chromium-Snap die Erlaubnis erteilen, direkt auf USB zuzugreifen. Führen Sie ihn einfach in einer Kommandozeile aus:

```
sudo snap connect chromium:raw-usb
```

(pmk@ct.de)

## Excel: Horizontal scrollen ohne Scrollbar

Ich arbeite mit recht breiten Tabellen in Excel für Windows und das Gefummel mit dem schmalen horizontalen Scrollbalken rechts unten nervt mich. Gibt es bessere Methoden?

Gibt es, sogar einige. Mit einem Notebook-Touchpad können Sie mit einer Zweifinger-Wischgeste horizontal scrollen, ebenso mit einer Maus, deren Scrollrad seitliche Schalter besitzt und das sich nach rechts und links kippen lässt. Auch mit dem Scrollrad selbst geht es: Halten Sie beim Scrollen einfach gleichzeitig die Strg- und Umschalttaste gedrückt. Die letzte Methode kommt ganz ohne Maus aus – sie dürfte auch die unbekannteste sein: Drücken Sie die ansonsten praktisch brachliegende Taste „Rollen“ (ScrollLock). Ist sie aktiv, was bei vielen Tastaturen durch eine Kontrollleuchte angezeigt wird, können Sie mit den Cursortasten scrollen ohne die gerade markierte Zelle zu verlassen. (swi@ct.de)

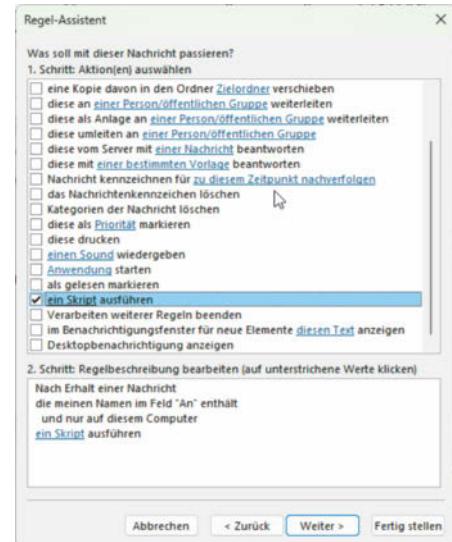
## Outlook: VBA-Script per Regel starten

Ich möchte per Outlook-Regel ein VBA-Skript starten. Ich bin mir sicher, dass ich eine entsprechende Option unter „Aktionen auswählen“ im Outlook-Regelassistenten schon mal gesehen habe, kann sie aber nicht mehr finden. Wo muss ich suchen?

Microsoft hat diese Option aus Sicherheitsgründen schon vor einiger Zeit aus dem Outlook-Regelassistenten entfernt. Sie lässt sich aber über die Windows-Registry reaktivieren. Öffnen Sie die zum Beispiel mit Windows+R und geben Sie regedit ein, navigieren Sie zu HKEY\_CURRENT\_USER\Software\Microsoft\Office\16.0\Outlook\Security und erzeugen Sie einen neuen DWORD-Schlüssel mit der Bezeichnung EnableUnsafeClientMailRules. Als Wert tragen Sie 1 ein. Das „16.0“ im Schlüsselpfad steht übrigens für alle Office-Versionen ab 2016. Für Outlook 2013 ersetzen Sie es durch „15.0“.

Nach einem Neustart von Outlook sollte die Option „ein Skript ausführen“ als mögliche Aktion im Regelassistenten wieder angeboten werden.

Es ist allerdings unklar, ob Microsoft diesen Workaround blockieren wird. Bei



Microsoft hat die Aktion „ein Skript ausführen“ schon vor einiger Zeit aus dem Outlook-Regelassistenten entfernt. Per Windows-Registry bringen Sie sie zurück.

unseren Tests mit der Outlook-/Office-Version 2210 Build 15726.20202 hat er sowohl unter Windows 10 als auch unter Windows 11 noch funktioniert. (swi@ct.de)

## Roborock-Staubsauger lädt nicht

Mein Roborock S50, ein Staubsaugerrbeiter der ersten Generation, funktionierte bis jetzt immer noch recht zuverlässig, obwohl er ja schon ein paar Jahre auf dem Buckel hat. Nun aber lädt er einfach nicht mehr. Wie es aussieht, ist eine Feder in der Ladestation gebrochen. Ersatzteile gibt es dafür nicht, eine neue Ladestation kostet rund 80 Euro. Das lohnt sich sicher nicht mehr, aber kann man das nicht vielleicht noch reparieren?

Fragen richten Sie bitte an

**ct** [hotline@ct.de](mailto:hotline@ct.de)

**f** [c't Magazin](#)

**t** [@ctmagazin](#)

Alle bisher in unserer Hotline veröffentlichten Tipps und Tricks finden Sie unter [www.ct.de/hotline](http://www.ct.de/hotline).



**Mit einem Stück Plastik, etwas Geschick und Sekundenkleber reparieren Sie die gebrochene Halterung der Ladekontakt-Federung eines Roborock-Staubsaugerroboters selbst.**

! Eine gebrochene Feder ist wahrscheinlich gar nicht schuld, wenn der Ladekontakt nicht mehr federt. Nach fünf Jahren ist das Plastik brüchig geworden. Wahrscheinlich ist nur die Befestigung der Feder ausgebrochen – das lässt sich reparieren.

Sie brauchen dazu ein scharfes Stechisen, Sekundenkleber und einen 1-Millimeter-Bohrer. Außerdem müssen Sie schauen, ob Sie irgendwo ein circa 6 Millimeter dickes Stück Plastik finden.

Auf der Unterseite der von der Steckdose abgestöpselten Ladestation finden Sie vier Schrauben, zwei davon sind unter den Gummifüßen versteckt. Kratzen Sie die gebrochene Befestigung der Feder weg und kleben Sie das Plastikstück an diese Stelle. Legen Sie nun die Ladefeder in ihre Position und kennzeichnen Sie das neue Schraubenloch. Dort bohren Sie ein kleines Loch hinein. Befestigen Sie die Feder darin und schrauben Sie die Ladestation wieder zu. Voilà, 80 Euro gespart. (ll@ct.de)

gegeben, die von 5,725 GHz bis 5,875 GHz reicht und – wie die meisten in der EU harmonisierten Frequenzzuteilungen – technologienutral ausgelegt ist. Der große Nachteil: Die Sendeleistung darf maximal 25 Milliwatt (das sind 14 dBm) an der Antenne (EIRP) betragen. Das ist in diesem Frequenzbereich nicht viel; die WLAN-Allgemeinzuteilung sieht 200 (23 dBm) beziehungsweise 1000 mW (30 dBm) vor.

Diese Leistung kann genügen, um dünnerne Wände ohne Metallbauteile zu durchdringen oder einen Garten auf Sicht mit flottem WLAN zu versorgen. Der Bereich hat dabei auch große Vorteile: Die Wetterradarerkennung, die von Kanal 50 bis 144 regelmäßig für nervige Abschaltungen sorgen kann, ist in der SRD-Allgemeinzuteilung (Short Range Device) nicht vorgeschrieben. Auch sonst gibt es abgesehen von der Sendeleistung keine Einschränkungen für den WLAN-Betrieb. Zudem nutzen viele WLAN-Router und Access Points die Kanäle nicht bei ihrer Autokanalsuche, sodass der Bereich auch in dicht besiedelter Nachbarschaft oft noch frei ist – ein Segen für alle, die aufgrund voller WLAN-Kanäle im Schnelltempo surfen.

Um den Frequenzbereich rechtssicher nutzen zu können, müssen Sie Ihrer WLAN-Basis das Betriebsland in den Einstellungen mitteilen. Meist heißt diese Einstellung einfach „Land“, gelegentlich aber auch „Regulatory Domain“. Das ist wichtig, da diese Kanäle auch in anderen Ländern mit mehr Sendeleistung genutzt werden dürfen. Anbieterrouter und auch viele freie Modelle erledigen diese Konfiguration oft automatisch. Konfigurieren Sie Ihren Router falsch, haften Sie auch dafür. Wenn das der Hersteller tut, ist er dafür verantwortlich, dass die Grenzwerte

eingehalten werden – außer Sie haben den Router aus dem Ausland in die EU importiert, dafür übernehmen Sie dafür die Verantwortung. (amo@ct.de)

**Allgemeinzuteilungen für WLAN und SRD-Anwendungen: [ct.de/y4zq](http://ct.de/y4zq)**

## ISO-Abbild von CD erstellen

! Ich möchte gern ein ISO-Abbild von einer alten CD erstellen. Die ist nicht mal kopiergeschützt, doch ich scheitere an etwas anderem: Ich finde keine passende Software. Haben Sie einen Tipp?

! Verwenden Sie die Freeware ImgBurn. Dieses Programm kann trotz des Namens keineswegs nur brennen. Obacht: Die Software hat selbstverschuldet einen schlechten Ruf erworben, weil ihr Installationsprogramm eine Zeit lang ungewollt Adware mitinstalliert hat. Sie brauchen das Setup-Programm aber nicht auszuführen. Laden Sie es von der Website <https://imgburn.com> herunter: Klicken Sie auf der Seite auf „Download“ und dann auf „Mirror 7 – Provided by ImgBurn“. Auf der Platte landet eine Datei namens „SetupImgBurn\_2.5.8.0.exe“ – Nicht starten!

Entpacken Sie stattdessen die heruntergeladene Datei mit 7-Zip (<https://7-zip.org>) in einen separaten Unterordner. Darin finden Sie die Datei ImgBurn.exe. Falls Sie dieser nicht trauen, laden Sie sie unter <https://virustotal.com> hoch, wo sie von über 70 Virensuchern geprüft wird. Es gab bei unseren Tests immer wieder einige wenige Scanner, die etwas an der Datei zu mäkeln hatten, doch sie fanden immer wieder andere angebliche Schädlinge darin. Das deutet auf Fehlalarme hin, zumal diese Datei (MD5-Prüfsumme: 4776c25e4ffda40783df8d31217ed085) bereits seit über fünf Jahren unverändert zum Download bereitsteht. Wäre wirklich etwas Gefährliches enthalten, würden die meisten anderen Virensuchern auch längst angeschlagen.

Starten Sie die Datei ImgBurn.exe (Administratorrechte sind nicht erforderlich) und klicken Sie auf „Create image file from disc“. Im nächsten Dialog wählen Sie oben unter „Source“ Ihr optisches Laufwerk aus. Unter „Destination“ tragen Sie Speicherort und Namen der ISO-Datei ein. Nun noch auf das Kopiersymbol unten klicken, dann brauchen Sie nur noch zu warten, bis die ISO-Datei erstellt ist. (axv@ct.de)

## Neue WLAN-Kanäle

! Mir ist aufgefallen, dass mir mein WLAN-Access-Point für das 5-GHz-Band auch die Kanäle von 149 bis 161 und von 165 bis 173 anbietet. Ich hatte vor einiger Zeit noch gelesen, dass diese Kanäle in Deutschland nicht genutzt werden dürfen. Hat sich daran etwas geändert?

! Ja, diese Kanäle sind tatsächlich für WLAN nutzbar. Dabei muss man jedoch einiges beachten: Der Bereich ist nicht Teil der Allgemeinzuteilung der WLAN-Frequenzen im 5-GHz-Band, die bis 5,725 GHz geht. Die Kanäle werden über die Allgemeinzuteilung für Funkanwendungen mit geringer Reichweite frei-



Julia Schneider, Kristina Laube,  
Nele Konopka

### SCHOKOROBOTER UND DEEPFAKES

Ein Comic-Essay über Künstliche Intelligenz aus der Perspektive von Jugendlichen

Tübingen AI Center (Hrsg.) / tradition, Tübingen 2022  
ISBN 978-3347726802  
78 Seiten, 15,70 €  
(PDF: kostenlos)

## Cool und klug

**In diesem Comic zur Künstlichen Intelligenz kommen junge Menschen zu Wort: Forscher vom Tübingen AI Center haben dafür Schüler zu ihren Wünschen, Hoffnungen und Ängsten rund um KI befragt.**

Dieser Comic entstand im Umfeld des jährlich ausgetragenen Bundeswettbewerbs für Künstliche Intelligenz, der Jugendliche und junge Erwachsene für KI begeistern will, aber auch den kritischen Umgang damit fördern soll. Organisiert wird der Wettbewerb vom „Tübingen AI Center“, einer Forschungseinrichtung der Universität Tübingen und des Max-Planck-Instituts für Intelligente Systeme. Forscher des Centers hatten Schüler von 11 bis 19 Jahren befragt, wie sie sich KI vorstellen und welche Assoziationen sie zum Thema haben.

Die originellen Zeichnungen der Grafikerin Nele Konopka füllen viele Seiten des Buchs. Sie wechseln sich ab mit farbigen Sprechblasen, die Zitate der befragten Schüler wiedergeben. Während die Comic-Teile des Buchs die Meinungen und Erfahrungen der Jugendlichen in den Vordergrund stellen, liefern knapp 30 Wissenseiten allgemeinverständliche Informationen. Sie beschreiben beispielsweise den Turing-Test und Asimovs Robotergesetze, Chatbots und autonome Drohnen, Filterblasen und Deepfakes. Andere Infotexte widmen sich der Rolle der KI beim Klimawandel oder der Frage, ob KI zum Multitasking fähig ist.

Zeichnungen und Texte ergänzen sich gut. Die bunten Comic-Elemente auf schwarzem Grund sowie die handgeschriebenen Zitate verleihen den Buchseiten Pep und Coolness. Sie machen neugierig und bieten viele Gesprächsanlässe. Die Wissenseiten beleuchten wichtige technische und gesellschaftspolitische Themen. Diese Kombination eignet sich für die Bildungsarbeit in Schule und außerschulischen Jugendeinrichtungen, aber auch zum privaten Schmökern. Jugendliche finden in der Lektüre leicht verständliche Informationen rund um die Wirkung von KI in unserem Alltag – Eltern und Lehrer lernen die unterschiedlichen Sichtweisen heutiger Jugendlicher auf das Thema kennen.

Die digitale Version von „Schokoroboter und Deepfakes“ bietet das Tübingen AI Center zum kostenlosen Download an ([ct.de/yjrt](http://ct.de/yjrt)). Ein gedrucktes Exemplar gibt es direkt beim Self-Publishing-Unternehmen tradition; auch der Buchhandel oder Amazon liefern eine Print-on-Demand-Ausgabe. (dwi@ct.de)

**Download oder Bestellung:** [ct.de/yjrt](http://ct.de/yjrt)

## In kleinen Schritten zum Ziel

**Abschlussberichte von Forschungsprojekten bieten selten viel Bezug zum Alltag. Dieser Projektbericht macht es besser: Konkrete Erfahrungen in zehn Projekt-Kitas machen Mut, sich mit Vorschülern auf den Weg zu zeitgemäßer Mediennutzung zu machen.**

Wenn es um PC und Tablet, Apps und Websites geht, dann herrscht in den meisten deutschen Kindergärten Zurückhaltung. Viele Eltern fürchten, dass ihre Kleinen vor der Mattscheibe von PC oder Mobilgerät alleingelassen werden könnten. Kitas, die gern mehr Medien in ihre pädagogische Arbeit einbeziehen möchten, kämpfen dann mit Widerstand der Elternschaft.

Das Forschungsprojekt „Medienerziehung im Dialog“ setzte daher von Anfang an auf intensiven Austausch zwischen Erziehern und Eltern. Die Stiftung Ravensburger Verlag hat das Projekt gefördert, durchgeführt wurde es von der Stiftung Digitale Chancen. Es startete 2018 mit einer intensiven Literaturrecherche rund um Medien in der Kita. Das knappe Grundlagenkapitel des Buchs fasst zusammen, was die Forscher dabei herausfanden, und bildet die theoretische Basis für die folgenden Kapitel.

In der Feldphase des Projekts erprobten zehn Einrichtungen zwei Jahre lang das kreative Potenzial von Medien im Vorschulbereich. Zahlreiche Zitate dokumentieren, wie unterschiedlich diese Phase in den Projekt-Kitas abließ. „Es spielt wirklich 'ne große Rolle, eine Leitung zu haben, die hinter einem steht. Ich kann jetzt nicht als Kollegin sagen, ihr macht jetzt alle hier mit – das funktioniert nicht“, sagt etwa eine frustrierte Erzieherin. Doch die meisten Zitate machen Mut. „Mit jedem kleinen Miniprojekt wurde es besser. Ich war am Anfang so nervös am Telefon mit den Eltern ...“, beschreibt eine andere Person erste Erfolge.

Wer nach praktischen Anregungen für die Medienarbeit mit Vorschülern sucht, etwa nach passenden Apps und Tipps für deren Nutzung, wird in diesem Projektbericht nicht fündig. Das Buch konzentriert sich allein auf die Schritte hin zur kindgerechten Mediennutzung. Dazu gehören Fortbildungen, die auch skeptische Mitarbeiter erreichen, sowie Elternabende, bei denen besorgte Väter und Mütter über ihre Bedenken sprechen dürfen. Ebenso wichtig ist es, sich mit anderen Einrichtungen auszutauschen und im stetigen Wechsel zwischen Praxis und Reflexion in kleinen Schritten voranzugehen. Dieses Buch ist dabei für Kitaleitung, Erzieher und Eltern gleichermaßen inspirierend. (dwi@ct.de)



Theresa Lienau, Matthias Röck

### Medienerziehung im Dialog

Nachhaltige digitale Bildung als gemeinsame Aufgabe von Kita und Familie – Gelingensbedingungen und Praxisempfehlungen

kopaed, München 2022  
ISBN 978-3968480749  
128 Seiten, 15 €  
(PDF-/Epub-/Kindle-E-Book: 11 €)

# FAQ

# BitLocker

**Die in Windows enthaltene Laufwerksverschlüsselung führt hin und wieder zu Verwirrung, Ärger und Beratungsbedarf. Hier beantworten wir die wichtigsten Fragen.**

**Von Jan Schüßler**

## BitLocker ohne Zutun aktiv

❓ Nach einem BIOS-Update konnte mein Rechner mit Windows 11 Home neulich nicht mehr booten, es kam nur die Aufforderung, den Wiederherstellungsschlüssel für die BitLocker-Verschlüsselung einzugeben. Ich habe aber keinen, denn ich habe BitLocker nie aktiviert. Was nun?

❗ Vermutlich haben Sie einen, wissen es nur nicht. Denn BitLocker steckt technisch auch in der Home-Edition von Windows, darf dort nur nicht so heißen. Statt dessen nennt Microsoft die Funktion dort „Geräteverschlüsselung“. Um sie zu nutzen, muss der Rechner ein paar Hardware-standards erfüllen. Wir erleben immer wieder Systeme, bei denen die Verschlüsselung fürs Systemlaufwerk nach einer sauberen Neuinstallation sofort aktiv ist.

Das ist einer der Gründe, warum Microsoft Ihnen bei der Ersteinrichtung so penetrant ein Microsoft-Konto aufs Auge drücken will: Sobald Sie sich mit einem solchen an Windows 10 oder 11 anmelden, landet der Wiederherstellungsschlüssel automatisch in Ihrem Konto – unter [account.microsoft.com/devices/recoverykey](https://account.microsoft.com/devices/recoverykey) können Sie ihn auslesen.

## Wiederherstellungsschlüssel ins Microsoft-Konto?

❓ Einen Wiederherstellungsschlüssel im Microsoft-Konto zu speichern erscheint mir unter Datenschutz- und Sicherheitsaspekten völlig grotesk. Wer tut sowas bei vollem Bewusstsein?

❗ Tatsächlich ist dieses Verfahren rational nachvollziehbar. Die Geräteverschlüsselung in Windows Home ist eine Funktion für die breite Masse, also für Menschen, die sich mit Verschlüsselung nicht auseinandersetzen wollen oder kön-

nen. Für die ist es allemal sinnvoller, eine Verschlüsselung zu haben, zu der Microsoft einen Hintereingang kennt, als komplett ohne Verschlüsselung herumzulauen. Bedenken Sie: Um mit einem Wiederherstellungsschlüssel überhaupt etwas anfangen zu können, muss ein Angreifer Ihren Rechner in seinem Besitz haben.

Ein Sicherheitsrisiko besteht in Extremfällen, und zwar dann, wenn jemand es ganz gezielt auf Ihre Daten abgesehen hat – und zu hohem Aufwand bereit ist, um sie zu erlangen. Der Angreifer müsste dafür erstens an den Schlüssel herankommen, was er entweder durch einen Einbruch in Ihr Microsoft-Konto schaffen kann (ein guter Grund für Zwei-Faktor-Authentifizierung), oder wenn es sich beim Angreifer um eine Ermittlungsbehörde handelt, die Microsoft zwingen kann, den Schlüssel herauszugeben. Und zweitens muss der Angreifer Ihren Rechner in die Finger bekommen, sprich: stehlen.

Sofern Sie ein so hochpreisiges Ziel sind, dass ein solcher Angriff realistisch ist, ist der Wiederherstellungsschlüssel im Microsoft-Konto tatsächlich ein Risiko – dann wäre es aber ohnehin grob fahrlässig, so zu verfahren. Für die allermeisten Windows-Nutzer ist dieses Szenario aber nicht relevant, sondern eher das Risiko, ein Notebook mit allerhand Dokumenten und Fotos in der Bahn zu verlieren. Und dann ist es gut zu wissen, dass ein Finder nichts auslesen kann.

## BitLocker-Zustand anzeigen

❓ Kann ich mir irgendwie anzeigen lassen, ob ein Laufwerk verschlüsselt ist, und wenn ja, mit weiteren Details? Vor allem unter Windows Home, wo die BitLocker-Verwaltung weder in der Systemsteuerung noch in den Einstellungen zu finden ist?

❗ Dafür gibt es das Kommandozeilentool `manage-bde.exe` – auch in Home-Editionen. Um den Verschlüsselungszustand aller Laufwerke anzuzeigen, öffnen Sie ein Terminal mit Administratorrechten, etwa via Windows-Taste+X. Der Befehl `manage-bde -status` zeigt Details zur Verschlüsselung jedes angeschlossenen Laufwerks an. Damit können Sie auch im Handumdrehen prüfen, ob Ihr Systemlaufwerk verschlüsselt ist: In der Zeile „BitLocker-Version“ meldet das Tool bei unverschlüsselten Laufwerken „Kein“, ansonsten eine Versionsnummer (meist 2.0).

## „Geräteverschlüsselung“ – sinnvoll oder nicht?

❓ Empfehlen Sie, die Geräteverschlüsselung in Windows 10 oder 11 Home zu nutzen?

❗ Wir empfehlen, eine Verschlüsselung zu nutzen, vor allem, wenn es um mo-

BitLocker-Wiederherstellungsschlüssel					
Gerätename	Schlüssel-ID	Wiederherstellungsschlüssel	Laufwerk	Schlüssel-Upload Datum	
DESKTOP-0E45IIR	FBB0FF7E	541167-096173-044858-686114-324269-236412-658768-069542	FDV	Invalid Date	<a href="#">Löschen</a>
DESKTOP-0E45IIR	DE6C3A60	038621-350075-306163-631851-692153-255068-628848-142032	FDV	12.2.2022	<a href="#">Löschen</a>

**Der Wiederherstellungsschlüssel im Microsoft-Konto ist nur in Sonderfällen ein Problem – und kann im Zweifelsfall ein rettender Notnagel sein.**

```
Administrator: Eingabeauffor... + - x
Microsoft Windows [Version 10.0.22621.1105]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\jss>manage-bde -status f:
BitLocker-Laufwerkverschlüsselung: Konfigurationstool, Version 10.0.22621
Copyright (C) 2013 Microsoft Corporation. Alle Rechte vorbehalten.

Volume "F:" [Backups]
[Datenvolume]

Größe: 233,24 GB
BitLocker-Version: 2.0
Konvertierungsstatus: Verschlüsselung wird durchgeführt
Verschlüsselt (Prozent): 1,4 %
Verschlüsselungsmethode: AES 128
Schutzstatus: Der Schutz ist deaktiviert.
Sperrenstatus: Entsperrt
ID-Feld: Unbekannt
Automatische Entsperrung: Deaktiviert
Schlüsselschutzvorrichtungen:
  Kennwort
  Numerisches Kennwort

C:\Users\jss>
```

Per Eingabeaufforderung lesen Sie im Handumdrehen aus, ob die Verschlüsselung aktiv ist, welcher Algorithmus zum Einsatz kommt und Ähnliches.

## Sicher unterwegs?

Reicht es im Hinblick auf Diebstahl- schutz und ähnliches, einfach Bit- Locker einzuschalten, oder muss ich mehr beachten?

! Sie müssen sich bei Windows per Kennwort, PIN oder ähnlichem anmelden. Haben Sie ein lokales Benutzerkonto, das ohne Kennwort direkt in den Desktop bootet, bringt Ihnen die Ver- schlüsselung nichts – jedenfalls nicht, so- lange das Systemlaufwerk beim Booten automatisch per Trusted Platform Modu- le (TPM) entsperrt wird. Sie müssten dann zusätzlich ein Bootkennwort oder einen Schlüssel-Stick einrichten (siehe auch fol- gender Tipp).

## BitLocker konfigurieren

! Gibt es Dinge, die ich einstellen sollte, bevor ich Windows meine Laufwerke verschlüsseln lasse?

! Hier gilt wieder einmal die Universal- antwort: kommt darauf an! Jede Menge Optionen finden Sie im Gruppen- richtlinien-Editor im Ordner „Computer- konfiguration/Administrative Vorlagen/ Windows-Komponenten/BitLocker-Lauf- werkverschlüsselung“. Wenn Sie BitLo- cker zum Beispiel auf einem PC ohne Trusted Platform Module (TPM) einrich- ten wollen, müssen Sie im Unterordner „Betriebssystemlaufwerke“ die Richtlinie „Zusätzliche Authentifizierung beim Start anfordern“ aktivieren (eine weitere Kon- figuration ist nicht nötig). Zum System- start brauchen Sie ein Kennwort oder einen USB-Stick mit einer Schlüsseldatei.

Ganz Vorsichtige finden zudem mit den Richtlinien zum „Verschlüsselungs- methode und Verschlüsselungsstärke für Laufwerk auswählen“ eine Möglichkeit, 256 Bit lange Schlüssel statt den vorein- gestellten 128-bittigen zu verwenden. Damit potenziert man die Zeit, die ein erfolgreicher Brute-Force-Angriff auf die Verschlüsselung bräuchte, doch der Si- cherheitsgewinn ist Stand heute sehr mar- ginal: Auch bei 128 Bit wären mit zurzeit verfügbarer Rechenleistung Millionen oder gar Milliarden Jahre erforderlich. An- sonsten sind viele der BitLocker-Optio- nen vor allem fürs Verschlüsselungsma- nagement in Firmenumgebungen ge- dacht.

(jss@ct.de)

bile Geräte geht, die schnell abhanden- kommen oder bei einem Wohnungsein- bruch gestohlen werden können. Es muss nicht zwingend die Geräteverschlüsselung sein, denn gerade diese Sparvariante von BitLocker lässt sich gar nicht konfigurie- ren, sondern nur ein- oder ausschalten, und sie funktioniert auch nicht für externe Datenträger. Teilen Sie Ihre System-SSD auf mehrere Partitionen auf, werden zwar alle durch die Geräteverschlüsselung ge- schützt, aber auch alle beim Systemstart automatisch entsperrt.

Wenn Sie also etwa USB-Medien schützen oder ein internes Laufwerk D: per Kennworteingabe entsperren wollen, sollten Sie die Geräteverschlüsselung ab- schalten und stattdessen ein flexibleres Tool wie VeraCrypt einsetzen. Das einzige, was Microsoft auf der Home-Edition mit USB-Medien erlaubt, ist das Verwenden bereits verschlüsselter Datenträger.

## BitLocker unter Home ausschalten

! Laut dem vorigen Tipp ist das System- laufwerk meines Windows 10 Home schon verschlüsselt, aber ich möchte es lie- ber mit VeraCrypt verschlüsseln. Wie werde ich die Microsoft-Verschlüsselung los?

! Da das BitLocker-Verwaltungsmodul der Systemsteuerung in Ihrer Home- Edition fehlt, schauen Sie zunächst im Be- reich „Geräteverschlüsselung“ in der Ein- stellungen-App nach, ob Sie die Funktion dort direkt abschalten können. Auf Win- dows 10 liegt das Menü unter „Update & Sicherheit“, auf Windows 11 unter „Daten- schutz und Sicherheit“.

Fehlt die Schaltfläche, oder behauptet Windows, die Verschlüsselung sei man- gels Microsoft-Konto nicht scharf geschal- tet, können Sie die Entschlüsselung auch erzwingen – in einem Terminal mit Ad- ministratorrechten per `manage-bde -off c:`. Je nach Laufwerksgröße und -geschwin- digkeit kann das ein paar Minuten oder auch ein, zwei Stunden dauern. Wie weit die Entschlüsselung vorangeschritten ist, können Sie mit dem zuvor genannten Statusbefehl auslesen: Sie ist abgeschlossen, sobald der Wert in der Zeile „Verschlüsselt (Prozent)“ auf 0,0 steht.

## BitLocker in Home per Kommandozeile?

! Wenn das Tool `manage-bde.exe` auch in Windows Home enthalten ist und bloß ein paar Konfigurationsmenüs feh- len, warum nicht BitLocker unter Home einfacher per Kommandozeile einrichten?

! Leider fehlt mehr als nur die Menüs: Kommandozeilenschalter für `manage- bde.exe`, die Sie zum Erstellen und Ver- walten von BitLocker bräuchten, verweig- ert das Tool unter Home mit einem Hin- weis auf fehlende Unterstützung in Ihrer Edition.

Dass Microsoft in Home-Editionen nicht wenigstens die BitLocker-Einrich- tung für USB-Medien erlaubt, wirkt im Jahr 2023 einigermaßen absurd – die Fä- higkeit, ein portables Laufwerk vor frem- den Blicken zu schützen, sollte zu den Grundfunktionen eines PC-Betriebssys- tems gehören. Der Schalter `-off` ist neben `-status` übrigens einer der wenigen, die auch mit der Home-Edition funktionieren.



# BERGUNGSMISION

von Jol Rosenberg

Der Notruf kam um 13:26 Uhr. Jandra lehnte sich zurück, um die Daten aufzunehmen. Es ging darum, eine havarierte Bergbauplattform aus der Atmosphäre eines Gasgiganten zu schaffen. Eine schwierige Aufgabe, selbst für einen Captain des Rettungs- und Bergungsunternehmens Sai-Fu. Genau nach ihrem Geschmack! Sie sagte zu. „Koordinaten ansteuern.“

Das Schiff bestätigte den Befehl. Jandra prüfte mit den Fingerspitzen die Verbindung, die sie gerade gelöst hatte, fuhr dann mit dem Prüflaser darüber. Die Daten bestätigten, dass sie ordentliche Arbeit geleistet hatte. Sie verstaute alles sorgfältig, damit es bei einem rauen Flug nicht durcheinanderpurzelte, und ging zur Brücke. Sie kannte den Weg und kam daher ohne Anweisungen des Schiffsleitsystems aus.

## Ankunft in 17 Minuten.

Jandra bestätigte. 17 Minuten reichten aus, um sich mit den Spezifikationen des Auftrags vertraut zu machen. Sie ließ sich in den Sessel gleiten, schnallte sich an und rief sich die benötigten Informationen in den Feed. Minon Taurus war klein. Für einen Giganten. Die Versicherung hatte die Bergbaumission von Beginn an in die Sicherheitsklasse C eingestuft. Die Police war aktuell – der Betreiber hatte sich dadurch die Dienste von Sai-Fu gesichert, somit auch Jandras Dienste. Sie versank in den Daten; den Zugriff darauf vermittelte ihr Implantat. Eine merkwürdige Sache war da auf der Plattform passiert. Eine Fehlfunktion kurz nach Start der Mission.

## JANDRA VERSANK IN DEN DATEN; DEN ZUGRIFF DARAUF VERMITTELTE IHR IMPLANTAT.

Jandra hörte Ropers Schritte näherkommen. Die Copilotin schwang sich in den Sessel, Verschlüsse klickten.

„Das ist doch wieder so ein Bergbauunternehmen, bei dem Geld wichtiger ist als die Folgen“, murkte Roper.

„Sie haben bezahlt, also helfen wir Ihnen“, entgegnete Jandra.

**Bei lebensgefährlichen Einsätzen im All stellt sich heraus, was echt ist.**

**Das Vordergründige verliert an Bedeutung. Menschliche Sinne, Sensordaten, technische Systeme, Kommunikation, Gewinn und Verlust, Wahrheit und Lüge – auf bizarre Weise kann sich das alles unter höchstem Druck neu ordnen und überraschende Verbindungen hervorbringen.**

Roper vertiefte sich schweigend in die Daten.

„Wow!“

Sie hatten Minon Taurus erreicht und Ropers Ausruf war die Reaktion auf das Aussehen des Gasgiganten. Jandra hatte die Beschreibungsroutine ihres Assistenten gestoppt, visuelle Schönheit war momentan nebensächlich. Offenbar sah Roper das anders.

„Wenn du das sehen könntest! Wirbelnde Gasflecken, braun und bläulich. Dazwischen farbige Bänder und weiße Flecken. Es ist wunderschön. Nichts, was man für Geld zerstören sollte.“

„Siehst du die Plattform?“, fragte Jandra. Sai-Fu hatte ihr die Daten bereits zur Verfügung gestellt, daher war Ropers „Ja“ keine Überraschung. Gut, jetzt war Roper hoffentlich wieder bei der Sache.

## Funkverbindung hergestellt.

„Sai-Fu, sind Sie das?“ Eine hektische Stimme erklang.

„Jandra Mensah, Pilotin der Sai-Fu. Wie ist Ihre Lage?“

„Prekär. Die Temperatur hier drin ist auf 38 Grad Celsius gestiegen, die Schräglage beträgt ...“ Sie ließ ihn reden. Jandra wusste das alles. Aber die meisten Menschen blieben ruhiger, wenn sie redeten. Sie nickte Roper zu. Deren Aufgabe musste es nun sein, die aufgeregte Crew bei der Stange zu halten. Jandra hatte andere Aufgaben. Sie konzentrierte sich auf die Strömungen in der Atmosphäre von Minon. Ein Schiff durch derartiges Wetter zu manövrieren, war eine Herausforderung. Sie ließ sich zur Seite kippen und von einem Oberflächenwind mitnehmen. Ein leichtes Rütteln erfasste Jandra, nein, das Schiff.

„Welche Schleuse ist erreichbar?“, fragte Jandra in eine kurze Gesprächspause hinein und bat das Schiff um die Daten des Gegenübers. Sie würde sie brauchen, um ihn zu beruhigen. Horrk Czish, männlich. Zum Glück gab es eine Aussprachedeatei für den Namen.

„Wir ...“ Der Mann machte eine Pause.

„Die Schleusen sind blockiert“, vermutete Jandra laut. Es war immer dasselbe mit diesen billig produzierten Plattformen. Sie brauchten nicht lange zu halten, also sparte man an jeder Ecke.

„Ja“, bestätigte Czish.

„Wir werden die Station in Schlepp nehmen.“ Dann hatten sie später ausreichend Zeit, die Leute rauszuholen.

„Die Hitzeresistenz unserer Außenhaut ist runter auf 53 Prozent“, meldete Czish.

## Über Jol Rosenberg

Die 1976 geborene Autorenpersönlichkeit, die in Berlin lebt und schreibt, sieht sich in binärer Geschlechteraufteilung nicht vertreten. Jol Rosenberg brennt für spannende Science-Fiction mit menschlichem Tiefgang, die der technischen Gegenwart mal mehr, mal weniger nah ist, und war in c't bereits mit den Stories „Oben“ (Heft 19/21) und „Geschäftsessen“ (Heft 3/2022) vertreten. Im vergangenen Herbst hat der Wiener Verlag Ohneohren Jol Rosenbergs Romandebüt „Das Geflecht: An der Grenze“ herausgebracht, das vom Kampf dreier Kulturen gegen eine skrupellose Macht auf einem Kolonieplaneten erzählt. Die neue Romandilogie „Etomi“, die der Plan-9-Verlag im Herbst 2023 veröffentlicht will, spielt hingegen in der gleichen Umgebung wie „Oben“ auf der postapokalyptischen Erde des 24. Jahrhunderts.



Bild: Jol Rosenberg

Der Feed hatte es Jandra bereits verraten. Sie würde mit der Plattform im Schlepp herumeiern müssen, um kühtere Strömungen zu reiten, bis sie eine Möglichkeit zum Absprung ins All fand, wo alles weiter herunterkühlte.

„Das ist kein Problem“, sagte Jandra.

„Hören Sie, die Strömungen hier sind mörderisch!“

„Weiß ich.“ Jandra schaltete den Kühlstrom des Raumschiffs ein und rief sich das Schemabild der Plattform in den Feed. Warum konnte nicht einmal jemand einfach davon ausgehen, dass sie ihren Job schon machen würde? „Die Aufhängungen sind getestet?“

„N ... nein. Das Testsystem ist ausgefallen.“

*Mist!* „Roper?“

„Ich schaue, was ich machen kann.“ Die Anspannung war ihr deutlich anzuhören. „Oh, sorry.“

„Was? Ach so. Alles gut.“ Als wäre Jandra gekränkt, nur weil Ropers Wortwahl daran erinnerte, dass Jandra nicht sehen konnte. Sehen war eindeutig überbewertet. „Mach die Außen-Bots fertig.“

„Aye.“

„Da gibt es noch eine ... Komplikation“, ließ sich Czishs Stimme vernehmen.

„Ich höre.“

„Wir hatten ... ein Problem mit der ... äh, Rettungsbake. Sie hat sich losgerissen und wir haben keine Ortung ihrer aktuellen Position.“

„Sie haben versucht, die Station zu verlassen?“ Die Anordnung war, zu warten, bis jemand sie einsammelte.

„Ja. Wir dachten, wir kommen Ihnen entgegen.“

Nur dass er dazu hätte wissen müssen, aus welcher Richtung Sai-Fu kam. Aber gestresste Menschen taten unsinnige Dinge.

Jandra wandte ihre Aufmerksamkeit dem Kurs zu, verschmolz mit den Daten in ihrem Feed. So mussten Vögel Winde unter den Schwingen fühlen. Jandas Winde waren

Sensordaten des Schiffs, eines Schiffs, mit dem sie so vertraut war wie mit dem eigenen Körper.

*Hitzewarnung. Kritisches Niveau auf der Plattform erreicht.*

Wenn sie das Ding nicht bald da rauszogen, würden die Menschen darin gekocht.

„Bereit“, sagte Roper. „Die Aufhängung sollte okay sein.“

Jandra setzte sich auf einen heißen Wind und glitt auf die Station zu, als eine Kollisionswarnung dröhnte. *Scheiße!* Jandra riss das Schiff zur Seite. Sie wurde in die Gurte geschleudert. Sofort richtete sie ihren Menschenkörper wieder auf, während sie Scanpulse an die Stelle schickte, wo das unbekannte Objekt war. Neben ihr winselte Roper gequält.

„Alles in Ordnung?“, fragte Jandra, während sie die einlaufenden Scannerdaten auswertete und das Schiff in eine Schlaufe steuerte. Sie waren an der Station vorbeigerast, hatten aber immerhin eine Kollision mit der Bake vermieden. Diese dümpelte im Schatten der Plattform, an einer der beiden Aufhängungen. Was hatte sie da zu suchen?

„Ja, danke. Ist das die Rettungsbake? Was macht die da?“ Roper war nicht augmentiert und musste alles mit den Augen aufnehmen.

Jandra sprach, während sie sich durch die Daten wühlte: „Gute Frage. Wir können keine weitere Annäherung wagen, solange das Ding da hängt.“

„Ist es benannt?“

Das war eine verdammt gute Frage.

„Sai-Fu, wo bleiben Sie?“ Czishs Stimme klang panisch.

Jandra konnte fast spüren, wie Roper sie fragend anstarrte. Das Schiff bestätigte es.

„Hier ist doch etwas faul“, sagte Roper langsam. Dann öffnete sie die Verbindung zur Plattform. „Wir sind fast mit dieser verdamten Bake kollidiert. Ist da jemand drin? Kann das Ding manövriren?“

**„HIER IST DOCH ETWAS FAUL“,  
SAGTE ROPER LANGSAM.**

Czishs Antwort kam den Bruchteil einer Sekunde später als erwartet. „Die ist leer. Schießen Sie sie ab.“

„Wir kümmern uns darum.“ Roper kappte die Verbindung. „Wir müssen die Bake bergen!“

Jandra stimmte ihr zu. Czish war eindeutig *zu* scharf darauf, das Ding loszuwerden. Sie hoffte nur, dass sie nicht in die Position kamen, sich zwischen Bake und Plattformcrew entscheiden zu müssen. Roper sandte drei Scandrohnen aus und wies ihnen ein Flugmuster zu.

„Kannst du die Bake anfunken?“, fragte Jandra.

„Keine Reaktion.“

Natürlich nicht. Wenn da jemand drin saß, der funken konnte, hätte er sich längst gemeldet.

„Wenn die Bake mit der Plattform verbunden ist, können wir vielleicht beide zusammen da rausholen“, schlug Roper vor. „An den unteren Aufhängungen.“

„Doppelschlepp?“ Jandra dachte darüber nach. „Knifflig, den nötigen Anflugwinkel hinzubekommen.“

Während die Drohnendaten eingingen, sortierte Jandra die vorhandenen Informationen. Die Truppe um Czish war als Wartungscrew eingetragen, die aufgrund unvorhergesehener Probleme außerhalb des Turnus angerückt war. Vier Leute, allesamt Techniker. Sie waren von einem Schiff abgesetzt worden, der Abholtermin stand in drei Tagen bevor. Weswegen hatte man sie gerufen, so kurz nach dem Start des Projekts?

Die eingehenden Daten der Scanner besagten, dass das Antriebsmodul, das die Plattform an Ort und Stelle in der oberen Atmosphäre hielt, beschädigt war. Die Art, wie die Luft um die Schadstelle wirbelte, erschien merkwürdig. So, als habe eine Explosion stattgefunden. Jandra sog Luft ein. Die Explosion musste *nach* dem Eintreffen des Teams stattgefunden haben.

„Das ist keine Rettungsbake.“

Jandra drehte den Kopf zu Roper. „Nicht?“

„Nein. Das ist ein sauteses Schiff. Offenbar eine Sonderanfertigung. Sieht nur auf den ersten Blick wie eine Bake aus.“ Sie schob Jandra die Daten in den Feed. „Hat sich irgendwie in den Aufhängungen verklemmt.“

*Nicht versehentlich*, vermutete Jandra. Sie stieß die Berechnungen für einen Schubimpuls an und setzte Roper davon in Kenntnis. Das war das einzige, was ihr einfiel, wie sie sich etwas Zeit verschaffen konnten: Wenn es ihnen gelang, die Plattform in eine entferntere Umlaufbahn zu schieben, konnten sie die Situation eruieren, während die Plattform herunterkühlte.

Jandra öffnete die Verbindung zur Wartungscrew. „Bitte sichern Sie Ihr Team. Wir schieben Sie nach draußen. Wird ein etwas unruhiger Flug.“

„Was ist mit der Bake? Wollten Sie uns nicht in Schlepp nehmen?“

„Wir haben das im Griff!“ Jandra klappte die Verbindung.

„Das stinkt sowas von gewaltig“, sagte Roper. „Du hättest sein Gesicht sehen sollen. Hast du die Temperatur im Blick?“

Jandra hatte. Sie brauchte die Schubimpulsberechnungen bald. Jetzt. Das Schiff empfahl ihr eine mögliche Flugroute. Sie würde unter der Plattform hindurchtauchen müssen. Schnell.

„Wir geben ihnen einen Schubimpuls und stoßen sie nach draußen“, sagte Jandra und machte sich daran, es umzusetzen. „Es wird unruhig“, warnte sie Roper, flog in eine enge Kurve und drückte die Schiffsnaß nach unten. Ein zunächst feines Vibrieren ging in zackiges Rucken über. Zum Glück hatte sie einen robusten Magen und stabile Sicherheitsgurte.

*Schubimpuls bereit.*

Sie tauchte unter die Plattform, folgte den Windströmungen, spürte, wie die Luft an ihr riss und drückte. Sie hielt sanft dagegen.

*Jetzt.*

Der Schub drückte Schiff und Plattform aus ihren Bahnen. Luftströme wirbelten, rissen das Schiff nach oben, dann sackte es plötzlich zur Seite weg. Jandra ließ sich in einen kontrollierten Trudelflug gleiten, der Roper wimmern ließ. Die Plattform schwebte nach oben, traf auf Seitenwind, fand

eine neue Bahn. Gerade als Jandra sich entspannen wollte, löste sich die falsche Bake von der Plattform und trudelte in Richtung Minon. Die visuellen Unterstützungsrouter informierten sie darüber, dass das Objekt beschädigt aussah und allem Anschein nach manövriertunfähig war.

„Mist!“

„Die Plattform ist sicher geparkt“, bestätigte Roper. *Na, wenigstens etwas!*

Jandra fing sich und setzte sich in einen kühleren Luftstrom. Die Bake, die keine war, trudelte langsam auf Minon zu. Und wurde ziemlich schnell schneller. Jandra prüfte die Temperaturen der Außenhaut, dann nahm sie die Verfolgung auf.

„Bergungs-Bot bereithalten“, wies sie Roper an.

„Aye.“

\* \* \*

Einige Minuten später hatten sie das Ding im Schlepp. Es war ein winziges Schiff ohne bekannte Klassifizierung. Da draußen konnte es ihnen nichts anhaben, was auch immer an Überraschungen darin wartete. Aber mit dem Klotz an der Seite bockte Jandras Sai-Fu-Schiff in den unruhigen Winden. Sie versuchte vergeblich, das Gleichgewicht wiederherzustellen. Ein Stöhnen entfuhr ihr.

„Was ist?“

„Das Ding muss rein. Wir sind so nicht ausgewogen genug, um die Plattform zu holen.“

Deren Crew schwebte zwar nicht mehr in unmittelbarer Kochgefahr, konnte aber auch nicht lange bleiben, wo sie war.

Jetzt stöhnte Roper. „Kannst du vorher wenigstens die Daten auslesen? Damit wir wissen, was uns erwartet?“

Jandra konnte nicht. Sie konnte nicht einmal feststellen, ob das Ding bemannt war. Oder ob es sich überhaupt um ein Schiff handelte. Nach dem, was sie an Informationen reinbekam, konnte es sich um eine Bombe handeln. Eine beschädigte, fliegende Bombe. Nicht dass es hilfreich gewesen wäre, das irgendjemandem auf die Nase zu binden.

„Der kleine Laderraum?“, fragte Roper.

„Entweder das – oder wir stoßen das Ding doch ins All.“ Immerhin hatte Czish behauptet, dass es unbemannt war. Aber der hatte auch behauptet, dass es sich um eine Rettungsbake handelte.

Roper schluckte laut. „Wenn da jemand drin ist ...“

„Ja, Scheiße! Selbst schuld, wenn man so ein abgeschirmtes Ding fliegt!“ Der Mangel an Daten hatte definitiv nichts damit zu tun, dass das Ding kaputt war.

Roper schluckte erneut und sagte: „Wir holen es rein.“

Jandra musste eine solche Entscheidung verantworten. Sie war die offiziell Ranghöhere.

„Natürlich holen wir es rein“, erwiderte sie.

Roper würde keine Fliege sterben lassen. Und Jandra würde sich nicht mit der Person anlegen, die so ziemlich die einzige war, die sie um sich herum ertragen konnte.

„Sai-Fu?“ Czish klang fordernd.

„Wir sammeln Sie gleich ein“, erwiderte Roper. „Sie sind nicht in unmittelbarer Gefahr. Halten Sie sich bereit. Derweil können Sie mir verraten, was passiert ist.“

Den Daten zufolge war die Temperatur auf der Station leicht gesunken und die strukturelle Integrität ausreichend.

Der neuralgische Punkt waren die Aufhängungen. Bergbauplattformen dieses Typs waren dazu gemacht, in Schlepp genommen zu werden. Und zwar nur einmal, bei ihrer Installation. Danach wurden sie benutzt, solange es sich lohnte, und dann bis zum Absturz in der Umlaufbahn belassen. Meistens evakuierte man die Crew vorher.

„Ich habe die Seitenkameras aktiviert“, sagte Czish. „Es sieht so aus, als seien die unteren Aufhängungen in besseren Zustand als die oberen.“ Er schob die Bilder in den allgemeinen Feed.

*Bestätigt.*

Jandra stimmte der Schiffs-KI zu. „Da gab es mehr als eine Explosion.“

*Den Strömungsmustern nach zu urteilen von außen nach innen.*

Von außen? Czish hatte offenbar keine Ahnung von dem, was Jandra wahrnehmen konnte. Aber erst einmal mussten sie diese fliegende Bombe einsammeln. Jandra grinste unfröhlich. Hoffentlich war das ein zu pessimistischer Arbeitstitel. Sie beschleunigte und wie immer, wenn es drauf ankam, hatte Roper im richtigen Moment die Bots bereit und die Schiffs-KI lenkte diese mit ihrer Fracht in den kleinen Laderaum.

\* \* \*

Czish hatte inzwischen mehrfach versucht, eine Verbindung aufzubauen, aber die Schiffs-KI hatte ihn mit Wartemeldungen abgespeist.

„Machen Sie sich bereit für eine Veränderung Ihrer Ausrichtung“, sagte Roper nun zu ihm. Da die Plattform nicht darauf ausgelegt war, längere Zeit bewohnt zu werden, war ihr eigenes Schwerkraftfeld schwach und fehleranfällig. Sie von unten in Schlepp zu nehmen, stellte da drinnen alles auf den Kopf.

„Bereit“, bestätigte Czish.

Jandra arbeitete sich erneut an die Plattform heran. Sie biss sich auf die Unterlippe.

„Bergungs-Bots bereit“, sagte Roper.

Jandra glich ihre Geschwindigkeit der Plattform an. Die Winde hier waren weniger turbulent als an der vorigen Position. „Bots ausklinken.“

Nachdem sie die Bots mit den Stahlseilen an die richtige Stelle gelenkt hatte und die Verbindungen eingeklinkt waren, gab Jandra vorsichtig Schub. Die Seile strafften sich, die Plattform eierte hinter dem Schiff her, langsam, vorsichtig. Sie verließen die Umlaufbahn von Minon. Roper überwachte das Einholen der Plattform und die Übernahme der Crew in den großen Frachtraum.

Jandra schaltete auf Autopilot um, atmete aus und lehnte sich zurück. Alle waren an Bord. Sollte sich doch die Station um die fliegende Bombe kümmern.

*Bewegungsalarm im kleinen Frachtraum.*

„Mist!“

Und da kam auch schon die Verbindung zustande: „Ros Markon, Geheimdienst von Rho 15“, meldete sich eine erschöpft klingende hohe Stimme. „Captain Jandra, Sie sollten mit mir sprechen!“

Jandra hätte es lieber vermieden. Geheimdienste waren ein Garant für Ärger.

„Sie braucht medizinische Hilfe“, sagte Roper. „Blutet ziemlich stark.“

„Auch das noch!“ Jandra löste die Gurte und stand auf. „Ich bringe sie in die medizinische Einheit und höre mal, was sie will.“

\* \* \*

Markon ließ sich ohne Widerspruch in die medizinische Einheit bringen. Sie zog dabei wohl eine Blutspur hinter sich her – Jandra schloss das aus dem Surren des eifrigen Reinigungsroboters, der hinter ihnen herwieselte.

„Haben Sie die Leute von der Plattform an Bord?“, fragte Markon.

„Ja.“

„Halten Sie sie fest.“ Die verletzte Geheimdienstoffizierin warf ihre Kleidung ab und hievte sich auf den Tisch der Med-Einheit, ohne mit dem Sprechen aufzuhören. Manchmal, fand Jandra, war es doch schade, nichts zu sehen. Den Beschreibungsrouterien zufolge war Markon muskulös. „Das ist eine Sabotageeinheit. Rho 15 wird auf Sie zukommen und die Sache übernehmen.“

Der Deckel der Med-Einheit schob sich über Markons Körper und verhinderte eine Fortsetzung des Gesprächs. Das Protokoll sah vor, dass Jandra nun die Gestrandeten begrüßte. Sie musste ja nichts von Markon erzählen. Sie trat auf den Gang und funkte Roper an.

„Stimmt der Kurs?“

„Stimmt.“

„Hat sich jemand von Rho 15 gemeldet?“

„Niemand.“

„Markon zufolge sind das keine Wartungs-, sondern Sabotageleute.“

Roper schwieg einen Moment. „Begrüßen wir sie zusammen?“

„Wir können sie auch einmotten. Bis zur Übergabe.“

„Dann hören wir aber ihren Teil der Geschichte nicht.“

*Natürlich.* Jandras Copilotin war auch deshalb so wertvoll, weil sie stets Wege fand, den Freiraum, den die Regularien ließen, unauffällig zu nutzen. Jandra folgte den bekannten Gängen zum großen Frachtraum. Ropers eilige Schritte tapsten um die Ecke, dann neben Jandra über den glatten Boden. Vor der Tür ließ Jandra sich die Positionen der dahinter befindlichen Personen durchgeben, dann gab sie den Befehl zum Öffnen.

\* \* \*

„Ah, unsere Retterin.“ Schritte kamen näher. Das System identifizierte Czisch. Jandra streckte ihm die Hand entgegen.

## Die c't-Stories als Hörversion

Unter [heise.de/-4491527](http://heise.de/-4491527) können Sie einige c't-Stories als Audiofassung kostenlos herunterladen oder streamen. Die c't-Stories zum Zuhören gibt es auch als RSS-Feed und auf den bekannten Plattformen wie Spotify, Player FM und Apple Podcasts ([ct.de/yz13](http://ct.de/yz13)).

Er ergriff sie und schüttelte sie enthusiastisch. „Sie kamen gerade im richtigen Moment!“

„Das ist unser Job.“

Czish schwieg. Das Schiff bezeichnete seinen Gesichtsausdruck als irritiert. Jandra biss die Zähne zusammen. In den Untiefen menschlicher Kommunikation konnte sie viel schlechter manövrieren als im Strudel von Planetenwinden.

„Wir würden gern verstehen, was vorgefallen ist“, sagte Roper.

## „WIR WÜRDEN GERN VERSTEHEN, WAS VORGEFALLEN IST.“

Die Temperatur im Raum sank gefühlt um mehrere Grad.

„Wir auch“, sagte Czish steif. „Ich nehme an, Sie haben nicht nur uns aufgenommen.“

„Nein, haben wir nicht“, sagte Roper leichthin.

Für einen Moment breitete sich Schweigen aus. Für gewöhnlich mochte Jandra Schweigen. Aber das hier mochte sie nicht.

„Sollen Sie uns ausliefern?“ Czish bemühte sich um einen nüchternen und souveränen Klang, scheiterte damit jedoch.

„Natürlich“, erwiderte Roper. „Es sei denn, Sie geben uns einen Grund, etwas anderes zu versuchen.“

Czish hielt für einen Moment die Luft an. Dann sagte er: „Wir sind Teil einer Organisation, die gegen automatisierte Plattformen kämpft. Sie sind nicht nur umweltschädlich, sondern auch tödlich für die Wartungsteams.“

„Wegen der nicht mehr benötigten Jobs.“ Roper schien das nichts Neues zu sein. Natürlich nicht. Politik war eins ihrer Steckenpferde.

„Genau. Wir hatten nur vor, einen Beweis zu liefern, dass ständige Crews auf den Plattformen nötig sind. Aber dann kam diese Agentin dazwischen und alles ging schief. Wenn Sie uns nach Rho 15 ausliefern, wird das Ganze nicht einmal untersucht.“

„Santal ist neutrales Territorium.“ Roper sagte es leicht hin.

„Und unsere Funkanlage ist gerade etwas wacklig“, fügte Jandra hinzu. Das Spiel kannte sie zur Genüge. „Das können Sie doch bestätigen, oder?“

Czish schwieg. Offenbar hatte er eine lange Leitung. Länger als die des angeblich wackligen Funksystems. Ein anderes Mitglied der Crew trat neben ihn.

„Doch“, sagte das neue Mitglied. „Das können wir. Wenn Sie keine anderen Anweisungen bekommen, bringen Sie uns nach Santal, nicht wahr?“

„Genau.“

Jandra konnte sich das zufriedene Grinsen auf Ropers Gesicht auch ohne die Beschreibung ihres Assistenten vorstellen. Und war gespannt, was bei einer Untersuchung herauskommen würde. (psz@ct.de) **ct**

# Die volle Ladung



Auch als Heft + PDF  
mit 29% Rabatt

Dieses c't-Sonderheft räumt auf mit Mythen rund ums E-Auto und schafft einen realen Überblick zu Vor- und Nachteilen der E-Mobilität.

- Leitfaden zum Kauf eines E-Autos
- Kostenvergleich: Strom vs. Sprit
- Fahrberichte und Tests
- Den Akku richtig nutzen und laden
- Überschussladen – Strom aus Photovoltaik nutzen
- Auch als Bundle mit Buch „E-Autos einfach erklärt“ vom dpunkt-Verlag erhältlich!

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

 [shop.heise.de/ct-eautos22](http://shop.heise.de/ct-eautos22)

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

 **heise Shop**

# Mastering GitOps

Schnell, stabil und sicher deployen

Das Heise-Online-Event  
am 2. März 2023

## Auf dem Weg zu Continuous Operations

Die Mastering GitOps bietet Ihnen online einen fundierten Überblick über die Konzepte und den praktischen Einsatz von GitOps. Lernen Sie die Chancen für Ihr eigenes Arbeitsumfeld einzuschätzen und erfahren Sie, wie das Deployment Ihrer Anwendungen schneller und sicherer wird.

### Highlights aus dem Programm:

- Was ist GitOps – und ist das was für mich?  
**Baris Cubukcuoglu**
- GitOps maßgeschneidert: Repos, Folders, Stages, Patterns  
**Johannes Schnatterer**
- GitOps geht auch ohne Kubernetes  
**Anja Kammer**
- Die GitOps-Delivery-Pipeline überwachen und härten mit Flux & Flagger  
**Florian Heubeck**
- Keynote: GitOps Emerging Developments and Predictions  
**Alexis Richardson**

Mit einer Keynote von  
**Alexis Richardson**,  
dem »Erfinder«  
von GitOps

Unsere Online-Konferenz vermittelt konzeptuelles Wissen und praktisches Know-how für Softwareentwicklerinnen und -entwickler, die GitOps für ihre Zwecke evaluieren oder eigene Erfahrungen mit Fachkolleginnen und -kollegen vergleichen wollen.

**Jetzt noch Frühbucherrabatt bis zum 8. Februar 2023 sichern!**

[www.mastering-gitops.de](http://www.mastering-gitops.de)

Veranstalter



heise Developer

dpunkt.verlag



**Nerdistan** 

**Neuland**

## Fernstudium IT-Security

Aus- und Weiterbildung zur Fachkraft für IT-Sicherheit.  
Vorbereitung auf das **SSCP- und CISSP-Zertifikat**.  
Ein Beruf mit Zukunft. Kostengünstiges und praxisge-  
rechtes Studium ohne Vorkenntnisse. Beginn jederzeit.

**NEU:** Roboter-Techniker, Netzwerk-Techniker,  
Qualitätsbeauftragter / -manager TÜV,  
Linux-Administrator LPI, PC-Techniker

Teststudium ohne Risiko.  
GRATIS-Infomappe gleich anfordern!

FERN SCHULE WEBER - seit 1959  
Neerstedter Str. 8 - 26197 Großenkneten - Abt. C14  
Telefon 0 44 87 / 263 - Telefax 0 44 87 / 264

[www.fernenschule-weber.de](http://www.fernenschule-weber.de)




Ich  
träume  
in  
 C#

WEBINAR-SERIE

 heise Academy

## Ethical Hacking für Admins

Mit Penetration Testing zu sicheren IT-Systemen

23. Februar

Informationsbeschaffung  
& Pentesting-Grundlagen

2. März

Shells & Backdoors

9. März

Einführung Netzwerk-  
protokolle

23. März

Passwort-Hacking

30. März

Schwachstelle Webseite:  
Injection-Angriffe



Jetzt Kombi-Rabatt sichern und fast 30 % sparen:

[webinare.heise.de/ethical-hacking](http://webinare.heise.de/ethical-hacking)



ORACLE Feuerwehr [www.oraservices.de](http://www.oraservices.de)

xxs-kurze Daten- & Netzkabel: [kurze-kabel.de](http://kurze-kabel.de)

softaktiv.datensysteme Datenbankapplikationen, Website Boosting, Online-Pressemitteilungen, Unterstützung bei Ihren V-Projekten. Einfach anrufen, Faxen oder eine E-Mail schicken. Telefon: 0511/3884511, Mobil: 0170/3210024, Telefax: 0511/3884512, E-Mail: [service@softaktiv.de](mailto:service@softaktiv.de), Internet: [www.softaktiv.de](http://www.softaktiv.de)

Alternativer Breitbandatlas - [Breitbandatlas.eu](http://Breitbandatlas.eu)

nginx-Webhosting: [timmehosting.de](http://timmehosting.de)

EDELSTAHL LED Schilder: [www.3D-buchstabe.com](http://www.3D-buchstabe.com)  
HAUSNUMMERN nobel 230V~: [www.3D-hausnummer.de](http://www.3D-hausnummer.de)

[www.patchkabel.de](http://www.patchkabel.de) - LWL und Netzwerk Kabel

Erfahrene Diplom-Fachübersetzerin übersetzt EDV-Texte aller Art (Software und Hardware) insbesondere Texte aus den Bereichen Telekommunikation und Netzwerke. Englisch-Deutsch. Tel. + Fax: 05130/37085

**Anzeigenschluss  
für die nächsten  
erreichbaren Ausgaben:**

**06/2023: 07.02.2023**

**07/2023: 21.02.2023**

**08/2023: 07.03.2023**

## c't – Kleinanzeigen

### Private Kleinanzeige:

erste Druckzeile € 10,-; jede weitere Zeile € 8,-

### Gewerbliche Kleinanzeige:

erste Druckzeile € 20,-; jede weitere Zeile € 16,-

### Chiffre-Anzeige: € 5,- Gebühr

**Hinweis:** Die Rechnungsstellung erfolgt nach Veröffentlichung der Anzeige!

Name/Vorname

Firma

Str./Nr.

PLZ/Ort

Bitte veröffentlichen Sie den Text in der nächsterreichbaren Ausgabe von c't.

Den Betrag habe ich auf Ihr Konto überwiesen.  
Sparkasse Hannover,  
IBAN DE98 2505 0180 0000 0199 68, BIC SPKH DE 2H

Bei Angeboten: Ich versichere, dass ich alle Rechte an den angebotenen Sachen besitze.

Datum \_\_\_\_\_ Unterschrift (unter 18, der Erziehungsberechtigte)

**Faxnummer: 05 11 / 53 52-200**

Bitte veröffentlichen Sie in der nächsterreichbaren Ausgabe (Vorlaufzeit mind. 3 Wochen) folgende Anzeige im Fließsatz  privat  gewerblich\* (werden in c't mit  gekennzeichnet)  Chiffre

€ 10,- (20,-)

€ 18,- (36,-)

€ 26,- (52,-)

€ 34,- (68,-)

€ 42,- (84,-)

€ 50,- (100,-)

€ 58,- (116,-)

€ 66,- (132,-)

Pro Zeile bitte jeweils 45 Buchstaben einschließlich Satzzeichen und Wortzwischenräumen. Wörter, die **fettgedruckt** (nur in der ersten Zeile möglich) erscheinen sollen, unterstreichen Sie bitte. Den genauen Preis können Sie so selbst ablesen. \*Der Preis für gewerbliche Kleinanzeigen ist in Klammern angegeben. Soll die Anzeige unter einer Chiffre-Nummer erscheinen, so erhöht sich der Endpreis um € 5,- Chiffre-Gebühr.

Ausfüllen und einsenden an:  Heise Medien GmbH & Co. KG  
c't-Magazin, Anzeigenabteilung  
Karl-Wiechert-Allee 10, 30625 Hannover

↳ Weiterlesen, wo andere aufhören.



# JOB GESUCHT?

Ein gutes Team braucht viele verschiedene kluge und kreative Köpfe – und gleichzeitig den Freiraum, diese Potenziale zu entfalten und einzusetzen.

Gestalten Sie mit uns die Zukunft der Medienwelt!

Jetzt informieren und bewerben unter  
[www.heise-gruppe.de/  
karriere](http://www.heise-gruppe.de/karriere).



An der Hochschule München ist an der Fakultät für Informatik und Mathematik ab dem Wintersemester 2023/2024 oder später folgende Stelle zu besetzen:

## Professur für Intelligent User Interfaces (W2)

Kennziffer: BV 0788

Erfahren Sie mehr in der detaillierten Stellenausschreibung unter: <https://stellen.hm.edu/gz71a>

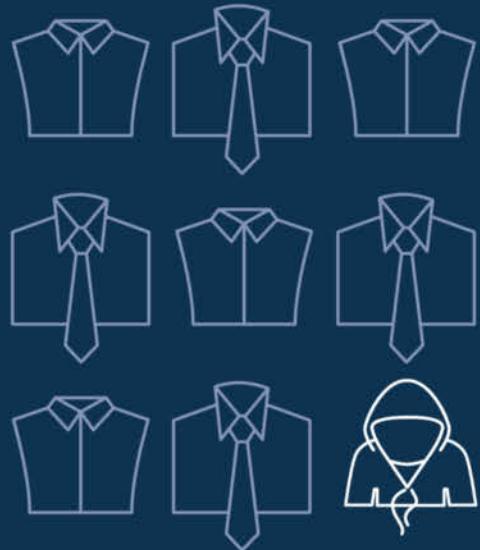
Bewerben Sie sich über unser Online-Portal bis zum 19.02.2023.

Wir freuen uns darauf, Sie kennenzulernen!



# Sei nicht wie alle Developer. Sei du selbst.

Sei Senior Java Developer /  
Java Architect\* bei IKOR.



### Komm in unser Spitzenteam!

In großartigen, cross-funktionalen und agilen Teams von Business Analysten, Developern, DevOps-Experts und Architects gestaltest du wirklich sinnvolle und wichtige Digitalisierungsprojekte im Public Sector. Die Grenzen deines persönlichen Wachstums setzt du dabei selbst. In unserem offenen, ehrlichen, lösungsorientierten und freundlichen Umfeld kannst du mehr und schneller lernen als anderswo.

Scanne den QR-Code und du bekommst weitere Einzelheiten zu unserem Job-Angebot. Alternativ kannst du dich auf [jobs.ikor.one](http://jobs.ikor.one) nach weiteren passenden Optionen umschauen.



\* Dieses Stellenangebot richtet sich natürlich an alle.

# Inserenten\*

1blu AG, Berlin	29	<b>Stellenanzeigen</b>	
Arctic GmbH, Braunschweig	7	Hochschule für angewandte Wissenschaften, München	191
B1 Systems GmbH, Vohburg	55	IKOR GmbH, Essen	191
Bundesministerium der Verteidigung, Berlin	2		
Cordaware GmbH, Pfaffenhofen	57	<b>Veranstaltungen</b>	
dpunkt.verlag GmbH, Heidelberg	51	c't workshop	10
easybell GmbH, Berlin	43	enterJS	67
Fernschule Weber, Großkenner	189	Javaland	77
Kentix GmbH, Idar-Oberstein	49	heise Academy	81
mitp Verlags GmbH & Co. KG, Frechen	37	secIT by Heise	114, 115
netfiles GmbH, Burghausen	27	Inside Agile Kanban Day	159
Nubert electronic GmbH, Schwäbisch Gmünd	195	Mastering GitOps	188
Ratiodata SE, Münster	41	Ethical Hacking für Admins	189
Reichelt Elektronik GmbH & Co., Sande	19	betterCode	192
Taiwan External Trade, ROC - Taipei, Taiwan	59		
WAGO Kontakttechnik GmbH & Co. KG, Minden	196	Teile dieser Ausgabe enthalten Beilagen der HACKATTACK	
WIBU-SYSTEMS AG, Karlsruhe	9	IT SECURITY GmbH, A-Vöcklamarkt und der Strato AG, Berlin.	
		* Die hier abgedruckten Seitenzahlen sind nicht verbindlich.	
		Redaktionelle Gründe können Änderungen erforderlich machen.	

betterCode()

## API 2023

Die Heise-Konferenz zu Design, Entwicklung und Management von HTTP-APIs

30.3. und 27.4.2023 · Online-Konferenz

**APIs – die Basis für moderne IT-Systeme**

In der Softwareentwicklung kommt man nicht mehr um APIs herum: Ob Private oder Public APIs – Software- und Webentwickler:innen müssen schwierige Fragen beantworten: Welche **Architekturparadigmen**, welche **Verfahren**, welche Protokolle nutze ich, wann welche besser nicht? Wie gewährleiste ich **Qualität, Kompatibilität und Sicherheit**?

Die **Vorträge** der betterCode() API am 30. März 2023 bieten **Softwareentwickler:innen, Softwarearchitekt:innen** sowie **API- und Integrationsbeauftragten** konzeptuelles Wissen, neueste Entwicklungen der API-Entwicklung sowie umsetzbares Praxis-Know-how und Entscheidungshilfen.

Jetzt  
Blind-Bird-Ticket  
sichern!

Veranstalter



heise Developer

dpunkt.verlag

api.bettercode.eu

# Impressum

## Redaktion

Heise Medien GmbH & Co. KG, Redaktion c't  
Postfach 61 04 07, 30604 Hannover  
Karl-Wiechert-Allee 10, 30625 Hannover  
Telefon: 05 11/53 52-300  
Telefax: 05 11/53 52-417  
Internet: [www.ct.de](http://www.ct.de), E-Mail: [ct@ct.de](mailto:ct@ct.de)

**Titelthemenkoordination in dieser Ausgabe:** „Selbstbau von Solaranlagen“:  
Georg Schnurer ([gs@ct.de](mailto:gs@ct.de)), „Datenschutz pragmatisch umsetzen“: Lutz Labs ([ll@ct.de](mailto:ll@ct.de))  
**Chefredakteur:** Dr. Jürgen Rink ([jr@ct.de](mailto:jr@ct.de)) (verantwortlich für den Textteil)  
**Stellv. Chefredakteur:** Axel Kossel ([ad@ct.de](mailto:ad@ct.de))  
**Chef vom Dienst:** Georg Schnurer ([gs@ct.de](mailto:gs@ct.de))  
**Leser & Qualität**

**Leitung:** Achim Barczok ([acb@ct.de](mailto:acb@ct.de))

**Textredaktion & Qualitätssicherung:** Oliver Lau ([ola@ct.de](mailto:ola@ct.de))

**Koordination Leserkommunikation:** Martin Triadan ([mat@ct.de](mailto:mat@ct.de))

**Ressort Internet, Datenschutz & Anwendungen**

**Leitende Redakteure:** Hartmut Gieselmann ([hag@ct.de](mailto:hag@ct.de)), Jo Bager ([jo@ct.de](mailto:jo@ct.de))  
**Redaktion:** Holger Bleich ([hob@ct.de](mailto:hob@ct.de)), Anke Brandt ([abr@ct.de](mailto:abr@ct.de)), Greta Friedrich ([gref@ct.de](mailto:gref@ct.de)),  
Tim Gerber ([tig@ct.de](mailto:tig@ct.de)), Arne Grävemeyer ([agr@ct.de](mailto:agr@ct.de)), Immo Junghärtchen ([imj@ct.de](mailto:imj@ct.de)),  
Markus Montz ([mon@ct.de](mailto:mon@ct.de)), Peter Schmitz ([psz@ct.de](mailto:psz@ct.de)), Sylvester Tremmel ([syt@ct.de](mailto:syt@ct.de)),  
Andrea Trinkwalder ([atr@ct.de](mailto:atr@ct.de)), Dorothee Wiegand ([dwi@ct.de](mailto:dwi@ct.de)), Stefan Wischner ([swi@ct.de](mailto:swi@ct.de))  
**Ressort Systeme & Sicherheit**

**Leitende Redakteure:** Peter Siering ([ps@ct.de](mailto:ps@ct.de)), Jan Mahn ([jam@ct.de](mailto:jam@ct.de))

**Redaktion:** Niklas Dierking ([ndi@ct.de](mailto:ndi@ct.de)), Mirko Dölle ([mid@ct.de](mailto:mid@ct.de)), Wilhelm Drehling ([wid@ct.de](mailto:wid@ct.de)),  
Liane M. Dubowy ([ldm@ct.de](mailto:ldm@ct.de)), Ronald Eikenberg ([rei@ct.de](mailto:rei@ct.de)), Pina Merkert ([pmk@ct.de](mailto:pmk@ct.de)),  
Dennis Schirrmacher ([des@ct.de](mailto:des@ct.de)), Hajo Schulz ([hos@ct.de](mailto:hos@ct.de)), Jan Schüßler ([js@ct.de](mailto:js@ct.de)),  
Kathrin Stoll ([kst@ct.de](mailto:kst@ct.de)), Keywan Tonekaboni ([ktn@ct.de](mailto:ktn@ct.de)), Axel Vahlhiedk ([avx@ct.de](mailto:avx@ct.de))  
**Ressort Hardware**

**Leitende Redakteure:** Christof Windeck ([civ@ct.de](mailto:civ@ct.de)), Ulrike Kuhlmann ([uk@ct.de](mailto:uk@ct.de)),  
Dušan Živadinović ([dz@ct.de](mailto:dz@ct.de))

**Redaktion:** Ernst Ahlers ([ea@ct.de](mailto:ea@ct.de)), Christian Hirsch ([chh@ct.de](mailto:chh@ct.de)), Benjamin Kraft ([bkr@ct.de](mailto:bkr@ct.de)),  
Lutz Labs ([ll@ct.de](mailto:ll@ct.de)), Andrijan Möcker ([amo@ct.de](mailto:amo@ct.de)), Florian Müsseg ([mue@ct.de](mailto:mue@ct.de)), Rudolf Opitz  
([rop@ct.de](mailto:rop@ct.de)), Carsten Spille ([csp@ct.de](mailto:csp@ct.de))  
**Ressort Mobiles, Entertainment & Gadgets**

**Leitende Redakteure:** Jörg Wirtgen ([jow@ct.de](mailto:jow@ct.de)), Jan-Keno Janssen ([jkj@ct.de](mailto:jkj@ct.de))

**Redaktion:** Robin Brand ([rbr@ct.de](mailto:rbr@ct.de)), Sven Hansen ([sha@ct.de](mailto:sha@ct.de)), Steffen Herget ([sht@ct.de](mailto:sht@ct.de)),  
Nico Jurran ([njj@ct.de](mailto:njj@ct.de)), André Kramer ([akr@ct.de](mailto:akr@ct.de)), Michael Link ([mil@ct.de](mailto:mil@ct.de)), Urs Mansmann  
([uma@ct.de](mailto:uma@ct.de)), Stefan Porteck ([spo@ct.de](mailto:spo@ct.de)), Christian Wölbert ([cwo@ct.de](mailto:cwo@ct.de))  
**c't online:** Ulrike Kuhlmann ([uk@ct.de](mailto:uk@ct.de))

**Social Media:** Jil Martha Baae ([jmb@ct.de](mailto:jmb@ct.de))

**Koordination News-Teil:** Hartmut Gieselmann ([hag@ct.de](mailto:hag@ct.de)), Christian Wölbert ([cwo@ct.de](mailto:cwo@ct.de))

**Koordination Heftproduktion:** Martin Triadan ([mat@ct.de](mailto:mat@ct.de))

**Redaktionsassistent:** Susanne Cölle ([suc@ct.de](mailto:suc@ct.de)), Christopher Tränkmann ([cht@ct.de](mailto:cht@ct.de))

**Software-Entwicklung:** Kai Wasserbäch ([kaw@ct.de](mailto:kaw@ct.de))

**Technische Assistenz:** Ralf Schneider (Ltg., [rs@ct.de](mailto:rs@ct.de)), Christoph Hoppe ([cho@ct.de](mailto:cho@ct.de)),  
Stefan Labusua ([sla@ct.de](mailto:sla@ct.de)), Arne Mertins ([ame@ct.de](mailto:ame@ct.de)), Jens Nohl ([jno@ct.de](mailto:jno@ct.de)), Daniel Ladeira  
Rodrigues ([dro@ct.de](mailto:dro@ct.de)), Wolfram Tege ([te@ct.de](mailto:te@ct.de))  
**Dokumentation:** Thomas Masur ([tm@ct.de](mailto:tm@ct.de))

**Verlagsbüro München:** Hans-Pinsel-Str. 10b, 85540 Haar, Tel.: 0 89/42 71 86-0,  
Fax: 0 89/42 71 86-10

**Ständige Mitarbeiter:** Leo Becker ([lbe@ct.de](mailto:lbe@ct.de)), Detlef Borchers, Herbert Braun ([heb@ct.de](mailto:heb@ct.de)),  
Tobias Engler, Monika Ermert, Stefan Krempel, Ben Schwan ([bsc@ct.de](mailto:bsc@ct.de)), Christiane Schulzki-Haddouti

**DTP-Produktion:** Mike Bunjes, Birgit Graff, Angela Hilberg, Jessica Nachtigall, Astrid Seifert,  
Ulrike Weis

**Junior Art Director:** Martina Bruns

**Fotografie:** Andreas Wodrich, Melissa Ramson

**Videoproduktion:** Johannes Börnsen

**Digitale Produktion:** Melanie Becker, Kevin Harte, Martin Kreft, Thomas Kaltschmidt,  
Pascal Wissner

**Illustrationen:**

Jan Bintakies, Hannover, Rudolf A. Blaha, Frankfurt am Main, Thorsten Hübner, Berlin, Albert  
Hulm, Berlin, Sven Hauth, Schülp, Thomas Kuhlenbeck, Münster, Timo Lenzen, Berlin,  
Andreas Martini, Wettin, Moritz Reichartz, Viersen, Michael Vogt, Berlin

**Editorial:** Hans-Jürgen „Mash“ Marhenke, Hannover, Schlagseite: Ritsch & Renn, Wien,  
c't-Logo: Gerold Kalter, Rheine

**c't-Krypto-Kampagne:** Infos zur Krypto-Kampagne unter <https://ct.de/pgp>. Die Authentizität  
unserer Zertifizierungsschlüssel lässt sich mit den nachstehenden Fingerprints überprüfen:

Key-ID: 5C1C1DC5BEEDD33A  
ct magazine CERTIFICATE <[pgpCA@heise.de](https://pgpCA@heise.de)>  
D337 FCC6 7EB9 09EA D1FC 8065 5C1C 1DC5 BEED D33A  
Key-ID: 2BAE3CF6DAFFB000  
ct magazine CERTIFICATE <[pgpCA@ct.heise.de](https://pgpCA@ct.heise.de)>  
A3B5 24C2 01A0 D0F2 355E 5D1F 2BAE 3CF6 DAFF B000  
Key-ID: DBD245FCB3B2A12C  
ct magazine CERTIFICATE <[pgpCA@ct.heise.de](https://pgpCA@ct.heise.de)>  
19ED 6E14 58EB A451 C5E8 0871 DBD2 45FC B3B2 A12C

**heise Investigativ:** Über diesen sicheren Briefkasten können Sie uns anonym informieren.  
Anonymer Briefkasten: <https://heise.de/investigativ>  
via Tor: [ayznmonmewb2tjvgf7ym4t2726muprjvwckzx2vhf2hbarbbzydm7oad.onion](https://ayznmonmewb2tjvgf7ym4t2726muprjvwckzx2vhf2hbarbbzydm7oad.onion)

## Verlag

Heise Medien GmbH & Co. KG  
Postfach 61 04 07, 30604 Hannover  
Karl-Wiechert-Allee 10, 30625 Hannover  
Telefon: 05 11/53 52-0  
Telefax: 05 11/53 52-129  
Internet: [www.heise.de](http://www.heise.de)

**Herausgeber:** Christian Heise, Ansgar Heise, Christian Persson

**Geschäftsführer:** Ansgar Heise, Beate Gerold

**Mitglieder der Geschäftsleitung:** Jörg Mühlé, Falko Ossmann

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

**Anzeigenpreise:** Es gilt die Anzeigenpreisliste Nr. 39 vom 1. Januar 2022.

**Anzeigen-Auslandsvertretung (Asien):** Media Gate Group Co., Ltd., 7F., No. 182, Section 4,  
Chengde Road, Shilin District, 11167 Taipei City, Taiwan, [www.mediagate.com.tw](http://www.mediagate.com.tw) Tel: +886-2-  
2882-5577, Fax: +886-2-2882-6000, E-Mail: [mei@mediagate.com.tw](mailto:mei@mediagate.com.tw)

**Leiter Vertrieb und Marketing:** André Lux (-299)

**Werbeleitung:** Julia Conrades (-156)

**Service Sonderdrucke:** Julia Conrades (-156)

**Druck:** Firmengruppe APPL, appl druck, Senefelderstr. 3-11, 86650 Wemding

**Kundenkonto in der Schweiz:** PostFinance, Bern, Kto.-Nr. 60-486910-4, BIC:  
POFICHBEXXX, IBAN: CH73 0900 0000 6048 6910 4

**Vertrieb Einzelverkauf:**

DMV Der Medienvertrieb GmbH & Co. KG

Meßberg 1

20086 Hamburg

Tel.: 040/3019 1800, Fax: 040/3019 1815

E-Mail: [info@dermedienvertrieb.de](mailto:info@dermedienvertrieb.de)

**c't erscheint 14-täglich**

Einzelpreis 5,90 €; Österreich 6,50 €; Schweiz 9,90 CHF; Belgien, Luxemburg 6,90 €;  
Niederlande 7,20 €; Italien, Spanien 7,40 €, Dänemark 64,00 DKK

**Abonnement-Preise:** Das Jahresabonnement kostet inkl. Versandkosten: Inland 144,20 €,  
Österreich 155,40 €, Europa 165,20 €, restl. Ausland 191,80 € (Schweiz 236,60 CHF);  
ermäßigt Abonnement für Schüler, Studenten, Auszubildende (nur gegen Vorlage einer  
entsprechenden Bescheinigung): Inland 105,00 €, Österreich 99,40 €, Europa 124,60 €,  
restl. Ausland 152,60 € (Schweiz 145,60 CHF). c't-Plus-Abonnements (inkl. Zugriff auf  
das c't-Artikel-Archiv sowie die App für Android und iOS) kosten pro Jahr 25,00 € (Schweiz  
30,80 CHF) Aufpreis. Ermäßigt Abonnement für Mitglieder von AUGE, bdvb e.V., BvD e.V.,  
/ch/open, GI, GUUG, ISACA Germany Chapter e.V., JUG Switzerland, VBIO, VDE und VDI  
(gegen Mitgliedsausweis): Inland 108,15 €, Österreich 116,55 €, Europa 123,90 €, restl. Ausland  
143,85 € (Schweiz 177,45 CHF). Luftpost auf Anfrage.

**Leserservice:**

Bestellungen, Adressänderungen, Lieferprobleme usw.

Heise Medien GmbH & Co. KG

Leserservice

Postfach 24 69

49014 Osnabrück

E-Mail: [leserservice@ct.de](mailto:leserservice@ct.de)

Telefon: 05 41/8 00 09-120

Fax: 05 41/8 00 09-122

**c't abonnieren:** Online-Bestellung via Internet ([www.ct.de/abo](http://www.ct.de/abo)) oder E-Mail ([leserservice@ct.de](mailto:leserservice@ct.de)).

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch  
die Redaktion vom Herausgeber nicht übernommen werden. Kein Teil dieser Publikation darf  
ohne ausdrückliche schriftliche Genehmigung des Verlags in irgendeiner Form reproduziert  
oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet  
werden. Die Nutzung der Programme, Schaltpläne und gedruckten Schaltungen ist nur zum  
Zweck der Fortbildung und zum persönlichen Gebrauch des Lesers gestattet.

Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Mit  
Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das  
Exklusivrecht zur Veröffentlichung. Honorierte Arbeiten gehen in das Verfügungssrecht des  
Verlages über. Sämtliche Veröffentlichungen in c't erfolgen ohne Berücksichtigung eines  
eventuellen Patentschutzes.

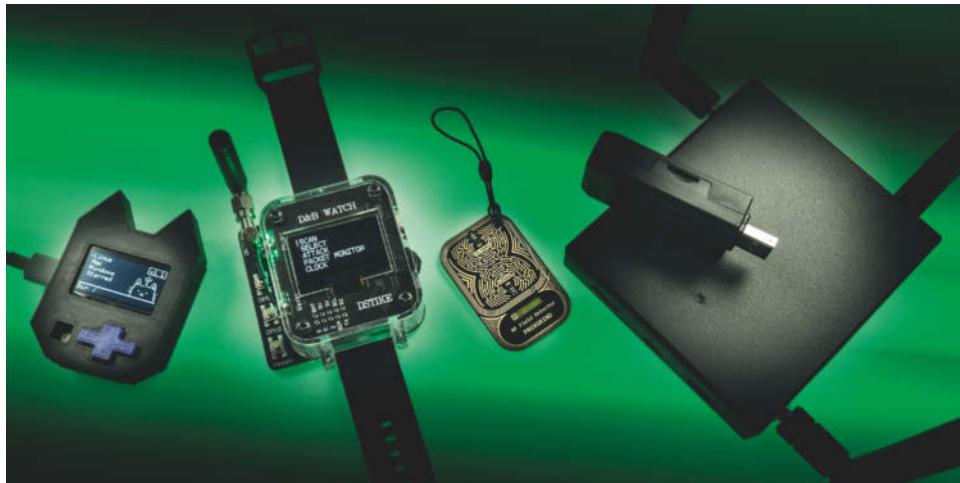
Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt. Hergestellt und  
produziert mit Xpublisher: [www.xpublisher.com](http://www.xpublisher.com). Printed in Germany. Alle Rechte vorbehalten.  
Gedruckt auf chlorfreiem Papier.

© Copyright 2023 by Heise Medien GmbH & Co. KG

**ISSN 0724-8679 AWA LAE ▲**

# Vorschau ct 5/2023

Ab 11. Februar im Handel und auf [ct.de](https://www.ct.de)



## Hacking-Gadgets

Von genial bis gefährlich: Hacking-Gadgets eignen sich für Angriffe auf Smartphones, Computer, WLANs und mehr, können aber auch extrem nützlich sein. Tests der interessantesten und skurrilsten Geräte aus aller Welt lesen Sie in der nächsten ct.



## Premium-In-Ears im Test

Wir haben die besten In-Ear-Kopfhörer von Apple bis Yamaha ins ct-Labor geholt. Nicht nur im Klang unterscheiden sie sich mitunter deutlich. Auch in Sachen Noise Cancelling und Transparenzmodus lohnt es sich, genauer hinzuhören.

## KI-Bot ChatGPT optimal nutzen

ChatGPT liefert Texte in vielen Stilformen, etwa Reden, Rap-Songs oder Blog-Beiträge. Doch der Chatbot kann mehr: Er findet Fehler in Programmen, löst Mathehausaufgaben (samt Lösungsweg) und fasst längere Texte zusammen. Mit unseren Tipps holen Sie noch mehr raus.

## So arbeitet die Schufa

Die Schufa bewertet die Kreditwürdigkeit von Verbrauchern und Unternehmen, hat aber nicht den besten Ruf. Mit Tools wie dem Score-Simulator will sie mehr Vertrauen und Transparenz schaffen. Wir haben uns die Pläne angeschaut und erklären, wie solche Auskunfteien arbeiten.

## Podcast-Apps für Ihr Programm

Spotify, Amazon, RTL und sogar die ARD locken Podcast-Fans mit exklusiven Inhalten zu ihren eigenen Apps. Wer unabhängig bleiben will und maximalen Komfort sucht, nutzt besser klassische Podcast-Clients, die so genannten Catcher. Wir testen sechs Apps für Android und iOS.

Noch mehr  
Heise-Know-how



ct Hacking-Praxis jetzt  
im Handel und auf  
[heise-shop.de](https://www.heise-shop.de)



iX 2/2023 jetzt im Handel  
und auf [heise-shop.de](https://www.heise-shop.de)



ct Fotografie 01/23 jetzt  
im Handel und auf  
[heise-shop.de](https://www.heise-shop.de)

# Klein. Schwarz. Stark. Mobiler HiFi-Genuss

nuGo! ONE

NEU



Viel mehr als eine Bluetooth-Box

- **Das portable HiFi-Stereo-System**  
Klangbrillantes Musik-Streaming mit Bluetooth aptX HD und 55 Hz Tiefgang
- **DAB+/FM HD Weltradioempfänger**  
für starken Empfang – mit Teleskop-Antenne
- **Großer Klang im Kompaktformat**  
durch 2 Breitbandtreiber, Passivradiator und DSP-Technologie
- **Ideal für unterwegs**  
Bis zu 24 Stunden Akkulaufzeit, Schnellladung, Weckfunktion, Spritzwasserschutz (IPX5)

nuGo! ONE, 2x20W HiFi-Stereo, 285 € inkl. MwSt. zzgl. Versandkosten

**Direkt + günstig vom Hersteller [nubert.de](http://nubert.de)**

Nubert electronic GmbH, Nubertstr. 1, D-73529 Schwäbisch Gmünd  
Webshop [www.nubert.de](http://www.nubert.de) · Vorführstudios in Schwäbisch Gmünd und  
Duisburg · Expertenberatung +49 (0) 7171 8712-0

**nubert**<sup>®</sup>  
EHRLICHE LAUTSPRECHER

# WAS KANN DAS?

# WAS DU WILLST!



## Maximale Flexibilität im Engineering mit dem neuen Ding von WAGO!

Egal, ob du deine Applikation im Container oder nativ ausführen willst, es ist deine Entscheidung. Du hast Zugriff auf die nötigen Schnittstellen, wie z.B. seriell, TCP/IP und I/Os.

Dabei kannst du auch bei der Wahl des Engineerings frei entscheiden. Egal, ob Hochsprachen wie, C/C#/C++, Python, Low-Code, Node-Red u.v.a. Oder doch lieber die klassische CODESYS Umgebung – WAGO bietet Offenheit und du hast die Wahl!

Du willst das neue Ding ausprobieren? Entdecke jetzt deine Möglichkeiten mit dem neuen **WAGO Compact Controller 100!**

**WAGO**

[www.wago.com/de/compactcontroller100](http://www.wago.com/de/compactcontroller100)

